การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

นางต่วนนูรีซันน์ สุริยะ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปรัชญาดุษฎีบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา คณะครุศาสตร์อุตสาหกรรม
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2561

ชื่อ : นางต่วนนูรีซันน์ สุริยะ
ชื่อวิทยานิพนธ์ : การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้
สาขาวิชา : เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม : รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข
ปีการศึกษา : 2561

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) วิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ 2) พัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ 3) ออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ 4) พัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ 5) ศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ กลุ่มตัวอย่างของการวิจัยนี้มี 2 กลุ่ม กลุ่มตัวอย่างที่ 1 เป็นผู้บริหาร ครู อาจารย์ บุคลากรทางการศึกษา จำนวน 198 คน ได้มาจากการสุ่มแบบแบ่งชั้น (Stratified Random Sampling) กลุ่มตัวอย่างที่ 2 เป็น ผู้บริหาร ครู อาจารย์ และบุคลากรทางการศึกษา จำนวน 50 คน ได้มาโดยวิธีการสุ่มอย่างง่ายการวิเคราะห์ข้อมูลใช้ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน

ผลการวิจัยพบว่า

1. การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วย 3 ด้าน คือ การรักษาความมั่นคงปลอดภัยเกี่ยวกับบุคคล การรักษาความปลอดภัยเกี่ยวกับสถานที่ การป้องกันและแก้ไขปัญหาด้านความไม่สงบ ซึ่งประกอบด้วยกระบวนการรักษาความปลอดภัย 4 ส่วน คือ 1) ระบบยืนยันตัวตน 2) ระบบควบคุมการเข้า - ออกยานพาหนะ 3) ระบบตรวจจับและแจ้งเตือนภัยภายในอาคาร 4) ระบบฐานข้อมูลด้านความมั่นคง

2. แบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แบ่งออกเป็น 4 มิติ คือ มิติด้านการรักษาความปลอดภัยสำหรับสถานศึกษา มิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา มิติด้านการบริหารจัดการข้อมูล มิติด้านการตรวจสอบหลักฐานดิจิทัล

3. สถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ พบว่าโมดูลย่อยของระบบที่งานร่วมกันมี 7 โมดูล ได้แก่ 1 ประกอบด้วย โมดูลการทำงานของระบบ 7 โมดูล ได้แก่ 1) โมดูลตรวจจับใบหน้า 2) โมดูลสแกนบัตร 3) โมดูลตรวจจับทะเบียนรถ 4) โมดูลตรวจจับควันไฟ 5) โมดูลตวจจับความร้อน 6) โมดูลตรวจจับก๊าซ 7) โมดูลตรวจจับแรงสั่นสะเทือน

4. ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีทั้งหมด 5 ส่วนได้แก่ 1) ผู้ที่เกี่ยวข้องกับระบบ 2) ไอโอทีดีไวซ์ สำหรับการตรวจจับบุคคลและวัตถุ 3) โมดูลย่อยของระบบ 4) การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย 5) เว็บเซิร์ฟเวอร์และดาต้าเบสเซอร์ฟเวอร์

5. การประเมินผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ พบว่า ผู้ใช้ระบบ มีความรู้ความเข้าใจในการใช้งานระบบ เกิดความสะดวกต่อการใช้งานระบบ กระบวนการทำงานของระบบที่ไม่ซับซ้อน สามารถเข้าถึงข้อมูลได้ง่ายด้วยเทคโนโลยีไร้สายที่ผู้ใช้ระบบส่วนใหญ่มักคุ้นชินกับการทำงานในชีวิตประจำวัน ผู้ใช้มีความตระหนักเนื่องจากนโยบายและการให้ความสำคัญเกี่ยวกับรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้ใช้มีความรู้สึกถึงความปลอดภัยเพิ่มขึ้น เนื่องจากระบบมีการแจ้งเตือนความมั่นคงปลอดภัย ทำให้ผู้ใช้สามารถวิเคราะห์และตัดสินใจได้ทันทวงทีในการวางแผนการเดินทางไปยังสถานที่เมื่อเกิดเหตุการณ์ความไม่ปลอดภัย

(วิทยานิพนธ์มีจำนวนทั้งสิ้น 210 หน้า)

คำสำคัญ : ระบบรักษาความมั่นคงปลอดภัยสูง เทคโนโลยีเชื่อมโยงสรรพสิ่ง หลักฐานดิจิทัล

_____อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Name : Mrs.Tuannurisan Suriya
Thesis Title : Development of High Integrated Security Management System Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Border Provinces.
Major Field : Information Technology and Communication for Education
King Mongkut's University of Technology North Bangkok
Thesis Advisor : Associate Professor Dr.Panita Wannapiroon
Co-Advisor : Associate Professor Dr.Prachyanun Nilsook
Academic Year : 2018

Abstract

This research has the following objectives: 1) to analyze of Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces 2) to build a model to Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces 3) to design a system architecture for Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces 4) to Development of Hight Integrated Security Management System Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces 5) to investigate the results of the Development of Hight Integrated Security Management System Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces. The sample. This research has 2, group 1 is executives, teachers, educational personnel, 198 people received from stratified sampling (Stratified sampling). Example 2, as the administrators, professors and educational personnel, 50 people received by simple random methods. The data analysis involves the use of both mean and standard deviation.

The research found that;

1. The Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces. Consists of 3 aspects: Personal security Place security Preventing and solving unrest problems Which consists

of 4 security procedures: 1) identity verification system 2) vehicle access control system 3) indoor alarm detection and notification system 4) security database system

2. The Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces. Four dimensons: 1) Security for educational institutions 2) Information technology supporting the security and 4) Digital Forensic

3. The system architecture for Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces. It was found that 7 sub-modules of the system that worked together were as follows: 1 consisted of 7 system modules, 1) face detection module 2) card scanning module 3) vehicle registration detection module 4) fire smoke detection module 5) Thermal capture module 6) Gas detection module 7) Vibration detection module

4. The Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces. There are 5 parts, including 1) those related to the system 2) iodide wich for Detection of individuals and objects 3) Sub-modules of the system 4) Notification and reporting of security results 5) Web servers and database servers

5. The assessment of the results of the Hight Integrated Security Using Internet of Things to Verify Digital Forensic for Educational Institutions in Southern Botder Provinces. found that administrators, system users have a better understanding of the use of the system. Convenient for using the system System processes that do not overlap Can access information easily with wireless technology that most users are accustomed to working in daily life Users are aware of the policies and the importance of maintaining security for educational institutions in the southern border provinces. Users have more sense of security. Because the system has a security warning Enabling users to analyze and make timely decisions in planning trips to places when incidents are not safe

(Total 210 Pages)

Keywords : Hight Integrated Security Management System, Internet of Things,
Digital Forensic.

_____Advisor

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงอย่างสมบูรณ์ได้เนื่องด้วยความกรุณาอย่างดียิ่งจากอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ และอาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข ที่ได้กรุณาให้คำปรึกษา แนวคิด ข้อชี้แนะ ตลอดจนข้อคิดเห็นอันเป็นประโยชน์อย่างยิ่งแก่งานวิจัยผู้วิจัยรู้สึกซาบซึ้งและขอกราบขอบพระคุณท่านอาจารย์ด้วยความเคารพอย่างสูงมา ณ ที่นี้

ขอกราบขอบพระคุณ ศาสตราจารย์เกียรติคุณ ดร.นิพนธ์ ศุขปรีดี ที่ให้ความเมตตาและกรุณาให้เกียรติเป็นประธานสอบป้องกันวิทยานิพนธ์ รองศาสตราจารย์ ดร.พัลลภ พิริยะสุรวงศ์ รองศาสตราจารย์ ดร.สุพจน์ อิงอาจ และ รองศาสตราจารย์ ดร.อนุชาติ ศรีศิริวัฒน์ คณะกรรมการสอบป้องกันวิทยานิพนธ์ที่ให้คำแนะนำที่มีคุณค่าต่อการปรับปรุงงานวิจัย ให้มีความสมบูรณ์มากยิ่งขึ้น ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูง

การวิจัยนี้ได้รับเงินอุดหนุนบางส่วนจากทุนอุดหนุนการวิจัยเพื่อทำวิทยานิพนธ์สำหรับนักศึกษาระดับบัณฑิตศึกษา และทุนสนับสนุนการตีพิมพ์บทความเผยแพร่ผลงานซึ่งเป็นส่วนหนึ่งของงานวิจัยในครั้งนี้ จากบัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ จึงขอขอบพระคุณบัณฑิตวิทยาลัยมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ที่ได้กรุณาให้ทุนอุดหนุนการทำวิทยานิพนธ์ฉบับนี้

ขอขอบพระคุณมหาวิทยาลัยราชภัฏสงขลา และ ผู้เชี่ยวชาญทุกท่านที่ได้สละเวลาให้ข้อเสนอแนะที่เป็นประโยชน์แก่งานวิจัยนี้สำเร็จลุล่วงอย่าง สมบูรณ์ รวมทั้งสาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษาที่ให้การสนับสนุนและ อำนวยความสะดวกในการทำวิทยานิพนธ์ในครั้งนี้

ท้ายนี้ผู้วิจัยใคร่ขอกราบขอบพระคุณบุพการี คุณพ่อสนิท สุกิจจานันท์ คุณแม่นาอีหมัะ สุกิจจานันท์ และคุณสามีอาคม สุริยะ ตลอดจน บุคคลในครอบครัวรวมทั้งบุคคลที่เกี่ยวข้องที่ยังไม่ได้กล่าวนามไว้ ณ ที่นี้ที่คอยส่งกำลังใจ ความห่วงใย จนเป็นแรงผลักดันให้ผู้วิจัยประสบความสำเร็จในครั้งนี้

ต่วนนูรีซันน์ สุริยะ

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง (ต่อ)

สารบัญภาพ

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

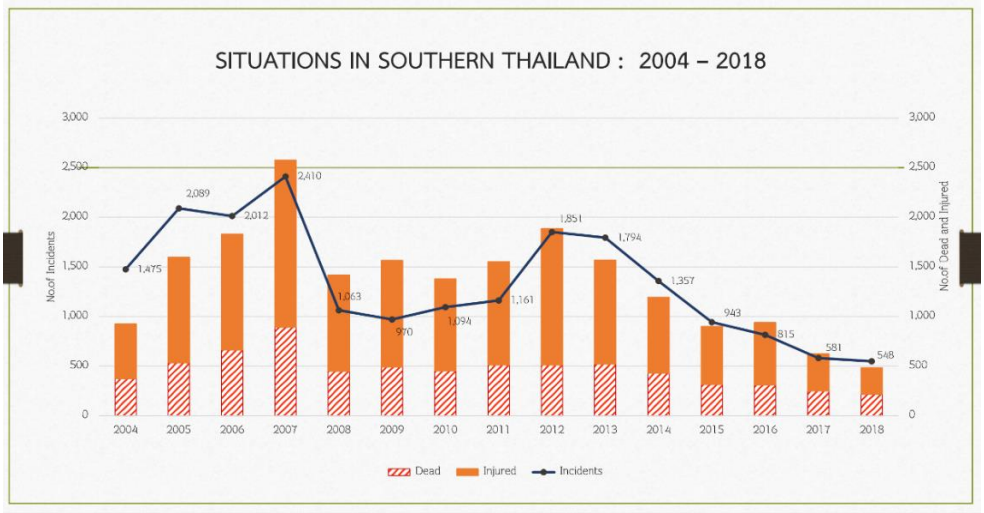
บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

จังหวัดชายแดนภาคใต้ของประเทศไทย ประกอบด้วย จังหวัด นราธิวาส ปัตตานี และยะลา ตั้งอยู่ตอนใต้สุดของประเทศไทย มีพื้นที่รวม 6.79 ล้านไร้ หรือ 10,936 ตารางกิโลเมตร เป็นพื้นที่ที่มีลักษณะพิเศษมากกว่าท้องถิ่นอื่น ๆ ทั้งในด้านของความเป็นมาทางประวัติศาสตร์และเป็นพื้นที่ที่มีประชากรหลากหลายทางเชื้อชาติศาสนาและวัฒนธรรม ซึ่งส่วนใหญ่เป็นชาวไทยเชื้อสายมลายู ประกอบด้วยจังหวัด นราธิวาส ยะลา และปัตตานี (รุ่ง แก้วแดง, 2548: 52 - 53) ในขณะนี้ พื้นที่ใน 3 จังหวัดชายแดนภาคใต้ได้เกิดปัญหาด้านความมั่นคงของชาติ เนื่องจากต้องประสบปัญหาความไม่สงบซึ่งเป็นอุปสรรคต่อการพัฒนาพื้นที่ 3 จังหวัดชายแดนภาคใต้

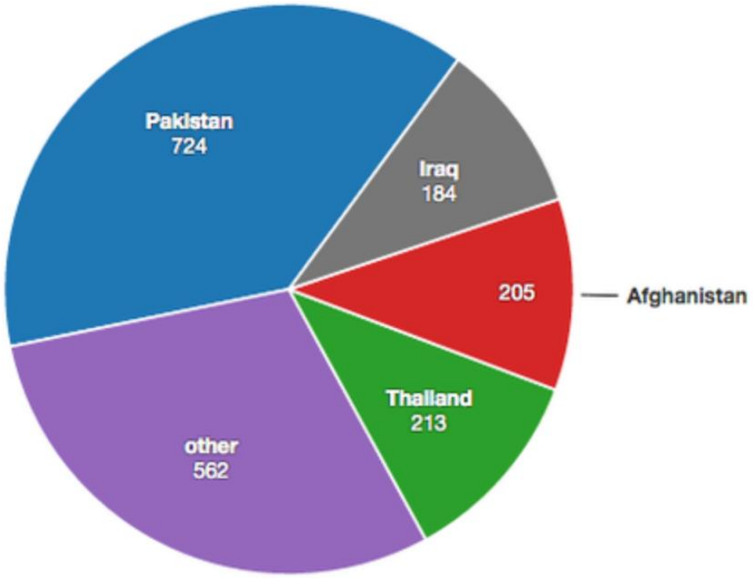
ในสถานการณ์ปัจจุบันจังหวัดชายแดนภาคใต้ ยังคงมีปัญหาความมั่นคงของชาติและความไม่สงบในพื้นที่ ซึ่งเป็นปัญหาที่มีความละเอียดอ่อนอย่างยิ่ง เนื่องจากความไม่สงบดังกล่าวมีสาเหตุมาจากการเมืองที่เกี่ยวเนื่องกับด้านประวัติศาสตร์ ด้านเศรษฐกิจ ด้านสังคมและวัฒนธรรม ด้านการศึกษาและ ด้านกระบวนการยุติธรรม เช่น ปัญหาการก่อการร้าย การวางเพลิง การซุ่มโจมตี การลอบทำร้าย การลอบวางระเบิดและก่อเหตุจลาจล เกิดขึ้นในพื้นที่อย่างรุนแรงและต่อเนื่อง ซึ่งปัญหาความไม่สงบที่เกิดขึ้นได้สร้างความเดือดร้อนในการดำรงชีวิต และส่งผลให้เกิดความสูญเสียในกลุ่มประชาชนและเจ้าหน้าที่ของรัฐ ทั้งทางด้านร่างกาย จิตใจ ชีวิต และทรัพย์สิน ส่งผลกระทบต่อการพัฒนาประเทศ ทั้งด้านสังคม เศรษฐกิจ และการเมืองในภาพรวม ทำให้ประชาชนในพื้นที่ขาดขวัญและกำลังใจในการดำเนินชีวิต ส่งผลให้เกิดความหวาดระเวงไม่กล้าอยู่ในพื้นที่และเกิดผลกระทบหลายด้านจากความรุนแรงที่เกิดขึ้นสามารถสรุปเหตุการณ์ความไม่สงบและจำนวนผู้เสียชีวิตและบาดเจ็บจากเหตุการณ์ ดังกล่าว ตั้งแต่ปี พ.ศ. 2547-2561 จากฐานข้อมูลเหตุการณ์ชายแดนใต้ ศูนย์เฝ้าระวังสถานการณ์ภาคใต้ สถิติจำนวนเหตุการณ์ความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ ตั้งแต่ปี 2547-2561 ข้อมูล ณ วันที่ 4 มกราคม 2562 เกิดเหตุการณ์ทั้งสิ้น 20,163 เหตุการณ์ มีผู้เสียชีวิตทั้งสิ้น 6,921 ราย ผู้ได้รับบาดเจ็บมีทั้งสิ้น 13,511 ราย (ศูนย์เฝ้าระวังสถานการณ์ภาคใต้ ,2561) จะเห็นได้ว่าเหตุการณ์ความไม่สงบ และความรุนแรงที่เกิดขึ้นเกือบ 15 ปี ในจังหวัดชายแดนภาคใต้ แสดงให้เห็นว่าสถานการณ์ความรุนแรงและความสูญเสียที่ผ่านมามีแนวโน้มของความรุนแรงที่ลดลง แต่กลุ่มผู้ก่อความไม่สงบในพื้นที่ยังคงมีขีดความสามารถที่จะปฏิบัติการและก่อเหตุร้ายได้ตลอดเวลาเพื่อต้องการสร้างความแตกแยกและความสูญเสียขึ้นในประเทศ ด้วยวิถีแห่งความรุนแรง

ย่อมส่งผลให้เกิดความขัดแย้งที่ยืดเยื้อและเรื้อรัง โดยมีลักษณะโจมตีตอบโต้กันไปมาระหว่างเจ้าหน้าที่รัฐและกลุ่มผู้เห็นต่างจากรัฐ ซึ่งจะทำให้มีผู้เสียชีวิตและบาดเจ็บเป็นจำนวนมาก แสดงดังภาพที่ 1-1



ภาพที่ 1-1 สถิติแสดงจำนวนเหตุการณ์ จำนวนผู้เสียชีวิติ และได้รับบาดเจ็บจากสถานการณ์ความไม่สงบในพื้นที่จังหวัดชายแดนใต้ ตั้งแต่ ปี 2547-2561 (ศูนย์เฝ้าระวังสถานการณ์ภาคใต้, 2561)

ภายใต้สถานการณ์ความไม่สงบในเขตพื้นที่ชายแดนภาคใต้ที่ทวีความรุนแรงขึ้นด้วยเหตุปัจจัยต่าง ๆ ทำให้การรักษาความปลอดภัยในเขตพื้นที่ชายแดนใต้ โดยเฉพาะสถานศึกษาในจังหวัดชายแดนภาคใต้ เป็นหนึ่งกลุ่มเป้าหมายที่จัดอยู่ในกลุ่มเป้าหมายอ่อนแอ ที่ผู้ก่อความไม่สงบต้องการโจมตีโรงเรียนและสถานศึกษา ซึ่งจากสถิติการโจมตีโรงเรียนและสถานศึกษาทั่วโลกของผู้ก่อการร้ายปรากฏว่าโรงเรียนในไทยติดอันดับการถูกโจมตีเป็น อันดับ 2 รองจากปากีสถาน แสดงดังภาพที่ 1-2 โดยที่ประเทศไทยมีสถิติการโจมตีโรงเรียน ก่อเหตุวางเพลิงเผาโรงเรียนในพื้นที่จังหวัดชายแดนภาคใต้ ตั้งแต่ปี 2547 ถึง 2560 ทั้งหมด 360 โรงเรียน ครูหรือบุคลากรทางการศึกษาเสียชีวิตรวม 136 คน บาดเจ็บและพิการรวม 151 คน (รายงานสถานการณ์เด็กในจังหวัดชายแดนใต้, 2561) โดยที่ครูหรือบุคคลากรทางการศึกษาเป็นเป้าหมายที่ถูกทำร้ายในช่วงเริ่มต้นของความรุนแรง ซึ่งมีตัวเลขที่สูงในช่วยปี 2549 และ 2555 หลังจากนั้นก็มีจำนวนที่ลดลงอย่างต่อเนื่องและในปี 2560 ไม่มีครูเสียชีวิตหรือบาดเจ็บจากสถาการณ์ความไม่สงบ แสดงดังตารางที่ 1,2 ทั้งนี้เหตุการณ์ความไม่สงบในพื้นที่ส่งผลให้กระทบต่อการพัฒนาเด็กคือการทำลายโรงเรียนสถาบันการศึกษาไม่เพียงแต่เป็นการทำให้เด็กไม่มีสถานที่สำหรับเรียนหนังสือแล้วยังทำให้เกิดความหลาดกลัวในการเดินทางไปโรงเรียนเพราะเกรงว่าเด็กหรือนักเรียนไม่ปลอดภัยในระหว่างการเดินทางหรือที่โรงเรียน และส่งผลให้ครูไม่กล้าไปโรงเรียน



ภาพที่ 1-2 สถิติการโจมตีโรงเรียนและสถานศึกษาทั่วโลก (The tlantic, 2561)

ตารางที่ 1-1 จำนวนโรงเรียนหรือสถานศึกษาที่ถูกวางเพลิง

ปี	จำนวน
2547	52
2548	28
2549	47
2550	192
2551	9
2552	16
2553	4
2554	1
2555	4
2556	3
2557	2
2558	0
2559	2
2560	0
รวม	**360**

ที่มา : รายงานสถานการณ์เด็กในจังหวัดชายแดนภาคใต้ประจำปี 2560

ตารางที่ 1-2 จำนวนโรงเรียนหรือสถานศึกษาที่ถูกวางเพลิง

ปี	ครู	
	เสียชีวิต	**บาดเจ็บและพิการ**
2547	14	10
2548	23	15
2549	19	24
2550	22	16
2551	10	16
2552	8	14
2553	10	8
2554	9	19
2555	8	13
2556	7	9
2557	5	2
2558	2	1
2559	1	5
2560	0	0
รวม	**136**	**151**

ที่มา : รายงานสถานการณ์เด็กในจังหวัดชายแดนภาคใต้ประจำปี 2560

นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558-2564 ของประเทศไทย (นโยบายความมั่นคงแห่งชาติ พ.ศ. 2548-2564) ได้กำหนด 16 ประเด็นนโยบาย โดยลำดับความสำคัญเพื่อให้การขับเคลื่อนนโยบายความมั่นคงให้มีทิศทางที่ชัดเจนกำหนดเป็นสองส่วน คือ ส่วนที่ 1 นโยบายสำคัญเพื่อเสริมสร้างความมั่นคงที่เป็นแก่นหลักของชาติ ประกอบด้วย 3 นโยบาย มุ่งการเสริมสร้างฐานรากความมั่นคงและเสริมสร้างสภาวะแวดล้อมที่สันติสุขในจังหวัดชายแดนภาคใต้ และส่วนที่ 2 นโยบายความมั่นคงแห่งชาติทั่วไป ประกอบด้วย 12 นโยบายมุ่งสร้างภูมิคุ้มกันของสังคมในทุกระดับ ให้พร้อมเผชิญปัญหาและภัยคุกคามต่าง ๆ รวมถึงการลดความเสี่ยงจากผลกระทบของภัยคุกคามดังกล่าวตลอดจนการเตรียมพร้อมเพื่อป้องกันและแก้ปัญหาความมั่นคงอย่างรอบด้าน มีความเข้มแข็งในการป้องกันประเทศ และการเสริมสร้างสภาวะแวดล้อมระหว่างประเทศที่เอื้อต่อการรักษาผลประโยชน์ของชาติ จากกรอบนโยบายความมั่นคงแห่งชาติ ในนโยบายที่ 15 พัฒนาระบบงานข่าวกรองให้มี

ประสิทธิภาพ ข้อที่ 14.1ดำเนินงานข่าวกรองที่มีคุณภาพและแจ้งเตือนภัยล่วงหน้าอย่างมีประสิทธิภาพทั้งภัยคุกคามต่อความมั่นคงแห่งชาติ และความเคลื่อนไหวที่สนับสนุนการเสริมสร้างความมั่นคงและผลประโยชน์แห่งชาติ ข้อที่ 14.2 เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง และหน่วยงานภาครัฐ รวมทั้งหน่วยงานข่าวกรองต่างประเทศ และมีเครือข่ายด้านข้อมูลข่าวสารกับภาคเอกชนและประชาชน ข้อที่ 14.3 เสริมสร้างและพัฒนาขีดความสามารถของระบบงานข่าวกรองอย่างต่อเนื่องโดยพัฒนาบุคลากรและเพิ่มศักยภาพของเทคโนโลยี ระบบฐานข้อมูลและองค์กรด้านการข่าวเสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ ซึ่งสอดคล้องกับกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554-2563 ของประเทศไทย (ICT2020) ในยุทธศาสตร์ที่ 4 ใช้ ICT เพื่อสร้างนวัตกรรมการบริการของภาครัฐที่สามารถให้บริการประชาชนและธุรกิจทุกภาคส่วนได้อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยสูง และมีธรรมาภิบาล (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2554) ซึ่งกรอบนโยบายดังกล่าวให้ความสำคัญกับการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการบริหารจัดการระบบสารสนเทศและความมั่นคงปลอดภัยสูงของชาติซึ่งการพัฒนาทางเทคโนโลยีได้รับอิทธิพลมาจากการใช้ชีวิตประจำวันของมนุษย์เพื่อที่จะนำเทคโนโลยีมาใช้เพื่ออำนวยความสะดวกในการติดต่อสื่อสาร ทำให้สามารถนำเสนอข้อมูลถึงตัวผู้ใช้ได้ทุกที่ทุกเวลาเพื่อประกอบการปฏิบัติภารกิจต่าง ๆ หรือสนับสนุนการตัดสินใจอย่างทันท่วงที ซึ่งจะนำไปสู่การใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสารได้เต็มที่ในการดำรงชีวิตและการประกอบอาชีพ เพื่อพัฒนาไปสู่สังคมดิจิทัลตามมาตรฐานสากล อันเป็นจุดมุ่งหมายเชิงวิสัยทัศน์ในการพัฒนาเพื่อก้าวเข้าสู้สังคมอุดมปัญญา หรือ สมาร์ทไทยแลนด์ (Smart Thailand) ที่วางไว้ ตามกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสารสู่ปี 2563 และตามเป้าหมายของแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 3) ของประเทศไทย พ.ศ. 2557-2563 บนพื้นฐานของการพัฒนาประเทศด้านเทคโนโลยีสารสนเทศและการสื่อสาร

การรักษาความมั่นคงปลอดภัย คือสภาพที่ปราศจากภัย หรือ พ้นจากสถานการณ์ที่ไม่ค่อยปลอดภัยที่เป็นหรืออาจเป็นอันตรายต่อชีวิตและทรัพย์สิน หรือการที่ร่างกายปราศจากอุบัติเหตุใดหรือทรัพย์สินปราศจากความเสียหายใด ๆ ซึ่งเป็นสิ่งที่คนเราทุกคนต้องการ อันเนื่องจากสภาพความเป็นอยู่ของคนในสังคมปัจจุบันได้เกิด ปัญหาทางด้านสังคม และภัยอันตรายที่เกิดจากปรากฏการณ์ธรรมชาติ เช่น พายุ น้ำท่วม ฟ้าผ่า แผ่นดินไหว ดินถล่ม และเพลิงไหม้ ภัยอันตรายที่เกิดจากการกระทำของมนุษย์ ได้แก่ การกระทำผิดโดยเปิดเผย เช่น การจลาจล การก่อความไม่สงบ และการโจมตีของฝ่ายตรงข้าม และกระทำโดยไม่เปิดเผย เช่น การโจรกรรม การจารกรรม การก่อวินาศกรรม และการก่อการร้าย (ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ, 2552) การหาแนวทางป้องกัน หรือหลีกเลี่ยงต่อภัยอันตรายดังกล่าว ส่วนใหญ่ในปัจจุบันนิยมเลือกใช้อุปกรณ์ด้านการป้องกันและรักษาความปลอดภัย คือ ระบบสัญญาเตือนภัย และบ่อยครั้งที่เกิด

เหตุการณ์ความไม่สงบในพื้นที่ ทำให้เกิดความสูญเสียและเสียหายต่อชีวิตและทรัพย์สินของหน่วยงานเป็นอย่างมาก การเพิ่มการรักษาความปลอดภัยในเขตพื้นที่จังหวัดชายแดนภาคใต้ การป้องกันไม่ให้เกิดเหตุร้ายหรือการที่จะสามารถติดตามแก้ไขปัญหาที่เกิดขึ้นได้ทันถ่วงที (สำนักข่าวกรองแห่งชาติ, 2553) หากมีเหตุการณ์ใดเกิดขึ้น จึงถือได้ว่าเป็นแนวทางปฏิบัติโดยทั่วไป การเพิ่มจุดตรวจเพื่อป้องกันและรักษาความปลอดภัยในพื้นที่จังหวัดชายแดนใต้ การติดตั้งกล้องวิดีโอวงจรปิด หรือ CCTV เมื่อติดตั้งแล้วก็จะทำให้เห็นภาพในมุมต่าง ๆ ของสถานที่ และสามารถทำให้เห็นพื้นที่ต่าง ๆ ได้อย่างครอบคลุม เพียงแค่นั่งรับชมผ่านทางจอมอนิเตอร์ ถ้าหากเกิดอุบัติเหตุหรือเกิด อาชญากรรม โจรกรรมขึ้น ก็จะทำให้เห็นภาพเหตุการณ์ได้อย่างทันท่วงที และภาพเหตุการณ์ถูกเก็บบันทึกได้ผ่านกล้องวงจรปิด ซึ่งปัจจุบันเทคโนโลยีของกล้องวงจรปิดและเทคโนโลยีทางด้าน Image Processing มีการพัฒนาขึ้นมากกว่าจะเป็นกล้องธรรมดาทั่วไป จึงได้มีการนำเทคโนโลยีทางด้าน Image Processing มาใช้เพื่อช่วยในงานต่าง ๆ เช่น ตรวจจับป้ายทะเบียนรถ ตรวจจับการเคลื่อนที่ของมนุษย์ การวิเคราะห์ใบหน้าของมนุษย์ว่ามีใบหน้าตรงกับฐานข้อมูลหรือไม่ รวมถึงการนำเอาอุปกรณ์เตือนภัยมาผนวกรวมกับกล้องวงจรปิด หรือ CCTVเชื่อมโยงเข้าด้วยกันผ่านทางเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการแจ้งเตือนเหตุการณ์ที่เกิดขึ้นซึ่งเรียกว่าเทคโนโลยี Internet of thing : IoT หรือเทคโนโลยีเชื่อมโยงสรรพสิ่ง

Internet of Thing : IoT หรือเทคโนโลยีเชื่อมโยงสรรพสิ่ง คือการที่อุปกรณ์อิเล็กทรอนิกส์สามารถเชื่อมต่อและสื่อสารกันได้ผ่านเครือข่ายอินเทอร์เน็ต โดยอาศัยเซ็นเซอร์ในการสื่อสาร (Kevin Ashton, 2009) โดยที่สิ่งต่าง ๆ ถูก เชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการควบคุมและใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต หรือการที่อุปกรณ์อัจฉริยะต่าง ๆ ถูกเชื่อมโยงเข้าด้วยกัน ผ่านทางเครือข่ายอินเทอร์เน็ตซึ่งทำให้มนุษย์สามารถสั่งการและควบคุมการทำงานและการใช้งานอุปกรณ์ต่าง ๆ ผ่านทาง ระบบเครือข่ายอินเทอร์เน็ตได้ และเป็นแนวคิดในการพัฒนาระบบบริหารจัดการร่วมกับ อุปกรณ์ต่างเพื่อทำการเชื่อมต่อสิ่งต่าง ๆ ได้อย่างอัตโนมัติ เพื่อเพิ่ม ศักยภาพด้านการติดต่อสื่อสารและแลกเปลี่ยนข้อมูลได้อย่างอัตโนมัติ รวมไปถึงการบริหารจัดการข้อมูล การจัดเก็บข้อมูล (ต่วนนูรีซันน์, 2559) เพื่อเป็นองค์ประกอบในการพัฒนาระบบรักษาความมั่นคงปลอดภัยที่มีการควบคุมอุปกรณ์ได้อย่างอัจฉริยะ และในอนาคตโลกที่เกือบทุกสิ่งสามารถเชื่อมต่อได้ ผ่านเครือข่ายอินเทอร์เน็ตที่เชื่อมโยงทุกสิ่งเข้าด้วยกัน ทำให้สรรพสิ่งต่าง ๆ มีวิธีการระบุตัวตนได้ รับรู้บริบทของสภาพแวดล้อมได้ และมีปฏิสัมพันธ์โต้ตอบให้สามารถทำงานร่วมกันได้ การนำเอาอุปกรณ์เครื่องมือทางด้านการรักษาความปลอดภัย อุปกรณ์แจ้งเตือนภัย เช่นอุปกรณ์ตรวจจับการบุกรุก ตรวจจับเสียง ตรวจจับสั่นสะเทือน ตรวจจับควันไฟ ตรวจวัดระดับน้ำ เป็นต้น ซึ่งอุปกรณ์เหล่านี้สามารถนำมาติดตั้งพร้อมกับระบบกล้องวงจรปิดเพื่อให้นำมาใช้ในด้านการเฝ้าระวังด้วยการ ตรวจจับของเซนเซอร์ จากเหตุการณ์ความไม่ปลอดภัยที่ครอบคลุมพื้นที่ตลอด 24 ชั่วโมง อย่างมีประสิทธิภาพสูงสุด ทำให้การรับข้อมูลมีความรวดเร็ว ถูกต้อง แม่นยำและสามารถ

บันทึกเหตุการณ์หรือแจ้งเตือนไว้เพื่อเป็นหลักฐานประกอบการพิจารณา สืบสวน สอบสวน เมื่อมีเหตุฉุกเฉิน หรือมีเหตุร้ายเกิดขึ้น โดยข้อมูลที่ได้จะถูกจัดเก็บอยู่รูปแบบของพยานหลักฐานดิทัล หรือ Digital Forensic

การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensic) มีกระบวนการทำงานแบ่งได้เป็น 3 ขั้นตอนหลัก คือ 1) การรวบรวมพยานหลักฐาน (Acquisition) 2) การวิเคราะห์ (Analysis) 3) การรายงานผลการตรวจพิสูจน์ (Report) ซึ่งในการตรวจสอบและเก็บหลักฐานทางดิจิทัลจากอุปกรณ์ IoT ในการตรวจจับความไม่ปลอดภัยที่อาจจะเกิดขึ้นเพื่อเป็นหลักฐานที่ใช้ในการพิสูจน์ข้อเท็จจริง เพื่อแสดงความบริสุทธิ์หรือความผิดของบุคคล โดยในปัจจุบันข้อมูลได้ถูกจัดเก็บอยู่ในรูปแบบของไฟล์ข้อมูลดิจิทัล และถูกบันทึกไว้ในระบบฐานข้อมูล (ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2560) ไม่ว่าจะเป็น ฐานข้อมูลหมายจับ หรือคดีความมั่นคงต่าง ๆ เพื่อดำเนินการตรวจสอบหลักฐานการกระทำความผิดได้อย่างสะดวกและรวดเร็ว ทำให้ข้อมูลที่ได้อยู่ในรูปแบบของพยานหลักฐานดิจิทัล (Digital Forensic) เพื่อให้ได้มาซึ่งรายงานผลที่มีประสิทธิภาพและสามารถนำไปใช้ประโยชน์ในการพิสูจน์หลักฐานต่อไป

จากความเป็นมาและความสำคัญของปัญหาที่กล่าวมาข้างต้นจึงจำเป็นต้องพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ เพื่ออำนวยความสะดวกในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัย สอดส่องดูแลเหตุการณ์ หรือสถานการณ์ต่าง ๆ การเฝ้าระวัง ซึ่งระบบที่พัฒนาขึ้นสามารถนำไปใช้เพื่อแก้ไขหรือลดปัญหาด้านความปลอดภัย ที่อาจเป็นเหตุ และส่งผลต่อการสร้างความไม่สงบในพื้นที่ เหมาะสำหรับสถานศึกษาและพื้นที่เสี่ยงภัยที่ต้องการความมั่นคงปลอดภัยสูง ซึ่งระบบสามารถตรวจสอบ วิเคราะห์ผลและรายงานผลได้อย่างรวดเร็ว พร้อมทั้งสามารถบันทึกข้อมูลทางด้านพยานหลักฐานดิจิทัลเพื่อใช้ประกอกการดำเนินการต่อไปได้อย่างชัดเจน

1.2 วัตถุประสงค์การวิจัย

1.2.1 เพื่อวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.2.2 เพื่อพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.2.3 เพื่อออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.2.4 เพื่อการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.2.5 เพื่อศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.3 ขอบเขตการวิจัย

1.3.1 ตัวแปรที่ใช้ในการวิจัย

1.3.1.1 ตัวแปรต้นได้แก่ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.3.1.2 ตัวแปรตามได้แก่ คือ ผลการตรวจสอบหลักฐานดิจิทัลที่ได้จากระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ซึ่งประกอบด้วย 3 ด้าน

1.3.1.2.1 การรวบรวมพยานหลักฐาน (Acquisition)

1.3.1.2.2 การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัย (Analysis)

1.3.1.2.3 การรายงานความมั่นคงปลอดภัยสูงสำหรับสถานศึกษา (Report)

1.3.2 ประชากรและกลุ่มตัวอย่าง

1.3.2.1 ประชากร คือ ผู้บริหาร ครู อาจารย์ และบุคลากรทางการศึกษา จำนวน 42,910 คน จากสถานศึกษาทั้งในและนอกระบบในเขตพื้นที่การศึกษาจังหวัดชายแดนภาคใต้ ประกอบด้วยจังหวัด นราธิวาส ยะลา ปัตตานี (ข้อมูล ณ วันที่ 10 มิถุนายน 2560)

1.3.2.2 กลุ่มตัวอย่างที่ 1 ทำการสอบถามเกี่ยวกับสภาพปัญหาและความต้องการในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ได้แก่

1.3.2.2.1 ขั้นที่ 1 ผู้วิจัยเก็บของมูลจากผู้บริหาร ครู อาจารย์ และบุคคลากรทางการศึกษา จำนวน 42,910 คน ของสถานศึกษาทั้งในระบบและนอกระบบในเขตพื้นที่การศึกษาจังหวัดชายแดนภาคใต้ประกอบด้วย จังหวัด นราธิวาส ยะลา ปัตตานี

1.3.2.2.2 ขั้นที่ 2 จากประชากร จำนวน 42,910 คน ผู้วิจัยได้สุ่มตัวอย่างจากผู้บริหาร ครู อาจารย์ และบุคลากรทางการศึกษา จำนวน 198 คน ได้มาจากการสุ่มแบบแบ่งชั้น (Stratified Random Sampling) การกำหนดกลุ่มตัวอย่างใช้สูตรของทาโร ยามาแน่ (Yamane, 1973) จากนั้นทำการเลือกตัวอย่างแบบเจาะจง (Purposive Sampling) และใช้วิธีสุ่มอย่างง่าย

1.3.2.3 กลุ่มตัวอย่างที่ 2 ทำการศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยใช้วิธีการสุ่มตัวอย่างแบบง่าย จากสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วย ผู้บริหาร ครู อาจารย์ และบุคลากรทางการศึกษาจำนวน จำนวน 50 คน

1.4 นิยามศัพท์เฉพาะ

1.4.1 การรักษาความมั่นคงปลอดภัย หมายถึง กระบวนการรักษาความปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.4.2 เทคโนโลยีเชื่อมโยงสรรพสิ่ง (Internet of Things : IoT) หมายถึง เทคโนโลยีอินเทอร์เน็ตที่ใช้การติดต่อสื่อสารระหว่างสิ่งที่ทำการตรวจจับเพื่อนำเข้าสู่ระบบ

1.4.3 หลักฐานดิจิทัล (Digital Forensic) หมายถึง ข้อมูล สารสนเทศ ที่ได้จากการรักษาความมั่นคงปลอดภัยประกอบด้วย ภาพถ่ายใบหน้า ภาพถ่ายทะเบียนรถ ข้อมูลยืนยันตัวตน ปริมาณควันไฟ ความร้อน ก๊าซ และแรงสั่งสะเทือน

1.4.4 การรวมพยานหลักฐาน (Acquisition) หมายถึง การเก็บข้อมูล สารสนเทศ ที่ได้จากใช้อุปกรณ์อิเล็กทรอนิคส์ หรือ IoT ในการตรวจจับและตรวจสอบหลักฐานดิจทัล (Digital Forensic)

1.4.5 การวิเคราะห์ความมั่นคงปลอดภัย (Analysis) หมายถึง การนำข้อมูล สารสนเทศที่ได้จากการรวมพยานหลักฐานดิจิทัล เข้าสู่ระบบรักษาความความมั่นคงปลอดภัยสูง เพื่อดำเนินการวิเคราะห์และตัดสินใจด้านความมั่นคงปลอดภัย

1.4.6 การรายงานผลการตรวจพิสูจน์หลักฐาน (Report) หมายถึง การนำผลการวิเคราะห์ความมั่นคงปลอดภัยสูง รายงานผลการตรวจพิสูจน์หลักฐานดิจิทัล และ รายงานความมั่นคงปลอดภัยสูงสำหรับสถานศึกษาในจังจัยน

1.4.7 สถานศึกษาในจังหวัดชายแดนภาคใต้ หมายถึง สถานศึกษาในระบบและนอกระบบในสังกัดพื้นที่การศึกษาจังหวัดนราธิวาส จังหวัดปัตตานี และจังหวัดยะลา

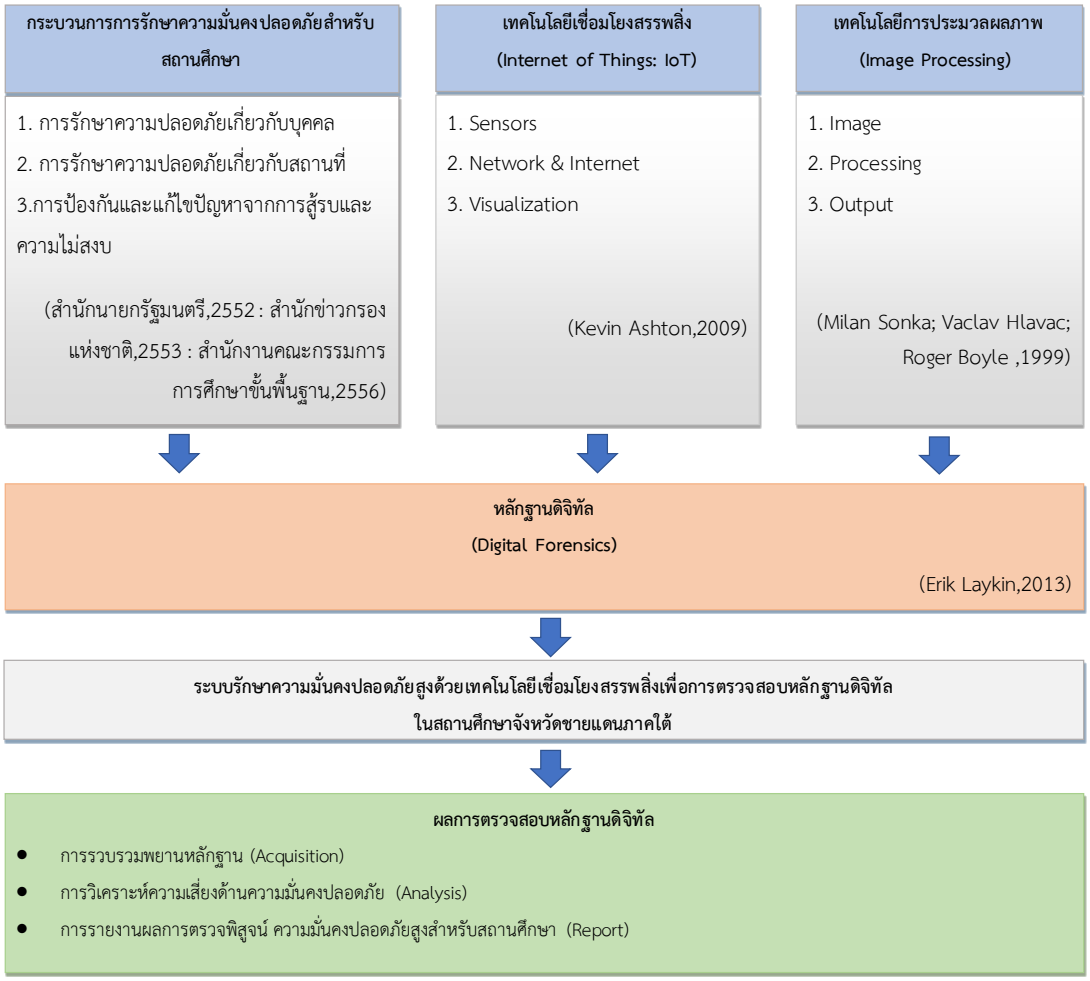
1.4.8 จังหวัดชายแดนภาคใต้ หมายถึง จังหวัดทางตอนใต้ของประเทศไทยที่มีเขตพื้นที่ระหว่างชายแดนภาคใต้ประกอบด้วย จังหวัดนราธิวาส จังหวัดปัตตานี และจังหวัดยะลา

1.4.9 ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ หมายถึง ระบบที่ใช้ในการตรวจสอบและบริหารจัดการข้อมูลด้านความมั่นคงปลอดภัยสูงสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ที่ผู้วิจัยพัฒนาขึ้นโดยใช้แนวคิดการบริหารจัดการสารสนเทศและเทคโนโลยีเชื่อมโยงสรรพสิ่ง

1.4.10 ผลการรักษาความมั่นคงปลอดภัย หมายถึง ผลลัพธ์ที่ได้จากการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล ผลที่ได้จะเป็นข้อมูลแสดงสถานะความปลอดภัยของสถานศึกษาแบบทันทีทันใด เพื่อการแจ้งเตือน และวิเคราะห์ผลการรักษาความปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.5 กรอบแนวคิดที่ใช้ในการวิจัย

การวิจัย เรื่อง ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีกรอบแนวคิดในการวิจัย ดังนี้ ภาพที่ 1- 3



ภาพที่ 1-3 กรอบแนวคิดในการวิจัย (Conceptual Framework)

จากภาพที่ 1-3 กรอบแนวคิดในการวิจัยระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วยรายละเอียด ดังนี้

1.5.1 กระบวนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา เป็นกระบวนการรักษาความปลอดภัยสำหรับสถานศึกษา แบ่งออกเป็น 3 ส่วนหลักคือ 1) การรักษาความปลอดภัยเกี่ยวกับบุคคล 2) การรักษาความปลอดภัยเกี่ยวสถานที่ 3) การป้องกันและแก้ปัญหาจากการสู้รบและความไม่สงบ

(สำนักนายกรัฐมนตรี, 2552) (สำนักข่าวกรองแห่งชาติ, 2553) (สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน, 2556) โดยงานวิจัยนี้มุ่งเน้นความปลอดภัยที่เป็นการตรวจสอบบุคคล ความปลอดภัยสำหรับอาคารสถานที่ และฐานข้อมูลด้านความมั่นคงเกี่ยวกับการก่อเหตุการณ์ความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้

1.5.2 เทคโนโลยีเชื่อมโยงสรรพสิ่ง (Internet of Things) สำหรับงานวิจัยนี้เลือกใช้เทคโนโลยีสื่อสารทางด้าน อุปกรณ์เซนเซอร์ตรวจจับ และ บัตร RFID เพื่อใช้ในการสื่อสารและแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์เพื่อส่งค่าข้อมูลเข้าสู่ระบบได้อย่างอัตโนมัติ (Kevin Ashton,2009) ประกอบด้วย อุปกรณ์ตรวจจับใบหน้า ตรวจจับป้ายทะเบียน สแกนบัตร อุปกรณ์ตรวจจับปริมาณ ควัน ความร้อน ก๊าซ และแรงสั่นสะเทือน เพื่อการประเมินและตรวจสอบความปลอดภัยตามที่ต้องการได้

1.5.3 เทคโนโลยีการประมวลผลภาพ (Image Processing) หรือการประมวลผลภาพเป็นกระบวนการจัดการและวิเคราะห์สารสนเทศของรูปภาพ โดยใช้คอมพิวเตอร์ในการประมวลผล ซึ่งงานวิจัยนี้เลือกใช้เทคโนโลยีในการตรวจจับใบหน้า และ ตรวจจับป้ายทะเบียนรถ เพื่อให้ได้มาซึ่งผลลัพธ์จากการตรวจสอบสารสนเทศที่มีอยู่ในระบบและแสดงผลเพื่อการตัดสินใจผลลัพธ์ตามที่ต้องการ

1.5.4 หลักฐานดิจิทัล (Digital Forensic) เป็นวิธีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลจากการเก็บหลักฐาน การค้นหา การวิเคราะห์ และการนำเสนอหลักฐานทางดิจิทัลที่อยู่ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ ซึ่งงานวิจัยนี้เลือกใช้การเก็บหลักฐานที่สามารถนำไปตรวจสอบความถูกต้องข้อมูลเพื่อใช้เป็นหลักฐานยืนยันหรือแสดงข้อมูลตามที่ต้องการ

1.5.5 ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ เป็นระบบที่ใช้ในการวิเคราะห์และตัดสินใจทางด้านความมั่นคงปลอดภัยที่สามารถทำการบันทึก แจ้งเตือนและรายงานผลความเสี่ยงและความปลอดภัยสำหรับสถานศึกษา

1.5.6 ผลการตรวจสอบหลักฐานดิจิทัล ผลลัพธ์ที่ได้จากการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล มีกระบวนการทำงานแบ่งได้เป็น 3 ขั้นตอน คือ 1) การรวบรวมพยานหลักฐาน (Acquisition) 2) การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัย (Analysis) 3) การรายงานผลการตรวจพิสูจน์ความมั่นคงปลอดภัยสูงสำหรับสถานศึกษา (Report)

1.6 ประโยชน์ที่ได้จากงานวิจัย

1.6.1 สถานศึกษามีระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ในรูปแบบของซอฟต์แวร์เชิงบริการ

1.6.2 สถานศึกษามีระบบฐานข้อมูลและระบบสารสนเทศที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยสูงจากการก่อเหตุการณ์ความไม่สงบในจังหวัดชายแดนภาคใต้

1.6.3 สถานศึกษามีระบบที่สามารถแจ้งเตือนข้อมูลที่อาจเป็นการก่อเหตุการณ์ความไม่สงบสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.6.4 ระบบที่พัฒนาขึ้นทำให้เกิดการบูรณาการการใช้ข้อมูลด้านความมั่นคงปลอดภัยสูงร่วมกันระหว่างสถานศึกษาและหน่วยงานที่เกี่ยวข้อง

1.6.5 ระบบที่พัฒนาขึ้นช่วยให้เพิ่มหลักฐานจากการก่อนเหตุการณ์ความไม่สงบสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.6.6 ระบบที่พัฒนาขึ้นช่วยเพิ่มการติดตามการก่อเหตุการณ์ความไม่สงบสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1.6.7 ระบบที่พัฒนาขึ้นช่วยลดการก่อให้เกิดความสูญเสียและความเสียจากการก่อเหตุการณ์ความไม่สงบสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษาเอกสารการศึกษาเอกสาร แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัยด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 การรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา

2.2 ระบบรักษาความมั่นคงปลอดภัยสูง (Hight Integrated Security Management System)

2.3 เทคโนโลยีเชื่อมโยงสรรพสิ่ง (Internet of Things : IoT)

2.4 เทคโนโลยีการประมวลผลภาพ (Image Processing)

2.5 หลักฐานดิจิทัล (Digital Forensic)

2.6 งานวิจัยที่เกี่ยวข้อง

2.7 สรุปเอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 การรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา

2.1.1 การรักษาความมั่นคงปลอดภัยภายในราชอาณาจักร หมายถึง การดำเนินการเพื่อป้องกัน ควบคุม แก้ไข และ ฟื้นฟู สถานการณ์ใดที่เป็นภัย อันเกิดจากบุคคลหรือกลุ่มบุคคลที่กระทำให้เกิดความไม่สงบสุข ทำลาย หรือทำความเสียหายต่อชีวิต ร่างกาย ทรัพย์สินของประชาชนหรือของรัฐ ให้กลับสู่สภาวะปกติเพื่อให้เกิดความสงบเรียบร้อยของประชาชน หรือความมั่นคงของรัฐ (มาตรา 3 พ.ร.บ.การรักษาความมั่นคงภายในฯ พ.ศ. 2551) สภาความมั่นคงแห่งชาติ (สมช.) ได้ยกร่างนโยบายความมั่นคงแห่งชาติ พ.ศ. 2558-2564 กำหนดปัญหาความมั่นคงของประเทศไว้ดังนี้ 1. ยาเสพติด 2. การก่อการร้ายและอาชญากรรมข้ามชาติ 3. ภัยพิบัติทางธรรมชาติ 4. ความไม่สงบในจังหวัดชายแดนภาคใต้ 5. ความขัดแย้งของคนในประเทศ เพื่อป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหาย ซึ่งภัยคุกคามในปัจจุบัน คือ เป็นภัยคุกคามรูปแบบใหม่ (Non-Traditional Threat)” ซึ่งใช้เรียกภัยหลังยุคสงครามเย็น (ความขัดแย้งระหว่างสหรัฐฯกับสหภาพโซเวียตระหว่าง พ.ศ. 2490-2534) เป็นภัยที่เกิดขึ้นในทุกมิติ ทั้งด้านเศรษฐกิจ สังคม การเมือง สิ่งแวดล้อม ข้อมูลข่าวสาร สารสนเทศฯเป็นต้น ลักษณะของปัญหาไม่ได้เกิดขึ้นจากความขัดแย้งระหว่างรัฐต่อรัฐเหมือนในอดีต และการแก้ปัญหาก็ไม่ได้ใช้กำลังทหารเข้าทำการรบ แต่เป็นการแก้ไขปัญหาตามสถานการณ์ที่เกิดขึ้น

2.1.2 มาตรฐานการรักษาความปลอดภัย หมายถึง ระดับที่ควรจะเป็นของมาตรการต่าง ๆ ที่ได้ถูกกำหนดขึ้นมาเพื่อให้หน่วยงานของรัฐ นำไปเป็นแนวทางในการปฏิบัติเพื่อพิทักษ์รักษาบุคคล ข้อมูล ข่าวสารลับ และสถานที่ ให้พ้นจากการโจรกรรมจากการบ่อนทำลาย การก่อวินาศกรรม และการก่อการร้าย รวมถึงการลดการเกิดความเสียหายที่อาจจะเกิดขึ้นจากการละเมิดการรักษาความปลอดภัย (สำนักข่าวกรองแห่งชาติ, 2553) มาตรฐานการรักษาความปลอดภัย ได้กำหนดแนวทางปฏิบัติ 5 ด้าน คือ

2.1.2.1 มาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล หมายถึง มาตรการที่ถูกกำหนดขึ้นเมื่อหน่วยงานนำไปเป็นแนวปฏิบัติ สามารถสรรหาบุคคลที่มีคุณสมบัติที่เหมาะสมและเชื่อแน่ว่าเป็นบุคคลที่ไม่เป็นภัยต่อความมั่งคงที่จะเข้ามาปฏิบัติหน้าที่ในหน่วยงาน การรักษาความปลอดภัยเกี่ยวกับบุคคลเป็นมาตรการที่ถูกกำหนดขึ้นมาเพื่อใช้สำหรับปฏิบัติต่อผู้ที่อยู่ระหว่างรอบรรจุหรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐหรือผู้ที่ จะได้รับความไว้วางใจให้เข้าถึงสิ่งที่เป็นความลับของทางราชการหรือให้ปฏิบัติ หน้าที่ราชการที่สำคัญเพื่อคัดเลือกและตรวจสอบให้ได้ผู้ที่มีคุณสมบัติเหมาะสมให้เป็นที่เชื่อแน่ว่าต้องเป็นผู้ที่ไม่เป็นภัยอันตรายต่อความมั่นคงและผลประโยชน์แห่งรัฐ หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติหรือมอบหมายให้มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคลดังนี้

2.1.2.1.1 ดำเนินการตรวจสอบประวัติและพฤติการณ์บุคคล เช่น ผู้ที่อยู่ระหว่างรอบรรจุหรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ ผู้ที่เป็นลูกจ้างทดลองปฏิบัติงาน หรือฝึกงานก่อนการบรรจุเข้ารับปฏิบัติหน้าที่ เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ และผู้ที่ขอกลับเข้ามารับราชการใหม่ เจ้าหน้าที่ของรัฐหรือบุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่หรือตำแหน่งงานสำคัญของหน่วยงานหรือเกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการ ทรัพย์สินที่มีค่าของแผ่นดิน ผู้ได้รับทุการศึกษาทั้งในประเทศหรือต่างประเทศแล้วมีข้อผู้กพันให้เข้าปฏิบัติงานให้แก่หน่ยงานของรัฐ ในกรณีที่ตรวจพบบุคคบที่มีพฤติการณ์หรือ ปรากฏข่าวสารที่น่าจะเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐหรือบุคคลที่เกี่ยวข้องกับชั้นความลับของทางราช หัวหน้าหน่วยงานของรัฐอาจขอให้องค์การรักษาความปลอดภัยตรวจสอบเพิ่มเติมได้

2.1.2.1.2 หน่วยงานของรัฐต้องจัดให้มีการรับรอบความไว้วางใจบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการโดยให้มีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษรและต้องผ่านการตรวจสอบประวัติและพฤติการณ์

2.1.2.1.3 เจ้าหน้าที่ทำการควบคุมการรักษาความภัยของหน่วยงานของรัฐต้องบันทึกชื่อบุคคลที่ได้รับการรับรองความไว้วางใจไว้ในทะเบียนความไว้วางใจของหน่วยงาน

2.1.2.1.4 หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการอบรมชี้แจงเกี่ยวกับระเบียบการรักษาความปลอดภัยแก่บุคคลที่ได้รับการบรรจุใหม่ ผู้ที่ไม่เคยได้รับการอบรมหรือผู้ที่จะได้รับ

การมแบหมายให้ปฏิบัติหน้าที่เกี่ยวกับความความของทางราชการรวมถึงการให้ความรู้ในวิทยาการด้านต่าง ๆ และต้องอบรมทบทวนตามระยะเวลาที่เหมาะสม เพื่อให้กระตุ้นจิตสำนึกและวินัยในด้านการักษาความปลอดภัย

2.1.2.2 มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ หมายถึง มาตรการที่ถูกกำหนดขึ้นเมื่อหน่วยงานนำไปเป็นแนวปฏิบัติที่จะทำให้การคุ้มครองข้อมูลข่าวสารลับดังกล่างไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง หรือ รั่วไหลไปสู่บุคคลที่ไม่มีความเกี่ยวข้องได้ เป็นการคุ้มครองข้อมูลข่าวสารลับไม่ให้สูญหาย ถูกทำลายเปลี่ยนแปลง หรือรั่วไหล การเปิดเผยข้อมูลข่าวสารลับต่อบุคคลหรือผู้ไม่มีอำนาจหน้าที่ที่ต้องอยู่ภายใต้เงื่อนไขโดยจะมีข้อยกเว้นที่ชัดเจนซึ่งสอดคล้องกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ข้อมูลข่าวสารลับที่ กล่าวถึงในมาตรฐานการรักษาความปลอดภัยข้อมูลข่าวสารลับนี้ หมายถึง ข้อมูลข่าวสารที่ได้มีคำสั่งไม่ให้เปิดเผยตามมาตรา 14 หรือ มาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และอยู่ในความครอบครองหรือการควบคุมดูแลของหน่วยงานของรัฐไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน โดยมีการกำหนดให้มีชั้นความลับ ชั้นลับ ลับมาก หรือลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของเจ้าหน้าที่ในหน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกันซึ่งเป็นข้อมูลข่าวสารในรูปแบบของเอกสาร แฟ้มรายงาน หนังสือแผนผัง แผนที่ ภาพวาด ภาพถ่ายฟิล์ม หรือการบันทึกภาพส่วนข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์จะมีการกำหนดมาตรฐานและคู่มือการปฏิบัติไว้ เป็นการเฉพาะของมาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติดังนี้

2.1.2.2.1 หัวหน้าหน่วยงานของรัฐต้องมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษรและให้มีการรับรองความไว้วางใจแก่บุคคลที่เกี่ยวข้องในการดำเนินการต่อข้อมูลข่าวสารลับดังนี้

2.1.2.2.2 การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับต้องดำเนินการตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ที่กำหนดไว้อย่างเคร่งครัด

2.1.2.2.3 หน่วยงานของรัฐต้องจัดให้มีแผนการปฏิบัติต่อข้อมูลข่าวสารลับในเวลาปกติและเวลาฉุกเฉินเพื่อให้ป้องกันการเข้าถึงของบุคคลที่ไม่มีอำนาจหน้าที่

2.1.2.3 มาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ หมายถึง มาตรการที่ถูกกำหนดขึ้นเมื่อหน่วยงานได้นำไปเป็นแนวปฏิบัติ จะทำให้พิทักษ์รักษาอาคาร สถานที่ วัสดุ อุปกรณ์ตลอดจนเจ้าหน้าที่และข้อมูลข่าวสารให้พ้นจากภัยอันตราย มาตรฐานที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ สถานที่ที่สงวนอาคารและสถานที่ของหน่วยงานของรัฐตลอดไปจนถึงวัสดุอุปกรณ์เจ้าหน้าที่ของรัฐและข้อมูลข่าวสารในอาคารสถานที่ดังกล่าว ให้พ้นจากการโจรกรรม

การจรกรรมการก่อวินาศกรรม และการก่อการร้ายหรือเหตุอื่นใดอันอาจทำให้เกิดการเสียสมรรถภาพในการปฏิบัติ ภารกิจของหน่วยงานซึ่งจะส่งผลให้เกิดความเสียหายต่อหน่วยงานของรัฐ ดังนั้น หน่วยงานของรัฐต้องดำเนินการสำรวจตรวจสอบและจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่การกำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้ดำเนินการดังนี้

2.1.2.3.1 หน่วยงานของรัฐต้องกำหนดพื้นที่รักษาความปลอดภัยตามความเหมาะสมและกำหนดขอบเขตที่แน่ชัดว่าพื้นที่ใดเป็นพื้นที่ควบคุมหรือพื้นที่ห่วงห้ามเพื่อทำการควบคุมการเข้า-ออกของบุคคลและยานพาหนะ

2.1.2.3.2 วางระบบป้องกันทางวัตถุเพื่อเป็นเครื่องหน่วงเหนี่ยวกีดขวาง และป้องกันบุคคลหรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยเช่น รั้ว เครื่องกีดขวางช่องทางเข้า-ออก รวมถึงระบบการให้แสงสว่างในยามวิกาล

2.1.2.3.3 การควบคุมบุคคลและยานพาหนะ

ก) การควบคุมบุคคลเพื่อตรวจสอบให้ทราบว่าเป็นบุคคลที่ได้รับอนุญาตให้ผ่านเข้าพื้นที่โดยจัดทำบัตรผ่าน บัตรแสดงตนและทำการบันทึกหลักฐานการผ่านเข้า-ออกนั้น

ข) การควบคุมยานพาหนะเพื่อให้ทราบว่ายานพาหนะใดได้รับอนุญาตให้ผ่านเข้าในบริเวณพื้นที่ได้และยังรวมถึงการควบคุมบุคคลรวมถึงสิ่งของต่าง ๆ บนยานพาหนะ

2.1.2.3.4 ระบบรักษาการณ์หน่วยงานของรัฐต้องจัดให้มี เจ้าหน้าที่รักษาความปลอดภัยประจำวัน เช่น เจ้าหน้าที่ยามรักษาการณ์ การวางระบบการติดต่อสื่อสารและสัญญาณแจ้งเตือนภัยสำหรับตรวจและเตือนให้ทราบเมื่อมีภัยอันตราย รวมถึงการติดตั้งอุปกรณ์เสริมมาตรการการรักษาความปลอดภัยทางเครื่องมือ หรือ เครื่องใช้อิเล็กทรอนิกส์ เป็นต้น เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น

2.1.2.3.5 ระบบป้องกันและระงับอัคคีภัยหัวหน้าหน่วยงานของรัฐต้องจัดให้มีมาตรการป้องกันและระงับอัคคีภัยที่มีประสิทธิภาพ

2.1.2.4 มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิคส์ หมายถึง มาตรการที่ถูกกำหนดขึ้นเมื่อหน่วยงานนำไปปฏิบัติ โดยจะคุ้มครองข้อมูลข่าวสรลับที่มีอยู่ในระบบอิเล็กทรอนิคส์ให้พ้นจากการสูญหาย ถูกทำลาย เปลี่ยนแปลง หรือรั่วไหลได้ เพื่อให้เป็นการคุ้มครองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิคส์ไม่ให้เกิดการสูญหาย ถูกทำลาย เปลี่ยนแปลงหรือรั่วไหล ให้มีความมั่นคงปลอดภัยและเชื่อถือได้ หน่วยงานของรัฐควรต้องพิจารณาถึงหลักการในการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ดังนี้

2.1.2.4.1 การควบคุมการเข้าถึงโดยให้มีการกำหนดตัวบุคคลการกำหนดรหัสจำกัดสิทธิของเจ้าหน้าที่ผู้ใช้งาน ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และกำหนดพื้นที่ที่ได้มีการรักษาความปลอดภัย

2.1.2.4.2 การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ การจัดทำต้องดำเนินการโดยเจ้าหน้าที่ที่เป็นผู้มีสิทธิในการเข้าถึงข้อมูข่าวสารลับและผ่านการตรวจสอบประวัติและพฤติการณ์ โดยชุดอุปกรณ์คอมพิวเตอร์ที่ใช้จัดทำข้อมูลข่าวสารลับไม่ควรใช้เครื่องที่เชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต สถานที่ที่ใช้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ควรเป็นพื้นที่ที่มีการักษาความปลอดภัย การดำเนินการจัดเก็บข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ทุกชั้นความลับต้องเข้ารหัสและจัดเก็บในเครื่องคอมพิวเตอร์ สถานที่จัดเก็บเครื่องคอมพิวเตอร์แม่ข่ายและสื่ออิเล็กทรอนิกส์ควรเป็นพื้นที่ที่มีการรักษาความปลอดภัย ควรมีระบบสำรองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์และเครื่องคอมพิวเตอร์แม่ข่ายสำรองโดยแยกจัดเก็บในสถานที่ปลอดภัย

2.1.2.4.3 การรับ-ส่ง ข้อมูลข่าวสารลับที่รับ – ส่งทางระบบโทรคมนาคม จะต้องดำเนินการเข้ารหัสแล้วเท่านั้น โดยกำหนดระเบียบปฏิบัติการรับ-ส่งทางระบบโทรคมนาคม

2.1.2.4.4 จัดทำทะเบียนเจ้าหน้าที่ควบคุมการเข้ารหัส

2.1.2.4.5 การทำลาย ขั้นตอนการขออนุมัติทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ให้ใช้หลักการเดียวกับข้อมูลข่าวสารลับที่เป็นเอกสาร โดยมีวิธีการทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์จะใช้ชุดคำสั่งในระบบปฏิบัติการหรือโปรแกรมซึ่งทำหน้าที่ลบแฟ้มข้อมูลโดยไม่สามารถกู้กลับคืนได้

2.1.2.5 มาตรฐานการรักษาวามปลอดภัยในการประชุมลับ หัวหน้ายหน่วยงานของรัฐต้องจัดให้มีมาตรการการรักษาความปลอดภัยในการประชุมลับโดยกำหนดมาตรการด้านการรักษาความปลอดภัยในการประชุมลับโดยกำหนดมาตรการด้านการรักษาความปลอดภัยเกี่ยวกับบุคคล ข้อมูล ข่าวสารลับ และสถานที่เพื่อพิทักษ์ รักษาในสิ่งที่เป็นความลับของทางราชการที่ปรากฏในการประชุมลับนั้นให้พ้นจากการก่อวินาศกรรม ทั้งนี้ให้นำมาตรฐานของการักษาความปลอดภัยแต่ละเรื่องมาปรับใช้โดยสามารถอนุโลมได้

2.1.2.6 มาตรฐานการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยหัวหน้าหน่วยงานของรัฐต้องกำหนดแนวทางปฏิบัติ หากเกิดการละเมิดด้านการรักษาความปลอดภัยเพื่อลดระดับความเสียหายกรณีเกิดการละเมิด ฝ่าฝืน หรือละเลยไม่ปฏิบัติ ตามมาตรการการรักษาความปลอดภัยที่ได้กำหนดไว้จะโดยเจตนาหรือไม่ก็ตามอันเป็นเหตุให้ความลับของทางราชการรั่วไหลหรือเป็นเหตุทำให้เจ้าหน้าที่ของรัฐ วัสดุ อุปกรณ์ ทรัพย์สินของรัฐ ได้รับความเสียหายและป้องกันไม่ให้เกิดซ้ำ ค้นหาข้อมูล สาเหตุเพื่อนำมาปรับปรุงแก้ไขมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้น

2.1.3 การบริหารจัดการด้านการรักษาความปลอดภัย

2.1.3.1 หัวหน้าหน่วยงานของรัฐมีหน้าที่รับผิดชอบและจัดให้มีระบบการรักษาความปลอดภัยในหน่วยงานของตน

2.1.3.2 หัวหน้าหน่วยงานของรัฐอาจมอบอำนาจหน้าที่ให้แก่ผู้ใต้บังคับบัญชาให้ปฏิบัติหน้าที่ โดยเป็นเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยเพื่อทำหน้าที่ดำเนินการควบคุมและกำกับดูแลตลอดจนให้คำปรึกษาเกี่ยวกับการรักษาความปลอดภัย ด้านบุคคล ข้อมูลข่าวสารลับ และสถานที่ของหน่วยงานนั้น ๆ ให้ปลอดภัย โดยมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษณและได้มีการรับรองความไว้วางใจให้เข้าถึงชั้นความลับ

2.1.3.3 หน่วยงานของรัฐมีหน้าที่รับผิดชอบในการจัดการอบรมเจ้าหน้าที่ของหน่วยงานให้ทราบถึงความจำเป็นและมาตรการเกี่ยวกับการรักษาความปลอดภัยรวมทั้งจัดให้มีการอบรมและทบทวนเพิ่มเติมอยู่เสมอตามระยะเวลาที่เหมาะสม

2.1.3.4 กรณีหน่วยงานของรัฐได้รับมอบหมายหรือทำสัญญาจ้างให้กับภาคเอกชนดำเนินการอย่างหนึ่งอย่างใดซึ่งเกี่ยวข้องกับการรักษาความปลอดภัยให้กับภาคเอกชนนั้นให้ถือปฏิบัติตามมาตรฐานการรักษาความปลอดภัยนี้ด้วย

2.1.4 การบริหารจัดการด้านการรักษาความปลอดภัย

2.1.4.1 หัวหน้าหน่วยงานของรัฐมีหน้าที่รับผิดชอบและจัดให้มีระบบการรักษาความปลอดภัยในหน่วยงานของตน

2.1.4.2 หัวหน่วยงานของรัฐอาจมอบอำนาจหน้าที่ให้แก่ผู้ใต้บังคับบัญชาให้ปฏิบัติหน้าที่โดยเป็นเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยเพื่อทำหน้าที่ดำเนินการควบคุมและกำกับดูแลตลอดจนให้คำปรึกษาเกี่ยวกับการรักษาความปลอดภัย ด้านบุคคล ข้อมูลข่าวสารลับ และสถานที่ของหน่วยงานนั้น ๆ ให้ปลอดภัย โดยมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษณและได้มีการรับรองความไว้วางใจให้เข้าถึงชั้นความลับ

2.1.4.3 หน่วยงานของรัฐมีหน้าที่รับผิดชอบในการจัดการอบรมเจ้าหน้าที่ของหน่วยงานให้ทราบถึงความจำเป็นและมาตรการเกี่ยวกับการรักษาความปลอดภัยรวมทั้งจัดให้มีการอบรมและทบทวนเพิ่มเติมอยู่เสมอตามระยะเวลาที่เหมาะสม

2.1.4.4 กรณีหน่วยงานของรัฐได้รับมอบหมายหรือทำสัญญาจ้างให้กับภาคเอกชนดำเนินการอย่างหนึ่งอย่างใดซึ่งเกี่ยวข้องกับการรักษาความปลอดภัยให้กับภาคเอกชนนั้นให้ถือปฏิบัติตามมาตรฐานการรักษาความปลอดภัยนี้ด้วย

2.1.5 การรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา

สถานศึกษาเป็นสถาบันที่จะสร้างเสริมประชาชนให้มีสุขภาพดี มีสติปัญญาที่เฉลียวฉลาด และมีพฤติกรรมที่ปลอดภัย สามารถดำรงชีวิตในสังคมได้อย่างมีความสุข และทำประโยชน์ให้แก่ประเทศชาติของไทยได้อย่างเต็มกำลังความสามารถ จากปัญหาต่าง ๆ ที่เกิดขึ้นได้ส่งผลกระทบต่อเด็กและเยาวชนในถานศึกษา ดังนั้นการจัดระบบรักษาความปลอดภัยสำหรับสถานศึกษาเป็นปัจจัยที่ส่งผลโดยตรงต่อคุณภาพการเรียนรู้ของผู้เรียน การพัฒนาผลสัมฤทธิ์ทางการเรียนรู้ที่จะประสบ

ผลสำเร็จหรือไม่เพียงใดขึ้นอยู่กับความสุขในการเรียนรู้ และการมีชีวิตที่ได้รับการปกป้องและคุ้มครองให้มีความปลอดดภัย มีความรู้สึกอบอุ่น มั่นในทั้งภายในและภายนอกสถานศึกษา และเพื่อเป็นการส่งเสริมให้สถานศึกษาสามารถดูแลช่วยเหลือผู้เรียนได้อย่างทั่วถึง และมีประสิทธิภาพ รวมทั้งมีแนวทางปฏิบัติเกี่ยวกับระบบการจัดการความปลอดภัยสำหรับสถานศึกษาที่ชัดเจน สามารถนำไปใช้ปฏิบัติได้จริง เกิดประสิทธิภาพและประสิทธิผล สามารถป้องกันความเสียหายที่อาจจะเกิดขึ้นกับผู้เรียน (สำนักอำนวยการ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน, 2556)

2.1.5.1 แนวทางหรือมาตรการรักษาความปลอดภัยสำหรับสถานศึกษา ประกอบด้วย 5 ขั้นตอน ดังนี้

2.1.5.1.1 ขั้นตอนที่ 1 การศึกษาสภาพทั่วไปของสถานศึกษา ชุมชน และความเข้มแข็งของเครือข่ายเพื่อวิเคราะห์ความเสี่ยงจากการเกิดอุบัติเหตุ อุบัติภัย และภัยที่เกิดจากสภาพแวดล้อมทางสังคม

2.1.5.1.2 ขั้นตอนที่ 2 การกำหนดมาตรการหลักเพื่อป้องกันหรือแก้ไขปัญหาที่เกิดขึ้น

2.1.5.1.3 ขั้นตอนที่ 3 การกำหนดมาตรการเสริมให้เหมาะสมกับความเชื่อวัฒนธรรมประเพฯของท้องถิ่น และสภาพความเสี่ยงของท้องถิ่น

2.1.5.1.4 ขั้นตอนที่ 4 การกำหนดกิจกรรมเพื่อสนับสนุนมาตรการหลักและมาตรการเสริม

2.1.5.1.5 ขั้นตอนที่ การกำหนดเวลาและผู้รับผิดชอบได้อย่างชัดเจนและสามารถปฏิบัติได้

2.1.4.2 แผนรักษาความปลอดภัยสำหรับสถานศึกษา

สถานศึกษาสามารถนำแนวทางและมาตรการรักษาความปลอดภัยของสถานศึกษาไปกำหนดให้เป็นแผนรักษาความปลอดภัยสำหรับสถานศึกษาได้ตามความเหมาะสมกับสถานศึกษา ด้านสภาพแวดล้อม ด้านสภาพทางภูมิศาสตร์และความต้องการของท้องถิ่น โดยอาจกำหนดรูปแบบของแผนดังนี้

2.1.5.1.6 แผนพัฒนาระบบความปลอดภัยสำหรับสถานศึกษา เป็นแผนที่ต้องมุ่งสร้างเสริมความเข้มแข็งของระบบการรักษาความปลอดภัยให้สอดคล้องกับสภาพแวดล้อมของสถานศึกษานั้น ๆ

2.1.5.1.7 มีการพัฒนาระบบรักษาความปลอดภัยสำหรับสถานศึกษาอย่างต่อเนื่องและมีประสิทธิภาพ

2.1.5.1.8 มีโครงสร้างการรักษาความปลอดภัยสำหรับสถานศึกษาที่ชัดเจน

2.1.5.1.9 มีระบบเครือข่ายเพื่อการมีส่วนร่วมในการดูแลรักษาความปลอดภัยสำหรับสถานศึกษา

2.1.5.1.10 มีระบบควบคุมภายในเกี่ยวกับการรักษาความปลอดภัยสำหรับสถานศึกษา

2.1.5.1.11 มีระบบการสื่อสารที่มีประสิทธิภาพ

2.1.5.1.12 มีแผนการป้องกันและแก้ไขอุบัติภัย ด้านสภาพแวดล้อมของสังคม ด้านสุขภาพอนามัยของ นักเรียน นักศึกษา ความปลอดภัยจากสัตว์ สัตว์ร้าย และแมลงมีพิษ และผลกระทบจากการสู้รบ และเหตุการณ์ความไม่สงบ โดยกำหนดให้ครอบคลุมทุกภัยที่อาจจะเกิดขึ้นกับนักเรียน นักศึกษา เช่น ความบกพร่องของอาคารเรียน บริเวณสถานศึกษา สภาพแวดลอมที่ไม่เอื้อต่อความมั่นคงปลอดภัย เครื่องมือเครื่องใช้ อุปกรณ์ในสถานศึกษา การเดินทางไป – กลับ ของนักเรียน นักศึกษา การพานักเรียน นักศึกษา ไปศึกษานอกสถานศึกษา และการจัดกิจกรรมการเรียนการสอน เป็นต้น

2.2 ระบบรักษาความมั่นคงปลอดภัยสูง

2.2.1 ความหมายของระบบรักษาความมั่นคงปลอดภัย

ระบบรักษาความปลอดภัยสูง (Hight Security System) เป็นระบบที่มีความสำคัญและจำเป็นต่อการดำรงชีวิตของมนุษย์ชาติในปัจจุบัน ไม่ว่าจะเป็นระบบรักษาความปลอดภัยแบบที่ใช้คน (Human Security System) ระบบรักษาความปลอดภัยแบบที่ใช้อุปกรณ์อิเล็กทรอนิกส์ (Electronic Security System) ระบบรักษาความปลอดภัยแบบที่ใช้อุปกรณ์อื่น ๆ (Mechanic Security System) และระบบรักษาความปลอดภัยบนเน็ตเวิร์ก (Network Security System) เป็นต้น และจากสถานการณ์ความไม่สงบที่เกิดขึ้น การก่อร้าย การก่ออาชญากรรรม ที่เกิดขึ้นและมีแนวโน้มเพิ่มสูงขึ้นทำให้มีความต้องการทางด้านการรักษาความปลอดภัยที่สูงขึ้นตามไปด้วย โดยมีวัตถุประสงค์หลักเพื่อการเฝ้าระวัง ปกป้องและป้องกัน เพื่อเพิ่มความปลอดภัยให้ชีวิตและทรัพย์สินขององค์กรนั้น ๆ รวมถึงเป็นการเพิ่มคุณภาพชีวิตความเป็นอยู่ให้กับผู้คนในสังคมอีกด้วย ทั้งนี้ระบบรักษาความปลอดภัยสูงที่จะทำหน้าที่เพื่อตอบสนองวัตถุประสงค์ข้างต้นได้ จะต้องประกอบไปด้วยหลาย ๆ ส่วนที่สำคัญ ได้แก่ การออกแบบระบบที่ดี มีอุปกรณ์ที่ดีพร้อมที่จะตอบสนองความต้องการและเทคโนโลยีที่ทันสมัยรวมถึงการใช้งานที่ถูกต้องได้อย่างมีประสิทธิภาพ

2.2.2 ประเภทของระบบรักษาความปลอดภัย

การรักษาความปลอดภัยแบ่งออกเป็น 3 ประเภท ดังนี้

2.2.2.1 การรักษาความปลอดภัย บุคคล/ชีวิต

การที่มนุษย์อยู่ด้วยการไม่มีความเสี่ยงหรืออันตรายที่อาจจะเกิดขึ้นให้ปลอดภัยโดยการหาวิธีการป้องกันให้ชีวิตดำรงอยู่ได้อย่างเป็นสุข

2.2.2.2 การรักษาความปลอดภัย อาคาร และสถานที่

บ้านพักที่อยู่อาศัย สำนักงาน สถานที่ราชการต่าง ๆ โรงเรียนสถานพิพิธภัณฑ์ หอประชุม โรงพยาบาล โรงแรม อาคารสถานที่เหล่านี้แต่ละแห่งมีค่าใช้จ่ายในการก่อสร้างสูง ถ้ามีการก่อการร้ายขึ้นในสถานที่เหล่านี้ ความเสียหายที่เกิดขึ้นต้องสูงอย่างแน่นอน ดังนั้นจึงควรมีการวางแผนหรือทำการป้องกันสถานที่เหล่านี้ให้ปลอดภัยจากภัย หรืออันตรายที่อาจเกิดขึ้นได้ทุกเมื่อ

2.2.2.3 การรักษาความปลอดภัย ข้อมูล ข่าวสาร เอกสาร

ทุกวันนี้ถือได้ว่าข้อมูล ข่าวสาร หรือจะเป็นเอกสารต่าง ๆ ก็มีความสำคัญต่อการดำเนินชีวิตเป็นอย่างมาก เนื่องจากข้อมูลข่าวสารที่นำมาใช้ในปัจจุบันอยู่ในรูปแบบของไฟล์ หรือ ข้อมูลดิจิทัล ที่อาจเกิดความเสียหายจากการกระทำบนเครือข่ายได้

2.2.3 ลักษณะของระบบรักษาความปลอดภัยที่ดี

2.2.3.1 มีการตรวจจับอัตโนมัติ เฝ้าระวัง ไม่ประมาท ตลอด 24 ชั่วโมง

2.2.3.2 มีระบบป้องกันหลายชั้น เช่น ทำประตูหลายชั้น ทั้งนี้ขึ้นอยู่กับอาคารสถานที่นั้น ๆ ว่าสามารถทำการแก้ไขแบบได้มากน้อยแค่ไหน, ทางเดินยาว เป็นต้น

2.2.3.3 การหน่วงเวลาผู้บุกรุก (การเตือนล่วงหน้า) ให้มีเวลาเตรียมรับมือเพื่อตอบโต้ได้เพียงพอ เช่น การทำประตูหลายชั้น หรือทางเดินยาว

2.2.3.4 การลดความเสี่ยงอันตรายของเจ้าหน้าที่รักษาความปลอดภัย และผู้ใช้อาคาร รวมถึงความเสียหายต่ออาคารสถานที่

2.2.3.5 ช่วยยับยั้ง จูงใจ ให้ละเว้น และการละมิดการทำกระทำความผิด เช่น การติดตั้งกล้องโทรทัศน์วงจรปิดหรือ CCTV ที่เปิดเผย ทำให้ผู้ที่จะกระทำความผิด ตระหนักที่จะไม่กล้าทำความผิด แต่ก็เสี่ยงต่อการถูกทำลาย ดังนั้น ควรซ่อนกล้องโทรทัศน์วงจรปิดอีก 1 กล้อง เพื่อเป็นป้องกันเหตุร้ายที่อาจจะเกิดขึ้นทำให้สมารถเห็นหน้าคนร้ายและใช้เป็นหลักฐานในการจับกุมต่อไปได้

2.2.3.6 ลดการพึ่งพาคน เช่น จากเดิมจ้างยาม 10 คน ก็อาจจะเหลือเพียง 3 คน เพื่อทำการผลัดเปลี่ยนเวรเฝ้ายามที่หน้าจอคอมพิวเตอร์

2.2.3.7 เพิ่มประสิทธิผล ซึ่งจากเดิมจ้างยาม 10 คน ก็สามารถลดการจ้างยามเหลือเพียง 3 คน โดยมีการนำระบบรักษาความปลอดภัยมาใช้ ทำให้จำนวนคนน้อยลง แต่มีประสิทธิผลเพิ่มขึ้น

2.2.4 ระบบรักษาความปลอดภัยแบบอิเล็กทรอนิกส์

ระบบรักษาความปลอดภัยแบบอิเล็กทรอนิกส์ (Electronics Security Systems) เป็นการรักษาความปลอดภัย โดยใช้เครื่องมือและอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เข้ามาช่วยปกป้อง ดูแล

สถานที่ให้ครอบคลุมพื้นที่ตลอด 24 ชั่วโมง ได้อย่างมีประสิทธิภาพสูงสุด ซึ่งจะเป็นการเน้นความรวดเร็วที่ ถูกต้อง แม่นยำและสามารถบันทึกเหตุการณ์ไว้เพื่อใช้เป็นหลักฐานประกอบการพิจารณาสืบสวน สอบสวน เมื่อเกิดเหตุฉุกเฉิน หรือมีเหตุร้ายเกิดขึ้น ซึ่งจุดเด่นนี้ได้มีการพัฒนาขีดจำกัดที่มีอยู่เดิมให้หมดไปในที่สุด สำหรับระบบรักษาความปลอดภัยแบบอิเล็กทรอนิกส์ จะประกอบด้วยระบบหลัก ๆ ดังนี้

2.2.4.1 ระบบสัญญาณเตือนภัยการบุกรุก (Intrusion Alarm System) คือระบบที่ทำหน้าที่แจ้งเตือนเมื่อมีผู้บุกรุกเข้ามาภายในบริเวณที่ได้มีการรักษาความปลอดภัย โดยการทำงานพื้นฐานนั้นจะรวมถึงสัญญาณเตือนภัยฉุกเฉิน เช่น การจี้ปล้น หรือกรณีที่น่าสงสัยอื่น ๆ เป็นต้น

2.2.4.2 ระบบสัญญาเตือนอัคคีภัย เป็นระบบเตือนภัยเมื่อมีเหตุการณ์ด้านการเกิดอัคคีภัยในบริเวณอาคารสถานที่ที่ได้มีการรักษาความปลอดภัย

2.2.4.3 ระบบกล้องโทรทัศน์วงจรปิด (Closed Circuit Television System) เป็นระบบที่ได้รับความนิยมนำมาติดตั้งใช้งานกันอย่างแพร่หลายในปัจจุบัน เพราะในสถานการณ์ปัจจุบันความปลอดภัยของชีวิตและทรัยสินเป็นสิ่งที่ผู้คนให้ความสำคัญมาก ดังนั้นการติดตั้งระบบกล้องโทรทัศน์วงจรปิด จึงช่วยเพิ่มความปลอดภัยให้กับผู้ใช้ตามมาด้วย

2.2.4.4 ระบบควบคุมการเข้า – ออกพื้นที่ (Access Control System) การใช้งานของระบบควบคุมการเข้า – ออก บริเวณพื้นที่ที่มีวัตถุประสงค์ เพื่อควบคุมการผ่านเข้า-ออกในบริเวณพื้นที่ที่จะควบคุม ทั้งส่วนของบุคคลหรือยานพาหนะใด ๆ ที่ได้รับอนุญาตให้สามารถเข้า – ออกบริเวณพื้นที่นั้น ๆ ในช่วงเวลาและวันที่กำหนดขึ้นไว้ล่วงหน้าได้

2.3 เทคโนโลยีเชื่อมโยงสรรพสิ่ง (Internet of Thing)

2.3.1 ความหมายของ Internet of Thing

เทคโนโลยีเชื่อมโยงสรรพสิ่ง (Internet of Things Technology : IoT Technology) หมายถึงเทคโนโลยีอินเทอร์เน็ตที่ถูกนำมาใช้ในการเชื่อมต่อการสื่อสารระหว่างอุปกรณ์ กับสิ่งของ (Devices and Physical Objects) (Sundmaeker, Guillemin, Friess and Woelffle, 2010) (Atzori, lera and Morabito, 2010) นอกจากนี้ กลุ่มเทคโนโลยี RFID ได้ให้คำนิยามความหมายของ IoT ว่าเป็นเครือข่ายการเชื่อมต่อของวัตถุระดับโลกที่มีความสามารถเชื่อมต่อถึงกันได้และสามารถระบุที่ของวัตถุนั้น ๆ ได้จากมาตรฐานของโพรโทคอลการเชื่อมต่อการสื่อสาร (Gubbi, Buyya, Marusic and Palaniswami, 2013) (Cardoso, Restivo, Guerra and Palma, 2017) (luo, Cheng and Ren, 2014) เช่น การใช้โทรศัพท์เคลื่อนที่ควบคุมหรือทำการสั่งการให้อุปกรณ์ต่าง ๆ ทำงานได้ ซึ่งจากระยะใกล้หรือระยะไกล โดยเชื่อมโยงและสื่อสารกันผ่านทางเครือข่ายอินเทอร์เน็ตได้ ทำให้สามารถควบคุมสิ่งของต่าง ๆ จากที่ใดก็ได้

2.3.2 แนวคิดหลักของเทคโนโลยีเชื่อมโยงสรรพสิ่ง

เทคโนโลยีเชื่อมโยงสรรพสิ่งเกิดจากแนวคิดของเทคโนโลยีที่ถูกกำหนดใช้ในการระบุสิ่งต่าง ๆ โดยอาศัยคลื่นวิทยุ (Radio Requency Identification : RFID) ที่ทำให้วัตถุทุกชนิดสามารถระบุตัวตนและระบุตำแหน่งของวัตถุหรือสิ่งของ (Things) ต่าง ๆ ได้ เครือข่าย IoT จะทำการเชื่อมต่อกับวัตถุ ต่าง ๆ ไปทั่วโลก ซึ่งสามารถระบุตำแหน่งของเฉพาะของอุปกรณ์ (Gluhak and Presser, 2009) รวมไปถึงการจัดเก็บบันทึกข้อมูลเพื่อใช้ในการแลกเปลี่ยนระหว่างอุปกรณ์เชื่อมต่อด้วยกันเอง (Sundmaeker, Guillemin, Friess and Woelffle, 2010) ทำให้วัตถุหรือสิ่งของนั้น ๆ มีความเป็นสมาร์ตและสามารถเชื่อมต่อกันได้ทั่วโลก (Haykin, 2005) ซึ่งจะขึ้นอยู่กับมาตรฐานของโพรโทคอลในการติดต่อสื่อสารระหว่างกัน นั้นหมายความว่า จะมีอุปกรณ์ ต่างชนิดกัน จำนวนมากที่มีความเกี่ยวข้อมงในกระยวนการนี้ จากแนวความคิดได้ปรับเปลี่ยนเป็นวิสัยทัศน์ที่สามารถเชื่อมโยงโลกแห่งความเป็นจริงและโลกดิจิทัลเข้าด้วยกันได้ (Gluhak and Presser, 2009) เทคโนโลยี IoT จึงเสมือนแนวคิดที่นำมาซึ่งการเปลี่ยนแปลงของนวัตกรรมทางด้านเทคโนโลยีสารสนเทศและการสื่อสารในยุคปัจจุบัน (Information Sciences Institute, 1981) (INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems in : Co-operation With The RFID Working Group of The EPOSS, 2016) (Piyare and Lee, 2013)

เทคโนโลยีเชื่อมโยงสรรพสิ่งถูกคิดค้นโดย เควิน แอชตัน (Devin Ashton) ในปี 1999 โดยได้เริ่มต้นจากการจัดตั้งศูนย์ออโต้ไอดี (Auto-ID Center) ที่สถาบันเทคโนโลยีแมสซาชูเซตส์ (Massachusettsl Institute o Technology : MIT) โดยเริ่มจากเทคโนโลยีอาร์เอฟไอดี RFID โดยการกำหนดให้เป็นอาร์เอฟไอดีเซ็นเซอร์ (RFID Sensors) ที่สามารถเชื่อมต่อกันได้อย่างเป็นมาตรฐานระดับโลก ต่อมาในยุคหลังปี 2000 ได้มีการพัฒนาอุปกรณ์อิเล็กทรอนิกส์เกิดขึ้นเป็นจำนวนมากและได้ใช้คำว่าสมาร์ต (Smart) เพิ่มขึ้น โดยมีโครงสร้างพื้นฐานที่สามารถทำการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตได้ จึงได้มีแนวคิดให้อุปกรณ์สามารถติดต่อสื่อสารกันโดยอาศัยเซ็นเซอร์ (Sensor) ในการติดต่อสื่อสาร ได้มีการระบุตัวตน และเชื่อมโยงไปยังอุปกรณ์สมาร์ต อื่น ๆ ได้ โดยให้ความหมายว่า “Internet Like” ซึ่งหมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่มีความสามารถติดต่อสื่อสารกันเองได้ (Sentell, 2014) (Veedvil Tech News and info, 2015) ซึ่งการคามดการณ์ในปี ค.ศ. 2020 นั้นสิ่งของต่าง ๆ กว่าแสนล้านชิ้นจะทำให้สามารถเชื่อมต่อระหว่างกันด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งทำให้มนุษย์รู้สึกคุ้นเคยกับเทคโนโลยีที่สามารถช่วยให้การควบคุมสิ่งของหรือวัสดุอุปกรณ์ต่าง ๆ จากที่ใดก็ได้ เช่น การควบคุมการเปิดปิดไฟฟ้า การควบคุมอุณภูมิ การควบคุมสั่งการให้เครื่องใช้ไฟฟ้าทำงาน เป็นต้น (Chuachan, Waidee and Meesiri, 2017) (Chen and Jin, 2012) เช่น ระบบเทคโนโลยีตรวจจับ หรือ เทคโนโลยเซ็นเซอร์ (Sensor Technology) มาตรฐานการเชื่อมต่อระหว่างอุปกรณ์ (Device) ระบบที่ฝั่งตัวอยู่ในคอมพิวเตอร์ เป็นต้น

การใช้งาน IoT ให้เป็นที่รู้จักอย่างกว้างขวางนั้นจำเป็นจะต้องใช้ระยะเวลา ซึ่งจะมีความเกี่ยวข้องกับการพัฒนาทางด้านเทคโนโลยีขั้นพื้นฐาน ความก้าวหน้าของเทคโนโลยีเครือข่ายไร้สายและมาตรฐานโพรโทคอล การติดตาม ของเทคโนโลยี IoT ถูกจัดให้อยู่ในกลุ่มของการวิเคราะห์และการสังเคราะห์ข้อมูลสารสนเทศ สามารถใช้เป็นประโยชน์สำหรับการติดตามพฤติกรรม รวมไปถึงการติดต่อสื่อสารกับวัตถุ (Trujillo, 2014) (Ketcham, 2016)

เทคโนโลยี IoT ได้ถูกนำไปใช้กับงานทางด้านอุตสาหกรรมที่มีการประยุกต์ใช้เพื่อช่วยสนับสนุนการดำเนินการทำงานร่วมกันระหว่างเครื่องจักร (Machine to Machine : M2M) โดยการมุ่งเน้นไปที่การบันทึกข้อมูลแบบเรียลไทม์ในโครงสร้างที่ซับซ้อน (Kanjanalap and Supaporn, 2015) (Honbo, 2013) (Holler, Tsiatsis, Mulligan, Karnouskos, Avesand and Boyle, 2014) เทคโนโลยี IoT สามารถประยุกต์ใช้ได้หลาย ๆ ด้าน เช่น โรงงานอุตสาหกรรม การแพทย์ การศึกษา การค้า และการเกษตร เป็นต้น องค์กรทั้งภาครัฐและภาคเอกชนได้มีการนำขีดความสามารถของเทคโนโลยี IoT เข้ามาช่วยในการบริหารจัดการองค์กร และพัฒนาสิ่งใหม่ ๆ ได้ (Grier, 2013)

สรุปได้ว่า Internet of Things (IoT) หรืออินเตอร์เน็ตในทุกสิ่ง หมายถึง การที่อุปกรณ์อัจฉริยะต่าง ๆ ได้ถูกนำมาเชื่อมโยงเข้าด้วยกัน ผ่านทางเครือข่ายอินเทอร์เน็ตซึ่งทำให้มนุษย์สามารถทำการสั่งการ ควบคุมการทำงาน และการใช้งานอุปกรณ์เชื่อมต่อต่าง ๆ ผ่านทาง ระบบเครือข่ายอินเทอร์เน็ตได้

2.3.3 สถาปัตยกรรมการสื่อสารผ่านอินเทอร์เน็ตสำหรับเทคโนโลยี IoT (IoT Architecture) การมีปฏิสัมพันธ์กับสภาพแวดล้อมทางกายภาพ ด้วย อุปกรณ์เชื่อมต่อกับอินเทอร์เน็ต เมื่อมีการผสมผสานระหว่าง Web Sensors และกรอบการสื่อสารของเทคโนโลยี IoT จึงเป็นสิ่งที่สามารถนำไปสู่การประยุกต์ใช้งานในรูปแบบต่าง ๆ ดังนี้ (D. Molloy,2015)

2.3.3.1 The BBB Web Server : สถาปัตยกรรมในรูปแบบที่ BBB (Beaglebone Black) เป็นการเชื่อมต่อระหว่างเซนเซอร์และ การทำงานเป็นแบบเว็บเซิร์ฟเวอร์ ซึ่งสามารถนำมาใช้เพื่อนำเสนอ ข้อมูลไปยังเว็บเมื่อมีการร้องขอโดยเว็บเบราว์เซอร์ ซึ่งการสื่อสารนี้เกิดขึ้นได้โดยใช้ Hypertext Transfer Protocol (HTTP)

2.3.3.2 The BBB Client : สถาปัตยกรรมในรูปแบบที่ BBB สามารถดำเนินการเริ่มต้นติดต่อกับเว็บเซิร์ฟเวอร์โดยทำการร้องขอ HTTP ในการรับส่งข้อมูล โดยมีการใช้โปรแกรม ภาษา C/C++ และใช้ TCP และ TCP sockets ในการสร้างเว็บเบราว์เซอร์ขั้นพื้นฐานที่จะสามารถสื่อสารผ่าน HTTP หรือ HTTPs เพื่อเพิ่มความปลอดภัยได้

2.3.3.3 The BBB TCP Client/Server : สถาปัตยกรรมในรูปแบบที่ได้มีการกำหนดให้มีการร้องขอระหว่าง Client กับ Server ด้วยความเร็วสูง ผ่าน TCP

2.3.3.4 The BBB Web Sensor Using a PaaS : สถาปัตยกรรมในรูปแบบที่ได้กำหนดรหัสซึ่งถูกเขียนขึ้นเพื่อเปิดใช้งาน BBB โดยใช้ HTTP และ APIs เพื่อทำการส่งและรับข้อมูลจากเว็บเซิร์ฟเวอร์ โดยมีการสร้างอาร์เรย์ขนาดใหญ่ของเซนเซอร์ที่จะทำให้สามารถสื่อสารและเก็บข้อมูลบนเซิร์ฟเวอร์ระยะไกลได้และเก็บบันทึกข้อมูลไว้ได้

2.3.4 องค์ประกอบของเทคโนโลยี IoT จากคำว่าเทคโนโลยีเชื่อมโยงสรรพสิ่ง ซึ่งแสดงให้เห็นถึงการ เชื่อมต่อระหว่างสรรพสิ่งที่สามารถจับต้องได้ ให้เกิดการสื่อสารระหว่างกันได้ผ่านเครือข่ายอินเทอร์เน็ต ดังนั้นจึงจำเป็นต้องมี การกล่าวถึงการเชื่อมต่อเพื่อเป็นช่องทางในการสื่อสารกันระหว่างสรรพสิ่ง ซึ่งประกอบไปด้วย 2 วิธีการ ดังนี้ (Want, Roy; Bill N. Schilit, Scott Jenson, 2015)

2.3.4.1 Cloud Service : เป็นการปฏิสัมพันธ์โดยตรงในรูปแบบ การเชื่อมต่อกันแบบ peer-to-peer protocols เช่น Bluetooth หรือ Wi-Fi และ เชื่อมโยงแบบ Internet protocols เช่น HTTP และ TCP

2.3.4.2 Proxy Web Service : เป็นการปฏิสัมพันธ์ผ่าน Proxy ในรูปแบบการปฏิสัมพันธ์แบบนี้จะเกิดขึ้นก็ต่อเมื่ออุปกรณ์รับข้อมูล เช่น smartphone อยู่ในระยะใกล้กับอุปกรณ์ที่เปิดใช้งานใน รูปแบบของเทคโนโลยี IoT และสามารถค้นหาข้อมูลเพิ่มเติมเกี่ยวกับสิ่งที่ สนใจผ่านเว็บไซต์ได้อย่างอัตโนมัติ โดยมีองค์ประกอบย่อย 6 ส่วน ดังนี้ (Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, 2015)

2.3.4.2.1 Identification เป็นการกำหนดรหัส (Code) เพื่อใช้สำหรับระบุตัวตน ซึ่งเป็นส่วนสำคัญสำหรับเทคโนโลยี IoT เพื่อให้ตรงตามความต้องการในการรับบริการ ในการระบุชื่อเพื่อกำหนดตัวตน สำหรับเทคโนโลยี IoT มีหลากหลายวิธี เช่น รหัสสินค้าอิเล็กทรอนิกส์ (EPC) และ รหัสแพร่หลาย (uCode) ซึ่งเป็นการใช้ IP เป็นส่วน กำหนด โดยในปัจจุบันได้มีการนำ IPv.6 เข้ามาใช้งาน เพื่อให้เกิด ความเพียงพอต่ออุปกรณ์ที่มีแนวโน้มในการขยายตัวเพิ่มขึ้นในอนาคตอย่างรวดเร็ว

2.3.4.2.2 Sensing เป็นการรวบรวมข้อมูลจากวัตถุที่เกี่ยวข้อง ภายในเครือข่ายและการส่งค่ากลับไปที่คลังข้อมูล ฐานข้อมูล หรือระบบคลาวด์ ข้อมูลที่มีการเก็บรวบรวมวิเคราะห์ดำเนินการ บางอย่างขึ้นอยู่กับการให้บริการที่จำเป็น เช่น Arduino Yun, Raspberry PI, BeagleBoneBlack เป็นต้น

2.3.4.2.3 Communication เป็นเทคโนโลยีการสื่อสารเทคโนโลยี IoT เพื่อทำการเชื่อมต่อวัตถุที่แตกต่างกันเพื่อให้บริการที่เฉพาะเจาะจง โดย ปกติโหนด เทคโนโลยี IoT มีการทำงานโดยใช้พลังงานต่ำ เช่น โปรโตคอลการสื่อสารที่ใช้สำหรับ เทคโนโลยี IoT ประกอบด้วย WiFi, Bluetooth, IEEE 802.15.4, Z-wave, และ LTEAdvanced นอกจากนี้ยังมีเทคโนโลยีบางส่วนที่มีรูปแบบการสื่อสารเฉพาะ เช่น RFID และ Near Field Communication (NFC) เป็นต้น

2.3.4.2.4 Computation หน่วยประมวลผลและการ ประยุกต์ใช้ซอฟแวร์เป็นตัวแทนของ "สมอง" และ ความสามารถในการคำนวณของ เทคโนโลยี IoT แพลตฟอร์ม ฮาร์ดแวร์ต่าง ๆ ถูกพัฒนาขึ้นเพื่อใช้งาน เทคโนโลยีIoT เช่น Arduino,UDOO, FriendlyARM, Intel Galileo, Raspberry PI, Gadgeteer,BeagleBone, Cubieboard, Z1, WiSense, Mulle, และ T-Mote Sky. แพลตฟอร์มคลาวด์เป็นรูปแบบการประมวลผลอีกส่วนหนึ่งที่มีความสำคัญของ เทคโนโลยี IoT แพลตฟอร์มเหล่านี้ได้มีสิ่งอำนวยความ สะดวกสำหรับ Smart Objects ที่จะส่งข้อมูลไปยังคลาวด์ โดยข้อมูลขนาดใหญ่ที่ต้องดำเนินการในเวลาจริง และผู้ใช้ จะต้องได้รับประโยชน์จากองค์ความรู้ที่ได้สกับออกมาจากข้อมูลที่มีจำนวนมากหรือ

2.3.4.2.5 Services โดยภาพรวม บริการเทคโนโลยี IoT สามารถแบ่ง ออกเป็น 4 Classes คือ 1) Identity-related Services บริการขั้นพื้นฐานที่สำคัญที่สุดที่ใช้ในประเภทอื่น ๆ ของการบริการ แอพลิเคชัน ที่ต้องการที่จะระบุตัวตนของวัตถุต่าง ๆ เพื่อสามารถนำเข้าสู่โลกแห่งความ จริงกับโลกเสมือน 2) Information Aggregation Services บริการที่ทำการรวบรวมและสรุปการวัดค่าการรับรู้ที่จะต้องมีการประมวลผล และสามารถทำการรายงานไปยังโปรแกรมประยุกต์เทคโนโลยี IoT 3) Collaborative-Aware Services ทำหน้าที่ด้าน บริการการรวมข้อมูล และใช้ข้อมูลที่ได้รับการตัดสินใจ และ ตอบสนองตาม 4) Ubiquitous Services การเปิดให้มีการบริการที่แพร่แพร่หลาย แต่มีจุดมุ่งหมายในการให้บริการความร่วมมือ ระหว่างอุปกรณ์ที่สามารถเข้าถึงได้ทุกที่ทุกเวลาตามต้องการ

2.3.4.2.6 Schematics หมายถึงความสามารถในการดึง ความรู้ได้อย่างชาญฉลาด โดยการสกัดความรู้จากอุปกรณ์ที่มีความ แตกต่างกัน รวมถึงการค้นพบและการใช้ทรัพยากร และการสร้างแบบจำลองข้อมูล นอกจากนี้ยังสาไม่รวมถึงการรับรู้และการวิเคราะห์ข้อมูลเพื่อให้เกิดความรู้สึกของการตัดสินใจที่เหมาะสมพร้อมที่จะให้บริการที่แน่นอนที่ ซึ่งจะให้บริการที่แน่นอน อาจหมายถึงสมองของเทคโนโลยี IoT ก็ได้ โดย การส่งข้อเรียกร้องไปยังทรัพยากรที่เหมาะสม ข้อกำหนดนี้ ได้รับการสนับสนุนโดยเทคโนโลยี Web Ontology เช่น Resource Description Framework (RDF) และthe Web Ontology Language (OWL)

จากองค์ประกอบหลักที่สำคัญของ เทคโนโลลี IoT สามารถสรุปได้ว่า การนำองค์ความรู้ที่ได้จากการรับรู้สภายแวดล้อมต่าง ๆ โดยผ่านทางอุปกรณ์ตรวจจับ ซึ่งเป็นหัวใจสำคัญของกระบวนการทำงานที่เกี่ยวข้องกับเทคโนโลยี IoT โดยเป็นการสกัดองค์ความรู้ที่เกิดขึ้นจากข้อมูลจำนวนมหาศาลเข้าสู่การแสดงผลลัพธ์ทางการดำเนินการในส่วนที่เกี่ยวข้องได้

2.4 เทคโนโลยีการประมาลผลภาพ (Image Processing)

การประมวลผลภาพ (Image Processing) หมายถึง การนำภาพถ่ายเข้ามาคำนวณและทำการประมวลผลด้วยเทคโนโลยีคอมพิวเตอร์ เพื่อให้ได้ข้อมูลที่เราต้องการหรือสนใจทั้งในส่วนของข้อมูลเชิงคุณภาพและข้อมูลเชิงปริมาณ โดยมีขั้นตอนหลายขั้นตอนที่สำคัญ เช่น การปรับให้ภาพมีคุณภาพที่ดีขึ้น การกำจัดสัญญาณรบกวนของภาพ การแบ่งสัดส่วนของวัตถุที่เราสนใจออกมาจากภาพ เพื่อที่จะทำการนำภาพวัตถุที่ได้ไปทำการวิเคราะห์หาข้อมูลเชิงปริมาณ เช่น ขนาดรูปร่างและทิศทางการเคลื่อนที่ของวัตถุในภาพ จากนั้นเราสามารถนำข้อมูลเชิงปริมาณเหล่านี้ไปวิเคราะห์และสร้างเป็นระบบขึ้นมา เพื่อใช้ประโยชน์ในงานด้านอื่น ๆ เช่น งานด้านการแพทย์งานด้านเทคโนโลยีทางด้านการเกษตร งานด้านอุตสาหกรรม เป็นต้น ซึ่งการประมวลผลภาพที่อยู่ในรูปแบบดิจิทัล (ภาพดิจิทัล) ภาพในที่นี้ รวมความหมายถึง สัญญาณดิจิทัลใน 2 มิติอื่น ๆ โดยทั่วไปคำนี้เมื่อใช้อย่างกว้าง ๆ จะครอบคลุมถึงสัญญาณวีดิโอ (Video) หรือภาพเคลื่อนไหว ซึ่งจะเป็นชุดของภาพนิ่ง เรียกว่า เฟรม (Frame) หลาย ๆ ภาพต่อกันไป ตามเวลา ซึ่งก็คือสัญญาณ 3 มิติ เมื่อนับเวลาเป็นมิติที่ 3 หรืออาจจะครอบคลุมถึงสัญญาณ 3 มิติ อื่น ๆ เช่น ภาพ 3 มิติทางการแพทย์ เป็นต้น

การประมวลผล (Image Processing) เป็นกระบวนการประมวลผลและการวิเคราะห์ภาพดิจิตอล ซึ่งการมองเห็นของมนุษย์มีกลไกของการรับภาพที่มีความสลับซับซ้อน เพื่อนำภาพที่มองเห็นมาเป็นข้อมูลสำหรับใช้ในการดำรงชีวิต เช่น การจดจำวัตถุ หรือใช้เป็นข้อมูลสำหรับงานที่มีความสลับซับซ้อน เช่น การวางแผน การตัดสินใจ การพัฒนาทางด้านความคิด และการค้นคว้าทางวิทยาศาสตร์ ทำให้มีการศึกษาและพัฒนาขบวนการที่พยายามเลียนแบบความสามารถในการมองเห็นของมนุษย์โดยใช้ความสามารถและเทคโนโลยีทางด้านดิจิตอลคอมพิวเตอร์ในการจัดการกับข้อมูลที่มีความเกี่ยวข้องกับการมองเห็นหรือข้อมูลภาพ ซึ่งการศึกษาและพัฒนานี้มีชื่อเรียกว่า การ ประมวลผลภาพดิจิตอล (Digital Image Processing) ซึ่งงานทางด้านการประมวลผลภาพมีการพัฒนาอย่างต่อเนื่อง และได้มีการนำไปใช้กันอย่างกว้างขวางสำหรับงานในหลาย ๆ ด้าน เช่น งานด้านการสื่อสารโทรคมนาคม ด้านการสื่อสารทางโทรทัศน์ งานด้านการแพทย์ งานด้านกราฟิก งานด้านการพิมพ์ งานด้านการค้นคว้าทางวิทยาศาสตร์ และในงานด้านอุตสาหกรรม

การประมวลภาพดิจิตอลเป็นกระบวนการแปลงข้อมูลภาพให้อยู่ในรูปแบบของข้อมูลดิจิตอล (Digital Format) ซึ่งสามารถนำเอาข้อมูลดังกล่าวผ่านกระบวนการต่าง ๆ ด้วยดิจิตอลคอมพิวเตอร์ อินพุตและเอาท์พุตของกระบวนการระบบซึ่งจะอยู่ในรูปแบบดิจิตอล การวิเคราะห์ภาพดิจิตอล (Digital Image Analysis) เป็น วิธีการอธิบายและการรู้จำข้อมูลภาพดิจิตอล โดยมีอินพุตของระบบเป็นข้อมูลภาพดิจิตอล และมีเอาท์พุตของระบบจะเป็นเครื่องหมายหรือความหมายที่ใช้แทนข้อมูลภาพดิจิตอลเหล่านั้น ซึ่งในการวิเคราะห์ภาพมีอยู่หลายวิธีด้วยกันที่ได้นำแนวความคิดมาจากการทำงานของอวัยวะดวงตาของมนุษย์ (Human Vision) เช่น

งานทางด้านคอมพิวเตอร์วิชั่น (Computer Vision) คือ การมองเห็นของมนุษย์นับว่าเป็นกระบวนการที่ซับซ้อนทางเทคนิค ทำให้กระบวนการของการประมวลผลภาพมีความซับซ้อน

งานทางด้านอุตสาหกรรม ได้แก่ กระบวนการผลิตที่มีความต้องการแรงงานที่ใช้ในส่วนของงานทางด้านการตรวจสอบ เพื่อดำเนินการตัดสินใจอย่างใดอย่างหนึ่ง แต่เนื่องจากข้อจำกัดทางด้านประสิทธิภาพของมนุษย์ ในเรื่องของความอ่อนล้า ความสม่ำเสมอ ทักษะความสามารถ ความเป็นมาตรฐานเดียวกัน และ อื่น ๆ จากหลายปัจจัยอื่น ที่อาจก่อให้เกิดปัญหาในเรื่องของประสิทธิภาพและคุณภาพในกระบวนการผลิต จึงได้มีความพยายามในการนำเอาเทคโนโลยีการประมวลผลและการวิเคราะห์ภาพมาประยุกต์ใช้ในการะบวนการทำงาน เพื่อเพิ่ม ประสิทธิภาพ และลดความผิดพลาดในกระบวนการผลิต หนึ่งในเทคโนโลยีนี้ก็คือ เครื่องจักรเกี่ยวกับ ภาพ หรือ แมชชีนวิชั่น (Machine Vision) (Pietikainen, M. and L. F. Pau.,1996) ซึ่งเทคโนโลยีดังกล่าวเป็นที่สนใจในกลุ่มของผู้ค้นคว้าและทำการวิจัย ทำให้มีการนำแนวคิดใหม่ ๆ ถูกนำไปใช้ในงานอุตสาหกรรม งานวิจัยหลายงานได้ถูกนำไปใช้กับ เครื่องจักรและกระบวนการควบคุมการผลิต เช่น กระบวนการควบคุมคุณภาพของการพิมพ์ (Print Quality Management) กระบวนการรู้จำรูปแบบ (Pattern Recognition) หุ่นยนต์ที่ใช้วิชั่นแบบสามมิติ (Robot Vision Concentrates on 3D) และกระบวนการตรวจสอบแบบสองมิติและสามมิติ (2D/3D Inspection)

กระบวนการพื้นฐานของการประมวลผลภาพดิจิตอลแบ่งได้เป็น 3 ระดับ คือ

1. กระบวนการประมวลผลระดับล่าง (Low Level Processing) เป็นกระบวนการจัดการภาพแบบดิจิตอล ก่อนการการประมวลผลภาพดิจิตอล โดยเริ่มด้วยขั้นตอนการได้มาซึ่งภาพดิจิตอล (Image Acquisition) จากอุปกรณ์อิเล็กทรอนิกส์ เซ็นเซอร์ จากนั้นดำเนินการเป็นไปตามขั้นตอนก่อนการประมวลผล (Pre Processing) ซึ่งหัวใจสำคัญของขั้นตอนนี้ คือการใช้เทคนิคเพื่อเพิ่มคุณภาพให้กับภาพ (Image Enhancement)

2. กระบวนการประมวลผลระดับกลาง (Intermediate Level Processing) เป็นกระบวนการขั้นตอนของการแยกข้อมูลภาพออกเป็นส่วน ๆ (Segmentation) โดยการแยกวัตถุ (Object) หรือบริเวณที่สนใจ (Region) ออกจากพื้นหลัง (Background) เพื่อเป็นตัวแทนและบรรยายข้อมูลของภาพที่ได้จากการแยกข้อมูลภาพออกมาเป็นส่วน ๆ (Representation and Description)

3. กระบวนการประมวลผลระดับสูง (High Level Processing) เป็นกระบวนการของการรู้จำภาพและแปลความหมาย (Recognition and Interpretation) ของสิ่งที่เราสนใจจากภาพ ซึ่งจะถือว่าเป็นส่วนหนึ่งของการวิเคราะห์ภาพดิจิตอล (Digital Image Analysis) โดยใช้ฐานความรู้ (Knowledge Base) เป็นแกนกลางในการรวบรวมข้อมูลจากองค์ความรู้พร้อมทั้งมีการกำหนดขอบเขตของปัญหาที่ กำลังสนใจนั้น ๆ เพื่อให้ได้ผลลัพธ์ตามวัตถุประสงค์ (Gonzalez, R. C. and R. E. Woods., 2002.)

2.5 หลักฐานดิจิทัล (Digital Forensic)

2.5.1 ความรู้เบื้องต้นเกี่ยวกับ Digital Forensic

ปัจจุบัน อุปกรณ์อิเล็กทรอนิกส์ หรืออุปกรณ์ดิจิทัลต่าง ๆ มีความจำเป็นต่อการดำรงชีวิตของคนในสมัยนี้เป็นอย่างมากโดยอาจเรียกได้ว่าเป็นส่วนหนึ่งของชีวิตประจำวันของมนุษย์ก็เป็นได้ และอุปกรณ์ดิจิทัลเหล่านี้ อาจเป็นส่วนหนึ่งของคดีความที่เกิดขึ้นเป็นจำนวนมาก โดยเจ้าหน้าที่ตำรวจต้องทำการตรวจค้นหาพยานหลักฐาน เพื่อสืบหาตัวผู้กระทำความผิด ที่เรียกว่า พยานหลักฐานทางดิจิทัล (Digital Evidence) โดยกระบวนการที่เรียกว่า Digital Forensics

การพิสูจน์หลักฐานจากอุปกรณ์หรือข้อมูลทางดิจิทัล คือการเก็บรวบรวมและการจัดเตรียมข้อมูลที่เกี่ยวข้องจากเครื่องคอมพิวเตอร์เพื่อดำเนินคดีในทางกฎหมาย หรือ การวิเคราะห์พิสูจน์หลักฐานจากคอมพิวเตอร์ เป็นกระบวนการของการได้มาซึ่งหลักฐานจากสื่ออิเล็กทรอนิกส์คอมพิวเตอร์และการรักษาหลักฐาน ซึ่งกระบวนการนี้อาจรวมถึง การกู้คืนไฟล์ที่ถูกลบ เช่น เอกสาร กราฟฟิกและภาพถ่าย ไฟล์ที่ซ่อนอยู่ ที่ไม่สามารถมองเห็นได้โดยทั่วไป ซึ่งจำเป็นต้องใช้เทคนิคในการทำ Computer Forensics เท่านั้นจึงจะสามารถมองเห็นได้ การวิเคราะห์ไฟล์ในระบบคอมพิวเตอร์เพื่ออธิบายถึงการเกิดเหตุการณ์อะไรขึ้นกับระบบคอมพิวเตอร์ กระบวนการทำงานของคอมพิวเตอร์ที่ไม่สามารถมองเห็นได้ ซึ่งกระบวนการเหล่านี้มักเป็นกระบวนการที่ไม่ได้เป็นผลดีกับคอมพิวเตอร์ เช่น การ ทำงานของ Malware เพื่อให้ผลการตรวจพิสูจน์ดังกล่าวมีความถูกต้อง น่าเชื่อถือและเป็นที่ยอมรับในชั้นศาลได้นั้น จะต้องทำการดำเนินการตามกระบวนการของการตรวจพิสูจน์และจะต้องเป็นไปตามหลักการมาตรฐานที่ได้รับการยอมรับ มาตรฐาน พื้นฐานของกระบวนการทั้งหมดที่เกี่ยวข้องกับการพิสูจน์พยานหลักฐานทางดิจิทัล ประกอบด้วย (Casey E., 2011)

1. การรวบรวมพยานหลักฐาน
2. การเก็บรักษาพยานหลักฐาน
3. การวิเคราะห์หลักฐาน
4. การนำเสนอผลต่อศาล

โดยทั้ง 4 ขั้นตอนดังกล่าว มีความสำคัญมาก เนื่องจากหลักฐานทางดิจิทัลนั้นอ่อนไหวมาก เพียงแค่ยึดคอมพิวเตอร์ ไป แล้วเจ้าหน้าที่ไม่ทำการสำเนาข้อมูล แต่เปิดคอมที่ยึดนั้นโดยตรงในระหว่างสอบสวน จำเลยก็สามารถทำการโต้แย้งได้เพราะทุกครั้งที่เปิดคอมพิวเตอร์จะกระทบต่อการกระบวนการจัดเก็บข้อมูลภายในไม่มากก็น้อย ซึ่งในต่างประเทศนั้นการต่อสู้ของคดีดิจิทัลนั้นให้น้ำหนักสำคัญใน 3 สิ่ง คือ

1. ความแท้จริงของข้อมูลโดยที่ข้อมูลจะไม่มีการแก้ไขเปลี่ยนแปลงหรือได้รับความเสียหาย ซึ่งก็อาศัยการสืบจากมาตรฐานขั้นต่ำในกระบวนการการจัดการหลักฐานทางดิจิทัลที่เกิดขึ้นระหว่างการสืบสวนสอบสวนของตำรวจ

2. ความน่าเชื่อถือของโปรแกรมหรือซอฟต์แวร์ที่นำมาใช้ในการวิเคราะห์หลักฐาน

3. ตัวผู้เชี่ยวชาญด้านกระบวนการพิสูจน์หลักฐานที่ต้องผ่านการอบรมด้านนี้โดยเฉพาะ ซึ่งจะต้องมีความรู้ความสามารถในการปฏิบัติงาน มีความสามารถในการวิเคราะห์ข้อมูล เข้าใจถึงระบบการทำงานของระบบปฏิบัติการและเครื่องมือที่ใช้ในการวิเคราะห์

นอกจากปัจจัยข้างต้นดังกล่าวแล้ว หัวใจสำคัญที่จะทำให้ผลการตรวจพิสูจน์ได้รับการยอมรับในชั้นศาล โดยไม่ถูกโต้แย้ง คือ จะต้องสามารถยืนยันได้ว่าหลักฐานที่ได้นำมาตรวจสอบ นั้นเป็นหลักฐานชิ้นเดียวกันกับที่เก็บมาจากสถานที่เกิดเหตุจริง (Authentication) และไม่มีการเปลี่ยนแปลงข้อมูลใด ๆ ไปจากเดิม (Integrity) ซึ่งในการที่จะยืนยันคุณสมบัติทั้งสองข้อนี้ได้นั้น จำเป็นจะต้องอาศัยหลักการสำคัญของการตรวจพิสูจน์พยานหลักฐานดิจิทัลคือ

1. Chain of Custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน” หมายถึง ข้อมูลที่จะต้องมีการระบุรายละเอียด ของพยานหลักฐานและการส่งต่อพยานหลักฐานโดยเจ้าหน้าที่ที่ได้มีการรับผิดชอบ ซึ่งจะต้องทำการบันทึกไว้เริ่มตั้งแต่ เมื่อพยานหลักฐานชิ้นนั้นถูกจัดเก็บมาจากที่เกิดเหตุแล้วมาอยู่ในความครอบครองของเจ้าหน้าที่ที่เกี่ยวข้อง จนกระทั่งเมื่อ สิ้นสุดคดี โดยจะต้องทำการระบุ ชื่อ ตำแหน่ง หน่วยงาน วัน และ เวลา ไว้ในแบบฟอร์ม Chain of Custody ซึ่งจะเป็นประโยชน์หากผู้ที่เกี่ยวข้องต้องไปให้การในชั้นศาล โดยจะต้องสามารถยืนยันได้ว่า ในระหว่างการครอบครองพยานหลักฐานชิ้นนั้นได้มีการจัดเก็บไว้ที่ไหน และได้ถูกนำไปทำอะไรบ้าง โดยมีปัจจัยที่จะทำให้พยานหลักฐาน เปลี่ยนแปลงหรือไม่ ได้ส่งต่อให้กับบุคคลอื่นหรือไม่ เมื่อวันและเวลาใด และทุกครั้งที่มีการเปลี่ยนผู้ครอบครองวัตถุ พยาน จะต้องทำการบันทึกไว้ในแบบฟอร์มดังกล่าวด้วย

2. Hash Value เป็นผลลัพธ์จากการนำข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์ (จะเป็นฮาร์ดดิสก์ทั้งลูกหรือไฟล์ชนิดหรือขนาดใดก็ได้) มาผ่านกระบวนการย่อย (Digest) หรือกระบวนการคำนวณด้วย Hash Function เรียกกระบวนการนี้ว่า Hashing โดยผลลัพธ์นี้จะเป็นข้อมูลค่าเฉพาะ หากข้อมูลที่มีเหมือนกันทุกประการได้ผ่านกระบวนการย่อย ผลลัพธ์ที่ได้จะ เหมือนกันทุกครั้ง แต่ถ้าหากข้อมูลที่นำมาย่อยมีความแตกต่างกันแม้เพียงบิตเดียว ผลลัพธ์ที่ได้ก็จะต่างกันทันที ซึ่ง Hashing จะคำนวณจากข้อมูลที่อยู่ในไฟล์เท่านั้น ไม่รวมกับ Metadata ซึ่งได้แก่ ชื่อไฟล์ วันเวลาที่ ไฟล์ถูกสร้าง เปลี่ยนแปลง/เข้าถึงครั้งสุดท้าย เป็นต้น (ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน))

2.6 งานวิจัยที่เกี่ยวข้อง

Xu Xingmei, Zhou Jing, Wang He. (2013) ได้นำเสนอ งานวิจัยเกี่ยวกับลักษณะพื้นฐาน, เทคโนโลยีที่สำคัญ, สถาปัตยกรรมเครือข่ายและปัญหาในการรักษาความปลอดภัยของ Internet of Things ว่าเป็นเทคโนโลยีที่กำลังได้รับความสนใจทั้งในประเทศ ต่างประเทศ รวมถึงผู้เชี่ยวชาญ นักวิชาการ และหน่วยงานรัฐบาล โดยบทความนี้แนะนำลักษณะพื้นฐาน เทคโนโลยีที่สำคัญ สถาปัตยกรรมเครือข่ายและปัญหาในการรักษาความปลอดภัยของ Internet of Things ที่เห็นได้เน้นชัด ได้แก่ ลักษณะของการรับรู้โดยรวมที่เชื่อถือได้ การประมวลผลอัจฉริยะ เทคโนโลยีที่สำคัญรวมถึงวิทยุระบุความถี่เทคโนโลยี (RFID) เทคโนโลยีเซ็นเซอร์ เทคโนโลยีการสื่อสารเครือข่ายระบบฝังตัว เทคโนโลยี ฯลฯ สถาปัตยกรรมเครือข่ายของ Internet of Things ที่จะแบ่งออกเป็นชั้น ๆ โดยจะมีการตรวจวัดชั้นของการขนส่งและการประยุกต์ใช้ชั้น และตอนท้ายของบทความนี้นำเสนอวิธีการแก้ปัญหาการรักษาความปลอดภัยของ Internet of Things

Jeannette and Vic (2013) ได้นำเสนองานวิจัย เรื่อง การศึกษา Living Labs โดยใช้ Internet of Things เป็นพื้นฐานการสอนและการวิจัย โดยบทความนี้จะมีการแนะนำการเรียนการสอนของนักศึกษาวิทยาการคอมพิวเตอร์ โดยการเรียนแบบผสมผสานจาก การเขียนโปรแกรมแบบ PiP (Pervasive Interactive Programming), Internet of Things, The iCampus, Living Labs and รูปแบบที่เรียกว่า "Smart-Box" สำหรับโครงสร้างพื้นฐานนี้จะทำหน้าที่เป็นแพลตฟอร์มการเรียนการสอน สำหรับตัวอย่างที่จะใช้อธิบายนี้เป็นการรวมกรอบแนวคิดที่เรียกว่า "“The Cloud of Things” (CoT)" วัตถุประสงค์ที่ตั้งไว้สำหรับงานนี้ คือ สามารถใช้ประโยชน์จาก Internet of Things, ทำตามแนวคิด Living Labs และ ตามวิสัยทัศน์ของ iCampus ที่จะใช้รูปแบบที่เรียกว่า "Smart-Box" และ การเขียนโปรแกรมแบบ PiP (Pervasive interactive Programming) ผลการวิจัยนี้ ได้นำมาใช้เพื่อสภาพแวดล้อมการของการศึกษาที่ดีขึ้น เป็นการสร้างแรงจูงใจสูงและเพิ่มประสิทธิภาพในการเรียนรู้ และยังแสดงให้เห็นถึงการทำงาน โดยการอธิบายการประยุกต์ใช้ความคิดเหล่านี้ ไปเป็นองค์กรที่เป็นบริษัท ร่วมทุนที่แท้จริงของโลก, ฮาร์โลว์ UTC (ในสหราชอาณาจักร) จุดสนใจหลักของงานวิจัยนี้ จะเกี่ยวข้องกับการใช้ PiP ร่วมกับ Internet of Things เพื่อที่จะสอนทักษะการเขียนโปรแกรมระดับประถมศึกษาโดยงานนี้ได้นำเสนอผลการประเมินของ PiP จากผู้เข้าร่วม (นักศึกษาและบุคลกร) จำนวน 18 คน ที่มีอายุและเพศที่แตกต่างกัน

Alessio, et al. (2016) ได้ทำงานวิจัย เรื่อง การสำรวจการบูรณาการระหว่าง Cloud Computing และ Internet of Things โดยสรุปได้ ดังนี้ Cloud Computing และ Internet of Things (IoT) เป็น 2 เทคโนโลยีที่แตกต่างกันมาก ซึ่งปัจจุบันก็มียอมรับและใช้งานเพิ่มมากขึ้นอย่างแพร่หลาย ทำให้มีความสำคัญสำหรับที่จะใช้เป็นองค์ประกอบของอินเทอร์เน็ตในอนาคต โดยต้องรวม Cloud และ IoT เข้าไว้ด้วยกัน ในงานวิจัยนี้ มุ่งเน้นความสนใจ Cloud และ IoT ซึ่งเป็น

สิ่งที่เราเรียกว่า กระบวนทัศน์ "CloudIoT" หลายชิ้นงานที่ผ่านมา ส่วนใหญ่ จะทำการสำรวจแบบแยกส่วน ระหว่าง Cloud และ IoT ออกจากกัน ทำให้เห็นคุณสมบัติพื้นฐาน เทคโนโลยี และสิ่งต่าง ๆ ชัดเจนขึ้น แต่ชิ้นงานส่นใหญ่ยังขาดการวิเคราะห์ในรายละเอียดของกระบวนทัศน์ใหม่แบบ CloudIoT ซึ่งเป็นสิ่งใหม่ รูปแบบการใช้งานที่ท้าทายและปัญหาการวิจัยนี้ ก็เพื่อลดช่องว่างนี้ ในบทความนี้ มีการสำรวจหนังสือที่เกี่ยวกับการรวมของ Cloud และ IoT เริ่มต้นโดยการวิเคราะห์พื้นฐานของทั้ง IoT และ Cloud ซึ่งจะต้องศึกษาเพิ่มเติมในส่วน Complementarity เพื่อบูรณาการ รวมถึงการยอมรับของกระบวนทัศน์ CloudIoT จำนวนการใช้งานและวันที่ของการใช้งาน CloudIoT จากข้อมูลเอกสารที่เกี่ยวข้องมีความสำคัญ เพราะ จะทำให้เกิดความท้าทายในการวิเคราะห์ถึงรายละเอียดต่าง ๆ การดำเนินกระบวนทัศน์ CloudIoT และทิศทางในอนาคต

2.7 สรุปเอกสารและงานวิจัยที่เกี่ยวข้อง

จากการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ พบว่า การรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาให้เกิดประสิทธิภาพนั้น มีหลายปัจจัยที่นำมาใช้ในการบูรณาการเพื่อให้เกิดความเหมาะสมกับสถานศึกษา สามารถแบ่งออกเป็น 3 ส่วน (1) การรักษาความปลอดภัยเกี่ยวกับบุคคล (2) การรักษาความปลอดภัยเกี่ยวกับสถานที่ (3) การป้องกันและแก้ไขปัญหาด้านความไม่สงบ ซึ่งมีความเกี่ยวข้องกับกระบวนการรักษาความมั่นคงปลอดภัย ซึ่งแบ่งออกเป็น 4 ระบบ คือ 1) ระบบยืนยันตัวตน 2) ระบบควบคุมการเข้า – ออกยานพาหนะ 3) ระบบตรวจจับและแจ้งเตือนภัยภายในอาคาร และ 4) ระบบฐานข้อมูลด้านความมั่นคง ในส่วนของเทคโนโลยีเชื่อมโยงใช้การตรวจจับด้วย กล้องตรวจจับ เซนเซอร์ และ บัตรอาร์เอฟไอดี โดยใช้กับโมดูลทั้ง 7 ส่วน ได้แก่ 1) โมดูลตรวจจับใบหน้า 2) โมดูลสแกนบัตร 3) โมดูลตรวจจับทะเบียนรถ 4) โมดูลตรวจจับควันไฟ 5) โมดูลตรวจจับความร้อน 6) โมดูลตรวจจับก๊าซ7) โมดูลตรวจจับแรงสั่นสะเทือน ซึ่งสารสนเทศที่ได้จากโมดูลทั้ง 7 จะอยู่ในรูปแบบของข้อมูลอิเล็คทรอนิกส์หรือหลักฐานดิจิทัล (Digital Forensic) ที่ประกอบด้วย 3 ส่วน คือ 1) การรวบรวมพยานหลักฐาน 2) การวิเคราะห์เพื่อประเมินความเสี่ยง 3) การรายงานความมั่นคงปลอดภัย ทำให้สถานศึกษาเพิ่มประสิทธิภาพทางด้านการป้องกันและรักษาความมั่นคงปลอดภัย ระบบสามารถทำการตรวจสอบและบันทึกกระบวนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา ไม่ว่าจะเป็นการรักษาความปลอดภัยสำหรับบุคคล การรักษาความปลอดภัยสำหรับสถานที่ การป้องกันและแก้ไขปัญหาด้านผลกระบทจาการสู้รบและความไม่สงบ ทำให้สถานศึกษามีความพร้อมในการรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้นได้ในอนาคต จากเข้ามาช่วยป้องกันและแก้ไขปัญหาดังกล่าวได้ สามารถส่งผลต่อการลดความเสี่ยงทางด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาได้อย่างมีประสิทธิภาพ

บทที่ 3
วิธีดำเนินงานวิจัย

การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ เป็นการวิจัยและพัฒนา (Research and Development) ผู้วิจัยได้ดำเนินการวิจัยและพัฒนา โดยแบ่งการดำเนินการวิจัยออกเป็น 5 ระยะ ดังนี้

ระยะที่ 1 การวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ระยะที่ 2 การพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ระยะที่ 3 การออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ระยะที่ 4 การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ระยะที่ 5 การศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1 ระยะที่ 1 การวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทับสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.1 วัตถุประสงค์การวิจัยระยะที่ 1

3.1.1.1 เพื่อวิเคราะห์การรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.1.2 เพื่อวิเคราะห์ความต้องการจากผู้ใช้ระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.1.3 เพื่อประเมินความเหมาะสมของคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.2 ขอบเขตการวิจัยระยะที่ 1

3.1.2.1 ประชากรและกลุ่มตัวอย่าที่ใช้ในการวิจัยระยะที่ 1 แบ่งออกเป็น 3 กลุ่มดังนี้

กลุ่มที่ 1 ผู้เชี่ยวชาญด้านเนื้อหาและแนวทางการรักษาความมั่นปลอดภัยสำหรับสถานศึกษา จำนวน 5 ท่าน ด้วยวิธีการเลือกแบบเจาะจง (Purposive Sampling) สำหรับประเมินดัชนีความสอดคล้องระหว่างข้อคำถามในแบบสอบถามการวิจัย

กลุ่มที่ 2 ผู้เชี่ยวชาญด้าน การพัฒนาระบบ เทคโนโลยีสารสนเทศ และการรักษาความมั่นปลอดภัยสำหรับสถานศึกษา จำนวน 20 ท่าน ด้วยวิธีการเลือกแบบเจาะจง (Purposive Sampling) สำหรับประเมินเหมาะสมของคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

กลุ่มที่ 3 ประชากรและกลุ่มตัวอย่างสำหรับวิเคราะห์สภาพปัญหาและความต้องการในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ประชากร คือ ผู้บริหาร ครู อาจารย์ และบุคคลากรทางการศึกษา จำนวน 42,910 คน ของสถานศึกษาทั้งในระบบและนอกระบบในเขตพื้นที่การศึกษาจังหวัดชายแดนภาคใต้ ประกอบด้วย จังหวัด นราธิวาส ยะลา ปัตตานี (ข้อมูล ณ วันที่ 10 มิถุนายน 2560)

กลุ่มตัวอย่าง คือ ผู้บริหาร ครู อาจารย์ และบุคลากรทางการศึกษา จำนวน 198 คน ได้มาจากการสุ่มแบบแบ่งชั้น (Stratified Random Sampling) การกำหนดกลุ่มตัวอย่างใช้สูตรของทาโร ยามาแน่ (Yamane, 1973) จากนั้นทำการเลือกตัวอย่างแบบเจาะจง (Purposive Sampling) และใช้วิธีสุ่มอย่างง่าย ดังนี้

1. กำหนดขนาดกลุ่มตัวอย่างโดยใช้สูตรของยามาเน่

$$n = N/1+Ne^2$$

เมื่อ n หมายถึง ขนาดกลุ่มตัวอย่าง

N หมายถึง ขนาดประชากร

E หมายถึง ค่าความคลาดเคลื่อน กำหนดเป็น .05

การวิจัยในครั้งนี้ใช้กลุ่มตัวอย่างจำนวนทั้งสิน 198 คน

2. เทียบสัดส่วนกลุ่มตัวอย่างจากจำนวนประชากรโดยคำนวณตามสัดส่วนของแต่ละชั้น (Proportionate Stratified Random Sampling) ดังนี้

3. กำหนดกลุ่มตัวอย่างที่ใช้ในการวิจัยด้วยวิธีการเลือกแบบเจาะจง แบ่งเป็น จังหวัด นราธิวาส ยะลา และปัตตนี

ตารางที่ 3-1 จำนวนประชากรและการกำหนดกลุ่มตัวอย่างที่ใช้ในการวิจัย

กลุ่มประชากร	จำนวนประชากร	จำนวนกลุ่มตัวอย่าง	กลุ่มตัวอย่างที่ใช้ในการวิจัย
นราธิวาส	11,990	111	55
ยะลา	12,232	113	56
ปัตตานี	18,688	173	87
รวม	**42,910**	**397**	**198**

3.1.3 ตัวแปรที่ศึกษา

3.1.3.1 การวิเคราะห์ความต้องการจากผู้ใช้ระบบสำหรับกำหนดคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรต้น คือ สภาพปัญหาและความต้องการในการพัฒนาระบบจากผู้ใช้งานระบบ ได้แก่ ผู้บริหาร ครู อาจารย์ และเจ้าหน้าที่ของสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรตาม คือ คุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.3.2 ประเมินความเหมาะสมของคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรต้น คือ คุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรตาม คือ ผลการประเมินความเหมาะสมของคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.4 เครื่องมือที่ใช้ในการวิจัยระยะที่ 1

3.1.4.1 แบบบันทึกการลงรายการเชิงสังเคราะห์ในลักษณะของการวิเคราะห์เนื้อหา เพื่อใช้ในการเก็บรวบรวมข้อมูลจากเอกสาร ตำรา บทความทางวิชาการ และบทความวิจัยที่กี่ยวข้อง

3.1.4.2 แบบสอบถามสำหรับวิเคราะห์สภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ เพื่อกำหนดคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.4.3 คุณลักษะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.4.4 แบบประเมินความเหมาะสมของคุณลักษะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.1.5 วิธีดำเนินการวิจัยระยะที่ 1

การดำเนินการวิจัยในระยะที่ 1 เป็นการนำเสนอแนวคิดเกี่ยวกับการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ประกอบด้วยกระบวนการ ดังนี้

ขั้นที่ 1 การวิเคราะห์และสังเคราะห์เอกสาร

ผู้วิจัยศึกษาข้อมูลจากเอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ที่ประกอบไปด้วย แนวปฏิบัติ มาตรการ ระเบียบ หลักการ แนวทางการป้องกันและรักษาความปลอดภัยสำหรับสถานศึกษา ทั้งในประเทศและต่างประเทศ โดยรวบรวมข้อมูลเพื่อนำมาสังเคราะห์และนำความรู้ที่ได้มาสรุปเป็นกรอบและประเด็นหลักเกี่ยวกับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้และใช้ผลจากการสังเคราะห์ข้อมูลดังกล่าวเป็นแนวทางในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ขั้นที่ 2 การสอบถามกลุ่มตัวอย่างเกี่ยวกับการวิเคราะห์สภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบเพื่อกำหนดคุณลักษะของระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วย ผู้บริหาร ครู อาจารย์ และบุคลากรทางการศึกษาจำนวน 198 คน ใช้วิธีสุ่มแบบแบ่งชั่น (Stratified Random Sampling) การกำหนดกลุ่มตัวอย่างใช้สูตรของทาโรยามาแน่ (Yamane, 1973) จากนั้นทำการเลือกตัวกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) และใช้วิธีสุ่มอย่างง่าย

1. ผู้วิจัยสร้างข้อคำถาม ที่ได้จากการวิเคราะห์และสังเคราะห์เอกสารเพื่อนำไปใช้สอบถามสภาพปัญหาและความต้องการในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

2. ผู้วิจัยสร้างแบบประเมินความเที่ยงตรงเชิงเนื้อหาของข้อคำถาม (Index of Item Objective Congruence : IOC) ที่จะใช้สำหรับการประเมินข้อคำถามข้างต้น

3. ผู้วิจัยนำแบบประเมินความเที่ยงตรงเชิงเนื้อหาของข้อคำถามให้อาจารย์ที่ปรึกษาพิจารณาและตรวจสอบความถูกต้อง และความเหมาะสมของเครื่องมือก่อนไปเก็บรวบรวมข้อมูลในขั้นตอนต่อไป ซึ่งกำหนดเกณฑ์พิจารณาเลือกข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถามตั้งแต่ 0.50 ขึ้นไป

4. จากนั้นนำแบบประเมินความเที่ยงตรงเชิงเนื้อหาของข้อคำถามโดยผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยและผู้บริหาร จำนวน 5 ท่าน ประเมินความเที่ยงตรงเชิงเนื้อหาของข้อคำถาม

5. ผู้วิจัยสรุปพิจารณาเลือกข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถามที่มีเกณฑ์ตั้งแต่ 0.50 ขึ้นไป

6. เมื่อได้ข้อคำถามที่ผ่านการประเมินความเที่ยงตรงเชิงเนื้อหาของข้อคำถามจึงนำไปสร้างเป็นแบบสอบถาม เพื่อนำไปใช้สอบถามจากกลุ่มตัวอย่าง ดังตารางที่ 3-1 แสดงจำนวนประชากรและการกำหนดกลุ่มตัวอย่างที่ใช้ในการวิจัย

7. ผู้วิจัยวิเคราะห์ข้อมูลโดยหาค่าเฉลี่ย ($\bar{X}$) และส่วนเบี่ยงเบนมาตรฐาน *(S.D)*

8. ผู้วิจัยสรุปผลการวิเคราะห์ข้อมูลที่ได้จากการสอบถามกลุ่มตัวอย่างทั้งหมด 198 ท่าน โดยหาค่าเฉลี่ย ($\bar{X}$) และส่วนเบี่ยงเบนมาตรฐาน *(S.D)*

ขั้นที่ 3 สร้างแบบประเมินคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยใช้มาตราส่วนประมาณค่า (Rating Scale) 5 ระดับ ตามมาตรวัดแบบลิเคิร์ท (Likert Scale)

ขั้นที่ 4 นำแบบประเมินความเหมาะสมของคุณลักษะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ไปสอบถามผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ จำนวน 10 ท่าน โดยการเลือกแบบเจาะจง (Purposive Sampling)

ขั้นที่ 5 ผู้วิจัยสรุปผลที่ได้จากการประเมินแล้วทำการปรับปรุงตามคำแนะนำของผู้เชี่ยวชาญ

ขั้นที่ 6 ผู้วิจัยนำเสนอให้อาจารย์ที่ปรึกษาเพื่อพิจารณาและตรวจสอบความถูกต้อง แล้วจึงดำเนินการวิจัยในระยะต่อไป

3.1.6 สถิติที่ใช้ในการวิจัยระยะที่ 1

3.1.6.1 ประเมินความเหมาะสมของคุณลักษะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้โดยหาค่าเฉลี่ย (Mean : $\bar{X}$) และ ค่าความเบี่ยงเบนมาตรฐาน (Standard Deviation : *S.D.*) โดยกำหนดเกณฑ์ในการประเมิน 5 ระดับ ดังนี้

5 หมายถึง เหมาะสมมากที่สุด

4 หมายถึง เหมาะสมมาก

3 หมายถึง เหมาะสมปานกลาง

2 หมายถึง เหมาะสมน้อย

1 หมายถึง เหมาะสมน้อยที่สุด

และกำหนดเกณฑ์การแปลความหมายดังนี้ (ประคอง, 2542)

4.50 – 5.00	หมายถึง	มีความเห็นว่าเหมาะสมมากที่สุด
3.50 – 4.49	หมายถึง	มีความเห็นว่าเหมาะสมมาก
2.50 – 3. 49	หมายถึง	มีความเห็นว่าเหมาะสมปานกลาง
1.50 – 2.49	หมายถึง	มีความเห็นว่าเหมาะสมน้อย
1.00 – 1.49	หมายถึง	มีความเห็นว่าเหมาะสมน้อยที่สุด

นำแบบสำรวจที่สร้างขึ้นเสนอต่อผู้เชี่ยวชาญ จำนวน 3 ท่าน เพื่อตรวจสอบความเที่ยงตรงเชิงเนื้อหา โดยหาดัชนีความสอดคล้อง (IOC) และปรับปรุงตามข้อเสนอแนะ

3.1.6.2 ประเมินดัชนีความสอดคล้องระหว่างข้อคำถามในแบบสอบถามการวิจัยกับความเหมาะสมของแบบจำลองโดยผู้เชี่ยวชาญเพื่อหาความเที่ยงตรงของแบบสอบถามการวิจัยโดยมีเกณฑ์การให้คะแนน ดังนี้

ระดับ +1	หมายถึง	เห็นด้วย
ระดับ 0	หมายถึง	ไม่แน่ใจ
ระดับ -1	หมายถึง	ไม่เห็นด้วย

และนำคะแนนการประเมินมาหาค่าดัชนีความสอดคล้องของประเด็นการประเมินโดยใช้ Index of Item Objective Congruence (IOC) (Rovinelli and Hambleton, 1977)

$$IOC = \frac{\sum R}{N}$$

เมื่อ

IOC หมายถึง ค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับจุดประสงค์

$\sum R$ หมายถึง ผลรวมคะแนนความเห็นของผู้เชี่ยวชาญ

N หมายถึง จำนวนผู้เชี่ยวชาญ

การวิเคราะห์ข้อมูล พิจารณาระดับค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับจุดประสงค์ที่ได้จากสูตรคำนวณซึ่งมีค่าอยู่ระหว่าง 0.00 ถึง 1.00 ถ้าประเด็นที่มีค่า IOC ตั้งแต่ 0.50 ขึ้นไป ถือเป็นประเด็นที่ใช้ได้ ส่วนประเด็นที่มีค่าน้อยกว่า 0.50 ควรพิจารณาปรับปรุงหรือตัดออก

3.2 ระยะที่ 2 การพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.2.1 วัตถุประสงค์การวิจัยระยะที่ 2

3.2.1.1 เพื่อพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้

3.2.1.2 เพื่อประเมินความเหมาะสมของแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้

3.2.2 ขอบเขตของการวิจัยระยะที่ 2

3.2.2.1 ประชากร คือ ผู้เชี่ยวชาญด้านเนื้อหาและกระบวนการ ด้านเทคโนโลยีสารสนเทศ และ เทคโนโลยีเชื่อมโยงสรรพสิ่ง

3.2.2.2 กลุ่มตัวอย่าง คือ ผู้เชี่ยวชาญด้านเนื้อหาและกระบวนการ ด้านเทคโนโลยีสารสนเทศ และ เทคโนโลยีเชื่อมโยงสรรพสิ่ง รวมทั้งหมด 15 ท่าน ด้วยวิธีการเลือกแบบเจาะจง (Purposive Sampling) โดยเป็นผู้ที่มีประสบการณ์ในด้านที่เกี่ยวข้องอย่างน้อย 5 ปี ซึ่งการวิจัยระยะที่ 2 แบ่งผู้เชี่ยวชาญออกเป็น 2 กลุ่มคือ

กลุ่มที่ 1 ผู้เชี่ยวชาญด้านเนื้อหาและกระบวนการ จำนวน 5 ท่าน สำหรับประเมินดัชนีความสอดค้องระหว่างข้อคำถามในแบบสอบถามการวิจัยกับความเหมาะสมของแบบจำลอง

กลุ่มที่ 2 ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ และเทคโนโลยีเชื่อมโยงสรรพสิ่ง จำนวน 10 ท่าน สำหรับประเมินความเหมาะสมของแบบจำลอง

3.2.3 ตัวแปรที่ใช้ในการวิจัย

3.2.3.1 ตัวแปรต้น คือ แบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาจังหวัดชายแดนภาคใต้

3.2.3.2 ตัวแปรตาม คือ ผลการประเมินความเหมาะสมของแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้

3.2.4 เครื่องมือที่ใช้ในการวิจัยระยะที่ 2

3.2.4.1 แบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้

3.2.4.2 แบบประเมินความเหมาะสมของแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้

3.2.5 วิธีดำเนินการวิจัยระยะที่ 2

การวิจัยระยะที่ 2 เป็นการนำผลวิจัยที่ได้จากการวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทับสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้มาเป็นแนวทางในการสร้างแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาจังหวัดชายแดนภาคใต้ โดยมีกระบวนการดำเนินการดังนี้

ขั้นที่ 1 นำคุณลักษะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ในวัตถุประสงค์การวิจัยระยะที่ 1 มาพัฒนาเป็นแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้ ประกอบด้วย (1) แบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาจังหวัดชายแดนภาคใต้ และ (2) ขั้นตอนการทำงานของระบบฯ

ขั้นที่ 2 ดำเนินการพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากการสังเคราะห์ข้อมูลในวัตถุประสงค์การวิจัยระยะที่ 1

ขั้นที่ 3 สร้างแบบประเมินแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้ โดยใช้มาตราส่วนประมาณค่า (Rating Scale) 5 ระดับ ตามมาตรวัดแบบลิเคิร์ท (Likert Scale)

ขั้นที่ 4 นำแบบประเมินให้ผู้เชี่ยวชาญด้านเนื้อหาและกระบวนการ จำนวน 5 ท่าน ประเมินความเที่ยงตรงเชิงเนื้อหาของข้อคำถาม (Index of Item Objective Congruence : IOC) โดยเลือกใช้สมการและกำหนดเกณฑ์พิจารณาเลือกข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถาม ตั้งแต่ 0.5 ขึ้นไป

ขั้นที่ 5 ผู้วิจัยสรุปพิจารณาเลือกข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถามตามเกณฑ์ที่กำหนด เมื่อได้ข้อคำถามที่ผ่านเกณฑ์แล้ว จึงนำไปสอบถามผู้เชี่ยวชาญด้านการรักษาความด้านเทคโนโลยีสารสนเทศ และ เทคโนโลยีเชื่อมโยงสรรพสิ่ง จำนวน 10 ท่าน โดยการเลือกแบบเจาะจง (Purposive Sampling)

ขั้นที่ 6 ผู้วิจัยสรุปผลที่ได้จากการประเมินแล้วทำการปรับปรุงตามคำแนะนำของผู้เชี่ยวชาญ

ขั้นที่ 7 ผู้วิจัยนำเสนอให้อาจารย์ที่ปรึกษาเพื่อพิจารณาและตรวจสอบความถูกต้อง แล้วจึงดำเนินการวิจัยระยะที่ 3

3.2.6 สถิติที่ใช้ในการวิจัยระยะที่ 2

3.2.6.1 ประเมินความเหมาะสมของแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยหาค่าเฉลี่ย (Mean : $\bar{X}$) และ ค่าความเบี่ยงเบนมาตรฐาน (Standard Deviation : *S.D.*) โดยกำหนดเกณฑ์ในการประเมิน 5 ระดับ ดังนี้

5 หมายถึง เหมาะสมมากที่สุด
4 หมายถึง เหมาะสมมาก
3 หมายถึง เหมาะสมปานกลาง
2 หมายถึง เหมาะสมน้อย
1 หมายถึง เหมาะสมน้อยที่สุด

และกำหนดเกณฑ์การแปลความหมายดังนี้ (ประคอง, 2542)

4.50 – 5.00 หมายถึง มีความเห็นว่าเหมาะสมมากที่สุด
3.50 – 4.49 หมายถึง มีความเห็นว่าเหมาะสมมาก
2.50 – 3. 49 หมายถึง มีความเห็นว่าเหมาะสมปานกลาง
1.50 – 2.49 หมายถึง มีความเห็นว่าเหมาะสมน้อย
1.00 – 1.49 หมายถึง มีความเห็นว่าเหมาะสมน้อยที่สุด

นำแบบสำรวจที่สร้างขึ้นเสนอต่อผู้เชี่ยวชาญ จำนวน 3 ท่าน เพื่อตรวจสอบความเที่ยงตรงเชิงเนื้อหา โดยหาดัชนีความสอดคล้อง (IOC) และปรับปรุงตามข้อเสนอแนะ

3.2.6.2 ประเมินดัชนีความสอดคล้องระหว่างข้อคำถามในแบบสอบถามการวิจัยกับความเหมาะสมของแบบจำลองโดยผู้เชี่ยวชาญเพื่อหาความเที่ยงตรงของแบบสอบถามการวิจัยโดยมีเกณฑ์การให้คะแนน ดังนี้

ระดับ +1 หมายถึง เห็นด้วย
ระดับ 0 หมายถึง ไม่แน่ใจ
ระดับ -1 หมายถึง ไม่เห็นด้วย

และนำคะแนนการประเมินมาหาค่าดัชนีความสอดคล้องของประเด็นการประเมินโดยใช้ Index of Item Objective Congruence (IOC) (Rovinelli and Hambleton, 1977)

$$IOC = \frac{\sum R}{N}$$

เมื่อ

IOC หมายถึง ค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับจุดประสงค์
$\sum R$ หมายถึง ผลรวมคะแนนความเห็นของผู้เชี่ยวชาญ
N หมายถึง จำนวนผู้เชี่ยวชาญ

การวิเคราะห์ข้อมูล พิจารณาระดับค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับจุดประสงค์ที่ได้จากสูตรคำนวณซึ่งมีค่าอยู่ระหว่าง 0.00 ถึง 1.00 ถ้าประเด็นที่มีค่า IOC ตั้งแต่ 0.50 ขึ้นไป ถือเป็นประเด็นที่ใช้ได้ ส่วนประเด็นที่มีค่าน้อยกว่า 0.50 ควรพิจารณาปรับปรุงหรือตัดออก

3.3 ระยะที่ 3 การออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.3.1 วัตถุประสงค์การวิจัยระยะที่ 3

3.3.1.1 เพื่อออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.3.1.2 เพื่อประเมินความเหมาะสมของสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.3.2 ตัวแปรที่ใช้ในการวิจัยระยะที่ 3

3.3.2.1 ตัวแปรต้น คือ สถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.3.2.2 ตัวแปรตาม คือ ผลการประเมินความเหมาะสมของสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.3.3 เครื่องมือที่ใช้ในการวิจัยระยะที่ 3

3.3.3.1 สถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.3.3.2 แบบประเมินความเหมาะสมของสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.3.4 วิธีดำเนินการวิจัยระยะที่ 3

การวิจัยระยะที่ 3 เป็นการนำผลวิจัยที่ได้จากการพัฒนาแบบจำลองที่เหมาะสมแล้ว มาเป็นแนวทางในการออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยมีกระบวนการดำเนินการดังนี้

ขั้นที่ 1 นำแบบจำลองรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ในวัตถุประสงค์การวิจัยระยะที่

2 มาพัฒนาเป็นสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วย (1) องค์ประกอบของสถาปัตยกรรมระบบฯ และ (2) องค์ประกอบของโมดูลการทำงานของระบบฯ

ขั้นที่ 2 ดำเนินการออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้จากการสังเคราะห์ข้อมูลในวัตถุประสงค์การวิจัยระยะที่ 1

ขั้นที่ 3 สร้างแบบประเมินความเหมาะสมของสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยใช้มาตราส่วนประมาณค่า (Rating Scale) 5 ระดับ ตามมาตรวัดแบบลิเคิร์ท (Likert Scale)

ขั้นที่ 4 นำแบบประเมินให้ผู้เชี่ยวชาญด้านเนื้อหาและกระบวนการ จำนวน 5 ท่าน ประเมินความเที่ยงตรงเชิงเนื้อหาของข้อคำถาม (Index of Item Objective Congruence : IOC) โดยเลือกใช้สมการและกำหนดเกณฑ์พิจารณาเลือกข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถาม ตั้งแต่ 0.5 ขึ้นไป

ขั้นที่ 5 ผู้วิจัยสรุปพิจารณาเลือกข้อคำถามที่มีความเที่ยงตรงเชิงเนื้อหาของข้อคำถามตามเกณฑ์ที่กำหนด เมื่อได้ข้อคำถามที่ผ่านเกณฑ์แล้ว จึงนำไปสอบถามผู้เชี่ยวชาญด้านการรักษาความด้านเทคโนโลยีสารสนเทศ และ เทคโนโลยีเชื่อมโยงสรรพสิ่ง จำนวน 10 ท่าน โดยการเลือกแบบเจาะจง (Purposive Sampling)

ขั้นที่ 6 ผู้วิจัยสรุปผลที่ได้จากการประเมินแล้วทำการปรับปรุงตามคำแนะนำของผู้เชี่ยวชาญ

ขั้นที่ 7 ผู้วิจัยนำเสนอให้อาจารย์ที่ปรึกษาเพื่อพิจารณาและตรวจสอบความถูกต้อง แล้วจึงดำเนินการวิจัยระยะที่ 4

3.4 ระยะที่ 4 การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.1 วัตถุประสงค์การวิจัยระยะที่ 4

3.4.1.1 เพื่อออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.1.2 เพื่อพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.1.3 เพื่อประเมินกระบวนการทำงานของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.1.4 เพื่อหาประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.2 ขอบเขตของการวิจัยระยะที่ 4

3.4.2.1 ประชากรและกลุ่มตัวอย่างที่ใช้ในวัตถุประสงค์การวิจัยระยะที่ 3 แบ่งออกเป็น 3 กลุ่มดังนี้

กลุ่มที่ 1 ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ด้านเทคโนโลยีเชื่อมโยงสรรพสิ่ง ด้านการพัฒนาระบบสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัย จำนวน 5 ท่าน ด้วยวิธีการเลือกแบบเจาะจง (Purposive Sampling) สำหรับประเมินดัชนีความสอดคล้องระหว่างข้อคำถามในแบบสอบถามการวิจัยกับ

1. ประเด็นความเหมาะสมของกระบวนการทำงานของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

2. ประเด็นการประเมินประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

กลุ่มที่ 2 ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ด้านเทคโนโลยีเชื่อมโยงสรรพสิ่ง ด้านการพัฒนาระบบสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัย จำนวน 20 ท่าน ด้วยวิธีการเลือกแบบเจาะจง (Purposive Sampling) สำหรับประเมินความเหมาะสมของกระบวนการทำงานของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

กลุ่มที่ 3 ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ด้านเทคโนโลยีเชื่อมโยงสรรพสิ่ง ด้านการพัฒนาระบบสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัย จำนวน 10 ท่าน ด้วยวิธีการเลือกแบบเจาะจง (Purposive Sampling) สำหรับประเมินสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.3 ตัวแปรที่ศึกษา

3.4.3.1 ประเมินความเหมาะสมของกระบวนการทำงานของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรต้น คือ กระบวนการทำงานของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรตาม คือ ผลการประเมินความเหมาะสมของกระบวนการทำงานของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.3.2 ประเมินประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรต้น คือ ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรตาม คือ ผลการประเมินประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.4 เครื่องมือที่ใช้ในการวิจัยระยะที่ 4

3.4.4.1 แบบประเมินความเหมาะสมของกระบวนการทำงานระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.4.2 ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.4.4.3 แบบประเมินประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สถาปัตยกรรมระบบเป็นแนวคิดหลักที่เรียกว่า กระบวนการทำงาน ที่มีส่วนประกอบสำคัญ

3.4.5 วิธีดำเนินการวิจัยระยะที่ 4

หลังจากที่ผู้วิจัยได้ออกแบบสถาปัตยกรรมระบบและให้ผู้เชี่ยวชาญทำการประเมินสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สถาปัตยกรรมระบบเป็นแนวคิดหลักที่เรียกว่า กระบวนการทำงาน ที่มีส่วนประกอบสำคัญ 6 ส่วน ได้แก่ 1. การตรวจสอบ (Checking) 2. การตัดสินใจ (Decision) 3. การบันทึก (Recording) 4. การแจ้งเตือน (Notifications) 5. การรายงาน (Reporting) 6. บริหารจัดการข้อมูล (Management) 7. การแสดงสถานะความเสี่ยง (Status) ซึ่งจะนำไปสู่การออกแบบระบบ ที่เป็นส่วน ของการต่อยอดทางระบบต่อไป มีขั้นตอนดังนี้

ขั้นที่ 1 การออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีรายละเอียดดังนี้

1. ผู้วิจัยปรับปรุงตามข้อเสนอแนะและได้ทำการออบแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

2. นำเสนออาจารย์ที่ปรึกษาพิจารณา และปรับปรุงแก้ไขตามข้อเสนอแนะ

3. สร้างแบบประเมินการออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ตามมาตราส่วนประมาณค่า (Rating Scale) ตามมาตรวัดของลิเคิร์ท (Likert) 5 ระดับ

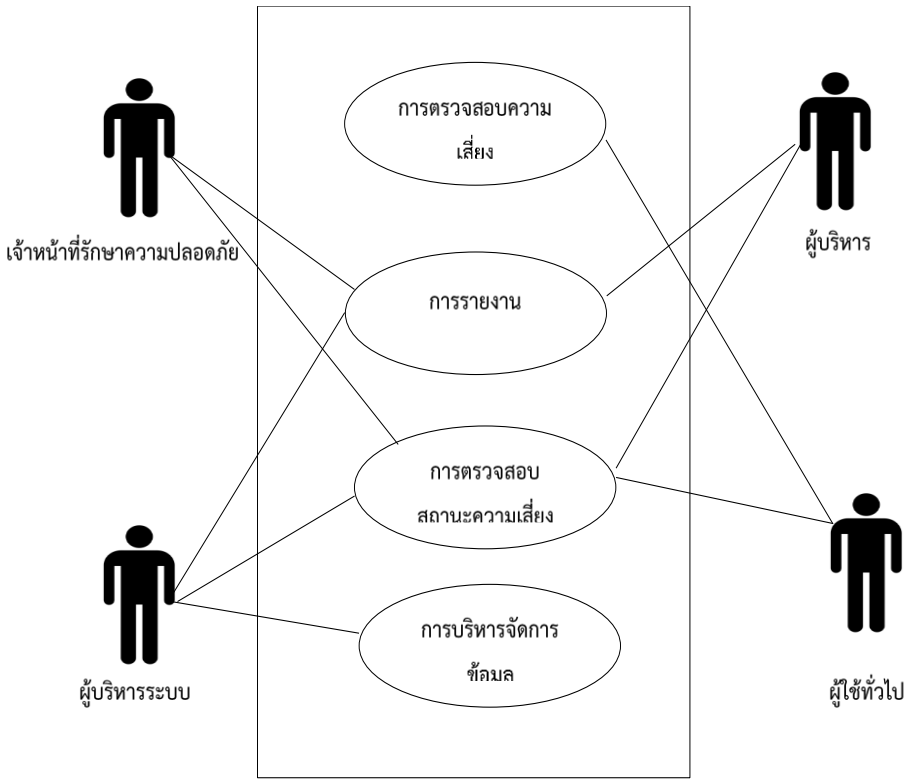
4. นำระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ที่ได้ออกแบบไว้ให้ ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและผู้บริหาร เป็นผู้ประเมินรวมจำนวน 10 ท่าน

5. ผู้วิจัยสรุปผลการประเมินและทำการปรับปรุงตามคำแนะนำของผู้เชี่ยวชาญ

3.4.5.1 ขั้นตอนการออกแบบระบบประกอบด้วยรายละเอียดดังนี้

3.4.5.1.1 แผนภาพยูสเคส (Use-case Diagram) ของผู้ใช้งานระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ เป็นแผนภาพที่แสดงขอบเขตการทำงานของผู้ใช้งานและความสัมพันธ์กับระบบย่อย (Sub System)

1. เบสยูสเคส (Base Use-case) ของผู้ใช้งานระบบ ประกอบด้วย 4 ยูสเคส คือ การตรวจสอบความเสี่ยง (Checking) การรายงาน (Reporting) การตรวจสอบสถานะความเสี่ยง (Status) การบริหารจัดการข้อมูล (Management) ดังภาพที่ 3-1



ภาพที่ 3-1 แผนภาพยูสเคสของผู้ใช้งานระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

1.1 บุคลากรที่มีส่วนเกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แบ่งออกเป็น 2 กลุ่มคือ

1.1.1 ผู้บริหารระบบ (Administrators) คือผู้ที่ทำหน้าที่ ควบคุมและจัดการระบบฯ ทั้งหมด โดยจัดการข้อมูลพื้นฐานที่จำเป็นของระบบฯ และผู้ใช้งาน นอกจากนี้ผู้บริหารระบบยังสามารถออกกฎต่าง ๆ ในการใช้งานระบบฯ มอบสิทธิ์ (Authorization) หรือยกเลิกสิทธิ์ให้กับผู้ใช้งาน

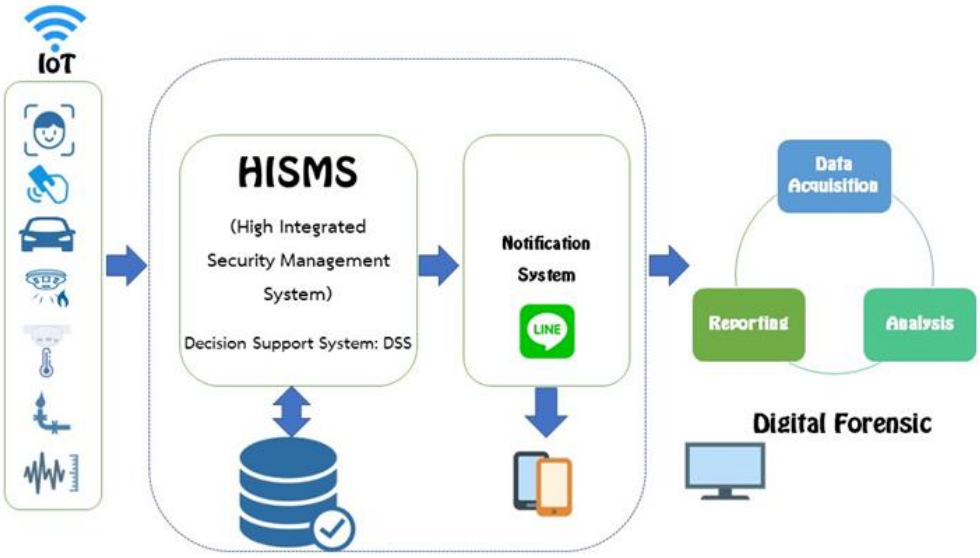
1.1.2 ผู้ใช้งานระบบ (User) คือกลุ่มของผู้ใช้งานที่ผู้บริหารระบบได้กำหนดสิทธิ์ในการเข้าถึงข้อมูลภายในระบบ ซึ่งในแต่ละกลุ่มมีสิทธิ์แตกต่างกันตามหน้าที่และคุณลักษณะของผู้ใช้งาน แบ่งออกเป็น 3 กลุ่ม ดังนี้

1.1.2.1 ผู้บริหาร ได้รับสินทธิ์ในการตรวจสอบรายงาน และสามารถดูสถานความเสี่ยงด้านความปลอดภัยของสถานศึกษาได้

1.1.2.2 เจ้าหน้าที่ตรวจสอบข้อมูลความมั่นคงปลอดภัย (Officers) คือ บุคลากรที่ได้รับสิทธิ์ในการตรวจสอบรายงานความมั่นคง และอัปเดตข้อมูลด้านความมั่นคงปลอดภัยให้เป็นปัจจุบันของระบบเป็นหลัก

1.1.2.3 ผู้ใช้ระบบสำหรับการตรวจสอบความมั่นคงปลอดภัย (User) คือ บุคคลทั่วไปที่ได้รับสิทธิ์เข้าใช้งานระบบเพื่อทำการตรวจสอบความมั่นปลอดภัยของระบบ และสามารถดูสถานะความเสี่ยงด้านความปลอดภัยของสถานศึกษาได้

2. แผนภาพกระบวนการ (Process Diagram) ของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ดังภาพที่ 3-2



ภาพที่ 3-2 แผนภาพกระบวนการของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

จากภาพที่ 3-2 แผนภาพกระบวนการ (Process Diagram) ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้ แสดงให้เห็นถึงกระบวนการที่ทำให้การตรวจจับบุคคล หรือ วัตถุ สามารถสื่อสารกันได้อัตโนมัติโดยใช้เซ็นเซอร์ (Sensor) ในการติดต่อสื่สารผ่านเครือข่ายอินเทอร์เน็ตเพื่อระบุตัวตน (Identification) ของบุคคล ทะเบียนรถ และระดับปริมาณของวัตถุ ทำให้สามารถแยกแยะหรือระบุได้ว่าเป็นข้อมูลอะไร ซึ่งกระบวนการทำงานแบ่งออกเป็น 4 ส่วน โดยมีรายละเอียดดังนี้

ส่วนที่ 1 Internet of Thing : IoTหรือ เทคโนโลยีเชื่อมโยงสรรพสิ่ง ที่ถูกคิดขึ้นโดย Kevin Ashton ในปี ค.ศ. 1999 ที่ต้องการให้อุปกรณ์อิเล็กทรอนิกส์มีโครงสร้างพื้นฐานที่สามารถ

เชื่อมต่อกับโลกอินเทอร์เน็ตได้ ทำให้อุปกรณ์ต่าง ๆ สามารถพูดคุยกันเองได้นั้นเอง (Ashton,1999) ทำให้มีการนำอุปกรณ์เทคโนโลยีเชื่อมโยงสรรพสิ่ง หรือ IoT เข้ามาเป็นเครื่องมือต้นแบบในการออกแบบกระบวนการรักษาความมั่นคงปลอดภัยด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งในสถานศึกษาจังหวัดชายแดนภาคใต้ ที่มีปัญหาด้านความมั่นคงโดยถูกระบุให้เป็นเขตพื้นที่เสี่ยงภัยที่ต้องการกระบวนการป้องกันและไขปัญหาความไม่สงบสุขในพื้นที่ ตามแนวนโยบายของคณะรักษาความสงบแห่งชาติ (คสช.) และนโยบายรัฐบาล ภายใต้กรอบแผนปฏิบัติการ การแก้ไขปัญหาและพัฒนาจังหวัดชายแดนใต้ (สำนักงานเลขานุการคณะกรรมการขับเคลื่อนการแก้ไขปัญหาชายแดนภาคใต้, 2559) เพื่อนำพาประเทศไทยเข้าสู่ Thailand 4.0 โมเดลขับเคลื่อนประเทศไทยสู่ความมั่งคั่ง มั่นคง และยั่งยืน เพื่อปฏิรูปโครงสร้างเศรษฐกิจของประเทศไปสู่ “Value-Based Economy” หรือเศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม โดยกำหนดให้มีการพัฒนากลุ่มดิจิทัลเทคโนโลยีอินเทอร์เน็ตที่เชื่อมต่ออุปกรณ์ต่าง ๆ และปัญญาประดิษฐ์ (กองบริหารงานวิจัยและประกันคุณภาพการศึกษา, 2560)

โดยการเลือกใช้เทคโนโลยี IoT ที่สามารถติดต่อสื่อสารกันได้เองโดยอาศัยเซ็นเซอร์ (Sensor) ในการติดต่อสื่อสาร ประกอบด้วย (Camera Sensor) สำหรับการตรวจจับใบหน้า และ ตรวจจับป้ายทะเบียนรถ (RFID) สำหรับสแกนบัตร (Sensor) สำหรับตรวจจับอุณหภูมิ ควัน ก๊าส มาใช้เป็นตัวกลางในการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตเพื่อระบุตัวตน (Identification) ของบุคคล ทะเบียนรถ และปริมาณการตรวจจับ อุณหภูมิ ควัน ก๊าส ทำให้แยกแยะหรือระบุได้ว่ามีเป็นข้อมูลประเภทใดบ้างเพื่อนำเข้าสู่ในส่วนที่ 2 หรือ ระบบ HISMS ซึ่งเป็นระบบที่สามารถเข้าถึงทุกที่ทุกเวลาจากทุกอุปกรณ์ (Device)

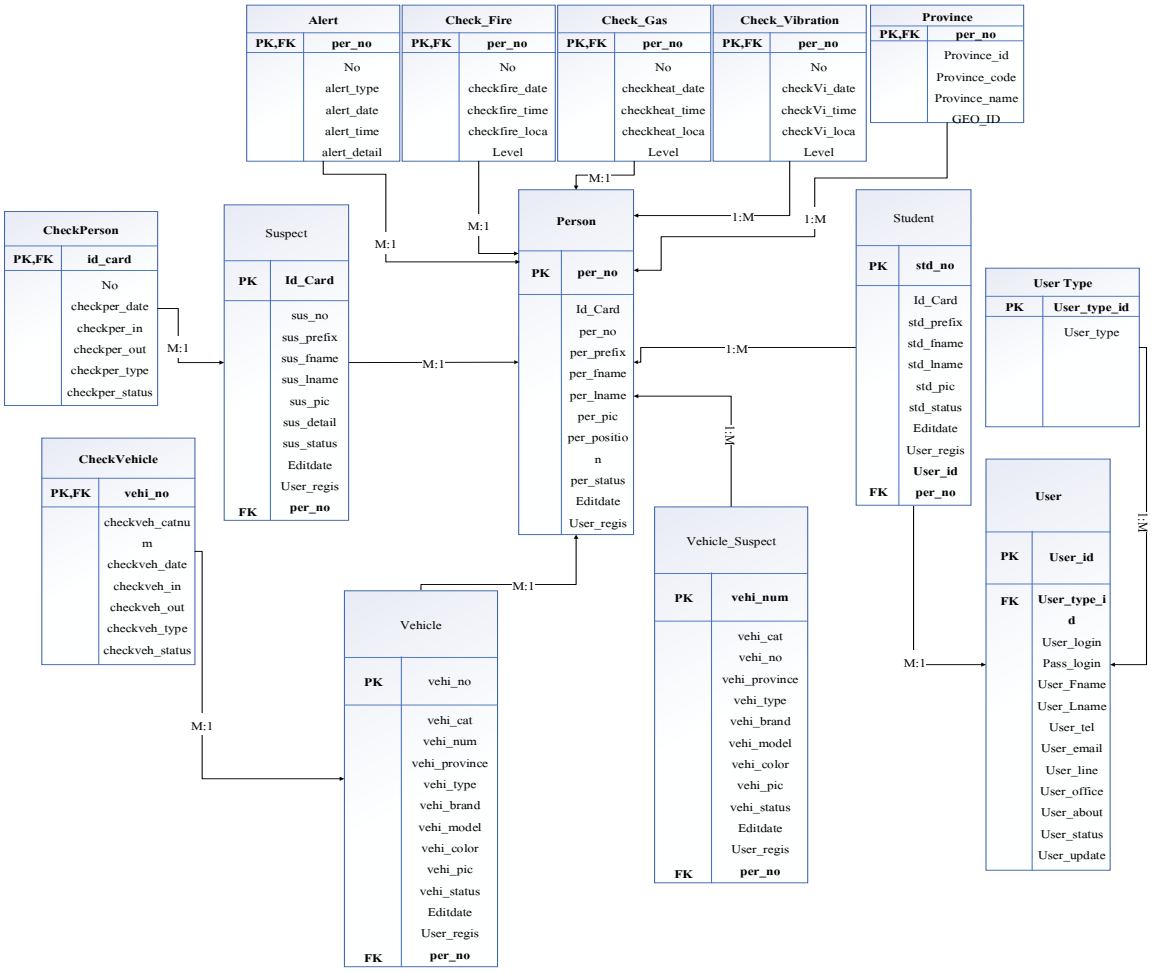
ส่วนที่ 2 High Integrated Security Management System : HISMS คือ ระบบบริหารจัดการฐานมูลด้านความมั่นคงปลอดภัยสูง ซึ่งเป็นวัตถุประสงค์หลักของงานวิจัยที่จะทำการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัล ซึ่งระบบดังกล่าวจะทำการดำเนินการผ่านทางเครื่องมืออุปกรณ์เทคโนโลยีเชื่อมโยงสรรพสิ่งจากส่วนที่ 1 และทำการวิเคราะห์ข้อมูลเชิงลึกและจัดการข้อมูลด้วยระบบสนับสนุนการตัดสินใจ Decision Support System และทำการบันทึกข้อมูลที่เข้าสู่ระบบฐานข้อมูลในดาต้าเบสเซิร์ฟเวอร์ (Database Sever)

ส่วนที่ 3 Notificatio คือ ระบบการแจ้งเตือนผลการรักษาความมั่นคงปลอดภัยภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยเลือกใช้ Application Line ในการนำเสนอผลการแจ้งเตือนของระบบ ซึ่งเป็น Application บนสมาร์ตโฟน (Smartphone) สามารถเข้าถึงข้อมูลการแจ้งเตือนได้ทุกที่ทุกเวลา

ส่วนที่ 4 Digital Forensics หรือ การตรวจสอบหลักฐานดิจิทัล คือ ส่วนของการนำผลที่ได้มาทำการวิเคราะห์เพื่อตรวจสอบหลักฐานดิจิทัล ซึ่งประกอบด้วย 3 ขั้นตอน คือ 1) Data Acquisition

การรวบรวมพยานหลักฐาน 2) Analysis การวิเคราะห์เพื่อประเมินความเสี่ยง 3) Reporting การรายงานความมั่งคงปลอดภัยสูงสำหรับสถานศึกษา

3 แผนภาพความสัมพันธ์ระหว่างเอ็นทิตี้ (Entity-relation Diagram)



ภาพที่ 3-3 แผนภาพความสัมพันธ์ระหว่างเอ็นทิตี้ (Entity-relation Diagram

4 พจนานุกรมข้อมูล (Data Dictionary) เป็นเครื่องมือสำหรับอธิบายการออกแบบโครงสร้างของฐานข้อมูลในระดับตรรกะ (Logical Database Design) ที่ใช้ในการวิจัยซึ่งพจนานุกรรมข้อมูลประกอบด้วยตาราง (Tables) ดังนี้

ตารางที่ 3-2 โครงสร้างตารางข้อมูลประเภทผู้ใช้ระบบ (User Type)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	User_type_id	Int	5	รหัสประเภทผู้ใช้ระบบ
2	User_type	Varchar	100	หน่วยงาน

ตารางที่ 3-3 โครงสร้างตารางข้อมูลผู้ใช้ระบบ (User)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	User_id	Int	5	รหัสผู้ใช้ระบบ
2	User_type_id	Int	5	รหัสประเภทผู้ใช้ระบบ
3	User_login	Varchar	100	ชื่อเข้าใช้ระบบ
4	Pass_login	Varchar	100	รหัสเข้าใช้ระบบ
5	User_Fname	Varchar	100	ชื่อผู้ใช้
6	User_Lname	Varchar	100	นามสกุลผู้ใช้
7	User_tel	Varchar	100	เบอร์โทร
8	User_email	Varchar	100	อีเมล์
9	User_line	Varchar	100	ไลน์
10	User_office	Varchar	100	หน่วยงาน
11	User_about	Varchar	100	หมายเหตุ
12	User_status	Int	1	สถานะผู้ใช้
13	User_update	Varchar	100	วันที่อัปเดทข้อมูลล่าสุด

ตารางที่ 3-4 โครงสร้างตารางข้อมูลบุคลากร เจ้าหน้าที่ (Person)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	Id_Card	Varchar	15	รหัสบัตรประชาชน
2	per_no	Int	10	รหัสบุคคลากร
3	per_prefix	Varchar	10	คำนำหน้าชื่อ
4	per_fname	Varchar	100	ชื่อ
5	per_lname	Varchar	100	นามสกุล
6	per_pic	Varchar	20	รูปภาพ
7	per_position	Varchar	10	ตำแหน่ง
8	per_status	Varchar	10	สถานะ
9	Editdate	Varchar	20	วันที่แก้ไข
10	User_regis	Varchar	100	ผู้ใช้ที่เพิ่มข้อมูล

ตารางที่ 3-5 โครงสร้างตารางข้อมูลนักศึกษา (Student)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	Id_Card	Varchar	15	รหัสบัตรประชาชน
2	std_no	Int	10	รหัสนักศึกษา
3	std_prefix	Varchar	10	คำนำหน้าชื่อ
4	std_fname	Varchar	100	ชื่อ
5	std_lname	Varchar	100	นามสกุล
6	std_pic	Varchar	20	รูปภาพ
7	std_status	Varchar	10	สถานะ
8	Editdate	Varchar	20	วันที่แก้ไข
9	User_regis	Varchar	100	ผู้ใช้ที่เพิ่มข้อมูล

ตารางที่ 3-6 โครงสร้างตารางข้อมูลผู้ต้องสงสัย (Suspect)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	Id_Card	Varchar	15	รหัสบัตรประชาชน
2	sus_no	Int	10	รหัสผู้ต้องสงสัย
3	sus_prefix	Varchar	10	คำนำหน้าชื่อ
4	sus_fname	Varchar	100	ชื่อ
5	sus_lname	Varchar	100	นามสกุล
6	sus_pic	Varchar	20	รูปภาพ
7	sus_detail	Varchar	200	รายละเอียดเพิ่มเติม
8	sus_status	Varchar	10	สถานะ
9	Editdate	Varchar	20	วันที่แก้ไข
10	User_regis	Varchar	100	ผู้ใช้ที่เพิ่มข้อมูล

ตารางที่ 3-7 โครงสร้างตารางข้อมูลยานพาหนะ (Vehicle)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	vehi_no	Int	10	รหัสยานพาหนะ
2	vehi_cat	Varchar	10	หมวดอักษรทะเบียน
3	vehi_num	Varchar	100	เลขทะเบียน
4	vehi_province	Varchar	100	จังหวัด
5	vehi_type	Varchar	100	ประเภทยานพาหนะ
6	vehi_brand	Varchar	10	ยี่ห้อ
7	vehi_model	Varchar	100	รุ่น
8	vehi_color	Varchar	100	สี
9	vehi_pic	Varchar	100	รูปภาพ
10	vehi_status	Int	2	สถานะการใช้งาน
11	Editdate	Varchar	20	วันที่แก้ไข
12	User_regis	Varchar	100	ผู้ใช้ที่เพิ่มข้อมูล

ตารางที่ 3-8 โครงสร้างตารางข้อมูลยานพาหนะ (Vehicle_Suspect)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	vehi_no	Int	10	รหัสยานพาหนะ
2	vehi_cat	Varchar	10	หมวดอักษรทะเบียน
3	vehi_num	Varchar	100	เลขทะเบียน
4	vehi_province	Varchar	100	จังหวัด
5	vehi_type	Varchar	100	ประเภทยานพาหนะ
6	vehi_brand	Varchar	10	ยี่ห้อ
7	vehi_model	Varchar	100	รุ่น
8	vehi_color	Varchar	100	สี
9	vehi_pic	Varchar	100	รูปภาพ
10	vehi_status	Int	2	สถานะการใช้งาน
11	Editdate	Varchar	20	วันที่แก้ไข
12	User_regis	Varchar	100	ผู้ใช้ที่เพิ่มข้อมูล

ตารางที่ 3-9 โครงสร้างตารางข้อมูลบุคคลเข้าออก (CheckPerson)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	No	Int	15	ลำดับ
2	id_card	Varchar	15	รหัสบัตรประชาชน
3	checkper_date	Date		วันที่ทำรายการ
4	checkper_in	Varchar	100	เวลาเข้า
5	checkper_out	Varchar	100	เวลาออก
6	checkper_type	Int	2	ประเภทบุคคล 1บุคลากร, 2นักศึกษา 3 บุคคลต้องสงสัย
7	checkper_status	Int	2	สถานะบุคคล 1ปกติ, 2ผู้ต้องสงสัย

ตารางที่ 3-10 โครงสร้างตารางข้อมูลยานพาหนะเข้าออก (CheckVehicle)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	No	Int	15	ลำดับ
2	vehi_no	Varchar	15	รหัสยานพาหนะ
3	checkveh_catnum	Varchar	100	ทะเบียนรถ
4	checkveh_date	date		วันที่ทำรายการ
5	checkveh_in	Varchar	100	เวลาเข้า
6	checkveh_out	Varchar	100	เวลาออก
7	checkveh_type	Int	2	ยานพาหนะประเภทใด 1บุคคลากร, 2นักศึกษา, 3ยานพาหนะต้องสงสัย
8	checkveh_status	Int	2	สถานะยานพาหนะ 1ปกติ, 2ยานพาหนะต้องสงสัย

ตารางที่ 3-11 โครงสร้างตารางข้อมูลการแจ้งเตือน (Alert)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	No	Int	15	ลำดับ
2	alert_type	Varchar	100	ประเภทการแจ้งเตือน
3	alert_date	Date		วันที่แจ้งเตือน
4	alert_time	Varchar	100	เวลาแจ้งเตือน
5	alert_detail	Varchar	100	รายละเอียดการแจ้งเตือน

ตารางที่ 3-12 โครงสร้างตารางข้อมูลการแจ้งเตือนควันไฟ (Check_Fire)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	No	Int	15	ลำดับ
2	checkfire_date	Date		วันที่แจ้งเตือนไฟไหม้
3	checkfire_time	Varchar	100	เวลาแจ้งเตือนไฟไหม้
4	checkfire_loca	Varchar	100	สถานที่
5	Level	Int	2	ระดับปริมาณควันไฟ 1ปกติ, 2สูง

ตารางที่ 3-13 โครงสร้างตารางข้อมูลการแจ้งเตือนอุณหภูมิสูง (Check_Heat)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	No	Int	15	ลำดับ
2	checkheat_date	Date		วันที่แจ้งเตือนอุณหภูมิสูง
3	checkheat_time	Varchar	100	เวลาแจ้งเตือนอุณหภูมิสูง
4	checkheat_loca	Varchar	100	สถานที่
5	Level	Int	2	ระดับปริมาณอุณหภูมิ 1ปกติ, 2สูง

ตารางที่ 3-14 โครงสร้างตารางข้อมูลการแจ้งเตือนก๊าซ (Check_Gas)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	No	Int	15	ลำดับ
2	checkgas_date	Date		วันที่แจ้งเตือนก๊าซ
3	checkgas_time	Varchar	100	เวลาแจ้งเตือนก๊าซ
4	checkgas_loca	Varchar	100	สถานที่
5	Level	Int	2	ระดับปริมาณก๊าซ 1ปกติ, 2สูง

ตารางที่ 3-15 โครงสร้างตารางข้อมูลการแจ้งเตือนแรงสั่นสะเทือน (Check_Vibration)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	No	Int	15	ลำดับ
2	checkVi_date	Date		วันที่แจ้งเตือนแรงสั่นสะเทือน
3	checkVi_time	Varchar	100	เวลาแจ้งเตือนแรงสั่นสะเทือน
4	checkVi_loca	Varchar	100	สถานที่
5	Level	Int	2	ระดับแรงสั่นสะเทือน 1ปกติ, 2สูง

ตารางที่ 3-16 โครงสร้างตารางข้อมูลจังหวัด (Province)

ลำดับ	ฟิลด์	ชนิด	ขนาด	คำอธิบาย
1	Province_id	Int	5	รหัสจังหวัด
2	Province_code	Varchar	2	รหัสย่อจังหวัด
3	Province_name	Varchar	150	ชื่อจังหวัด
4	GEO_ID	Int	5	ภาค

ขั้นที่ 2 การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

หลังจากที่ได้ปรับปรุงตามคำแนะนำของผู้เชี่ยวชาญในส่วนของการออกแบบระบบ ผู้วิจัยจึงดำเนินการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้ มีรายละเอียดดังนี้

1. สร้างแบบประเมินเพื่อประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยใช้มาตราส่วนประมาณค่า (Rating Scale) ตามมาตรวัดของลิเคิร์ท (Likert) 5 ระดับ

2. นำแบบประเมินให้ผู้เชี่ยวชาญด้านการวิเคราะห์และออกแบบระบบ วิศวกรรมซอฟต์แวร์ วิทยาการคอมพิวเตอร์หรือเทคโนโลยีสารสนเทศ และเทคโนโลยีเชื่อมโยงสรรพสิ่ง จำนวน 10 ท่าน เป็นผู้ประเมินโดยการเลือกแบบเจาะจง (Purposive Sampling)

3. การประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ใช้วิธีการทดสอบระบบแบบแบล็คบ๊อกซ์ (Black-Box Testing) เป็นการตรวจสอบกระบวนการทำงานของฟังก์ชันระบบงานทั้งหมด เพื่อหาประสิทธิภาพของระบบ 4 ด้าน คือ 1) การประเมินโมดูลย่อย (Module Test) ของระบบ 2) การประเมินการทำงานของระบบทั้งหมด (System Test) 3) การประเมินการใช้งานระบบ (Usability Test) และ 4) การประเมินความปลอดภัยของระบบ (Security Test) เพื่อตรวจสอบข้อผิดพลาดของระบบ แล้วนำมาแก้ไขปรับปรุงให้ระบบมีประสิทธิภาพมากขึ้น

4. วิเคราะห์แบบประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยการหาค่าเฉลี่ย ($\bar{X}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) โดยวิเคราะห์ข้อมูลจากแบบสอบถามตามมาตราส่วนประมาณค่าของลิเคิร์ท (Likert Scale) กำหนดเกณฑ์โดยประกอบด้วยมาตรอันดับ (Rating Scale) เชิงคุณภาพ 5 ระดับ และมาตรวัดอันดับเชิงปริมาณ 5 ระดับ

5. ผู้วิจัยสรุปผลการประเมินและทำการปรับปรุงตามคำแนะนำของผู้เชี่ยวชาญ

6. ผู้วิจัยนำเสนอให้อาจารย์ที่ปรึกษาเพื่อพิจารณาและตรวจสอบความถูกต้องแล้วจึงดำเนินการในขั้นต่อไป

3.4.6 สถิติที่ใช้ในการวิจัยระยะที่ 4

3.4.6.1 ประเมินความเหมาะสมของระบบการจัดการเรียนรู้แบบจินตวิศวกรรมแบบร่วมมือด้วยเกมิฟิเคชันบนสังคมคลาวด์ โดยหาค่าเฉลี่ย (Mean : $\bar{X}$) และ ค่าความเบี่ยงเบนมาตรฐาน (Standard Deviation : *S.D.*) โดยกำหนดเกณฑ์ในการประเมิน 5 ระดับ ดังนี้

5 หมายถึง เหมาะสมมากที่สุด
4 หมายถึง เหมาะสมมาก
3 หมายถึง เหมาะสมปานกลาง
2 หมายถึง เหมาะสมน้อย
1 หมายถึง เหมาะสมน้อยที่สุด

และกำหนดเกณฑ์การแปลความหมายดังนี้ (ประคอง, 2542)

4.50 – 5.00	หมายถึง	มีความเห็นว่าเหมาะสมมากที่สุด
3.50 – 4.49	หมายถึง	มีความเห็นว่าเหมาะสมมาก
2.50 – 3. 49	หมายถึง	มีความเห็นว่าเหมาะสมปานกลาง
1.50 – 2.49	หมายถึง	มีความเห็นว่าเหมาะสมน้อย
1.00 – 1.49	หมายถึง	มีความเห็นว่าเหมาะสมน้อยที่สุด

3.5 ระยะที่ 5 การศึกษาผลการรักษามั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.5.1 วัตถุประสงค์การวิจัยระยะที่ 5

3.5.1.1 เพื่อศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.5.1.2 เพื่อประเมินผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.5.2 ขอบเขตของการวิจัยระยะที่ 5

ประชากรที่ใช้ในการวิจัย คือ ผู้บริหาร ครู อาจารย์ บุคลากรทางการศึกษา จำนวน 42,910 คน จากสถานศึกษาทั้งในระบบและนอกระบบในเขตพื้นที่การศึกษาจังหวัดชายแดนภาคใต้ ประกอบด้วย นราธิวาส ยะลา ปัตตานี (ข้อมูล ณ วันที่ 10 มิถุนายน 2560)

กลุ่มตัวอย่างที่ใช้ในวิจัย คือ ผู้บริหาร ครู อาจารย์ บุคลากรทางการศึกษา จำนวน 50 คน จากสถานศึกษาทั้งในระบบและนอกระบบในเขตพื้นที่การศึกษาจังหวัดชายแดนภาคใต้ ประกอบด้วย นราธิวาส ยะลา ปัตตานี โดยใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling)

3.5.3 ตัวแปรที่ศึกษา

ตัวแปรต้น คือ ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

ตัวแปรตาม คือ ผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.5.4 เครื่องมือที่ใช้ในการวิจัยระยะที่ 5

3.5.4.1 ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้

3.5.4.2 แบบประเมินผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

3.5.5 วิธีดำเนินการวิจัยระยะที่ 5

หลังจากที่ผู้วิจัยได้ปรับปรุงตามคำแนะนำของผู้เชี่ยวชาญในส่วนของการพัฒนาระบบผู้วิจัยได้ดำเนินการ นำระบบไปทดลองใช้และทำการศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีขั้นตอนดังนี้

ขั้นที่ 1 การศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากกลุ่มตัวอย่าง 50 ท่าน ประกอบด้วย ผู้บริหาร ครู อาจารย์ บุคลากรทางการศึกษา จากสถานศึกษาทั้งในระบบและนอกระบบในเขตพื้นที่การศึกษาจังหวัดชายแดนภาคใต้ ประกอบด้วย นราธิวาส ยะลา ปัตตานี โดยใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling)

ขั้นที่ 2 สร้างแบบประเมินผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ตามมาตราส่วนประมาณค่า (Rating Scale) ตามมาตรวัดของลิเคิร์ท (Likert) 5 ระดับ

ขั้นที่ 3 นำระบบการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้ ไปทดลองใช้และทำการศึกษาผล

ขั้นที่ 4 การประเมินผลใช้หลักการวิเคราะห์ข้อมูลทางสถิติ โดยการหาค่าเฉลี่ย ($\bar{x}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) โดยวิเคราะห์ข้อมูลจากแบบสอบถามตามมาตราส่วนประมาณค่าของลิเคิร์ท (Likert Scale) กำหนดเกณฑ์โดยประกอบด้วยมาตรอันดับ (Rating Scale) เชิงคุณภาพ 5 ระดับ และมาตรวัดอันดับเชิงปริมาณ 5 ระดับ

3.5.6 สถิติที่ใช้ในการวิจัยระยะที่ 5

3.5.6.1 สถิติที่ใช้ในการประเมินผลการตรวจสอบหลักฐานดิจิทัล ด้วยระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยหาค่าเฉลี่ย (Mean : $\bar{x}$) และ ค่าความเบี่ยงเบนมาตรฐาน (Standard Deviation : *S.D.*) โดยกำหนดเกณฑ์ในการประเมิน 5 ระดับ ดังนี้

5 หมายถึง เหมาะสมมากที่สุด
4 หมายถึง เหมาะสมมาก
3 หมายถึง เหมาะสมปานกลาง
2 หมายถึง เหมาะสมน้อย
1 หมายถึง เหมาะสมน้อยที่สุด

และกำหนดเกณฑ์การแปลความหมายดังนี้ (ประคอง, 2542)

4.50 – 5.00	หมายถึง	มีความเห็นว่าเหมาะสมในระดับมากที่สุด
3.50 – 4.49	หมายถึง	มีความเห็นว่าเหมาะสมในระดับมาก
2.50 – 3. 49	หมายถึง	มีความเห็นว่าเหมาะสมในระดับปานกลาง
1.50 – 2.49	หมายถึง	มีความเห็นว่าเหมาะสมในระดับน้อย
1.00 – 1.49	หมายถึง	มีความเห็นว่าเหมาะสมในระดับน้อยที่สุด

บทที่ 4
ผลการวิจัย

การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยได้แบ่งการนำเสนอผลที่ศึกษาเป็น 5 ระยะ ตามวัตถุประสงค์ของการวิจัย ดังนี้

4.1 ผลการวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

4.2 ผลการพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

4.3 ผลการออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

4.4 ผลการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

4.5 ผลการประเมินผลการตรวจสอบหลักฐานดิจิทัลที่ได้จากระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

4.1 ผลการวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ผลการวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แบ่งออกเป็น 5 ส่วน ได้แก่ (1) ผลการวิเคราะห์เอกสาร (Document Analysis) เกี่ยวกับการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ (2) ผลการสัมภาษณ์แบบเชิงลึก (In Depth Interview) จากผู้เชี่ยวชาญประเด็นเกี่ยวกับสภาพปัญหาและความต้องการระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา (3) ผลการสอบถามกลุ่มตัวอย่าง เกี่ยวกับความต้องการระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา และ (4) ผลการประเมินความเหมาะสมของคุณลักษณะการรักษาความมั่นคงปลอดภัยสูงด้วย

เทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ซึ่งมีรายละเอียดดังนี้

4.1.1 ผลการวิเคราะห์และสังเคราะห์เอกสาร (Document Analysis) เกี่ยวกับการ การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีรายละเอียดดังนี้

ผลการวิเคราะห์เอกสาร (Document Analysis) เกี่ยวกับการรักษาความมั่นคงปลอดภัย ประกอบด้วย ระเบียบ และ มาตรการทางด้านการรักษาความปลอดภัยสำหรับสถานศึกษา เป็นเกณฑ์มาตรฐานหนึ่งที่ได้กำหนดขึ้นจากหน่วยงานของรัฐบาล ที่แสดงให้เห็นถึงแนวทางการรักษาความปลอดภัยสำหรับสถานศึกษา สามารถสรุปได้จาการวิเคราะห์เกณฑ์มาตรการได้ดังตารางที่ 4-1 ถึง 4-1 และ 4-2 ตามลำดับ

ตารางที่ 4-1 ผลการวิเคราะห์ด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา

การรักษาความมั่นคงปลอดภัยของสถานศึกษา	**สำนักนายกรัฐมนตรี(2552)**	**สำนักข่าวกรองแห่งชาติ(2553)**	**สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (2556)**
การรักษาความปลอดภัยเกี่ยวกับบุคคล	√	√	√
การรักษาความปลอดภัยเกี่ยวกับสถานที่	√	√	√
การรักษาความปลอดภัยในการประชุมลับ	√	√	
การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ		√	
การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์		√	
การป้องกันและแก้ไขอุบัติเหตุ			√
การป้องกันและแก้ไขอุบัติภัย			√
การป้องกันและแก้ไขปัญหาทางสังคม			√
การรักษาความปลอดภัยด้านสุขอนามัยของนักเรียน			√
การป้องกันและแก้ไขปัญหาจากสัตว์และแมลงมีพิษ			√
การป้องกันและแก้ไขปัญหาด้านผลกระทบจากการสู้รบและความไม่สงบ	√	√	√

จากตารางที่ 4-1 แสดงให้เห็นว่า การวิเคราะห์การรักษาความปลอดภัยของสถานศึกษาได้มีการใช้ ระเบียบ มาตรฐาน และ มาตรการด้านการรักษาความปลอดภัย ประกอบด้วย (1) ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 (2) มาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน (3) มาตราการรักษาความปลอดภัยของสถานศึกษาฉบับปรับปรุง 2556 โดยนำมาเป็นแนวทางในการกำหนดหลักการรักษาความปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ จากการศึกษาการรักษาความมั่นคงปลอดภัย ประกอบด้วย การรักษาความปลอดภัยเกี่ยวบุคคล การรักษาความปลอดภัยเกี่ยวกับสถานที่ การรักษาความปลอดภัยในการประชุมลับ การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็คทรอนิกส์ การป้องกันและแก้ไขอุบัติเหตุ การป้องกันและแก้ไขอุบัติภัย การป้องกันและแก้ไขปัญหาทางสังคม การรักษาความปลอดภัยด้านสุขอนามัยของนักเรียน การป้องกันและแก้ไขปัญหาจากสัตว์และแมลงมีพิษ การป้องกันและแก้ไขด้านผลกระทบจากการสู้รบและความไม่สงบ โดยการรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ไม่จำเป็นต้องประกอบด้วยส่วนต่าง ๆ ทุกขั้นตอน ขึ้นอยู่กับบริบทขององค์กรและการออกแบบที่เหมาะสมโดยต้องคำนึงถึงความต้องการในการใช้งานทางด้านการักษาความมั่นคงปลอดภัยในรูปแบบของการรักษาความปลอดภัยที่เกิดจากความต้องการขององค์กรในการนำมาใช้เพื่อป้องกันและแก้ไขปัญหาทางด้านความมั่นคงปลอดภัยขององค์กร และ การดำเนินชีวิตของบุคคล การรักษาความปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ จึงประกอบไปด้วย 3 ส่วน คือ

1. การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal Security)
2. การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Place Security)
3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ (Prevention of War and its Environment Consequence)

โดยทั้ง 3 ส่วนที่ผู้วิจัยได้เลือกเพื่อนำมาใช้ในการวิเคราะห์การรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ เพื่อให้สอดคล้องกับความต้องการทางด้านการป้องกันและแก้ไขปัญญหาให้ตรงตามบริบทและความต้องการของสถานศึกษาในจังหวัดชายแดนภาคใต้

ตารางที่ 4-2 ผลการวิเคราะห์ด้านองค์ประกอบของการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

องค์ประกอบของการรักษาความมั่งคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้	**สำนักนายกรัฐมนตรี(2552)**	**สำนักข่าวกรองแห่งชาติ (2553)**	**สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน(2556)**	O. Fatma et al.(2010)	F.Lawrence and P.Marianna (2014)	R. Nunes-Vaz (2014)	T. Paul (2015)	k. Sami et al. (2015)	D. Wen-hui et al. (2016)	J. Gregory and R. Scott McCoy (2017)
1. การรักษาความปลอดภัยเกี่ยวกับบุคคล										
1.1 การตรวจสอบประวัติและพฤติกรรมบุคคล	√	√	√	√						
1.2 การควบคุมบุคคลเข้า – ออก		√	√		√		√			
1.3 การฝึกอบรมด้านการรักษาความปลอดภัย				√						
2. การรักษาความปลอดภัยเกี่ยวกับสถานที่										
2.1 เจ้าหน้าที่รักษาความปลอดภัย อาคารสถานที่ และพื้นที่ที่ต้องควบคุมดูแล	√	√	√							
2.2 วางระบบป้องกันทางวัตถุ เช่น รั้ว เครื่องขวางช่องทางเข้า	√	√					√			
2.3 ใช้แสงสว่างเพื่อปกป้องพื้นที่มีความสำคัญ	√	√	√				√			
2.4 จัดให้มีระบบสัญญาณเตือนภัย	√	√					√		√	
2.5 ระบบแจ้งเตือนมวลชนสามารถให้คำแนะนำแก่ผู้ปกครองผ่านทางอีเมลและระบบส่งข้อความด้วยเสียงและข้อความ				√			√			√
2.6 ควบคุมยานพาหนะเข้า-ออก	√	√			√			√		
2.7 กล้องวิดีโอวงจรปิด				√			√			√
2.8 ระบบป้องกันและระงับอัคคีภัย	√	√			√				√	√
3. **การป้องกันและแก้ไขปัญหาด้านความไม่สงบ**										
3.1 แต่งตั้งผู้รับผิดชอบติดสถานการณ์ที่เกี่ยวข้องกับการสู้รบและความไม่สงบ			√				√			

ตารางที่ 4-2 (ต่อ)

องค์ประกอบของการรักษาความมั่งคงปลอดภัย สำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้	สำนักนายกรัฐมนตรี(2552)	สำนักข่าวกรองแห่งชาติ (2553)	สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน(2556)	O. Fatma et al.(2010)	F.Lawrence and P.Marianna (2014)	R. Nunes-Vaz (2014)	T. Paul (2015)	k. Sami et al. (2015)	D. Wen-hui et al. (2016)	J. Gregory and R. Scott McCoy (2017)
3.2 ประสานความร่วมมือกับหน่วยงานด้านความมั่นคงและสร้างสายสื่อสารฉุกเฉินเพื่อสื่อสารกับหน่วยงานและองค์กรที่จำเป็น	√		√	√			√			
3.3 ข้อมูลด้านความมั่นคง	√	√		√			√	√		

จากตารางที่ 4-2 แสดงให้เห็นว่า ผลการวิเคราะห์องค์ประกอบของการรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยใช้ทั้ง 3 ส่วนของการวิเคราะห์การรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ประกอบด้วย (1) การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal Security) (2) การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Place Security) (3) การป้องกันและแก้ไขปัญหาด้านความไม่สงบ (Prevention of War and its Environment Consequence) โดยทั้ง 3 ส่วนดังกล่าวผู้วิจัยได้ทำการวิเคราะห์แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปมาเพื่อใช้ให้เหมาะสมกับบริบทที่ต้องการ ประกอบด้วย

1. การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal Security)
   1.1 การตรวจสอบประวัติและพฤติกรรมบุคคล
   1.2 การควบคุมและบันทึกเวลาการเข้า - ออก ของบุคคล
2. การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Place Security)
   2.1 ระบบตรวจจับและแจ้งเตือนภัย
   2.2 ระบบแจ้งเตือนมวลชนผ่านข้อความโทรศัพท์มือถือ
   2.3 ระบบควบคุมยานพาหนะเข้า – ออก

2.4 กล้องโทรทัศน์วงจรปิด

3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ (Prevention of War and its Environment Consequence)

3.1 การประสานความร่วมมือกับหน่วยงานด้านความมั่นคง

3.2 ฐานข้อมูลด้านความมั่นคง

โดยองค์ประกอบของการรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ดังกล่าวผู้วิจัยได้นำมาเป็นข้อคำถามสำหรับนำไปใช้ในการสัฒภาษณ์เชิงลึก จากผู้เชี่ยวชาญในขั้นที่ 2

4.1.2 ผลการสอบถามกลุ่มตัวอย่างเกี่ยวกับสภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบเพื่อกำหนดคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ จากผู้เชี่ยวชาญในประเด็นที่เกี่ยวกับ การรักษาความปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีรายละเอียดดังนี้

ผลจากการสัมภาษณ์เชิงลึก (In-Depth Interview) จากผู้เชี่ยวชาญเห็นว่าข้อคำถามที่มีความเหมาะสมแต่มีข้อเสนอแนะเพิ่มเติมโดยให้ปรับปรุงแก้ไขในบางประเด็น ดังข้อมูลในตารางที่ 4-3

ตารางที่ 4-3 ผลการสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญประด็นเกี่ยวการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ และ ข้อเสนอแนะของผู้เชี่ยวชาญ

ประเด็นคำถาม	**ข้อคิดเห็น/ข้อเสนอแนะของผู้เชี่ยวชาญ**
ด้านที่ 1. การรักษาความปลอดภัยเกี่ยวกับบุคค (Personal security)	
1.1 การตรวจสอบประวัติและพฤติกรรมบุคคล	- สถานศึกษามีข้อมูลประวัติบุคคลเบื้องต้น ทั้งที่อยู่ในรูปแบบแฟ้มเอกสาร และฐานข้อมูลบุคคล - แฟ้มเอกสาร และ ฐานข้อมูลบุคคล มีข้อมูลไม่ครบถ้วน - แฟ้มเอกสาร และฐานข้อมูลบุคคล ไม่มีการอัปเดทและปรับปรุงข้อมูลให้เป็นปัจจุบัน - สถานศึกษาบางที่ไม่มีการจัดเก็บพฤติการณ์บุคคล - หากต้องการทราบประวัติบุคคลหรือพฤติกรรมบุคคล จะทำการตรวจสอบจากแฟ้มประวัติ ซึ่งเกิดความล้าช้าหรือข้อมูลที่ได้ไม่เป็นปัจจุบัน - สถานศึกษาบางแห่งมีประวัติข้อมูลในรูปแบบของระบบฐานข้อมูล ซึ่งบางแห่งมักจะพบปัญหาข้อมูลที่ไม่เป็นปัจจุบัน - ไม่มีเจ้าหน้าที่คอยดูแลบริหารจัดการระบบฐานข้อมูลในบางแห่ง - สถานศึกษามีความต้องการระบบจัดเก็บข้อมูลประวัติและพฤติกรรมบุคคล ที่สามารถตรวจสอบข้อมูลได้ตรงตามความต้องการและการใช้งานและมีระบบการป้องการการเข้าถึงข้อมูลอย่างมีประสิทธิภาพ

ตารางที่ 4-3 (ต่อ)

ประเด็นคำถาม	ข้อคิดเห็น/ข้อเสนอแนะของผู้เชี่ยวชาญ
1.2 การควบคุมและบันทึกเวลาการเข้า – ออก ของบุคคล	- มีการตรวจสอบบุคคลเข้าออกในรูปแบบพื้นฐานทั่วไปที่ใช้ เจ้าหน้าที่รักษาความปลอดภัย ไม่ว่าจะเป็น การแลกบัตร ประชาชน บัตรนักเรียน นักศึกษา บัตรข้าราชการ หรือบัตรที่หน่วยงานราชการเป็นผู้ออกให้ - มีการจดบันทึกในรูปแบบของกระดาษา เพื่อบันทึกเวลาเข้า เวลาออกภายในสถานศึกษา - ไม่มีการตรวจสอบประวัติบุคคลที่มีการเข้า ออกในสถานศึกษา - บางครั้งเกิดปัญหาจากบุคคลภายนอกเข้ามาทำความเสียหายภายในสถานศึกษา - สถานศึกษามีความต้องการระบบควบคุมการเข้าออกที่สามารถบันทึกข้อมูลบุคคล เข้าออก เวลา จำนวนครั้ง ในการเข้าออก และจัดเก็บตรวจสอบได้อย่างเป็นระบบและมีประสิทธิภาพ
ด้านที่ 2. การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Place security)	
2.1 ระบบตรวจจับและแจ้งเตือนภัย	- สถานศึกษาหลายแห่งมีระบบแจ้งเตือนไฟไหม้ - มีการตรวจวัดและตรวจจับ โดยเครื่องมือทางด้านการรักษาความปลอดภัย และการเกิดเพลิงไหมภายในอาคาร - มีระบบแจ้งเพลิงไหม้ อยู่ในรูปแบบสัญญาแจ้งเตือกเพื่อประกาศการแจ้งเตือนครอบคลุมพื้นที่ - สถานศึกษาต้องการระบบแจ้งเตือนผ่านอุปกรณ์โทรศัพท์เคลื่อนที่
2.2 ระบบแจ้งเตือนมวลชนผ่านข้อความโทรศัพท์มือถือ	- สถานศึกษาบางแห่ง ยังไม่มีระบบแจ้งเตือนผ่านระบบข้อความโทรศัพท์มือถือ - ผู้บริหารต้องการให้มีการแจ้งเตือนผ่านโทรศัพท์มือถือในรูปแบบของข้อความหรือบริหารอื่น ๆ ที่สะดวกและง่าย
2.3 ระบบควบคุมยานพาหนะเข้า – ออก	- มีการตรวจสอบยานพาหนะ เข้า ออก โดยสถานศึกษาบางแห่งมีการใช้เจ้าหน้าที่รักษาความปลอดภัยคอยควบคุมการเข้าออก ภายในโรงเรียน - มีการจดบันทึกเวลา เข้าออก ในรูปแบบของแฟ้มเอกสาร - สถานศึกษามีความต้องการระบบควบคุมการเข้าออกที่สามารถบันทึกข้อมูลบุคคล เข้าออก เวลา จำนวนครั้ง ที่สามารถทำการตรวจสอบได้อย่างเป็นระบบ
2.4 กล้องโทรทัศน์วงจรปิด	- สถานศึกษาหลายแห่งมีการติดตั้งกล้องวงจรปิด เพื่อคอยบันทึกและติดตามสถานการณ์ภายในสถานศึกษา - สามารถเรียกดูข้อมูลย้อนหลังได้

ตารางที่ 4-3 (ต่อ)

ประเด็นคำถาม	ข้อคิดเห็น/ข้อเสนอแนะของผู้เชี่ยวชาญ
3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ (Prevention of War and its Environment Consequence)	
3.1 การประสานความร่วมมือกับหน่วยงานด้านความมั่นคง	- มีการติดต่อผ่านประสานงานกับหน่วยงานภายนอกโดยการใช้โทรศัพท์สายด่วน หรือ หมายเลขแจ้งโดยตรงไปยังสถานที่หรือหน่วยงานที่รับผิดชอบโดยตรง เช่น สถานีตำรวจ โรงพยาบาย สถานีดับเพลิง เป็นต้น
3.2 ฐานข้อมูลด้านความมั่นคง	- สถานศึกษาบางแห่งได้รับการแจ้งเตือนเป็นเอกสารเกี่ยวกับข้อมูล ของบุคคล หรือ ยานพาหะนะ ที่อาจก่อเหตุความไม่สงบในพื้นที่ได้ - ผู้บริหารอยากให้มีการสร้างฐานข้อมูลที่สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานทางด้านความปลอดภัยในเขตพื้นที่จังหวัดชายแดนภาคใต้

จากตารางที่ 4-3 ผลการสอบถามจากกลุ่มตัวอย่าง ประเด็น เกี่ยวกับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ พร้อมทั้งข้อเสนอแนะของผู้เชี่ยวชาญและผู้วิจัยได้นำเอาข้อเสนอแนะ มาปรับข้อมูลตามคำแนะนำ โดยทำการสังเคราะห์จากงานวิจัยเพื่อกำหนดคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ดังตารางที่ 4-4

ตารางที่ 4-4 ผลการสังเคราะห์คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้	O. Fatma et al.(2010)	Thomas L. Norman (2012)	R. Nunes-Vaz (2014)	M.Gasparik and P. Solek (2014)	F.Lawrence and P.Marianna (2014)	k. Sami et al. (2015)	T. Paul (2015)	D. Wen-hui et al. (2016)	A. Muhammad Rizwan at al. (2017)	L. Maros and R, Jozef (2017)	G.Cristian Gonzalez et al. (2017)	J. Gregory and R. Scott McCoy (2017)	พิศณุ คมีชัย (2557)	อรวัตร จิตต์โสภักตร และคณะ (2558)
1. การรักษาความปลอดภัยเกี่ยวกับบุคคล														
1.1 ระบบยืนยันตัวตน														
1. บัตรเข้าออก	√	√	√		√									
2. ระบบตรวจจับใบหน้า										√	√		√	√

ตารางที่ 4-4 (ต่อ)

คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้	O. Fatma et al.(2010)	Thomas L. Norman (2012)	R. Nunes-Vaz (2014)	M.Gasparik and P. Solek (2014)	F.Lawrence and P.Marianna (2014)	k. Sami et al. (2015)	T. Paul (2015)	D. Wen-hui et al. (2016)	A. Muhammad Rizwan at al. (2017)	L. Maros and R, Jozef (2017)	G.Cristian Gonzalez et al. (2017)	J. Gregory and R. Scott McCoy (2017)	พิศณุ ศุมีชัย (2557)	อรฉัตร จิตต์โสภัคตร และคณะ (2558)
2. การรักษาความปลอดภัยเกี่ยวกับสถานที่														
2.1 ระบบควบคุมการเข้า-ออกยานพาหนะ														
2.1.1 บัตรเข้าออก	√	√			√									
2.1.2 ระบบอ่านป้ายทะเบียนรถ						√			√					
2.2 ระบบตรวจจับและแจ้งเตือน														
2.2.1 ตรวจจับความร้อน		√			√			√				√		
2.2.3 ตรวจจับควัน		√			√			√				√		
2.2.3 ตรวจจับก๊าซ		√			√							√		
2.2.4 ตรวจจับแรงสั่นสะเทือน		√			√							√		
3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ														
3.1 ระบบฐานข้อมูลด้านความมั่นคง														
1. ระบบแจ้งเตือนผู้ต้องสงสัย	√	√	√	√	√		√			√			√	√
2. ระบบแจ้งเตือนรถต้องสงสัย						√			√					

จากตารางที่ 4-4 แสดงให้เห็นว่า คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยนำการใช้เทคโนโลยีทางด้านความปลอดภัยเพื่อเป็นแนวทางในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปได้ 5 ส่วน คือ 1) ระบบยืนยันตัวตน 2) ระบบควบคุมการเข้า-ออกยานพาหนะ 3) ระบบตรวจจับและแจ้งเตือนภัยภายในอาคาร 4) ระบบฐานข้อมูลด้านความมั่นคง โดยทั้ง 4 ส่วนสามารถสรุปผลการนำมาเป็นองค์ประกอบด้านการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดนดังตารางที่ 4-5 ดังนี้

ตารางที่ 4-5 สรุปผลองค์ประกอบของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

องค์ประกอบด้านการรักษาความมั่นคงปลอดภัยด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้	**คุณลักษณะของการรักษาความมั่นคงปลอดภัย**				**เทคโนโลยีเชื่อมโยงสรรพสิ่ง (Internet of Thing**		**กระบวนการตรวจสอบหลักฐานดิจิทัล (Digital Forensic)**		
	ระบบยืนยันตัวตน	**ระบบควบคุมการเข้า-ออกยานพาหนะ**	**ระบบตรวจจับและแจ้งเตือนภัยภายใน**	**ระบบฐานข้อมูลด้านความมั่นคง**	**Camera Sensor**	**RFID Card**	**Data Acquisition การรวบรวม**	**Analysis การวิเคราะห์เพื่อประเมินความ**	**Reporting การรายงานความมั่งคง**
					Module				
1. การรักษาความปลอดภัยเกี่ยวกับบุคคล	√				1. โมดูลตรวจจับใบหน้า 2. โมดูลสแกนบัตร - บุคลากรภายใน - นักเรียน/นักศึกษา - บุคคลภายนอก		√	√	√
2. การรักษาความปลอดภัยเกี่ยวกับสถานที่		√	√		1. โมดูลตรวจจับทะเบียนรถ - ทะเบียนรถบุคคลภายใน - ทะเบียนรถบุคคลภายนอก 2. โมดูลตรวจจับควันไฟ 3. โมดูลตรวจจับความร้อน 4. โมดูลตรวจจับก๊าซ 5. โมดูลตรวจจับแรงสั้นสะเทือน		√	√	√
3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ				√	1. โมดูลตรวจจับใบหน้า - บุคคลต้องสงสัย 2. โมดูลตรวจจับทะเบียนรถ - ทะเบียนรถต้องสงสัย		√	√	√

จากตารางที่ 4-5 ผลสรุปองค์ประกอบของคุณลักษณะการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แสดงให้เห็นว่า ระบบรักษาความมั่นคงปลอดภัยสูง ประกอบด้วย 3 ส่วนคือ การรักษาความมั่นคงปลอดภัยเกี่ยวกับบุคคล การรักษาความมั่นคงปลอดภัยเกี่ยวกับสถานที่ และ การป้องกันและแก้ไขปัญหาด้านความไม่สงบ ซึ่งมีความเกี่ยวข้องกับกระบวนการรักษาความมั่นคงปลอดภัย ซึ่งแบ่งออกเป็น 4 ระบบ คือ 1) ระบบยืนยันตัวตน 2) ระบบควบคุมการเข้า – ออก ยานพาหนะ 3) ระบบตรวจจับและแจ้งเตือนภัยภายในอาคาร และ 4) ระบบฐานข้อมูลด้านความมั่นคง ในส่วนของเทคโนโลยีเชื่อมโยงใช้การตรวจจับด้วย กล้องตรวจจับ เซนเซอร์ และ บัตรอาร์เอฟไอดี โดยใช้กับโมดูลทั้ง 7 ส่วน ได้แก่ 1) โมดูลตรวจจับใบหน้า 2) โมดูลสแกนบัตร 3) โมดูลตรวจจับทะเบียนรถ 4) โมดูลตรวจจับควันไฟ 5) โมดูลตรวจจับความร้อน 6) โมดูลตรวจจับก๊าซ 7) โมดูลตรวจจับแรงสั่นสะเทือน ซึ่งสารสนเทศที่ได้จากโมดูลทั้ง 7 จะอยู่ในรูปแบบของข้อมูลอิเล็คทรอนิกส์ หรือหลักฐานดิจิทัล (Digital Forensic) ที่ประกอบด้วย 3 ส่วน คือ 1) การรวบรวมพยานหลักฐาน 2) การวิเคราะห์เพื่อประเมินความเสี่ยง 3) การรายงานความมั่นคงปลอดภัย

4.1.3 ผลการประเมินความเหมาะสมของการวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปได้ดังตารางที่ 4-6

ตารางที่ 4-6 ผลประเมินความเหมาะสมของการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ผลการประเมิน**		
	$\bar{x}$	**S.D.**	**ความเหมาะสม**
การรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้			
1. การรักษาความปลอดภัยเกี่ยวกับบุคคล			
1.1 การตรวจสอบประวัติและพฤติกรรมบุคคล	4.76	0.44	มากที่สุด
1.2 การควบคุมและบันทึกเวลาการเข้า - ออก ของบุคคล	4.76	0.44	มากที่สุด
รวม	**4.76**	**0.44**	**มากที่สุด**
2. การรักษาความปลอดภัยเกี่ยวกับสถานที่			
2.1 ระบบตรวจจับและแจ้งเตือนภัย	4.80	0.41	มากที่สุด
2.2 ระบบแจ้งเตือนมวลชนผ่านข้อความโทรศัพท์มือถือ	4.77	0.42	มากที่สุด
2.3 ระบบควบคุมยานพาหนะเข้า - ออก	4.80	0.41	มากที่สุด
รวม	**4.79**	**0.42**	**มากที่สุด**

ตารางที่ 4-6 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ			
3.1 การประสานความร่วมมือกับหน่วยงานด้านความมั่นคง	4.77	0.42	มากที่สุด
3.2 ฐานข้อมูลด้านความมั่นคง	4.80	0.41	มากที่สุด
รวม	**4.79**	**0.42**	**มากที่สุด**
ผลประเมินเฉลี่ยรวม	**4.78**	**0.43**	**มากที่สุด**

จากตารางที่ 4-6 ผลประเมินความเหมาะสมของการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.78, S.D. = 0.43) โดยการรักษาความปลอดภัยเกี่ยวกับสถานที่ และ การป้องกันและแก้ไขปัญหาด้านความไม่สงบมีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.79, S.D. = 0.42) และการรักษาความปลอดภัยเกี่ยวกับบุคคลมีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.76, S.D. = 0.44)

ตารางที่ 4-7 ผลประเมินความเหมาะสมของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้			
1. ระบบยืนยันตัวตน			
1.1 บัตรเข้าออก	4.80	0.41	มากที่สุด
1.2 ระบบตรวจจับใบหน้า	4.87	0.40	มากที่สุด
รวม	**4.84**	**0.41**	**มากที่สุด**
2. ระบบควบคุมการเข้า-ออกยานพาหนะ			
2.1 บัตรเข้าออก	4.76	0.44	มากที่สุด
2.2 ระบบอ่านป้ายทะเบียนรถ	4.87	0.40	มากที่สุด
รวม	**4.82**	**0.42**	**มากที่สุด**

ตารางที่ 4-7 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
3. ระบบตรวจจับและแจ้งเตือนภายในอาคาร			
4.1 ตรวจจับควันไฟ	4.77	0.42	มากที่สุด
4.2 ตรวจจับความร้อน	4.77	0.42	มากที่สุด
4.3 ตรวจจับก๊าซ	4.77	0.42	มากที่สุด
4.4 ตรวจจับแรงสั่นสะเทือน	4.77	0.42	มากที่สุด
รวม	**4.77**	**0.42**	**มากที่สุด**
4. ระบบฐานข้อมูลด้านความมั่นคง			
5.1 ระบบแจ้งเตือนผู้ต้องสงสัย	4.87	0.40	มากที่สุด
5.2 ระบบแจ้งเตือนรถต้องสงสัย	4.87	0.40	มากที่สุด
รวม	**4.87**	**0.40**	**มากที่สุด**
ผลประเมินเฉลี่ยรวม	**4.81**	**0.42**	**มากที่สุด**

จากตารางที่ 4-7 ผลประเมินความเหมาะสมผลประเมินความเหมาะสมของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.81, S.D. = 0.42) โดยระบบยืนยันตัวตน มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.84, S.D. = 0.41) ระบบควบคุมการเข้าออกยานพาหนะ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.82, S.D. = 0.42) ระบบตรวจจับและแจ้งเตือนภายในอาคาร มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.77, S.D. = 0.42) ระบบฐานข้อมูลด้านความมั่นคง มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.87, S.D. = 0.40)

ตารางที่ 4-8 ผลประเมินความเหมาะสมขององค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ผลการประเมิน**		
	$\bar{x}$	**S.D.**	**ความเหมาะสม**
องค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้			
1. องค์ประกอบด้านการรักษาความมั่นคงปลอดภัย	4.60	0.50	มากที่สุด
2. องค์ประกอบด้านเทคโนโลยีเชื่อมโยงสรรพสิ่ง (The Internet of Things : IoT)	4.64	0.49	มากที่สุด
2.1 กล้องตรวจจับ (Camera Sensors)	4.80	0.41	มากที่สุด
2.2 บัตรอาร์เอฟไอดี (RFID)	4.64	0.49	มากที่สุด
2.3 เซ็นเซอร์ตรวจจับ (Sensors Detector)	4.76	0.44	มากที่สุด
3. องค์ประกอบด้านการแสดงผลการแจ้งเตือน โดยเลือกใช้ Application Line ในการแจ้งความมั่นคงปลอดภัย	4.80	0.41	มากที่สุด
4. องค์ประกอบด้านการตรวจสอบหลักฐานดิจิทัล (Digital Forensic)	4.77	0.51	มากที่สุด
4.1 Data Acquisition การรวบรวมพยานหลักฐาน	4.76	0.44	มากที่สุด
4.2 Analysis การวิเคราะห์เพื่อประเมินความเสี่ยง	4.77	0.51	มากที่สุด
4.3 Reporting การรายงานความมั่งคงปลอดภัยสูงสำหรับสถานศึกษา	4.77	0.51	มากที่สุด
ผลประเมินเฉลี่ยรวม	**4.61**	**0.49**	**มากที่สุด**
มีความเหมาะสมในการนำไปใช้จริงอยู่ในระดับใด			
คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้	**4.52**	**0.51**	**มากที่สุด**

จากตารางที่ 4-8 ผลประเมินความเหมาะสมขององค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.61, S.D. = 0.49) และมีความเหมาะสมในการนำไปใช้จริงมีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.52, S.D. = 0.51)

4.2 ผลการพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

4.2.1 ผลประเมินความเหมาะสมของแบบจำลองการการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปได้ดังตารางที่ 4-9 ดังนี้

ตารางที่ 4-9 ผลประเมินความเหมาะสมของแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ผลการประเมิน**		
	$\bar{x}$	**S.D.**	**ความเหมาะสม**
1. มิติด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา			
1.1 การรักษาความปลอดภัยเกี่ยวกับบุคคล	5.00	0.00	มากที่สุด
1.2 การรักษาความปลอดภัยเกี่ยวกับสถานที่	5.00	0.00	มากที่สุด
1.3 การป้องกันและแก้ไขปัญหาด้านความไม่สงบ	5.00	0.00	มากที่สุด
รวม	**5.00**	**0.00**	**มากที่สุด**
2. มิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา			
2.1 เทคโนโลยีเชื่อมโยงสรรพสิ่ง	5.00	0.00	มากที่สุด
2.2 ระบบตรวจจับและรู้จำ	4.71	0.49	มากที่สุด
2.3 ระบบจัดการฐานข้อมูล	5.00	0.00	มากที่สุด
2.4 ระบบจัดการรายงาน	4.86	0.38	มากที่สุด
2.5 ระบบแสดงผลข้อมูล	4.71	0.49	มากที่สุด
2.6 ระบบแจ้งเตือน	5.00	0.00	มากที่สุด
รวม	**4.88**	**0.33**	**มากที่สุด**
3. มิติด้านการบริหารจัดการข้อมูล			
3.1 การแจ้งเตือน (Application Line)	4.86	0.38	มากที่สุด
3.2 การรายงานความเสี่ยง (Dash Board)	5.00	0.00	มากที่สุด
3.3 การบำรุงรักษาและตรวจสอบ (Maintain & Improve)	5.00	0.00	มากที่สุด
รวม	**4.93**	**0.19**	**มากที่สุด**
4.มิติด้านการตรวจสอบหลักฐานดิจิทัล			
4.1 การรวบรวมพยานหลักฐาน Data Acquisition	4.86	0.38	มากที่สุด

ตารางที่ 4-9 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
4.2 การวิเคราะห์เพื่อประเมินความเสี่ยง Analysis	5.00	0.00	มากที่สุด
4.3 การรายงานความมั่งคงปลอดภัย Reporting	5.00	0.00	มากที่สุด
รวม	**4.93**	**0.19**	**มากที่สุด**
ผลประเมินเฉลี่ยรวม	**4.94**	**0.17**	**มากที่สุด**

จากตารางที่ 4-9 ผลประเมินความเหมาะสมของแบบจำลองการการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.94, S.D. = 0.17) โดยมิติด้านการรักษาความปลอดภัยสำหรับสถานศึกษามีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 5.00, S.D. = 0.00) มิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษามีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.88, S.D. = 0.33) มิติด้านการบริหารจัดการข้อมูล มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.93, S.D. = 0.19) และ มิติด้านการตรวจสอบหลักฐานดิจิทัล มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.93, S.D. = 0.19)

4.3 ผลการออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ผลประเมินความเหมาะสมของสถาปัตยกรรมระบบการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปได้ดังตารางที่ 4-10 ดังนี้

ตารางที่ 4-10 ผลประเมินความเหมาะสมของสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ผลการประเมิน**		
	$\bar{x}$	**S.D.**	**ความเหมาะสม**
1. ผู้ที่เกี่ยวข้องกับระบบ (Stakeholders)			
1.1 ผู้บริหารระบบ (Administrators)	4.70	0.48	มากที่สุด
1.2 ผู้บริหารสถานศึกษา (CEO)	4.80	0.42	มากที่สุด
1.3 เจ้าหน้าที่รักษาความปลอดภัย (Staff)	4.70	0.67	มากที่สุด
1.4 ผู้ใช้งานระบบ (Users)	4.60	0.51	มากที่สุด
รวม	**4.70**	**0.52**	**มากที่สุด**
2. ไอโอทีดีไวซ์ สำหรับการตรวจจับบุคคลและวัตถุ			
2.1 กล้องตรวจจับใบหน้า	4.70	0.67	มากที่สุด
2.2 บัตร RFID	4.60	0.51	มากที่สุด
2.3 กล้องตรวจจับป้ายทะเบียน	4.60	0.69	มากที่สุด
2.4 เซนเซอร์ตรวจจับควัน	4.50	0.84	มากที่สุด
2.5 เซนเซอร์ตรวจจับความร้อน	4.30	0.82	มาก
2.6 เซนเซอร์ตรวจจับก๊าซ	4.40	0.84	มาก
2.7 เซนเซอร์ตรวจจับแรงสั่นสะเทือน	4.40	0.96	มาก
รวม	**4.50**	**0.76**	**มากที่สุด**
3. โมดูลย่อยของระบบ			
3.1 โมดูลตรวจจับใบหน้า	4.70	0.67	มากที่สุด
3.2 โมดูลสแกนบัตร	4.60	0.51	มากที่สุด
3.3 โมดูลตรวจจับป้ายทะเบียนรถ	4.60	0.69	มากที่สุด
3.4 โมดูลตรวจจับควันไฟ	4.50	0.84	มากที่สุด
3.5 โมดูลตรวจจับความร้อน	4.30	0.82	มาก
3.6 โมดูลตรวจจับก๊าซ	4.40	0.84	มาก
3.7 โมดูลตรวจจับแรงสั่นสะเทือน	4.40	0.96	มาก
รวม	**4.50**	**0.76**	**มากที่สุด**
4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย			
4.1 แจ้งเตือนผ่านไลน์แอพพลิเคชั่น Application Line	4.80	0.42	มากที่สุด
4.2 การประเมินและควบคุมความเสี่ยง Dashboard	4.80	0.42	มากที่สุด

ตารางที่ 4-10 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{X}$	S.D.	ความเหมาะสม
4.3 ระบบจัดการรายงาน Report Management System	4.70	0.67	มากที่สุด
รวม	**4.76**	**0.50**	**มากที่สุด**
5. เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)			
5.1 เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)	4.70	0.67	มากที่สุด
รวม	**4.70**	**0.67**	**มากที่สุด**
6. หลักการทำงานของสถาปัตยกรรมระบบ			
6.1 หลักการทำงานของระบบ	4.80	0.42	มากที่สุด
6.2 ความเหมาะสมของอุปกรณ์ตรวจจับ	4.80	0.42	มากที่สุด
6.3 ความเหมาะสมของระบบการแจ้งเตือน	4.70	0.67	มากที่สุด
6.4 ความเหมาะสมของระบบจัดเก็บข้อมูล	4.70	0.67	มากที่สุด
รวม	**4.70**	**0.50**	**มากที่สุด**
ผลประเมินเฉลี่ยรวม	**4.60**	**0.6**	**มากที่สุด**

จากตารางที่ 4-10 พบว่า ผลการประเมินการออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากผู้เชี่ยวชาญพบว่า ผลการประเมินอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ = 4.60, S.D. = 0.6) ซึ่งจากผลการประเมินใน 6 ด้าน ได้แก่ 1. ผู้ที่เกี่ยวข้องกับระบบพบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.70, S.D. = 0.52) 2. ไอโอทีดีไวท์สำหรับการตรวจจับบุคคลและวัตถุ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.76) 3. โมดูลย่อยของระบบ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.76) 4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.76, S.D. = 0.50) 5. เว็บเซิร์ฟเวอร์และดาด้าเบสเซิร์เวอร์ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.70, S.D. = 0.67) 6.หลักการทำงานของสถาปัตยกรรมระบบ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.70, S.D. = 0.50)

4.4 ผลการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ผลการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถแบ่งออกเป็น 2 ส่วน ได้แก่ (1) ผลการประเมินการออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ (2) ผลการประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ซึ่งมีรายละเอียดดังนี้

4.4.1 ผลการประเมินการออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้จากผู้เชี่ยวชาญ ดังตารางที่ 4-11

ตารางที่ 4-11 ผลประเมินการออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
1. ผู้ที่เกี่ยวข้องกับระบบ (Stakeholders)			
1.1 ผู้บริหารระบบ (Administrators)	4.80	0.42	มากที่สุด
1.2 ผู้บริหารสถานศึกษา (CEO)	4.90	0.31	มากที่สุด
1.3 เจ้าหน้าที่รักษาความปลอดภัย (Staff)	4.80	0.42	มากที่สุด
1.4 ผู้ใช้งานระบบ (Users)	4.80	0.42	มากที่สุด
1.5 บุคคลากรภายนอกด้านการรักษาความปลอดภัยสำหรับสถานศึกษา	4.70	0.48	มากที่สุด
รวม	**4.80**	**0.41**	**มากที่สุด**
2. ไอโอทีดีไวซ์ สำหรับการตรวจจับบุคคลและวัตถุ			
2.1 กล้องตรวจจับใบหน้า	4.70	0.67	มากที่สุด
2.2 บัตร RFID	4.60	0.51	มากที่สุด
2.3 กล้องตรวจจับป้ายทะเบียน	4.60	0.69	มากที่สุด
2.4 เซนเซอร์ตรวจจับควัน	4.70	0.67	มากที่สุด
2.5 เซนเซอร์ตรวจจับความร้อน	4.70	0.67	มากที่สุด
2.6 เซนเซอร์ตรวจจับก๊าซ	4.70	0.67	มากที่สุด
2.7 เซนเซอร์ตรวจจับแรงสั่นสะเทือน	4.70	0.67	มากที่สุด

ตารางที่ 4-11 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{X}$	S.D.	ความเหมาะสม
2.8 ความสะดวกในการปรับเปลี่ยนหรือเพิ่มอุปกรณ์ในอนาคตที่จะสนับสนุนการทำงานของระบบ	4.80	0.42	มากที่สุด
รวม	**4.50**	**0.70**	**มากที่สุด**
3. โมดูลย่อยของระบบรักษาความมั่นคงปลอดภัย HISMSystem			
3.1 โมดูลตรวจจับใบหน้า	4.86	0.38	มากที่สุด
3.2 โมดูลสแกนบัตร	4.86	0.38	มากที่สุด
3.3 โมดูลตรวจจับป้ายทะเบียนรถ	4.80	0.42	มากที่สุด
3.4 โมดูลตรวจจับควันไฟ	4.90	0.31	มากที่สุด
3.5 โมดูลตรวจจับความร้อน	4.80	0.42	มากที่สุด
3.6 โมดูลตรวจจับก๊าซ	4.80	0.42	มากที่สุด
3.7 โมดูลตรวจจับแรงสั่นสะเทือน	4.70	0.48	มากที่สุด
3.8 ความสะดวกในการเพิ่มขยายโมดูลในอนาคตที่จะสนับสนุนการทำงานของระบบ	4.80	0.42	มากที่สุด
รวม	**4.93**	**0.19**	**มากที่สุด**
4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย			
4.1 แจ้งเตือนผ่านไลน์แอพพลิเคชั่น Application Line	4.80	0.42	มากที่สุด
4.2 รายงานผลในรูปแบบกราฟแสดงผล Dashboard	4.90	0.31	มากที่สุด
4.3 ระบบจัดการรายงาน Report Management System	4.80	0.42	มากที่สุด
4.4 ความสะดวกในการเพิ่มส่วนการแจ้งเตือนและรายงานผล	4.80	0.42	มากที่สุด
รวม	**4.93**	**0.19**	**มากที่สุด**
5. เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)			
5.1 เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)	4.70	0.48	มากที่สุด
5.2 ความสะดวกในการเพิ่ม ขยาย หรือปรับปรุงเว็บเซิร์เวอร์และดาต้าเบสเซิร์ฟเวอร์ เพื่อรองรับการทำงานในอนาคตได้	4.80	0.42	มากที่สุด
รวม	**4.93**	**0.19**	**มากที่สุด**

ตารางที่ 4-11 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{X}$	S.D.	ความเหมาะสม
6. หลักการทำงานของระบบ			
6.1 หลักการทำงานของระบบ	4.70	0.48	มากที่สุด
6.2 ความเหมาะสมของอุปกรณ์ตรวจจับ	4.80	0.42	มากที่สุด
6.3 ความเหมาะสมของระบบการแจ้งเตือน	4.70	0.48	มากที่สุด
6.4 ความเหมาะสมของระบบจัดเก็บข้อมูล	4.80	0.42	มากที่สุด
6.5 ความสะดวกในการเพิ่ม ขยาย หรือปรับปรุงการทำงานของระบบ	4.70	0.48	มากที่สุด
6.6 มีแนวโน้มในการปรับปรุงระบบได้ง่ายและรวดเร็ว	4.80	0.42	มากที่สุด
รวม	**4.93**	**0.19**	**มากที่สุด**
ผลประเมินเฉลี่ยรวม	**4.94**	**0.17**	**มากที่สุด**

จากตารางที่ 4-11 พบว่า ผลการประเมินการออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากผู้เชี่ยวชาญ พบว่า ในภาพรวมอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ = 4.94, S.D. = 0.17) ซึ่งจากผลการประเมินใน 6 ด้าน ได้แก่ 1. ผู้ที่เกี่ยวข้องกับระบบพบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.80, S.D. = 0.42) 2. ไอโอทีดีไวท์สำหรับการตรวจจับบุคคลและวัตถุ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.70) 3. โมดูลย่อยของระบบ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19) 4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19) 5. เว็บเซิร์ฟเวอร์และดาด้าเบสเซิร์เวอร์ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19) 6. หลักการทำงานของระบบ มีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.94, S.D. = 0.17)

สรุปจากผลการประเมินการออกแบบระบบทำให้ทราบว่าการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ อยู่ในระดับความเหมาะสมมากที่สุดแสดงให้เห็นถึงความสามารถของระบบที่สามารถนำไปใช้ในการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้เสริมประสิทธิภาพด้านบริหารจัดการความมั่นคงปลอดภัยของสถานศึกษาให้เกิดประโยชน์สูงสุดจากผลการประเมินผู้วิจัยนำผลที่ได้ไปใช้การพัฒนาระบบ

4.4.2 ผลการประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้จากผู้เชี่ยวชาญ ดังตารางที่ 4-12

ตารางที่ 4-12 ผลประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ผลการประเมิน**		
	$\bar{x}$	**S.D.**	**ความเหมาะสม**
1. การประเมินโมดูลย่อย (Module Test) ของระบบ			
1.1 โมดูลการวางระบบโครงสร้างพื้นฐาน (Infrastructure Management System : IMS			
1.1.1 ความสามารถในการเพิ่มข้อมูล	4.72	0.45	มากที่สุด
1.1.2 ความสามารถในการลบข้อมูล	4.71	0.46	มากที่สุด
1.1.3 ความสามารถในการปรับปรุงข้อมูล	4.72	0.45	มากที่สุด
1.1.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
1.1.5 ความสามารถในการจัดเก็บข้อมูล	4.61	0.49	มากที่สุด
1.1.6 ความเหมาะสมของข้อมูลในโมดูล	4.49	0.68	มาก
รวม	**4.66**	**0.49**	**มากที่สุด**
1.2 โมดูลระบบตรวจจับใบหน้า (Face Detection System)			
1.2.1 ความสามารถในการเพิ่มข้อมูล	4.72	0.45	มากที่สุด
1.2.2 ความสามารถในการลบข้อมูล	4.61	0.49	มากที่สุด
1.2.3 ความสามารถในการปรับปรุงข้อมูล	4.61	0.49	มากที่สุด
1.2.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
1.2.5 ความสามารถในการจัดเก็บข้อมูล	4.61	0.49	มากที่สุด
1.2.6 ความเหมาะสมของข้อมูลในโมดูล	4.59	0.82	มากที่สุด
รวม	**4.64**	**0.53**	**มากที่สุด**
1.3 โมดูลระบบแสกนบัตร (RFID System)			
1.3.1 ความสามารถในการเพิ่มข้อมูล	4.18	0.57	มาก
1.3.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
1.3.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก

ตารางที่ 4-12 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{X}$	S.D.	ความเหมาะสม
1.3.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
1.3.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
1.3.6 ความเหมาะสมของข้อมูลในโมดูล	4.48	0.68	มาก
รวม	**4.52**	**0.60**	**มากที่สุด**
1.4 โมดูลตรวจจับป้ายทะเบียนรถ (License Plate Detection)			
1.4.1 ความสามารถในการเพิ่มข้อมูล	4.72	0.45	มากที่สุด
1.4.2 ความสามารถในการลบข้อมูล	4.61	0.49	มากที่สุด
1.4.3 ความสามารถในการปรับปรุงข้อมูล	4.61	0.49	มากที่สุด
1.4.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
1.4.5 ความสามารถในการจัดเก็บข้อมูล	4.61	0.49	มากที่สุด
1.4.6 ความเหมาะสมของข้อมูลในโมดูล	4.59	0.82	มากที่สุด
รวม	**4.64**	**0.53**	**มากที่สุด**
1.5 โมดูลตรวจจับความร้อน (Heat Detection System)			
1.5.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.68	มาก
1.5.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
1.5.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
1.5.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
1.5.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
1.5.6 ความเหมาะสมของข้อมูลในโมดูล	4.48	0.68	มาก
รวม	**4.53**	**0.66**	**มากที่สุด**
1.6 โมดูลตรวจจับความควัน (Smoke Detection System)			
1.6.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.82	มาก
1.6.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
1.6.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
1.6.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
1.6.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
1.6.6 ความเหมาะสมของข้อมูลในโมดูล	4.58	0.82	มากที่สุด
รวม	**4.55**	**0.71**	**มากที่สุด**

ตารางที่ 4-12 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{X}$	S.D.	ความเหมาะสม
1.7 โมดูลตรวจจับก๊าซ (Gas Detection System)			
1.7.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.82	มาก
1.7.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
1.7.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
1.7.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
1.7.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
1.7.6 ความเหมาะสมของข้อมูลในโมดูล	4.31	0.65	มาก
รวม	**4.50**	**0.68**	**มากที่สุด**
1.8 โมดูลตรวจจับแรงสั่นสะเทือน (Vibration Detection System)			
1.8.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.82	มาก
1.8.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
1.8.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
1.8.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
1.8.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
1.8.6 ความเหมาะสมของข้อมูลในโมดูล	4.58	0.82	มาก
รวม	**4.55**	**0.71**	**มากที่สุด**
1.9 โมดูลการแจ้งเตือน (Notification)			
1.9.1 ความสามารถในการแสดงผล	4.80	0.40	มากที่สุด
1.9.2 ความเหมาะสมของข้อมูลในโมดูล	4.71	0.46	มากที่สุด
รวม	**4.75**	**0.43**	**มากที่สุด**
1.10 โมดูลการประเมินและควบคุมความเสี่ยง (Risk Assessment & Control)			
1.10.1 ความสามารถในการแสดงผล	4.80	0.40	มากที่สุด
1.10.2 ความเหมาะสมของข้อมูลในโมดูล	4.72	0.45	มากที่สุด
รวม	**4.76**	**0.42**	**มากที่สุด**
ผลรวม	**4.61**	**0.57**	**มากที่สุด**

ตารางที่ 4-12 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{X}$	S.D.	ความเหมาะสม
2. การประเมินการทำงานของระบบทั้งหมด (System Test)			
2.1 ความสามารถในการพิสูจน์ตัวตน (Authentication)	4.80	0.40	มากที่สุด
2.2 ความสามารถของระบบจัดเก็บข้อมูล	4.70	0.64	มากที่สุด
2.3 ความสามารถของความสัมพันธ์ในแต่ละรบบงานย่อยในการใช้ข้อมูลร่วมกัน	4.80	0.40	มากที่สุด
2.4 ความสามารถในการลดเวลาและทรัพยากรในการทำงาน	4.70	0.46	มากที่สุด
2.5 ความครบถ้วนของฟังก์ชันการทำงานของระบบ	4.60	0.49	มากที่สุด
2.6 ความสามารถเชื่อมต่อประสาน (Plug) ส่วนเพิ่มเติม	4.70	0.46	มากที่สุด
2.7 มีแนวโน้มในการปรับปรุงระบบได้ง่ายและรวดเร็ว	4.70	0.46	มากที่สุด
รวม	**4.70**	**0.40**	**มากที่สุด**
3. การประเมินการใช้งานระบบ (Usability Test)			
3.1 ความง่ายและความสะดวกในการใช้งานระบบ	4.90	0.30	มากที่สุด
3.2 ความเหมาะสมของตำแหน่งการจัดวางส่วนต่าง ๆ บนจอภาพ	4.50	0.50	มากที่สุด
3.3 การแบ่งเมนูของระบบสามารถเข้าใจได้ง่าย	4.50	0.50	มากที่สุด
3.4 ความชัดเจนของข้อความที่แสดงบนจอภาพ	4.60	0.49	มากที่สุด
3.5 ความเหมาะสมของตัวอักษรเกี่ยวกับขนาด สี ความชัดเจนง่าย ต่อการอ่าน	4.40	0.66	มาก
3.6 ความเหมาะสมของปริมาณข้อมูลที่นำเสนอในแต่ละหน้าจอ	4.50	0.50	มากที่สุด
3.7 ความเหมาะสมในการตอบสนองระบบในภาพรวม	4.70	0.46	มากที่สุด
รวม	**4.58**	**0.48**	**มากที่สุ**
4. การประเมินความปลอดภัยของระบบ (Security Test)			
4.1 การตรวจสอบสิทธิ์ในการเข้าใช้งานของผู้ใช้ระบบ	4.60	0.52	มากที่สุด
4.2 การแจ้งเตือนเมื่อพบข้อผิดพลาดในการเข้าใช้งาน	4.80	0.40	มากที่สุด
4.3 ความเหมาะสมในการรักษาความปลอดภัยของระบบโดยภาพรวม	4.60	0.49	มากที่สุด
รวม	**4.66**	**0.47**	มากที่สุด
ผลประเมินเฉลี่ยรวม	**4.63**	**0.48**	**มากที่สุด**

จากตารางที่ 4-12 พบว่า ผลการประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากผู้เชี่ยวชาญพบว่าในภาพรวมอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ = 4.63, S.D. = 0.48) ซึ่งจากผลการประเมินใน 4 ด้าน ได้แก่ 1. การประเมินโมดูลย่อย (Module Test) ของระบบ พบว่ามีค่าเฉลี่ยระบดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.61, S.D. = 0.57) 2. การประเมินการทำงานของระบบทั้งหมด (System Test) พบว่ามีค่าเฉลี่ยระบดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.0, S.D. = 0.40) 3. การประเมินการใช้งานระบบ (Usability Test) พบว่ามีค่าเฉลี่ยระบดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.58, S.D. = 0.48) และ 4. การประเมินความปลอดภัยของระบบ (Security Test) พบว่ามีค่าเฉลี่ยระบดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.66, S.D. = 0.47)

สรุปจากผลจากการประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แสดงให้เห็นถึงความสามารถของระบบที่พัฒนาขึ้นด้วยเทคโนโลยีสารสนเทศ และมีการนำเทคโนโลยีอินเทอร์เน็ตออฟธิงส์มาใช้เพื่อสนับสนุนการทำงานของระบบและการนำเทคโนโลยีการแจ้งเตือนเพื่อแสดงผลการรายงานความเสี่ยง และมีการออกแบบตามหลักการออกแบบส่วนต่อประสานผู้ใช้ (Graphical User Interface : GUI) ทำให้ระบบง่ายต่อการใช้งานเข้าใจง่าย ระบบมีความยืดหยุ่นและผู้วิจัยใช้วิธีการแบบแบล็คบ๊กซ์ (Black-Box Testing) ซึ่งเป็นการตรวจสอบกระบวนการการทำงานของฟังก์ชันงานระบบทั้งหมด เพื่อตรวจสอบหาข้อผิดพลาดของระบบแล้วนำมาแก้ไขปรับปรุงให้ระบบมีความสมบูรณ์มากยิ่งขึ้นส่งผลให้การประเมินระบบมีความเหมาะสมอยู่ในระดับมากที่สุด ส่งผลให้ระบบที่พัฒนาขึ้นสามารถเข้ามาช่วยในการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ในการรักษาความปลอดภัยเกี่ยวกับบุคคล การรักษาความปลอดภัยเกี่ยวกับสถานที่ ฐานข้อมูลแจ้งเตือนด้านความมั่นคง สามารถเสริมประสิทธิภาพด้านบริหารจัดการความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

4.5 ผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้จากผู้ใช้งานระบบ ดังตารางที่ 4-13

ตารางที่ 4-13 ผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ผลการประเมิน**		
	$\bar{x}$	**S.D.**	**ความเหมาะสม**
1. โมดูลการวางระบบโครงสร้างพื้นฐาน (Infrastructure Management System : IMS			
1.1 ความสามารถในการเพิ่มข้อมูล	4.72	0.45	มากที่สุด
1.2 ความสามารถในการลบข้อมูล	4.71	0.46	มากที่สุด
1.3 ความสามารถในการปรับปรุงข้อมูล	4.72	0.45	มากที่สุด
1.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
1.5 ความสามารถในการจัดเก็บข้อมูล	4.61	0.49	มากที่สุด
1.6 ความเหมาะสมของข้อมูลในโมดูล	4.49	0.68	มาก
รวม	**4.66**	**0.49**	**มากที่สุด**
2. โมดูลระบบตรวจจับใบหน้า (Face Detection System)			
2.1 ความสามารถในการเพิ่มข้อมูล	4.72	0.45	มากที่สุด
2.2 ความสามารถในการลบข้อมูล	4.61	0.49	มากที่สุด
2.3 ความสามารถในการปรับปรุงข้อมูล	4.61	0.49	มากที่สุด
2.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
2.5 ความสามารถในการจัดเก็บข้อมูล	4.61	0.49	มากที่สุด
2.6 ความเหมาะสมของข้อมูลในโมดูล	4.59	0.82	มากที่สุด
รวม	**4.64**	**0.53**	**มากที่สุด**
3 โมดูลระบบแสกนบัตร (RFID System)			
3.1 ความสามารถในการเพิ่มข้อมูล	4.18	0.57	มาก
3.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
3.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
3.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
3.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
3.6 ความเหมาะสมของข้อมูลในโมดูล	4.48	0.68	มาก

ตารางที่ 4-13 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
รวม	**4.52**	**0.60**	**มากที่สุด**
4 โมดูลตรวจจับป้ายทะเบียนรถ (License Plate Detection)			
4.1 ความสามารถในการเพิ่มข้อมูล	4.72	0.45	มากที่สุด
4.2 ความสามารถในการลบข้อมูล	4.61	0.49	มากที่สุด
4.3 ความสามารถในการปรับปรุงข้อมูล	4.61	0.49	มากที่สุด
4.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.72	0.45	มากที่สุด
4.5 ความสามารถในการจัดเก็บข้อมูล	4.61	0.49	มากที่สุด
4.6 ความเหมาะสมของข้อมูลในโมดูล	4.59	0.82	มากที่สุด
รวม	**4.64**	**0.53**	**มากที่สุด**
5 โมดูลตรวจจับความร้อน (Heat Detection System)			
5.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.68	มาก
5.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
5.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
5.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
5.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
5.6 ความเหมาะสมของข้อมูลในโมดูล	4.48	0.68	มาก
รวม	**4.53**	**0.66**	**มากที่สุด**
6 โมดูลตรวจจับความควัน (Smoke Detection System)			
6.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.82	มาก
6.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
6.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
6.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
6.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
6.6 ความเหมาะสมของข้อมูลในโมดูล	4.58	0.82	มากที่สุด
รวม	**4.55**	**0.71**	**มากที่สุด**
7 โมดูลตรวจจับก๊าซ (Gas Detection System)			
7.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.82	มาก
7.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
7.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก

ตารางที่ 4-13 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
7.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
7.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
7.6 ความเหมาะสมของข้อมูลในโมดูล	4.31	0.65	มาก
รวม	**4.50**	**0.68**	**มากที่สุด**
8 โมดูลตรวจจับแรงสั่นสะเทือน (Vibration Detection System)			
8.1 ความสามารถในการเพิ่มข้อมูล	4.48	0.82	มาก
8.2 ความสามารถในการลบข้อมูล	4.58	0.82	มากที่สุด
8.3 ความสามารถในการปรับปรุงข้อมูล	4.48	0.68	มาก
8.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข	4.48	0.68	มาก
8.5 ความสามารถในการจัดเก็บข้อมูล	4.72	0.45	มากที่สุด
8.6 ความเหมาะสมของข้อมูลในโมดูล	4.58	0.82	มาก
รวม	**4.55**	**0.71**	**มากที่สุด**
9 โมดูลการแจ้งเตือน (Notification)			
9.1 ความสามารถในการแสดงผล	4.80	0.40	มากที่สุด
9.2 ความเหมาะสมของข้อมูลในโมดูล	4.71	0.46	มากที่สุด
รวม	**4.75**	**0.43**	**มากที่สุด**
10 โมดูลการประเมินและควบคุมความเสี่ยง (Risk Assessment & Control)			
10.1 ความสามารถในการแสดงผล	4.80	0.40	มากที่สุด
10.2 ความเหมาะสมของข้อมูลในโมดูล	4.72	0.45	มากที่สุด
รวม	**4.76**	**0.42**	**มากที่สุด**
11. ภาพรวมของผลการใช้ระบบ			
11.1 ความง่ายและสะดวกในการใช้งานระบบ	4.80	0.40	มากที่สุด
11.2 ความเหมาะสมของตำแหน่งการจัดวางส่วนต่าง ๆ บนจอภาพ	4.58	0.82	มากที่สุด
11.3 การแบ่งเมนูของระบบสามารถเข้าใจได้ง่าย	4.48	0.50	มาก
11.4 ความชัดเจนของข้อความที่แสดงบนจอภาพ	4.72	0.45	มากที่สุด
11.5 ความเหมาะสมของตัวอักษรเกี่ยวกับขนาด สี ความชัดเจน ง่าย ต่อการอ่าน	4.55	0.71	มากที่สุด

ตารางที่ 4-13 (ต่อ)

รายการประเมิน	ผลการประเมิน		
	$\bar{x}$	S.D.	ความเหมาะสม
11.6 ความเหมาะสมของปริมาณข้อมูลที่นำเสนอในแต่ละหน้าจอ	4.58	0.82	มากที่สุด
11.7 ความเหมาะสมในการตอบสนองระบบในภาพรวม	4.68	0.46	มากที่สุด
รวม	**4.62**	**0.59**	**มากที่สุด**
ผลประเมินเฉลี่ยรวม	**4.94**	**0.17**	**มากที่สุด**

จากตารางที่ 4-13 พบว่า ผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากผู้ใช้ระบบ พบว่ามีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.94, S.D. = 0.17) ที่ประกอบด้วย 1) การวางระบบโครงสร้างพื้นฐาน 2) ระบบตรวจจับใบหน้า 3) ระบบสแกนบัตร 4) ตรวจจับป้ายทะเบียนรถ 5) ตรวจจับความร้อน 6) ตรวจจับควัน 7) ตรวจจับก๊าซ 8) ตรวจจับแรงสั่นสะเทือน 9) การแจ้งเตือน 10) การประเมินและควบคุมความเสี่ยง 11) ภาพรวมของผลการใช้ระบบ

สรุปจากผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากผู้ใช้ระบบ พบว่ามีความเหมาะสมอยู่ในระดับมากที่สุด เนื่องจากผู้ใช้ระบบเกิดความสะดวกต่อการใช้งานระบบ กระบวนการทำงานของระบบที่ไม่ซับซ้อน สามารถเข้าถึงข้อมูลได้ง่าย ด้วยเทคโนโลยีไร้สายที่ผู้ใช้ระบบส่วนใหญ่มักคุ้นชินกับการทำงานในชีวิตประจำวัน และผู้ใช้ระบบมีทักษะการใช้เทคโนโลยีและมีความตระหนักเนื่องจากนโยบายและการให้ความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ความพึงพอใจของผู้ใช้ต่อการใช้งานระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ พบว่า ผู้ใช้มีความพึงพอใจอยู่ในระดับมากที่สุด เนื่องจากผู้ใช้ระบบเกิดความสะดวกต่อการใช้งานระบบ กระบวนการทำงานของระบบที่ไม่ซันซ้อน สามารถเข้าถึงข้อมูลได้ง่ายด้วยเทคโนโลยีไร้สายที่ผู้ใช้ระบบส่วนใหญ่มักคุ้นชินกับการทำงานในชีวิตประจำวัน ผู้ใช้มีความตระหนักเนื่องจากนโยบายและการให้ความสำคัญเกี่ยวกับรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้ใช้มีความรู้สึกถึงความปลอดภัยเพิ่มขึ้น เนื่องจากระบบมีการแจ้งเตือนความมั่นคงปลอดภัยทำให้ผู้ใช้สามารถวิเคราะห์และตัดสินใจได้ทันทวงทีในการวางแผนการเดินทางไปยังสถานที่เมื่อเกิดเหตุการณ์ความไม่ปลอดภัย

บทที่ 5
ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้

ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีรายละเอียดดังนี้

5.1 บทนำ

5.2 ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

5.3 การนำระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ไปใช้

5.1 บทนำ

5.1.1 ความเป็นมา เหตุผลและความจำเป็นในการพัฒนาระบบ

จากการวิเคราะห์การรักษาความมั่นคงปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ การสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญ การสอบถามจากผู้เชี่ยวชาญ เกี่ยวกับความปลอดภัยของสถานศึกษาในจังหวัดชายแดนภาคใต้ และการศึกษาเอกสารและ งานวิจัยที่เกี่ยวข้องกับการพัฒนารักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

เนื่องจากปัญหาจากความไม่สงบในเขตพื้นที่จังหวัดชายแดนภาคใต้ การรักษาความปลอดภัยของสถานศึกษา เมื่อพิจารณาแล้วพบว่า การรักษาความปลอดภัยของสถานศึกษาใจจังหวัดชายแดนภาคใต้ ยังคงใช้การเฝ้าระวังด้วยเจ้าหน้าที่ของรัฐไม่ว่าจะเป็น ตำรวจ และ ทหาร คอยเฝ้าสังเกตการณ์และไม่มีการใช้เทคโนโลยีทางด้านการรักษาความปลอดภัย ทำให้ไม่มีการเตือนภัยล่วงหน้าหรือบ่งบอกถึงความเสี่ยงที่จะเกิดขึ้นได้ เพื่อกำจัดปัญหาที่เกิดจากการรักษาความปลอดภัยด้วยเหตุนี้ การจัดการบริหารข้อมูลการรักษาความมั่นคงปลอดภัย โดยใช้ ระบบรักษาความมั่นคงปลอดภัยด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่ง การจัดเก็บข้อมูลโดยใช้ฐานมูล การแจ้งเตือนภัยตลอดทันทีทันได้ สามารถช่วยรวมรวมข้อมูลทางด้านความมั่นคงปลอดภัยให้อยู่ในแหล่งเดียวกันอย่างเป็นระบบ อีกทั้งยังช่วยในเรื่องของการวิเคราะห์พยานหลักฐานที่สามารถสรุปหรือจัดทำสถิติที่สำคัญและเป็น

ประโยชน์ให้แก่สถาบันการศึกษาเป็นการจัดเก็บเพื่ออำนวยความสะดวกเรื่องการสืบค้นข้อมูลที่ต้องการทราบในภายหลังได้

เทคโนโลยีเชื่อมโยงสรรพสิ่ง (Internet of Things : IoT) ในทุกวันนี้เทคโนโลยีเข้ามามีบทบาทในกรใช้ชีวิตประจำวันของเรามากขึ้น ไม่ว่าจะเป็น โทรศัพท์มือถือ สมาร์ทโฟน แท็บเล็ต ยานพาหนะ หรือแม้กระทั้งเครื่องใช้ไฟฟ้าในบ้าน ที่มีการพัฒนาให้ฉลาดและอัจฉริยะ สามารถตอบสนองอำนวยความสะดวกต่อผู้ใช้มากขึ้น แนวคิด IoT ที่ย่อมาจาก Internet of Thing เป็นเทคโนโลยีถูกผนวกเข้าไปในทุกสิ่ง ทำให้มนุษย์สามารถสั่งการควบคุมการใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต ทำให้เกิดบริการดิทัล (Digital Service) ที่มีระบบอัจฉริยะอยู่เบื้องหลัง ซึ่งเทคโนโลยี IoT มีความจำเป็นต้องทำงานร่วมกับอุปกรณ์ประเภท RFID และ Sensors ร่วมกับเครือข่ายอินเทอร์เน็ต เพื่อให้อุปกรณ์สามารถรับส่งข้อมูลถึงกันได้ ทำให้การใช้ชีวิตประจำวันเกิดความสะดวกสบายและปลอดภัยมากขึ้น

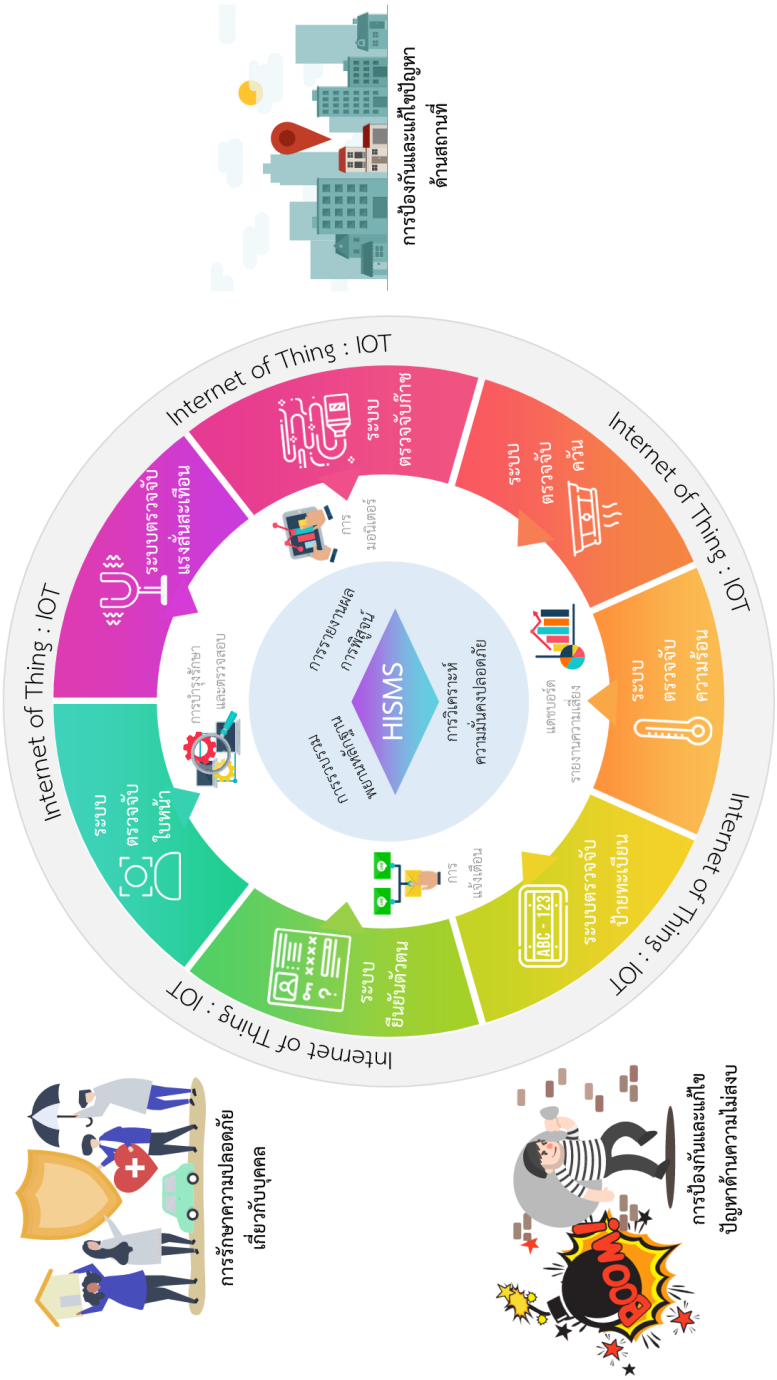
ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ในงานวิจัยนี้ ออกแบบโดยการนำแนวคิดของเทคโนโลยีเชื่อมโยงสรรพสิ่งและการพัฒนาระบบสารสนเทศเพื่อให้เกิดระบบแจ้งเตือนสถานะความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยพัฒนาระบบออกเป็น 3 ส่วน คือ 1) ส่วนตรวจจับ (Detection) หรือ ไอโอทีดีไวซ์ (IoT Device) เป็นอุปกรณ์สำหรับการตรวจจับบุคคลหรือวัตถุเพื่อใช้ในการตรวจสอบความปลอดภัยเพื่อดำเนินการเชื่อมต่อกับระบบในส่วนที่ 2 2) ส่วนตรวจสอบและตัดสินใจ (Process and Decision) เป็นส่วนของการตรวจสอบความมั่นคงปลอดภัยของระบบซึ่งจะประกอบไปด้วยโมดูลย่อย ๆ สำหรับการดำเนินการประมวลผลและตัดสินใจ 3) ส่วนบันทึกและแจ้งเตือน (Notification) ในส่วนนี้ระบบจะทำการบันทึกข้อมูลลงในระบบฐานข้อมูลและจะทำการแจ้งเตือนข้อมูลความไม่ปลอดภัยผ่านทาง Application Line 4) ส่วนแสดงผลและรายผลความมั่นคงปลอดภัยสำหรับสถานศึกษา (Report) ในส่วนนี้ระบบได้เลือกใช้การแสดงผลด้วย Dashboard ซึ่งเป็นการแสดงผลข้อมูลสรุปแบบ Executive ในมุมมองทางด้านความปลอดภัยในแต่ละส่วน เพื่อให้สามารถดูข้อมูลเพื่อวิเคราะห์ความเสี่ยงได้ง่ายขึ้น และได้เห็นการเปลี่ยนแปลงของข้อมูลได้ตลอดทุกที่ทุกเวลา

การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถตอบสนองความเป็นสถานบันการศึกษาที่มีการรักษาความมั่นคงปลอดภัยสูงได้ จะต้องมีเทคโนโลยีที่นำมาใช้ในกระบวนการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ซึ่งเทคโนโลยีรักษาความปลอดภัยที่ผนวกกับเทคโนโลยี Internet of Things จึงมีส่วนสำคัญที่จะทำให้ ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สอดรับการทำงาน

กระบวนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาให้เกิดประโยชน์สูงสุด เป็นผลให้สามารถวิเคราะห์ และ ตัดสินใจได้อย่างทันท่วงที ผู้วิจัยจึงนำแนวคิด และจุดเด่นของเทคโนโลยี Internet of Things มาพัฒนาเป็นระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

5.2 ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

5.2.1 แบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้ ดังภาพที่ 5-1



ภาพที่ 5-1 แบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

จากภาพที่ 5-1 แบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลในสถานศึกษาจังหวัดชายแดนภาคใต้ (Hight Integrated Security Management System Model Base on The Internet of Things) แสดงให้เห็นกลยุทธ์และเทคโนโลยีสนับสนุนที่นำมาประยุกต์ใช้เพื่อให้เข้ากับแนวทางในการพัฒนาระบบรักษาความมั่นคงปลอดภัย (Hight Integrated Security Management System : HISMS) เพื่อใช้ในการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา โดยแบบจำลองนี้แบ่งออกเป็น 4 มิติ มีรายละเอียดดังนี้

5.2.1.1 มิติด้านกระบวนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วย

5.2.1.1.1 การรักษาความมั่นคงปลอดภัยสำหรับบุคคล

5.2.1.1.2 การรักษาความมั่นคงปลอดภัยเกี่ยวกับสถานที่

5.2.1.1.3 การป้องกันและแก้ไขปัญหาด้านความไม่สงบ

5.2.1.2 มิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนกลยุทธ์ ประกอบด้วย

5.2.1.2.1 เทคโนโลยีเชื่อมโยงสรรพสิ่ง (The Internet of Things Technology คือ เทคโนโลยีอินเทอร์เน็ตที่ใช้ในการติดต่อสื่อสารระหว่างอุปกรณ์ตรวจจับกับระบบรักษาความมั่นคงปลอดภัย โดยสามารถเชื่อมต่อสื่อสารกันได้เองระหว่างสิ่งที่ตรวจจับด้วยกันและระบุข้อมูลต่าง ๆ ที่มีความเกี่ยวข้องกับความมั่นคงปลอดภัย ซึ่งได้แก่ อุปกรณ์กล้องตรวจจับ บัตร RFID อุปกรณ์เซนเซอร์ตรวจจับต่าง ๆ ซึ่งมีการเชื่อมต่ออินเทอร์เน็ตและติดต่อสื่อสารกันได้เองอัตโนมัติก็จะส่งผลให้การทำงานมีความสะดวกรวดเร็วง่ายต่อการใช้งาน

5.2.1.2.2 ระบบตรวจจับใบหน้า (Face Detection)

5.2.1.2.3 ระบบสแกนบัตร (RFID Card)

5.2.1.2.4 ระบบตรวจจับป้ายทะเบียน (License Plate Detection)

5.2.1.2.5 ระบบตรวจจับความร้อน (Heat Detection)

5.2.1.2.6 ระบบตรวจจับควัน (Smoke Detection)

5.2.1.2.7 ระบบตรวจจับก๊าซ (Gas Detection)

5.2.1.2.8 ระบบตรวจจับแรงสั่นสะเทือน (Vibration Detection)

5.2.1.3 มิติด้านการบริหารจัดการความมั่นคงปลอดภัย

5.2.1.3.1 ระบบแจ้งเตือน (Notification)

5.2.1.3.2 ระบบรายงานความเสี่ยง

5.2.1.3.3 ระบบจัดการฐานข้อมูล

5.2.1.3.4 การบำรุงรักษาและตรวจสอบ

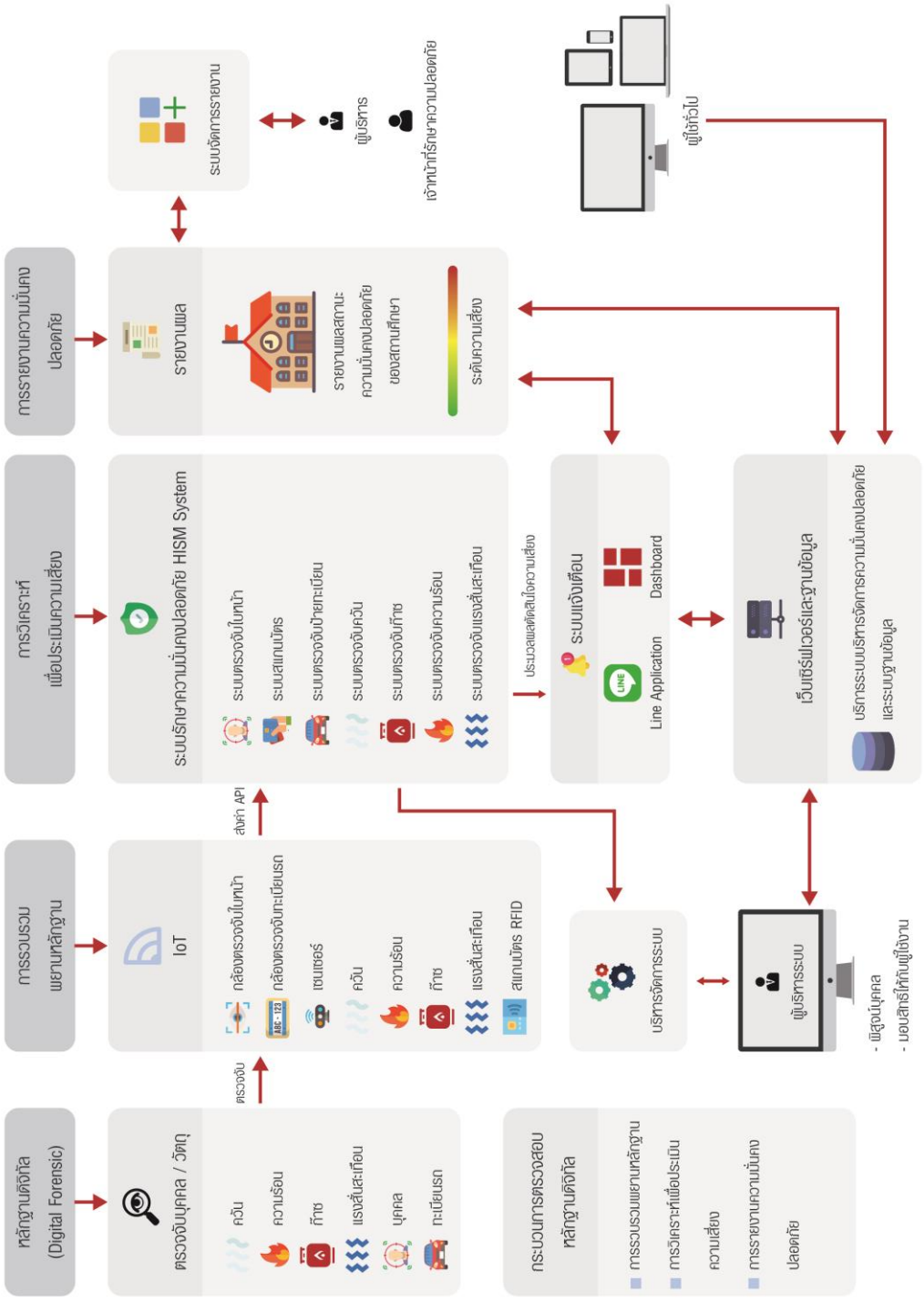
5.2.1.4 มิติด้านผลการพิสูจน์หลักฐานดิจิทัล

5.2.1.4.1 การรวบรวมพยานหลักฐาน

5.2.1.4.2 การวิเคราะห์เพื่อประเมินความเสี่ยง

5.2.1.4.3 การรายงานความมั่นคงปลอดภัย

5.2.2 สถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ภาพที่ 5-2



ภาพที่ 5-2 สถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

จากภาพที่ 5-2 สถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แสดงให้เห็นถึงหน้าที่ขององค์ประกอบภายในสถาปัตยกรรมและการสื่อสารในระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แบ่งออกเป็น 4 ส่วนหลัก ดังนี้

5.2.2.1 ส่วนของผู้ที่เกี่ยวข้องกับระบบ เมื่อใช้งานระบบจะต้องผ่านการพิสูจน์ตัวบุคคล (Authentication) และมอบสิทธิให้กับผู้ใช้งาน (Authorization) ก่อนถึงจะสามารถเข้าใช้งานระบบตามสิทธิ์ที่ตัวเองได้รับ แบ่งออกเป็น 2 กลุ่ม ดังนี้

5.2.2.1.1 ผู้บริหารระบบ (Administrators) คือ ผู้ที่ทำหน้าที่วางแผน ควบคุม และจัดการระบบ HISMS ทั้งหมด โดยจัดการข้อมูลพื้นฐานที่จำเป็นให้กับผู้ใช้งาน นอกจากนี้ยังสามารถออกกฎต่าง ๆ ในการใช้งานระบบ มอบสิทธิ์ (Authorization) หรือยกเลิกสิทธิ์ให้กับผู้ใช้งาน

5.2.2.1.2 ผู้ใช้งานระบบ (User) คือ กลุ่มของผู้ใช้งานที่ผู้บริหารระบบได้กำหนดสิทธิ์ในการเข้าถึงข้อมูลภายในระบบ ซึ่งในแต่ละกลุ่มมีสิทธิ์แตกต่างกันตามหน้าที่และคุณลักษณะของผู้ใช้งาน แบ่งออกเป็น 3 กลุ่ม ดังนี้

ก) ผู้บริหาร (Chief Executive Officer : CEO) คือ ผู้บริหารของสถานศึกษาแต่ละแห่งที่สามารถเข้าถึงข้อมูล (Data) ได้ทุกส่วนภายในระบบ รวมถึงรายงานความมั่นคงปลอดภัยของสถานศึกษาแล้วนำสารสนเทศ (Information) ที่ได้ไปช้สนับสนุนการตัดสินใจหรือวางแผนกลยุทธ์ในด้านต่าง ๆ

ข) เจ้าหน้าที่รักษาความปลอดภัย คือ ผู้ปฏิบัติงานที่ทำหน้าที่จัดการความปลอดภัย โดยมีภาระงานหลักคือ ควบคุมและบันทึกข้อมูลด้านความปลอดภัย

ค) ผู้ใช้ทั่วไป ผู้ที่เข้าใช้งานระบบเพื่อดูสถานะความปลอดภัยสำหรับสถานศึกษา แต่ไม่สามารถทำการแก้ไขข้อมได้นอกจากการได้สิทธิ์จากผู้ดูแลระบบ

5.2.2.2 ส่วนของอุปกรณ์ตรวจสอบหรือไอโอทีดีไวซ์ (IoT Device) ทำหน้าที่หลักเป็นอุปกรณ์ที่ใช้ในการตรวจจับข้อมูลเพื่อทำการส่งค่าข้อมูลที่ได้ไปทำการตรวจสอบความปลอดภัย เครื่องมือสำหรับการติดต่อสารแบบเทคโนโลยีเชื่อมโยงสรรพสิ่ง (IoT) ประกอบด้วย

5.2.2.2.1 กล้องตรวจจับ (Camera Sensors) เป็นอุปกรณ์ที่ใช้สำหรับการตรวจจับรูปลักษณ์ใบหน้าของบุคคล และ ป้ายทะเบียนรถ เพื่อใช้ตรวจสอบและยืนยันข้อมูลดังกล่าว

5.2.2.2.2 บัตรอาร์เอฟไอดี (RFID) เป็นบัตรประจำตัวของบุคคลภายใน เพื่อตรวจสอบและยืนยันข้อมูลดังกล่าว

5.2.2.2.3 เซนเซอร์ตรวจจับ (Sensors) เป็นอุปกรณ์ตรวจจับปริมาณของวัตถุ ได้แก่ ควัน ความร้อน ก๊าซ และแรงสั่นสะเทือน เป็นต้น

5.2.2.3 ส่วนของระบบ HISMS เป็นระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ซึ่งสามารถทำงานได้บนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่หลายประเภท โดยที่ระบบจะมีหน้าที่ตรวจสอบข้อมูลที่ถูกส่งมาจากอุปกรณ์ IoT Device เพื่อทำการตรวจสอบ บันทึกผล และตัดสินใจเกี่ยวกับความปลอดภัย ในการตรวจจับข้อมูลรูปลักษณ์บุคคล ทะเบียนรถ และปริมาณของวัตถุ โดยแบ่งเป็นระบบการทำงานย่อย 7 โมดูล ได้แก่

5.2.2.3.1 ระบบตรวจจับใบหน้า เป็นโมดูลการตรวจจับและตรวจสอบบุคคล ประกอกด้วย

ก) บุคคลภายใน คือ ผู้บริหาร อาจารย์ เจ้าหน้าที่ และนักเรียนนักศึกษา เพื่อทำการยืนยันตัวตน เมื่อระบบทำการตรวจจับและตรวจจอบแล้วพบข้อมูลที่ได้มีการจัดเก็บข้อมูลไว้ในระบบฐานข้อมูล ระบบจะทำการจัดเก็บบันทึกข้อมูลเข้า ออก พร้อมแสดงรายงานการเข้าออก

ข) บุคคลภายนอก คือ บุคคลที่ไม่ได้มีการจัดเก็บข้อมูลไว้ในระบบฐานข้อมูล ระบบจะทำการบันทึกข้อมูลการเข้าออกของบุคคลและแสดงรายงานการเข้าออก

ค) บุคคลต้องสงสัย คือ บุคคลที่มีข้อมูลอยู่ในฐานข้อมูลด้านความมั่นคงที่มีการออกหมายจับดำเนินคดีด้านความมั่นคง เมื่อระบบสามารถตรวจสอบพบบุคคลต้องสงสัยดังกล่าว ระบบจะดำเนินแจ้งเตือนไปยังระบบแจ้งเตือนด้านความมั่นคงปลอดภัยผ่านทางแอพพลิเคชั่นแจ้งเตือน หรือ Line Notification และแสดงสถานะความเสี่ยงที่เกิดขึ้นจากรายงานวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสถานศึกษา

5.2.2.3.2 ระบบสแกนบัตร เป็นโมดูลการสแกนบัตรประจำตัวของบุคคลกรและนักศึกษา เพื่อทำการตรวจสอบและยืนยันตัวตนโดยการใช้บัตร RFID

5.2.2.3.3 ระบบตรวจจับป้ายทะเบียน คือ เป็นโมดูลการตรวจจับและตรวจสอบทะเบียนรถ ประกอบด้วย

ก) ทะเบียนรถบุคคลภายใน คือ ยานพาหนะของ ผู้บริหาร อาจารย์ เจ้าหน้าที่ และนักเรียนนักศึกษา เพื่อทำการยืนยันตัวตน เมื่อระบบทำการตรวจจับและตรวจจอบแล้วพบข้อมูลที่ได้มีการจัดเก็บข้อมูลไว้ในระบบฐานข้อมูล ระบบจะทำการจัดเก็บบันทึกข้อมูลเข้า-ออก พร้อมแสดงรายงานการเข้าออก

ข) ทะเบียนรถบุคคลภายนอก คือ ยานพาหนะบุคคลที่ไม่ได้มีการจัดเก็บข้อมูลไว้ในระบบฐานข้อมูล ระบบจะทำการบันทึกข้อมูลการเข้าออกของบุคคลและแสดงรายงานการเข้าออก

ค) ทะเบียนรถต้องสงสัย คือ ยานพาหนะที่มีข้อมูลอยู่ในฐานข้อมูลด้านความมั่นคงที่มีการออกหมายจับดำเนินคดีด้านความมั่นคง เมื่อระบบสามารถตรวจสอบพบทะเบียนรถต้องสงสัยดังกล่าว ระบบจะดำเนินแจ้งเตือนไปยังระบบแจ้งเตือนด้านความมั่นคงปลอดภัยผ่านทางแอพพลิเคชั่นแจ้งเตือน หรือ Line Notification และแสดงสถานะความเสี่ยงที่เกิดขึ้นจากรายงานวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสถานศึกษา

5.2.2.3.4 ระบบตรวจจับควัน ระบบจะทำการตรวจจับปริมาณควันไฟ หากมีปริมาณเกินกับค่าที่กำหนดไว้ในระบบฐานข้อมูล ระบบดังกล่าวจะทำการแจ้งเตือนไปยังระบบแจ้งเตือนด้านความมั่นคงปลอดภัยผ่านทางแอพพลิเคชั่นแจ้งเตือน หรือ Line Notification

5.2.2.3.5 ระบบตรวจจับความร้อน ระบบจะทำการตรวจจับปริมาณค่าอุณหภูมิความร้อน หากมีปริมาณเกินกับค่าที่กำหนดไว้ในระบบฐานข้อมูล ระบบดังกล่าวจะทำการแจ้งเตือนไปยังระบบแจ้งเตือนด้านความมั่นคงปลอดภัยผ่านทางแอพพลิเคชั่นแจ้งเตือน หรือ Line Notification

5.2.2.3.6 ระบบตรวจจับก๊าซ ระบบจะทำการตรวจจับปริมาณก๊าซ หากมีปริมาณเกินกับค่าที่กำหนดไว้ในระบบฐานข้อมูล ระบบดังกล่าวจะทำการแจ้งเตือนไปยังระบบแจ้งเตือนด้านความมั่นคงปลอดภัยผ่านทางแอพพลิเคชั่นแจ้งเตือน หรือ Line Notification

5.2.2.3.7 ระบบตรวจจับแรงสั่นสะเทือน ระบบจะทำการตรวจจับระดับแรงสั่นสะเทือน หากมีระดับเกินกับค่าที่กำหนดไว้ในระบบฐานข้อมูล ระบบดังกล่าวจะทำการแจ้งเตือนไปยังระบบแจ้งเตือนด้านความมั่นคงปลอดภัยผ่านทางแอพพลิเคชั่นแจ้งเตือน หรือ Line Notification

5.2.2.4 ส่วนของระบบบริหารจัดการรายงานความมั่นคงปลอดภัย เป็นระบบแจ้งเตือนความมั่นคงปลอดภัยประกอบด้วย 2 ส่วน คือ

5.2.2.4.1 ระบบแจ้งเตือน (Notification) เป็นการแจ้งเตือนความเสี่ยงที่เกิดขึ้นจากระบบ HISMS ผ่านแอพพลิเคชั่นไลน์ (Application Line) โดยจะทำการแจ้งเตือนบุคคลต้องสงสัย ทะเบียนรถต้องสงสัย และปริมาณค่าระดับความร้อน ควัน ก๊าส และแรงสั่นสะเทือนที่อยู่ในระดับที่กำหนดให้มีการแจ้งเตือน

5.2.2.4.2 ระบบแสดงผลการวิเคราะห์ความเสี่ยง (Dashboard) เป็นการแสดงผลข้อมูลสรุปแบบ Executive ในมุมมองทางด้านความปลอดภัยในแต่ละส่วน เพื่อให้สามารถดูข้อมูลเพื่อวิเคราะห์ความเสี่ยงได้ง่ายขึ้น และได้เห็นการเปลี่ยนแปลงของข้อมูลได้ตลอดเวลา โดยแสดงข้อมูลผ่านเว็บเบราว์เซอร์ (Web Browser) ในรูปแบบของรายงานและกราฟ

5.2.2.4.3 ระบบจัดการรายงาน (Report) เป็นการแสดงผลการพิสูจน์หลักฐานดิจิทัลเพื่อใช้สำหรับวิเคราะห์และประเมินผลความมั่นคงปลอดภัยสำหรับสถานศึกษา ได้แก่

1) การรวบรวมพยานหลักฐานที่ได้จากระบบ HISMS 2) การวิเคราะห์เพื่อประเมินความเสี่ยงที่ได้จากผลการวิเคราะห์ความเสี่ยง 3) การรายงานความมั่นคงปลอดภัย

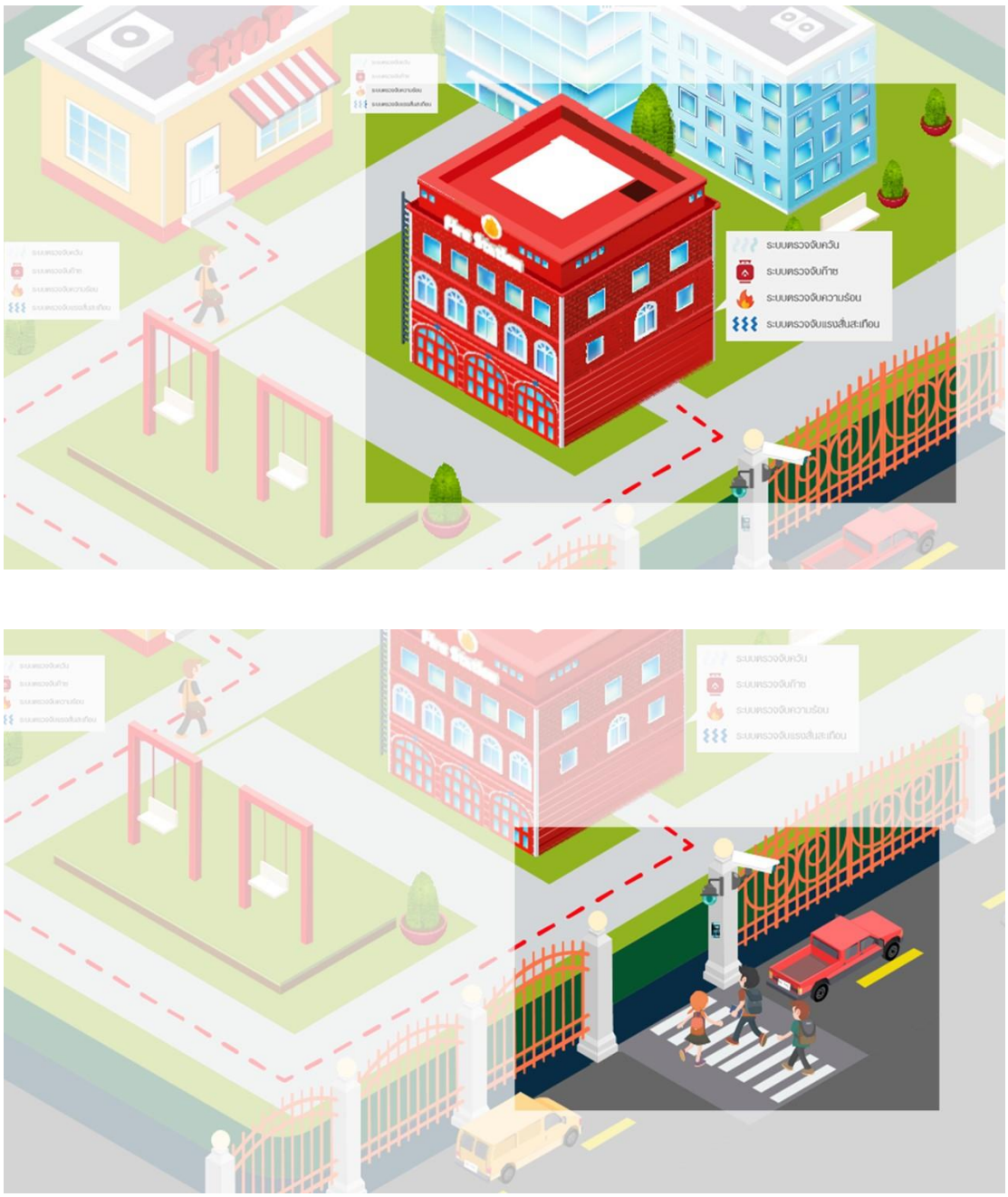
5.2.2.5 ส่วนของเว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server) ประกอบด้วย เซิร์ฟเวอร์ที่ให้บริการเว็บไซต์ของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ (HISMS Web Server) และระบบจัดการฐานข้อมูล (Database Management System : DBMS) ในส่วนนี้จะมีการพิสูจน์ตัวบุคคล (Authentication) และตั้งค่าสิทธิ์ผู้ใช้งาน (User Permissions) จากแอคทีฟ ไดเร็กทอรี่/แอลแดป (Active Directory Service) ทำหน้าที่ให้บริการแก่ยูสเซอร์และผู้บริหารระบบ และแอคที ๆ ไดเร็กทอรี่ ดาต้าเบส (Active Directory Database) ทำหน้าที่เป็นฐานข้อมูลสำหรับใช้ในการเก็บไดเร็กทอรี่ ออบเข็ค (Directory Object) ต่าง ๆ ที่เกี่ยวกับบัญชีผู้ใช้งาน (User Account) และบัญชีกลุ่มผู้ใช้งาน (Group Account)

5.2.3 ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แบ่งออกเป็น 2 ส่วน โดยมีรายละเอียดดังนี้

5.2.3.1 ระบบตรวจสอบความมั่นคงปลอดภัยสำหรับสถานศึกษา ทำหน้าที่หลักเป็นอุปกรณ์สำหรับการตรวจจับข้อมูลเพื่อนำเข้าสู่ระบบการตรวจสอบความมั่นคงปลอดภัย แสดงดังภาพที่ 5-3

ภาพที่ 5-3 แผนภาพแสดงการติดตั้งอุปกรณ์เชื่อมต่อการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้



ภาพที่ 5-4 แผนภาพแสดงการติดตั้งอุปกรณ์เชื่อมต่อการรักษาความมั่นคงปลอดภัย สำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

จากภาพที่ 5-3 แสดงการติดตั้งอุปกรณ์ตรวจสอบความมั่นคงปลอดภัยสำหรับสถานศึกษาซึ่งมีรายละเอียดดังนี้

5.2.3.1.1 ระบบตรวจจับใบหน้า (Face Detection) คือ โมดูลที่ใช้สำหรับตรวจจับใบหน้า โดยมีการติดตั้งอุปกรณ์กล้องตรวจจับเพื่อดำเนินการตรวจจับใบหน้าบุคคลเข้าออกภายในสถานศึกษา

5.2.3.1.2 ระบบสแกนบัตร (RFID Card)

5.2.3.1.3 ระบบตรวจจับป้ายทะเบียนรถ (License Plate Detection)

5.2.3.1.4 ระบบตรวจจับความร้อน (Heat Detection)

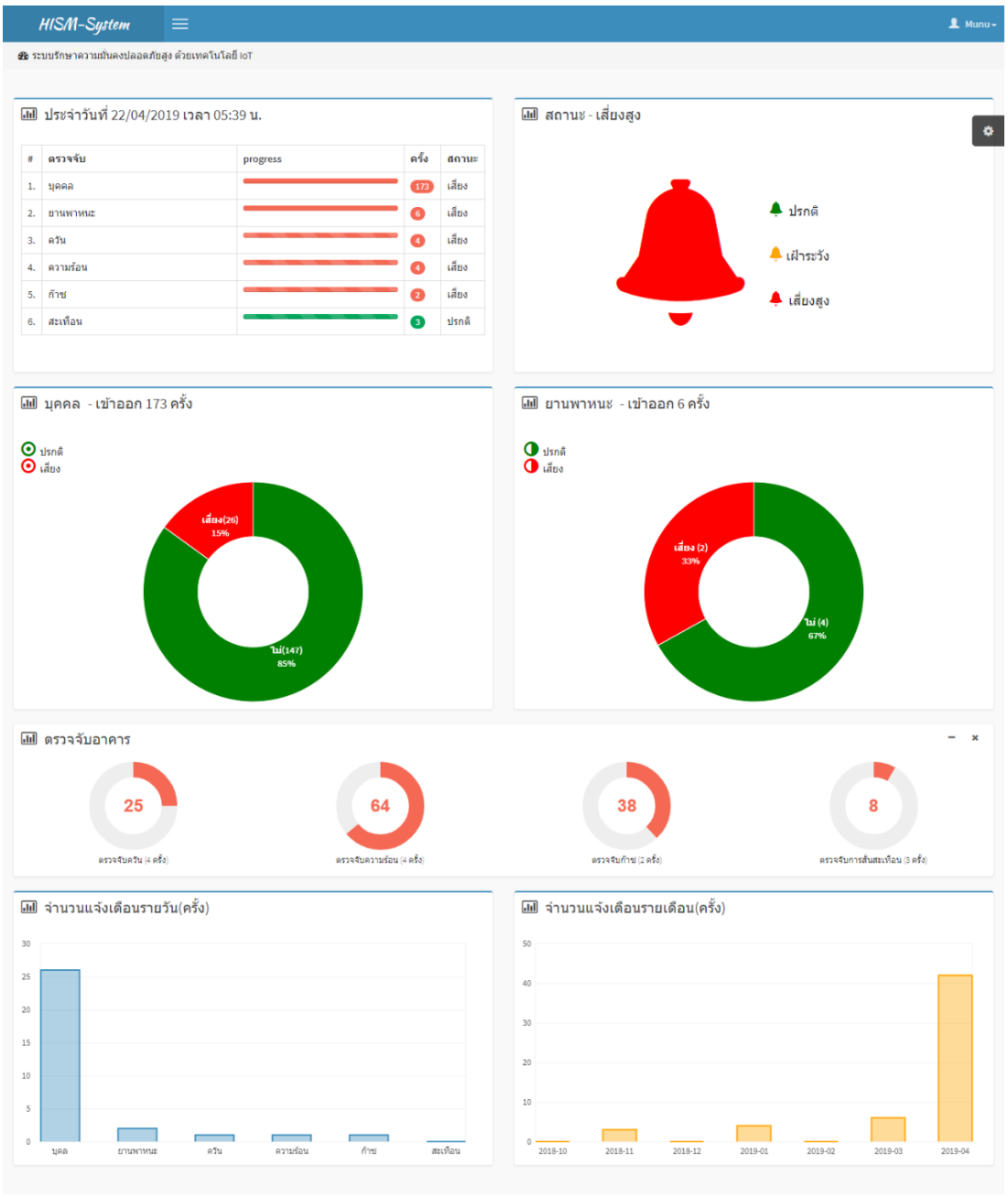
5.2.3.1.5 ระบบตรวจจับควัน (Smoke Detection)

5.2.3.1.6 ระบบตรวจจับก๊าซ (Gas Detection)

5.2.3.1.7 ระบบตรวจจับแรงสั่นสะเทือน (Vibration Detection)

5.2.3.2 ระบบบริหารจัดการความมั่นคงปลอดภัยด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีรายละเอียดดังนี้

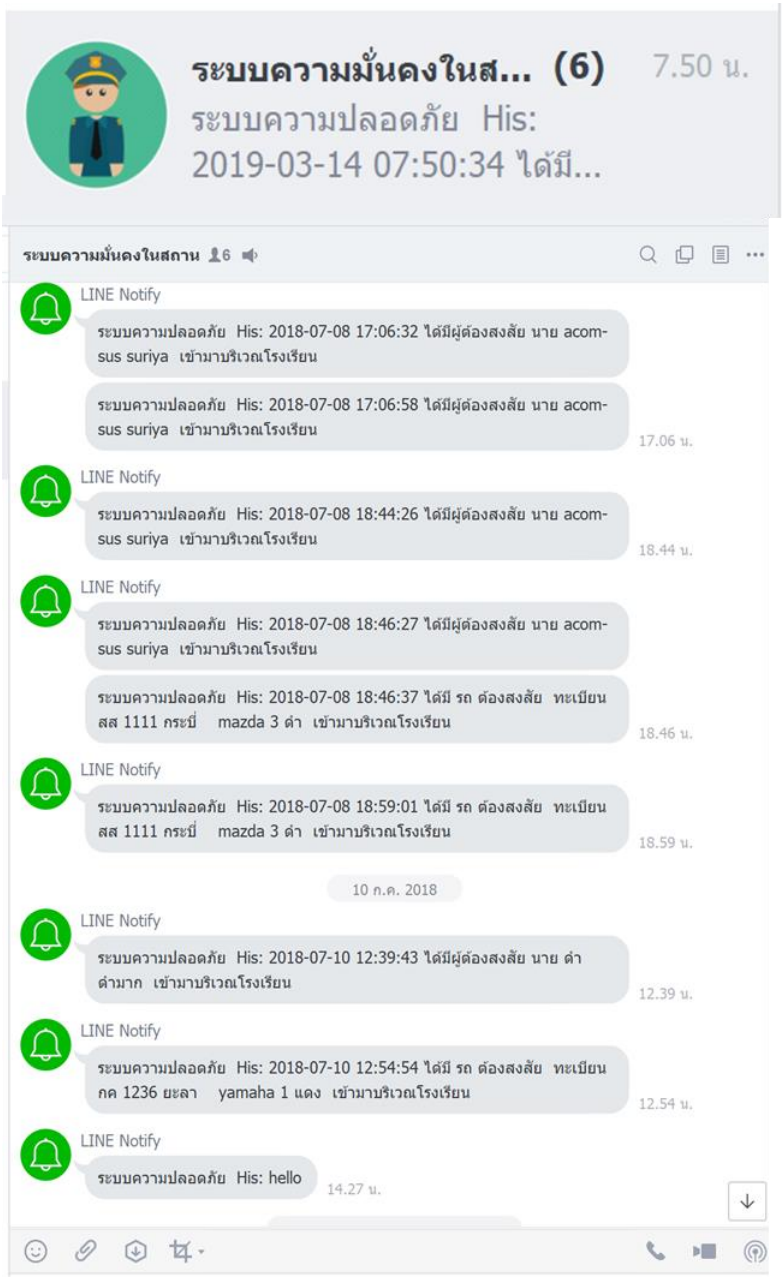
5.2.3.2.1 หน้าจอแสดงผลการวิเคราะห์ความเสี่ยง (Dashboard) เป็นการแสดงผลข้อมูลสรุปแบบ Executive ในมุมมองทางด้านความปลอดภัยในแต่ละส่วน เพื่อให้สามารถดูข้อมูลเพื่อวิเคราะห์ความเสี่ยงได้ง่ายขึ้น และได้เห็นการเปลี่ยนแปลงของข้อมูลได้ตลอดเวลา โดยแสดงข้อมูลผ่านเว็บเบราว์เซอร์ (Web Browser) ในรูปแบบของรายงานและกราฟ สถานะความเสี่ยงของสถานศึกษา แสดงดังภาพที่ 5-5



ภาพที่ 5-5 หน้าจอแสดงผลการวิเคราะห์ความเสี่ยง (Dashboard) โดยภาพรวมของสถานศึกษา

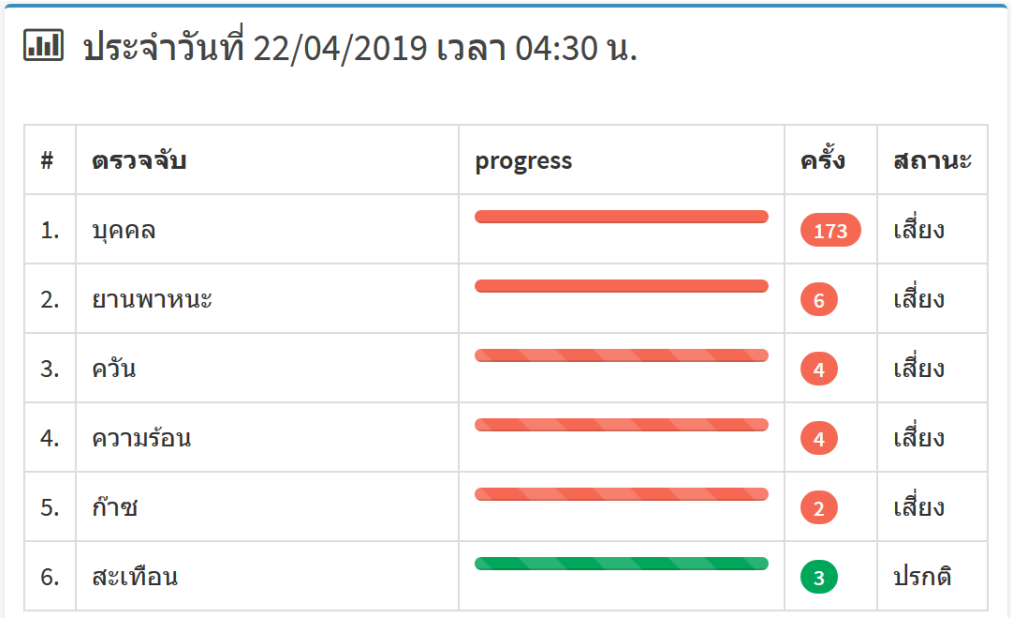
จากภาพที่ 5-5 เป็นการแสดงผลการวิเคราะห์ความเสี่ยงในรูปแบบตารางภาพรายงานสรุป (Dashboard) โดยแสดงผลผ่านทางอุปกรณ์เชื่อมต่อระบบ HISMS ซึ่งจะแสดงให้เห็นถึงภาพรวมของโมดูลความมั่นคงปลอดภัยสำหรับสถานศึกษา

5.2.3.2.2 หน้าจอแสดงผลการแจ้งเตือนความมั่นคงปลอดภัย โดยระบบเลือกใช้ แอพพลิเคชั่นไลน์ (Line Application) สำหรับการแจ้งเตือนบุคคลต้องสงสัย รถต้องสงสัย และแจ้งเตือนความปลอดภัยอาคารสถานที่เกิดจาก ควัน ความร้อน ก๊าซ และแรงสั่นสะเทือนที่ค่าความอันตรายเกินระดับที่กำหนด แสดงดังภาพที่ 5-6



ภาพที่ 5-6 หน้าจอแสดงผลการแจ้งความมั่นคงปลอดภัย

จากภาพที่ 5-6 เป็นการแสดงผลการแจ้งเตือนความเสี่ยง โดยการแจ้งเตือนผ่านแอพพลิเคชั่นไลน์ ที่ทำการเชื่อมต่อระบบ HISMS ซึ่งเป็น LINE Notify ใช้สำหรับการแจ้งเตือนความเสี่ยงผ่านทางอุปกรณ์สื่อสาร หรือ สมาร์ทโฟน (Smart Phone)

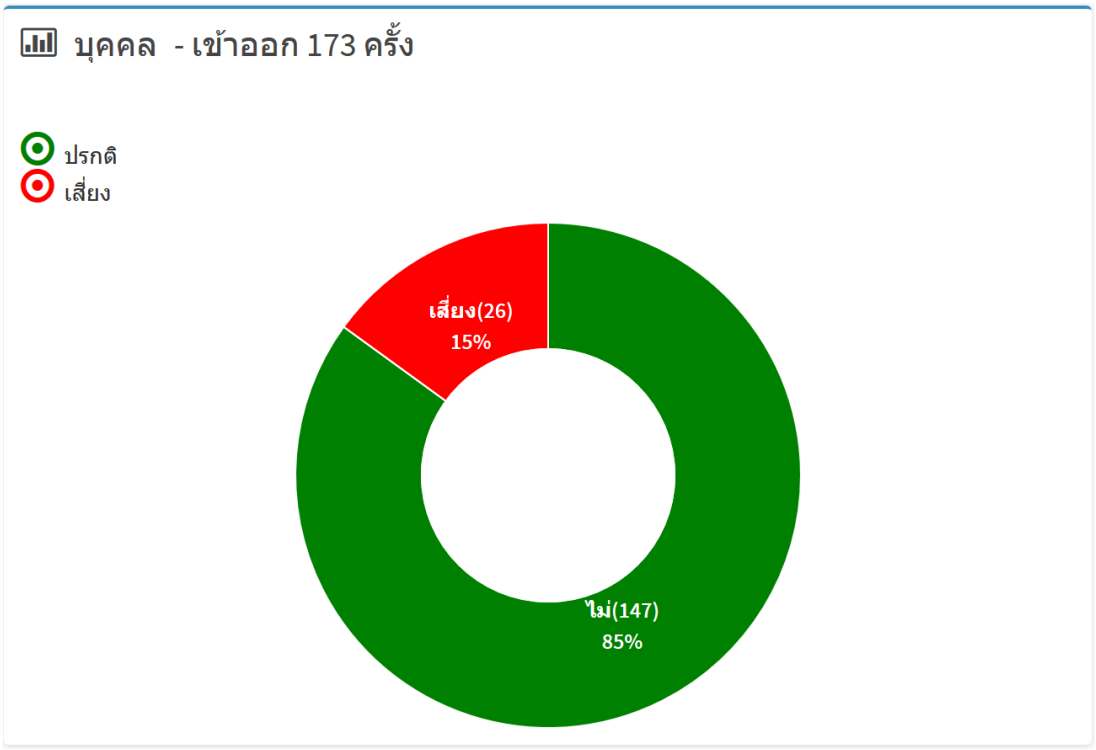


ภาพที่ 5-7 หน้าจอแสดงข้อมูลสรุปรายงานความเสี่ยงประจำวัน

จากภาพที่ 5-7 แสดงข้อมูลสรุปรายงานความเสี่ยงประจำวัน ในรูปแบบของ Dashboard ซึ่งระบบจะทำการสรุปข้อมูลประจำวันโดยแสดงตามรายการตรวจจับความปลอดภัย ซึ่งแสดงข้อมูลความปกติปลอดภัยด้วยแทบที่ เขียว และแสดงข้อมูลความผิดปกติหรือความเสี่ยงด้วยแทบที่แดง ประกอบด้วยการตรวจจับบุคคล ยานพาหนะ ควันไฟ ความร้อน ก๊าซ และ แรงสั่นสะเทือน

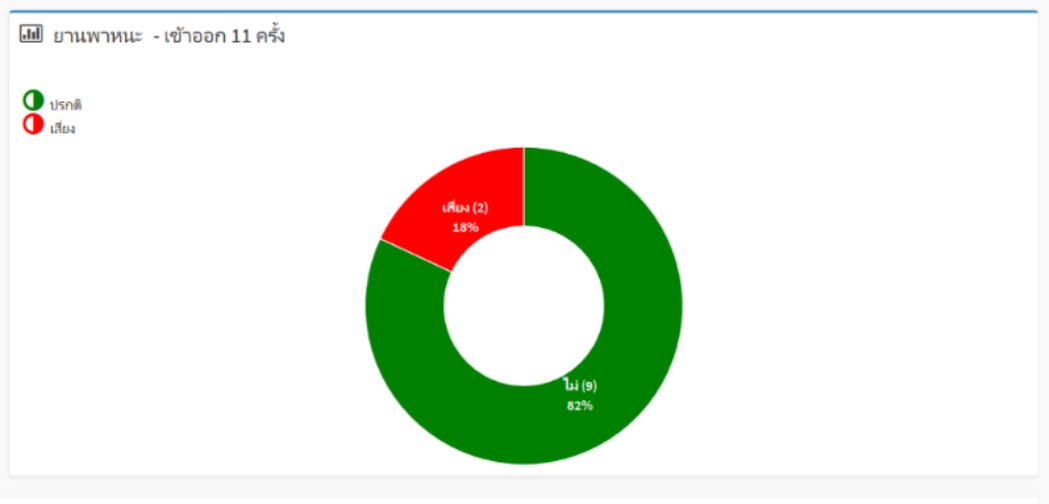
ภาพที่ 5-8 หน้าจอแสดงสถานะการแจ้งเตือนความเสี่ยงของระบบ

จากภาพที่ 5-8 แสดงข้อมูลสถานะความเสี่ยงภาพรวมของระบบ HISMS ในรูปแบบของ Dashboard โดยใช้สัญลักษณ์แจ้งเตือน ประกอบด้วย 1) แทบสีเขียว หมายถึง ความปกติของระบบที่ยังไม่ได้ตรวจผิดความผิดปกติ 2) แทบที่เหลือง หมายถึง เฝ้าระวัง ซึ่งระบบมีการตรวจจับความผิดปกติของระบบที่อยู่ในระดับต้องเฝ้าระวังที่อาจเกิดจากการตรวจจับอาคารที่อยู่ในระดับใกล้ถึงความผิดปกติ 3) แทบสีแดง หมายถึง เสี่ยงสูง ระบบจะดำเนินการแจ้งเตือนทันที่เมื่อระบบสามารถตรวจจับบุคคล ยานพาหนะ ต้องสงสัยที่ถูกบันทึกไว้ในระบบฐานข้อมูล และการตรวจจับปริมาณวัตถุควันไฟ ความร้อน ก๊าซ แรงสั่นสะเทือน ที่เกินระดับความปลอดภัย



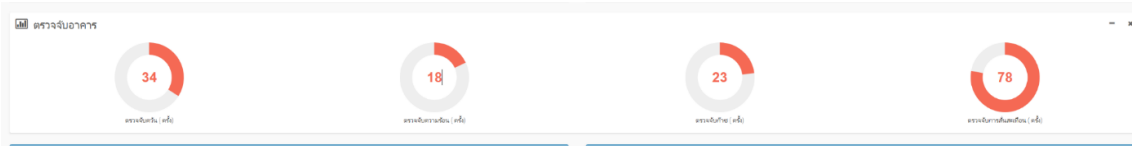
ภาพที่ 5-9 หน้าจอแสดงข้อมูลบุคคลเข้า - ออก ประจำวัน

จากภาพที่ 5-9 แสดงข้อมูลบุคคลเข้า - ออก ประจำวันในรูปแบบของ Dashboard ซึ่งระบบจะแสดงข้อมูลความปกติปลอดภัยด้วยแทบที่ เขียว และแสดงข้อมูลความผิดปกติหรือความเสี่ยงด้วยแทบที่ แดง



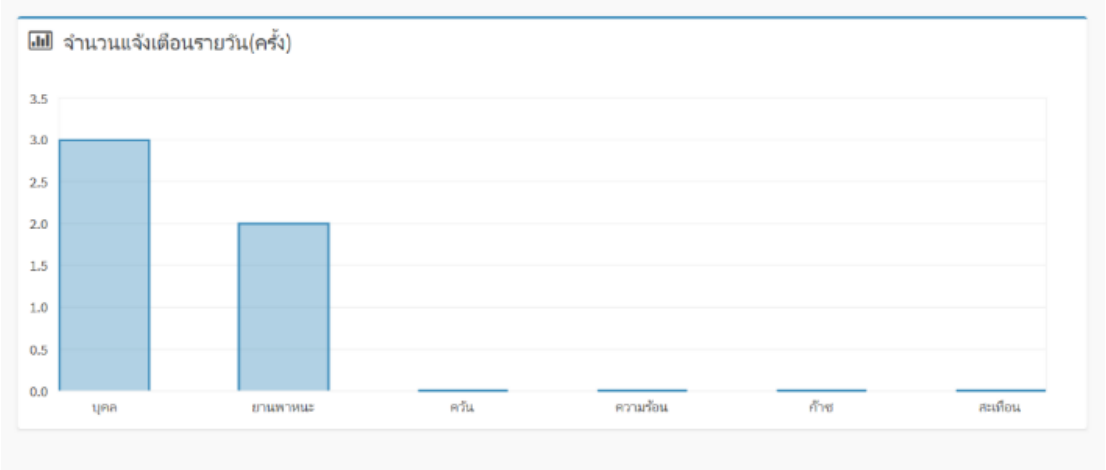
ภาพที่ 5-10 หน้าจอแสดงข้อมูลยานพาหนะเข้า - ออก ประจำวัน

จากภาพที่ 5-10 แสดงข้อมูลยานพาหนะเข้า - ออก ประจำวันในรูปแบบของ Dashboard ซึ่งระบบ จะแสดงข้อมูลความปกติปลอดภัยด้วยแทบที่ เขียว และแสดงข้อมูลความผิดปกติหรือความเสี่ยงด้วยแทบที่ แดง



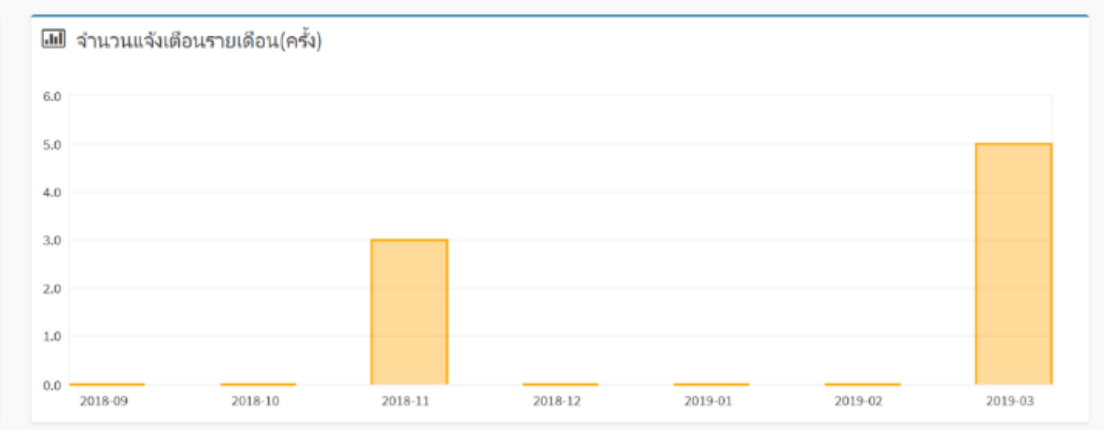
ภาพที่ 5-11 หน้าจอแสดงข้อมูลการตรวจจับภายในอาคารสถานที่ประจำวัน

จากภาพที่ 5-11 แสดงข้อมูลการตรวจจับภายในอาคารสถานที่ ประจำวันในรูปแบบของ Dashboard ซึ่งระบบ จะแสดงข้อมูลจำนวนครั้งที่ระบบสามารถทำการตรวจจับปริมารวัตถุที่เกิดค่าความผิดปกติ ประกอบด้วยการตรวจจับปริมาณ ควันไฟ ความร้อน ก๊าซ และ แรงสั่นสะเทือน แสดงปริมาณการตรวจจับด้วยแทบที่สีแดง



ภาพที่ 5-12 หน้าจอแสดงรายงานสรุปการแจ้งเตือนรายวัน

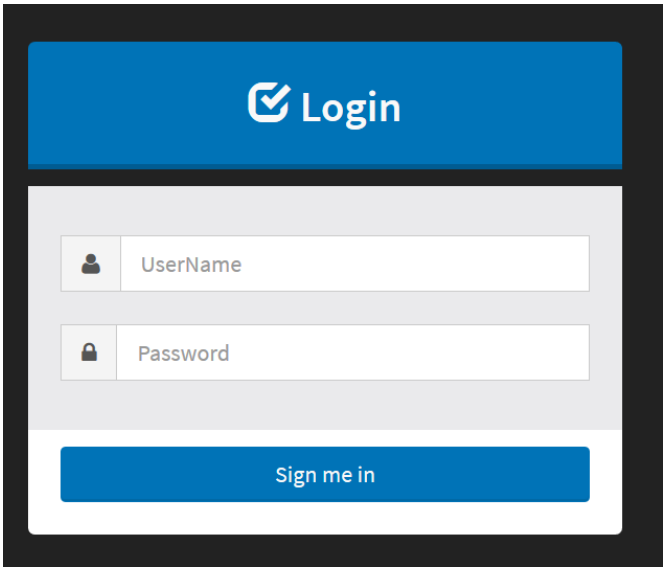
จากภาพที่ 5-12 แสดงข้อมูลสรุปรายงานจำนวนการแจ้งเตือนรายวัน โดยแสดงในรูปแบบของ Dashboard ลักษณะแผนภูมิ ซึ่งระบบจะทำการสรุปข้อมูลจำนวนการแจ้งเตือนความเสี่ยงหรือความไม่ปลอดภัยประจำเดือน เป็นจำนวนครั้งที่ระบบได้ทำการตรวจจับและแจ้งเตือน ซึ่งประกอบด้วย จำนวนการแจ้งเตือนประจำวันเป็นจำนวนครั้ง ประกอบด้วย การแจ้งเตือน บุคคล ยานพาหนะ ควันไฟ ความร้อน ก๊าซ และแสงสั่นสะเทือน



ภาพที่ 5-13 หน้าจอแสดงรายงานสรุปประจำเดือน

จากภาพที่ 5-13 แสดงข้อมูลรายงานสรุปจำนวนการแจ้งเตือนประจำเดือน โดยแสดงในรูปแบบของ Dashboard ลักษณะแผนภูมิ ซึ่งระบบจะทำการสรุปข้อมูลจำนวนการแจ้งเตือนความเสี่ยงหรือความไม่ปลอดภัยประจำเดือน เป็นจำนวนครั้งที่ระบบได้ทำการตรวจจับและแจ้งเตือนของแต่ละเดือนว่ามีการแจ้งเตือนทั้งหมดกี่ครั้ง

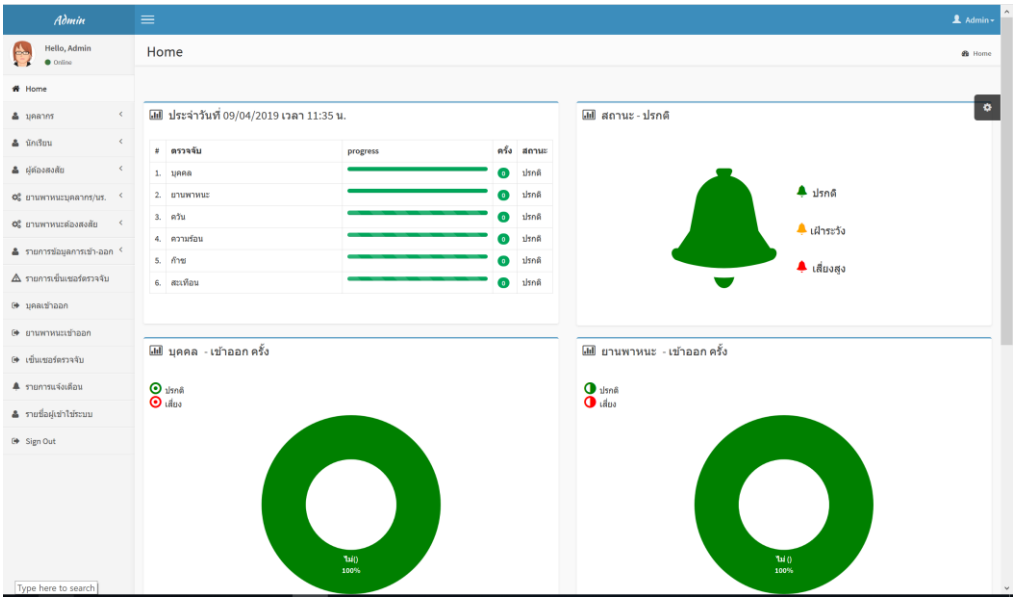
5.2.3.2.3 หน้าจอการเข้าใช้งานระบบฝั่งแบ็คเอนด์ ดังภาพที่ 5-14



ภาพที่ 5-14 หน้าจอการเข้าใช้งานระบบฝั่งแบ็คเอนด์

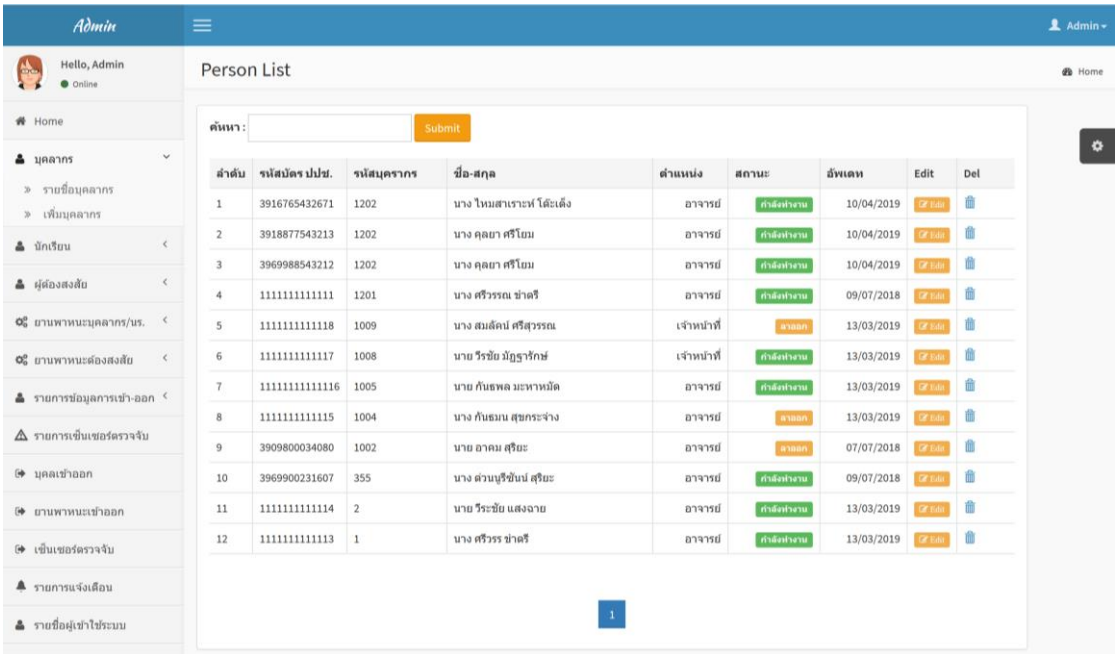
จากภาพที่ 5-14 หน้าจอการเข้าใช้งานระบบฝั่งแบ็คเอนด์ แสดงให้เห็นถึงการเข้าใช้งานระบบจะต้องป้อนชื่อผู้ช้าน (Username) และรหัสผ่าน (Password) เพื่อทำการล็อกอิน (Log in) ก่อนการใช้งานระบบ

5.2.3.2.4 หน้าจอโมดูลของระบบฝั่งแบ็คเอนด์ ดังภาพที่ 5-15



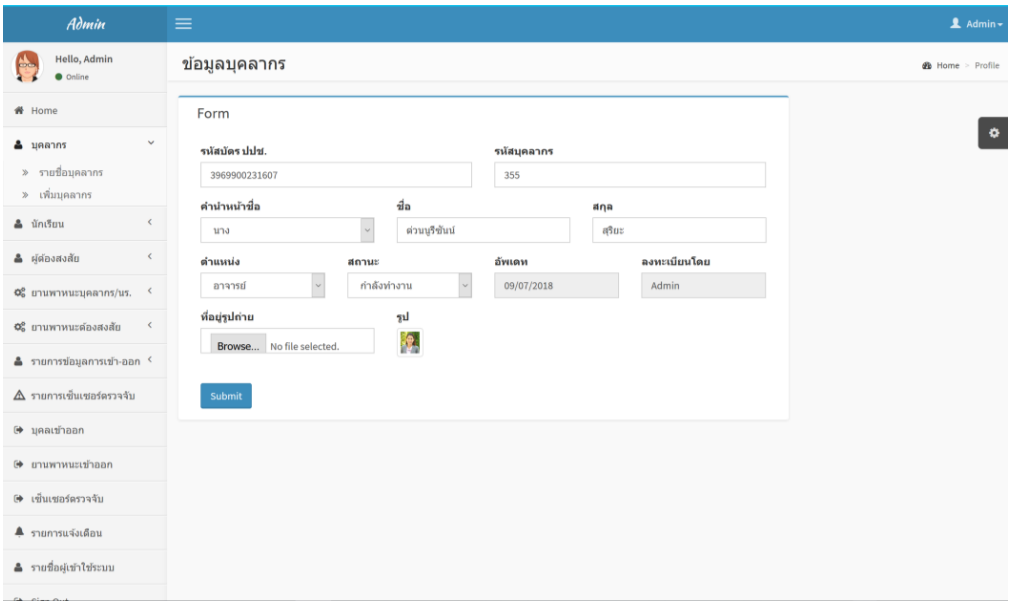
ภาพที่ 5-15 หน้าจอโมดูลของระบบฝั่งแบ็คเอนด์

จากภาพที่ 5-15 หน้าจอโมดูลของระบบฝั่งแบ็คเอนด์ แสดงให้เห็นถึง โมดูลทั้งหมดที่สามารถเข้าใช้งานได้ แบ่งออกเป็น 6 โมดูลหลักคือ โมดูลการตรวจสอบบุคคล โมดูลการตรวจสอบยานพาหนะ โมดูลตรวจควัน โมดูลตรวจความร้อน โมดูลตรวจก๊าซ โมดูลตรวจแรงสั่นสะเทือน



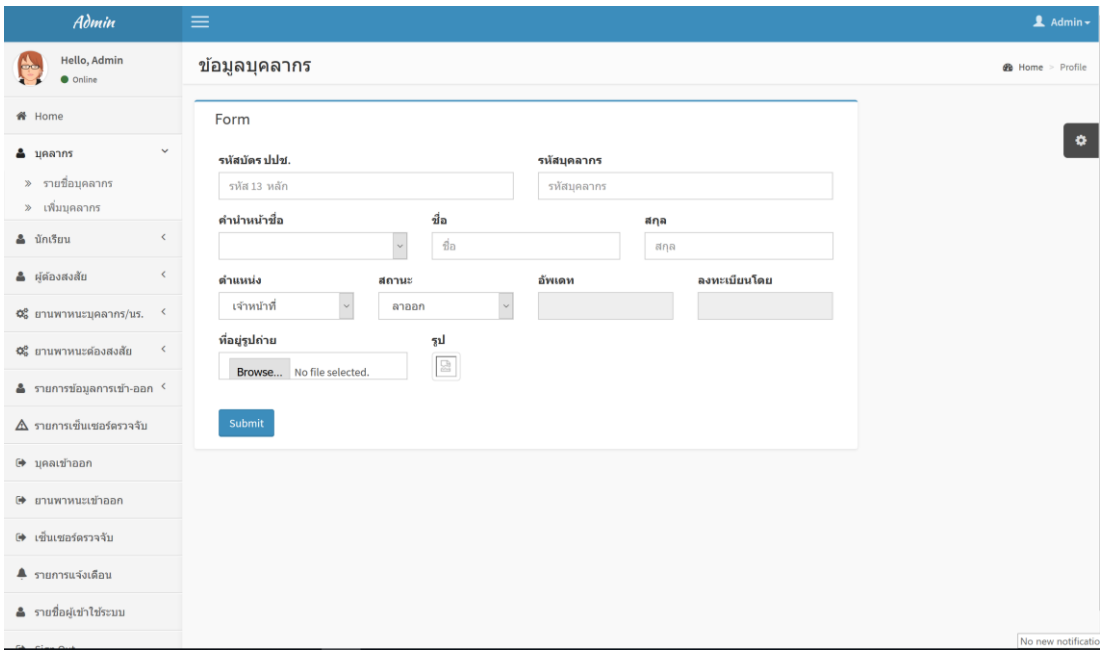
ภาพที่ 5-16 หน้าจอแสดงรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS

จากภาพที่ 5-16 แสดงหน้าจอรายรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS ประกอบไปด้วยข้อมูลส่วนบุคลากรรวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดังภาพที่ 5-17



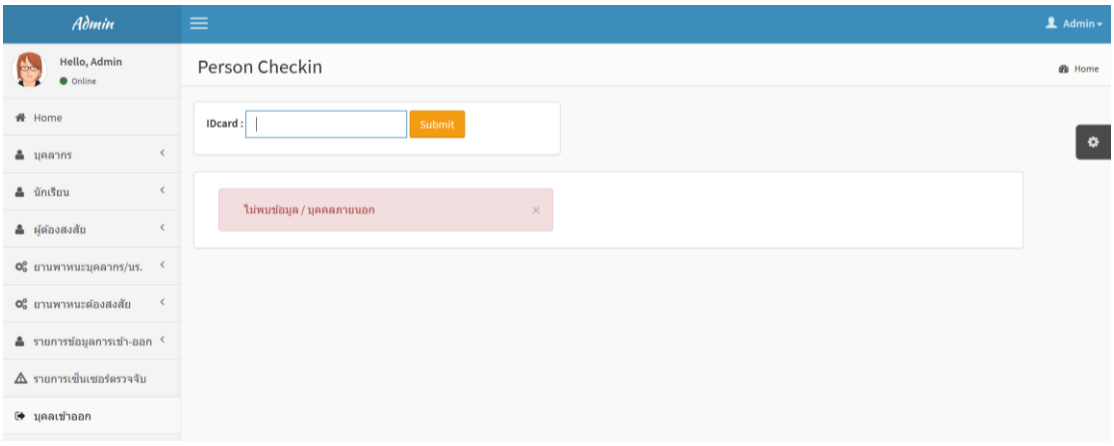
ภาพที่ 5-17 หน้าจอแสดงรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS เพิ่มเติม

จากภาพที่ 5-17 หน้าจอแสดงรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS เพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้

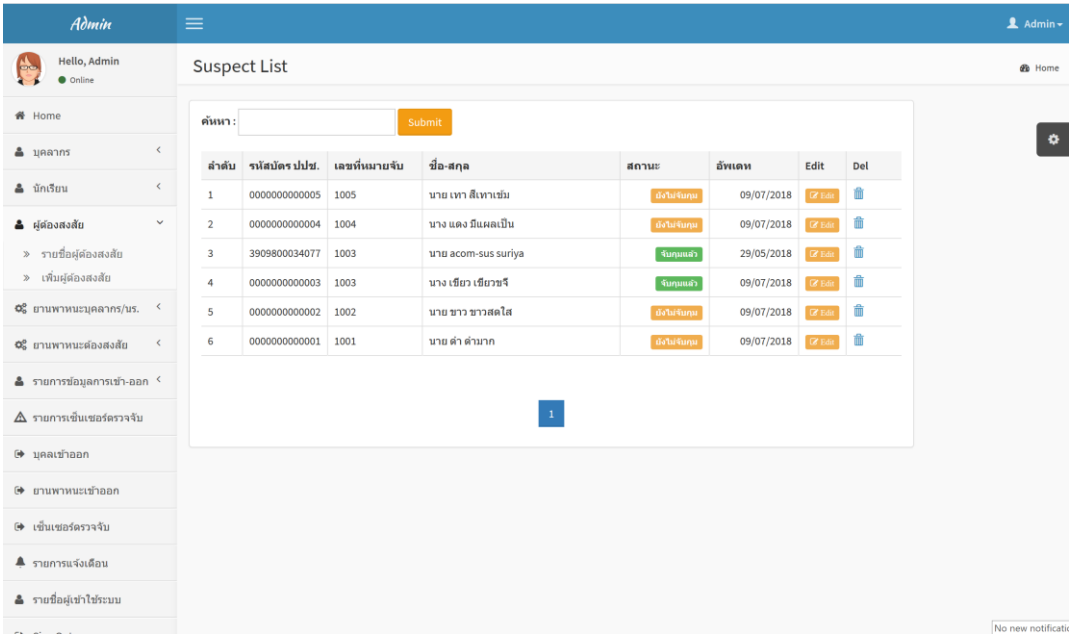


ภาพที่ 5-18 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS

จากภาพที่ 5-18 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS ผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ

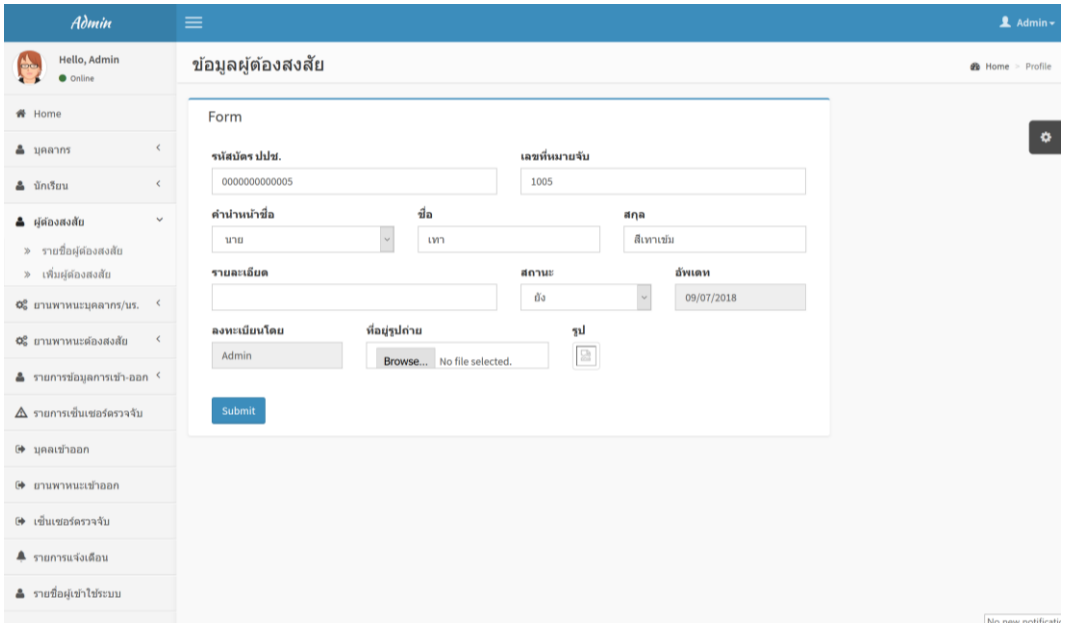


ภาพที่ 5-19 หน้าจอการค้นหาข้อมูลบุคคล



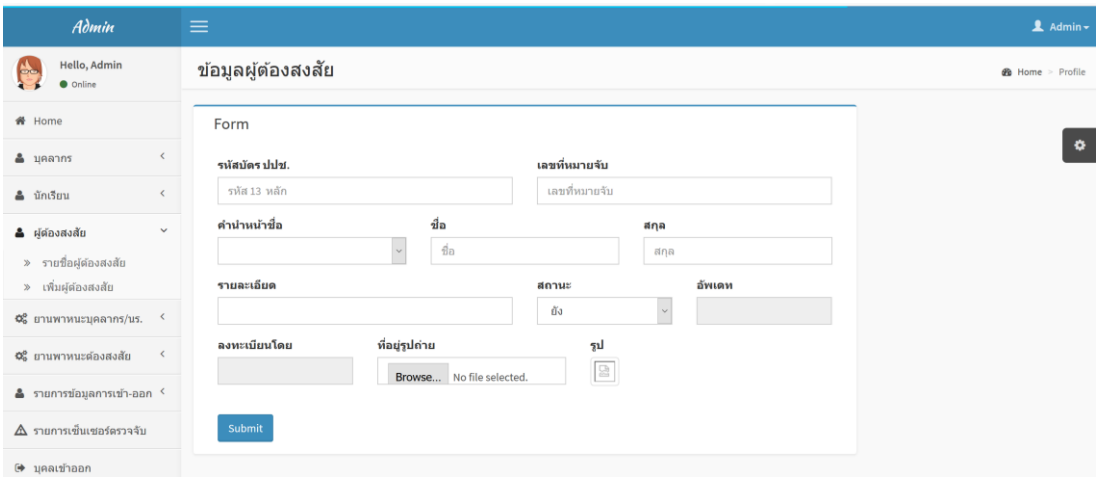
ภาพที่ 5-20 หน้าจอแสดงรายละเอียดข้อมูลผู้ต้องสงสัย

จากภาพที่ 5-20 แสดงหน้าจอรายรายละเอียดข้อมูลผู้ต้องสงสัยที่ถูกจัดเก็บข้อมูลไว้ในระบบฐานข้อมูล HISMS ประกอบไปด้วยรายละเอียดข้อมูลผู้ต้องสงสัยรวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดังภาพที่ 5-21



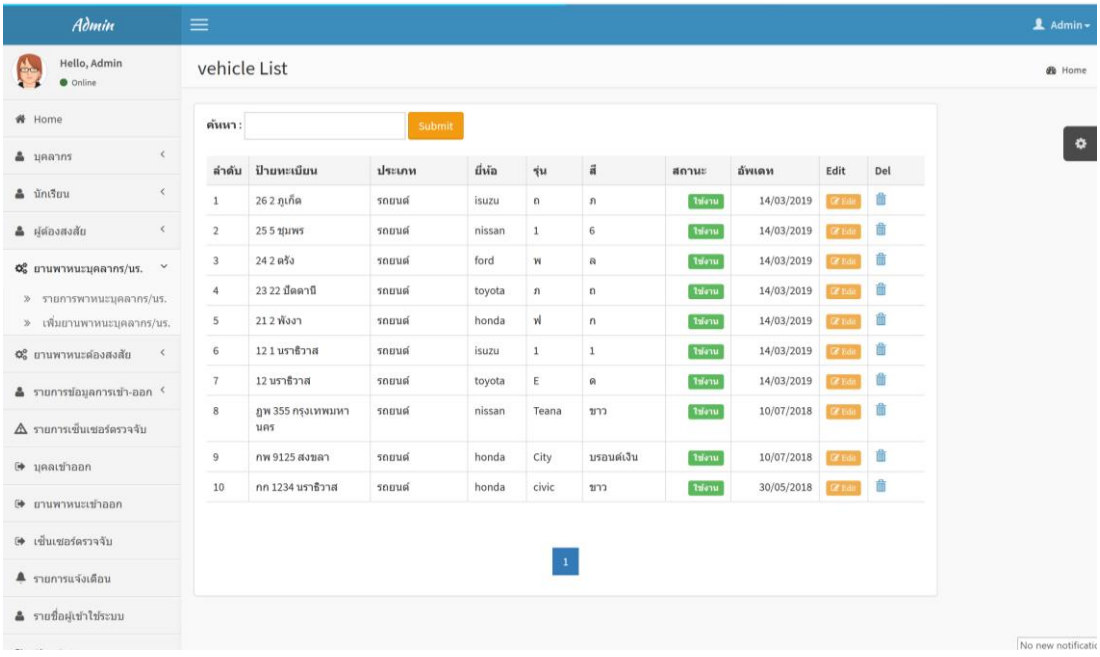
ภาพที่ 5-21 หน้าจอแสดงรายละเอียดข้อมูลผู้ต้องสงสัยเพิ่มเติม

จากภาพที่ 5-21 หน้าจอแสดงรายละเอียดข้อมูลผู้ต้องสงสัย เพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้



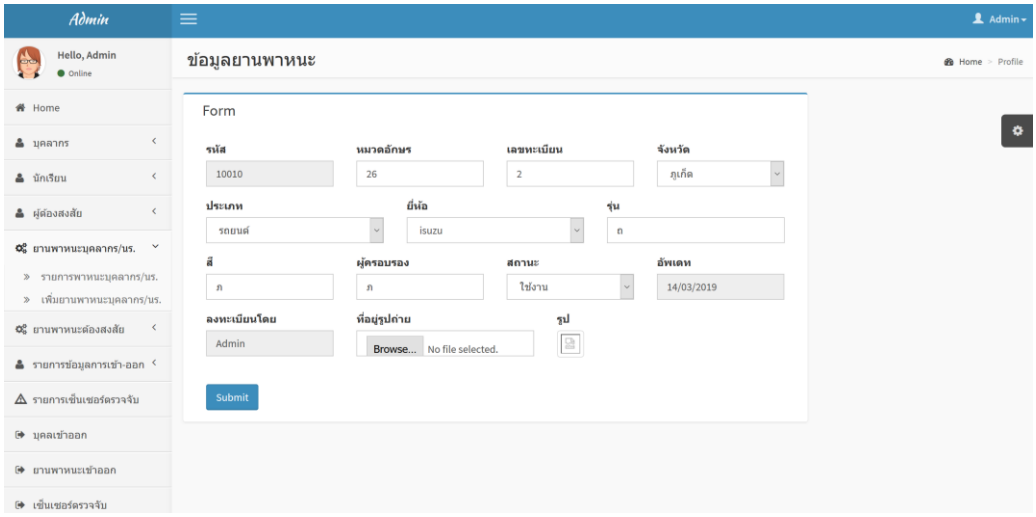
ภาพที่ 5-22 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลผู้ต้องสงสัย

จากภาพที่ 5-22 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลผู้ต้องสงสัย ซึ่งผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ



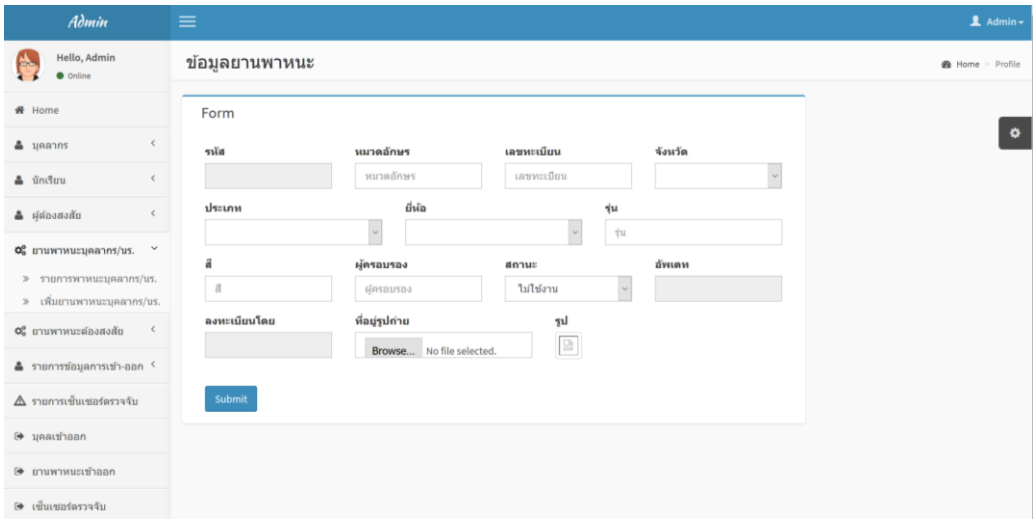
ภาพที่ 5-23 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะบุคลากรภายในและนักเรียนนักศึกษาของสถานศึกษาที่ใช้งานระบบ HISMS

จากภาพที่ 5-23 แสดงหน้าจอแสดงรายละเอียดข้อมูลยานพาหนะบุคลากรภายในและนักเรียนนักศึกษาของสถานศึกษาที่ใช้งานระบบ HISMS ประกอบไปด้วยข้อมูลรายละเอียดของยานพาหนะ รวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดังภาพที่ 5-24



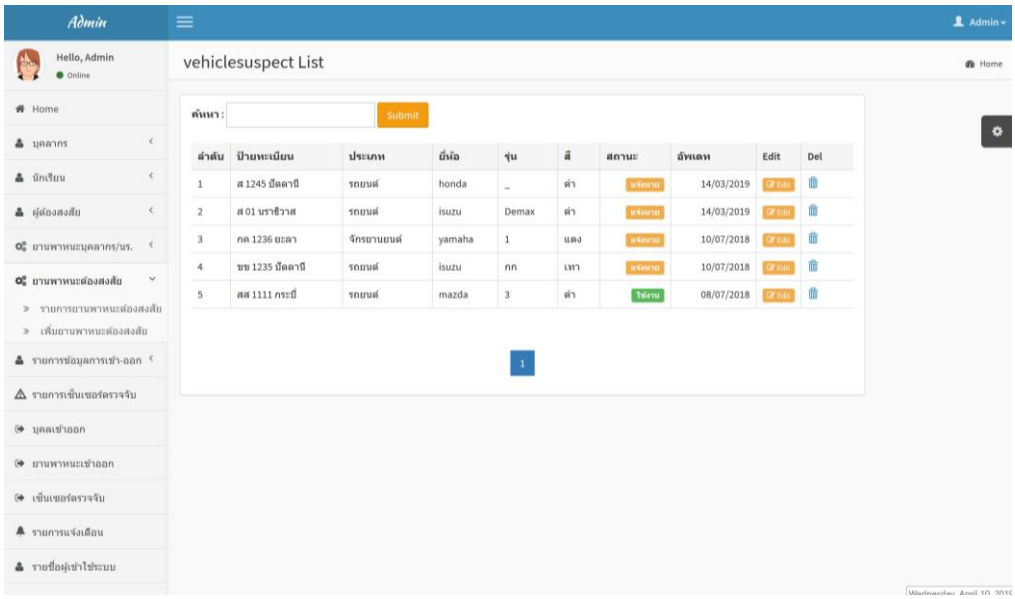
ภาพที่ 5-24 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะเพิ่มเติม

จากภาพที่ 5-24 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะเพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้



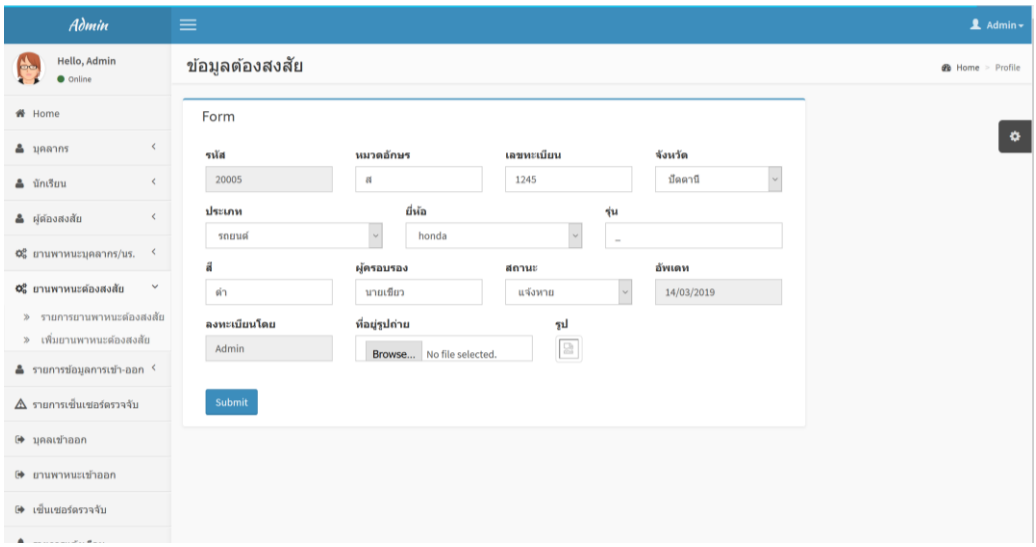
ภาพที่ 5-25 หน้าจอแสดงรายละเอียดการเพิ่มยานพาหนะ

จากภาพที่ 5-25 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลยานพาหนะ ซึ่งผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ



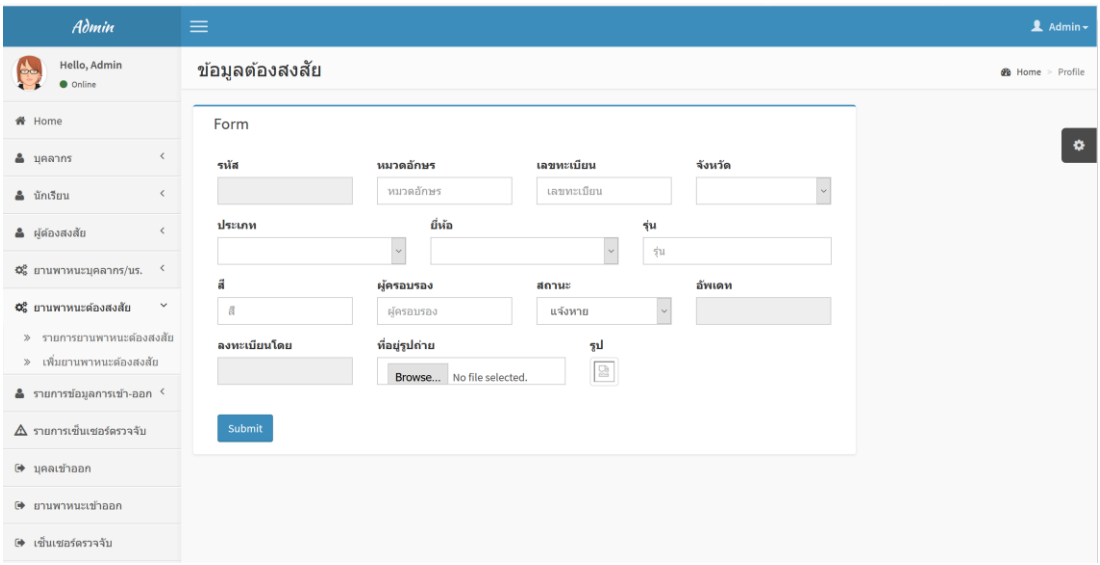
ภาพที่ 5-26 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัย

จากภาพที่ 5-26 แสดงหน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัย ประกอบไปด้วยข้อมูลรายละเอียดของยานพาหนะรวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดังภาพที่ 5-27



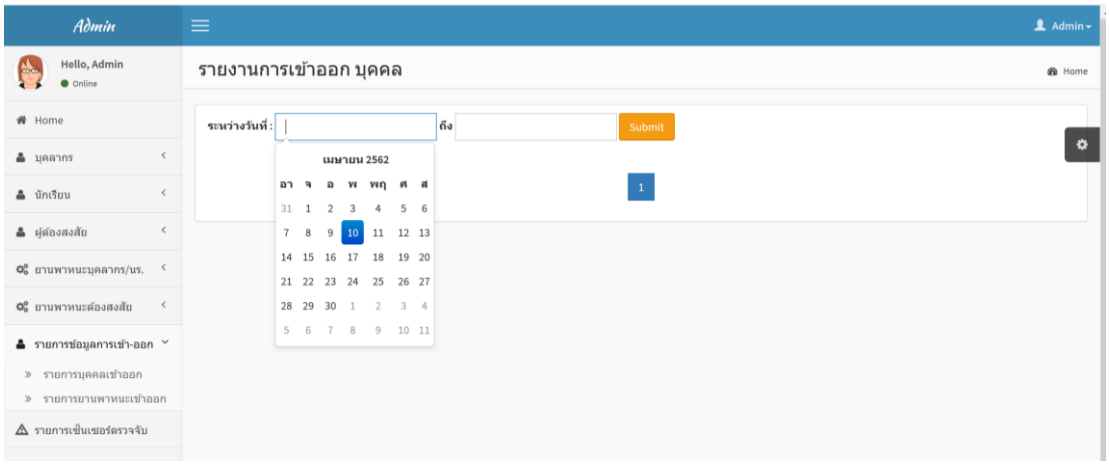
ภาพที่ 5-27 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัยเพิ่มเติม

จากภาพที่ 5-27 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัยเพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้



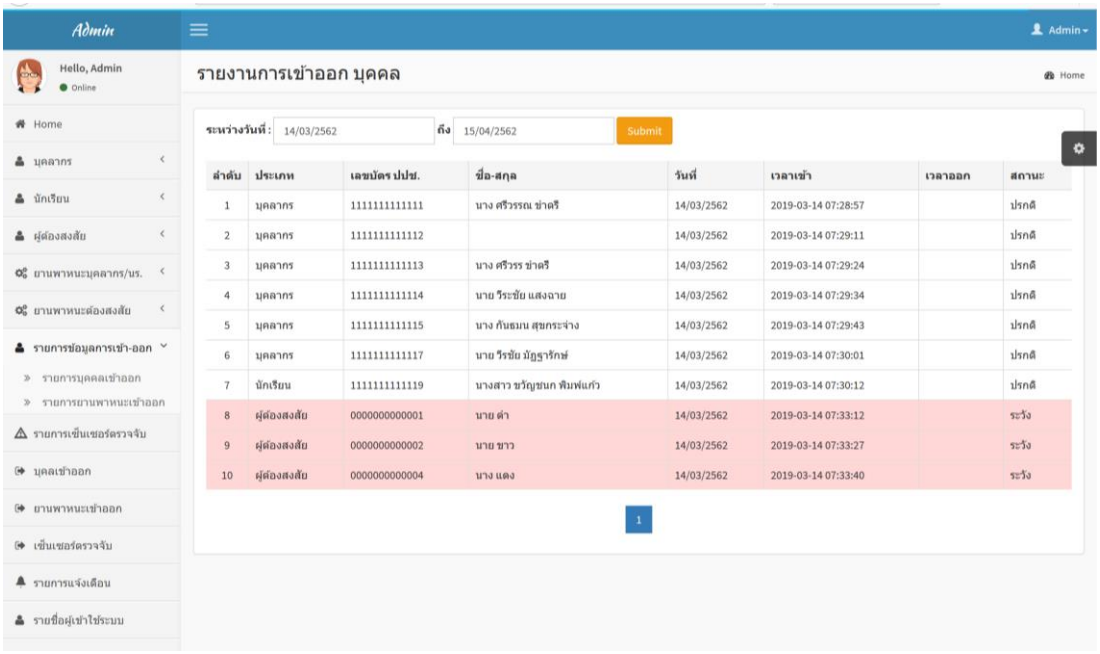
ภาพที่ 5-28 หน้าจอแสดงรายละเอียดการเพิ่มยานพาหนะต้องสงสัย

จากภาพที่ 5-28 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลยานพาหนะต้องสงสัย ซึ่งผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ



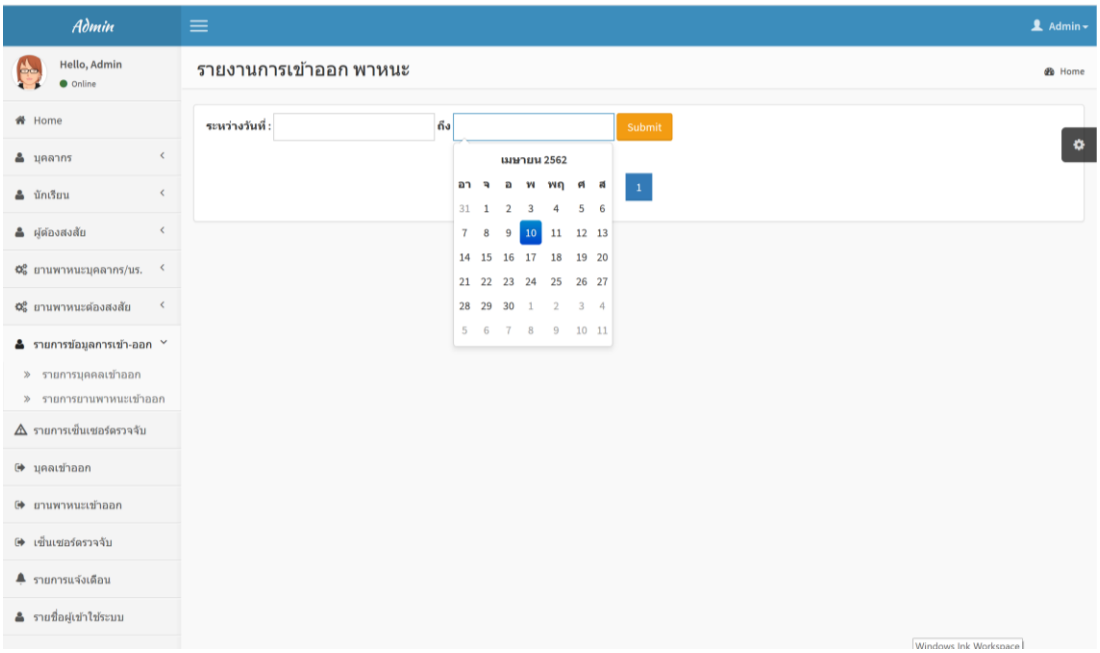
ภาพที่ 5-29 หน้าจอแสดงรายการค้นหารายงานข้อมูลบุคคลเข้าออก

จากภาพที่ 5-29 หน้าจอแสดงรายการค้นหารายงานข้อมูลบุคคลเข้าออก สามารถค้นหาข้อมูลจำนวนบุคคลเข้าออกโดยแสดงเป็นรายงานสรุปดังภาพที่ 5-30



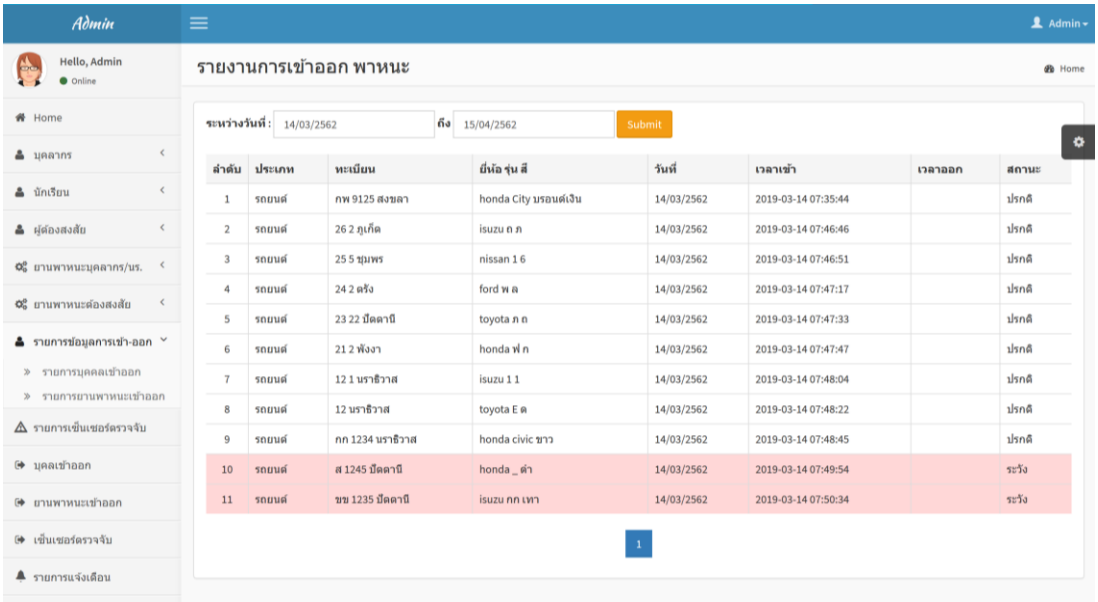
ภาพที่ 5-30 หน้าจอแสดงรายงานการค้นหาข้อมูลบุคคลเข้าออก

จากภาพที่ 5-30 หน้าจอแสดงรายงานค้นหาข้อมูลบุคคลเข้าออก สามารถแสดงรายงานสรุปวันที่ เวลาเข้าออก และ สถานะของบุคคลเข้าออกได้



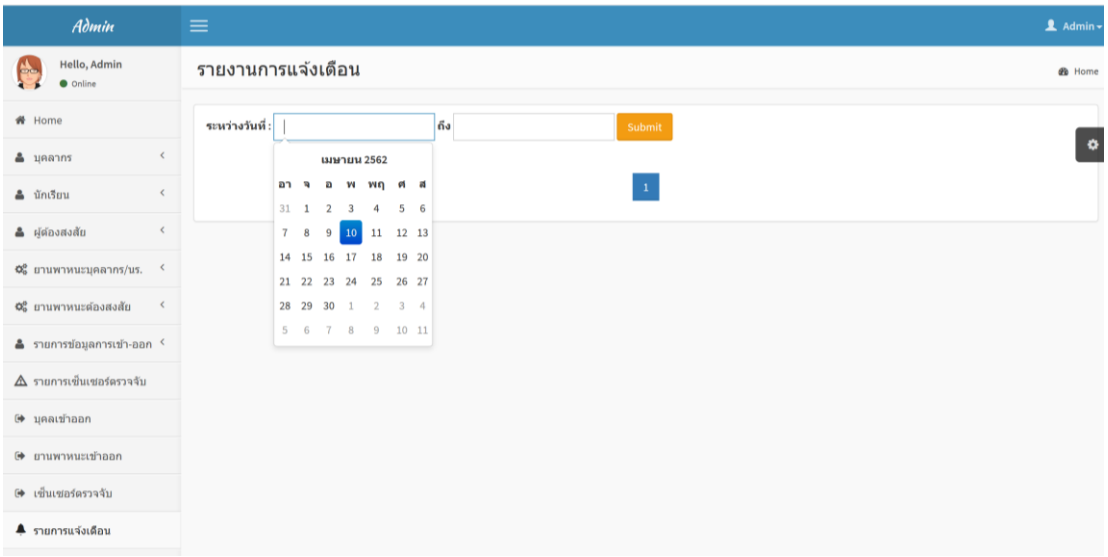
ภาพที่ 5-31 หน้าจอแสดงรายการค้นหารายงานข้อมูลยานพาหนะเข้าออก

จากภาพที่ 5-31 หน้าจอแสดงรายการค้นหารายงานข้อมูลยานพาหนะเข้าออก สามารถค้นหาข้อมูลจำนวนยานพาหนะเข้าออกโดยแสดงเป็นรายงานสรุปดังภาพที่ 5-32



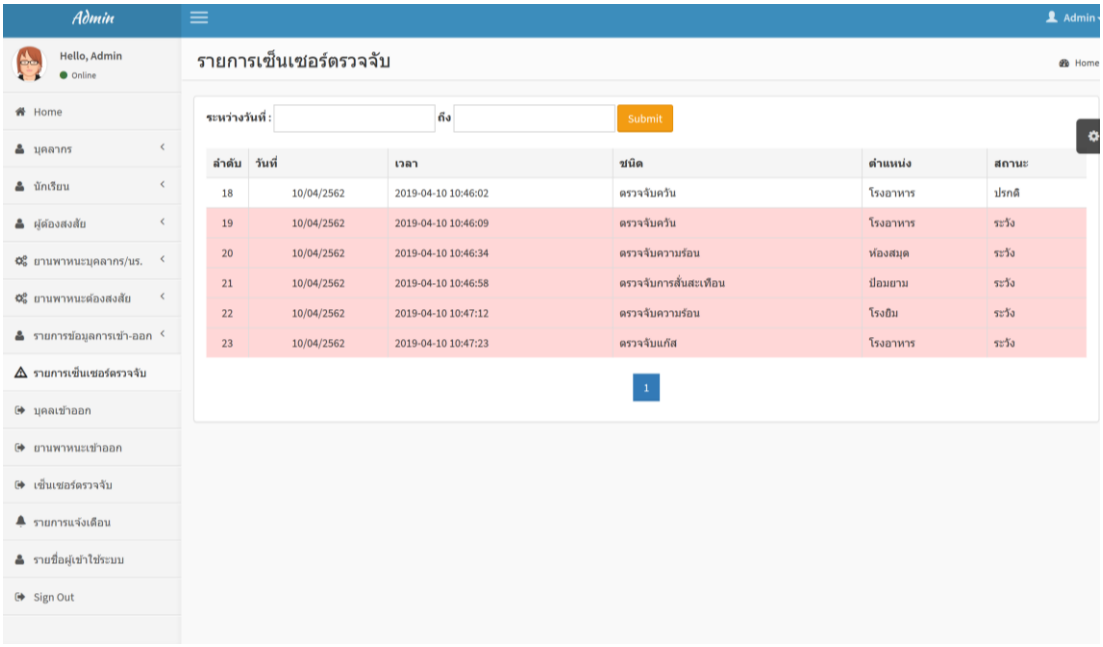
ภาพที่ 5-32 หน้าจอแสดงรายงานการค้นหาข้อมูลบุคคลเข้าออก

จากภาพที่ 5-32 หน้าจอแสดงรายงานค้นหาข้อมูลยานพาหนะเข้าออก สามารถแสดงรายงานสรุปวันที่ เวลาเข้าออก และ สถานะของยานพาหนะเข้าออกได้



ภาพที่ 5-33 หน้าจอแสดงรายการค้นหารายงานข้อมูลการแจ้งเตือนอาคารสถานที่

จากภาพที่ 5-33 หน้าจอแสดงรายการค้นหารายงานข้อมูลการแจ้งเตือนอาคารสถานที่ สามารถค้นหาข้อมูลอาคารสถานที่ ประเภทการตรวจจับ จำนวนครั้ง และสถานะความเสี่ยงของอาคารสถานที่โดยแสดงเป็นรายงานสรุปดังภาพที่ 5-34



ภาพที่ 5-34 หน้าจอแสดงรายงานการค้นหาข้อมูลบุคคลเข้าออก

จากภาพที่ 5-34 หน้าจอแสดงรายงานค้นหาข้อมูลายงานข้อมูลการแจ้งเตือนอาคารสถานที่ สามารถค้นหาข้อมูลอาคารสถานที่ได้

บทที่ 6
สรุปผล อภิปรายผล ข้อเสนอแนะ

การวิจัยเรื่อง ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยได้ทำการสรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ ซึ่งมี รายละเอียดดังต่อไปนี้

6.1 สรุป

6.2 อภิปรายผล

6.3 ข้อเสนอแนะ

6.1 สรุป

การสรุปผลการวิจัย เรื่อง ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปตามวัตถุประสงค์ของการวิจัยโดยมีรายละเอียดดังนี้

6.1.1 สรุปผลการวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แบ่งออกเป็น 7 ส่วน ได้แก่ (1) ผลการวิเคราะห์เอกสาร (Document Analysis) เกี่ยวกับการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ (2) ผลการสอบถามกลุ่มตัวอย่าง เกี่ยวกับความต้องการระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา (3) ผลการสังเคราะห์คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ (4) ผลการสังเคราะห์องค์ประกอบของคุณลักษณะการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ และ (5) ผลการประเมินความเหมาะสมของคุณลักษณะการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ (6) ผลประเมินความเหมาะสมผลประเมินความเหมาะสมของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ (7) ผลประเมินความเหมาะสมขององค์ประกอบหลัก

ของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปได้ดังนี้

6.1.1.1 ส่วนที่ 1 ผลการวิเคราะห์เอกสาร (Document Analysis) เกี่ยวกับการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยได้ทำการศึกษา ข้อมูลจากเอกสาร ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ทั้งในประเทศและต่างประเทศ โดยทำการรวบรวมข้อมูล เพื่อนำมาสังเคราะห์ และนำความรู้ที่ได้มาสรุปเป็นกรอบและประเด็นหลักเกี่ยวกับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา สรุปผลการวิเคราะห์และสังเคราะห์เอกสารที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีทั้งหมด 3 ส่วน ได้แก่ (1) การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal Security) (2) การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Place Security) (3) การป้องกันและแก้ไขปัญหาด้านความไม่สงบ (Prevention of War and its Environment Consequence) ผลจากการสังเคราะห์ข้อมูลดังกล่าวสามารถนำเป็นแนวทางในการสัมภาษณ์แบบเชิงลึก (In Depth Interview) จากผู้เชี่ยวชาญประเด็นเกี่ยวกับ การรักษาความปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

6.1.1.2 ส่วนที่ 2 ผลการสอบถามความคิดเห็นจากกลุ่มตัวอย่างเกี่ยวการวิเคราะห์สภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบเพื่อกำหนดคุณลักษณะของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ เพื่อให้ได้มาซึ่งข้อมูลสำหรับนำไปใช้ในการพัฒนาระบบ แบบสัมภาษณ์มีการออกแบบในลักษณะแบบคำถามปลายเปิด (Open-end Qusestion) เพื่อดำเนินการสัมภาษณ์ แบบเชิงลึกจากกลุ่มตัวอย่างของผู้บริหาร ครู อาจารย์ และบุคลากรทางการศึกษา รวม 198 ท่าน เพื่อเก็บข้อมูลอย่างอิสระ และใช้คำถามลักษณะกึ่งโครงสร้างสอบถามประเด็นเกี่ยวกับการรักษาความปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

6.1.1.3 ส่วนที่ 3 ผลการสังเคราะห์คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยนำการใช้เทคโนโลยีทางด้านความปลอดภัยเพื่อเป็นแนวทางในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถสรุปได้ 5 ส่วน คือ 1) ระบบยืนยันตัวตน 2) ระบบควบคุมการเข้า-ออกยานพาหนะ 3) ระบบตรวจจับและแจ้งเตือนภัยภายในอาคาร 4) ระบบฐานข้อมูลด้านความมั่นคง โดยทั้ง 4 ส่วนสามารถสรุปผลการนำมาเป็นองค์ประกอบด้านการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลของสถานศึกษาในจังหวัดชายแดน

6.1.1.4 ส่วนที่ 4 ผลการสังเคราะห์องค์ประกอบของคุณลักษณะการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แสดงให้เห็นว่า ระบบรักษาความมั่นคงปลอดภัยสูง ประกอบด้วย 3 ส่วน คือ การรักษาความมั่นคงปลอดภัยเกี่ยวกับบุคคล การรักษาความมั่นคงปลอดภัยเกี่ยวกับสถานที่ และ การป้องกันและแก้ไขปัญหาด้านความไม่สงบ ซึ่งมีความเกี่ยวข้องกับกระบวนการรักษาความมั่นคงปลอดภัย ซึ่งแบ่งออกเป็น 4 ระบบ คือ 1) ระบบยืนยันตัวตน 2) ระบบควบคุมการเข้า–ออกยานพาหนะ 3) ระบบตรวจจับและแจ้งเตือนภัยภายในอาคาร และ 4) ระบบฐานข้อมูลด้านความมั่นคง ในส่วนของเทคโนโลยีเชื่อมโยงใช้การตรวจจับด้วย กล้องตรวจจับ เซนเซอร์ และ บัตรอาร์เอฟไอดี โดยใช้กับโมดูลทั้ง 7 ส่วน ได้แก่ 1) โมดูลตรวจจับใบหน้า 2) โมดูลสแกนบัตร 3) โมดูลตรวจจับทะเบียนรถ 4) โมดูลตรวจจับควันไฟ 5) โมดูลตรวจจับความร้อน 6) โมดูลตรวจจับก๊าซ 7) โมดูลตรวจจับแรงสั่นสะเทือน ซึ่งสารสนเทศที่ได้จากโมดูลทั้ง 7 จะอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิคส์หรือหลักฐานดิจิทัล (Digital Forensic) ที่ประกอบด้วย 3 ส่วน คือ 1) การรวบรวมพยานหลักฐาน 2) การวิเคราะห์เพื่อประเมินความเสี่ยง 3) การรายงานความมั่นคงปลอดภัย

6.1.1.5 ส่วนที่ 5 ผลประเมินความเหมาะสมของการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.78, S.D. = 0.43) โดยการรักษาความปลอดภัยเกี่ยวกับสถานที่ และ การป้องกันและแก้ไขปัญหาด้านความไม่สงบ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.79, S.D. = 0.42) และการรักษาความปลอดภัยเกี่ยวกับบุคคล มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.76, S.D. = 0.44)

6.1.1.6 ส่วนที่ 6 ผลประเมินความเหมาะสมผลประเมินความเหมาะสมของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ =4.81, S.D. = 0.42) โดยระบบยืนยันตัวตน มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.84, S.D. = 0.41) ระบบควบคุมการเข้าออกยานพาหนะ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.82, S.D. = 0.42) ระบบตรวจจับและแจ้งเตือนภายในอาคาร มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.77, S.D. = 0.42) ระบบฐานข้อมูลด้านความมั่นคง มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.87, S.D. = 0.40)

6.1.1.7 ผลประเมินความเหมาะสมขององค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.61, S.D. = 0.49) และมีความเหมาะสมในการนำไปใช้จริงมีค่าเฉลี่ยอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.52, S.D. = 0.51)

6.1.2 สรุปผลการพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ซึ่งมีการประเมินความเหมาะสมของแบบจำลอง ใน 4 มิติ โดยผู้เชี่ยวชาญ จำนวน 10 ท่าน พบว่า ผลการประเมินอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ = 4.94, S.D. = 0.17) โดยแบ่งออกเป็น 4 มิติ ประกอบด้วย 1. มิติด้านการรักษาความปลอดภัยสำหรับสถานศึกษา 2. มิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา 3. มิติด้านการบริหารจัดการข้อมูล 4. มิติด้านการตรวจสอบหลักฐานดิจิทัล ซึ่งมีรายละเอียดการประเมินดังนี้

6.1.2.1 ผลการประเมินความเหมาะสมของมิติด้านการรักษาความปลอดภัยสำหรับสถานศึกษา ประกอบด้วย (1) การรรักษาความปลอดภัยเกี่ยวกับบุคคล (2) การรักษาวามปลอดภัยเกี่ยวกับสถานที่ (3) การป้องกันและแก้ไขปัญหาด้านความไม่สงบ พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 5.00, S.D. = 0.00)

6.1.2.2 ผลการประเมินความเหมาะสมของมิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา ประกอบด้วย (1) เทคโนโลยีเชื่อมโยงสรรพสิ่ง (2) ระยยตรวจจับและรู้จำ (3) ระบบจัดการฐานข้อมูล (4) ระบบจัดการรายงาน (5) ระบบแสดงผลข้อมูล (6) ระบบแจ้งเตือน พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.88, S.D. = 0.33)

6.1.2.3 ผลการประเมินความเหมาะสมของมิติด้านการบริหารจัดการข้อมูล ประกอบด้วย (1) การแจ้งเตือน (2) การรายงานความเสี่ยง (3) การบำรุงรักษาและตรวจสอบ พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19)

6.1.2.4 ผลการประเมินความเหมาะสมของมิติด้านการตรวจสอบหลักฐานดิจิทัล ประกอบด้วย (1) การรวบรวมพยานหลักฐาน (2) การวิเคราะห์เพื่อประเมินความเสี่ยง (3) การรายงานความมั่นคงปลอดภัย พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19)

6.1.3 สรุปผลการออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ซึ่งมีการประเมินใน 6 ด้านโดยผู้เชี่ยวชาญ จำนวน 10 ท่าน พบว่า ผลการประเมินอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ = 4.60, S.D. = 0.6) โดยแบ่งออกเป็น 5 ส่วน ประกอบด้วย 1. ผู้ที่เกี่ยวข้องกับระบบ (Stakeholders) 2. ไอโอทีดีไวซ์ สำหรับการตรวจจับบุคคลและวัตถุ 3. โมดูลย่อยของระบบ 4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย 5. เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server) 6. หลักการทำงานของสถาปัตยกรรมระบบ ซึ่งมีรายละเอียดการประเมินดังนี้

6.1.3.1 ผลการประเมินความเหมาะสมด้าน ผู้ที่เกี่ยวข้องกับ ประกอบด้วย (1) ผู้บริหารระบบ (2) ผู้บริหารสถานศึกษา (3) เจ้าหน้าที่รักษาความปลอดภัย (4) ผู้ใช้งานระบบ พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุดระบบพบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.70, S.D. = 0.52)

6.1.3.2 ผลการประเมินความเหมาะสมด้าน ไอโอทีดีไวท์สำหรับการตรวจจับบุคคลและวัตถุ ประกอบด้วย (1) กล้องตรวจจับใบหน้า (2) บัตร RFID (3) กล้องตรวจจับป้ายทะเบียน (4) เซนเซอร์ตรวจจับควัน (5) เซนเซอร์ตรวจจับความร้อน (6) เซนเซอร์ตรวจจับก๊าซ (7) เซนเซอร์ตรวจจับแรงสั่นสะเทือน พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.76)

6.1.3.3 ผลการประเมินความเหมาะสมด้าน โมดูลย่อยของระบบ ประกอบด้วย (1) โมดูลตรวจจับใบหน้า (2) โมดูลสแกนบัตร (3) โมดูลตรวจจับป้ายทะเบียน (4) โมดูลตรวจจับควัน (5) โมดูลตรวจจับความร้อน (6) โมดูลตรวจจับก๊าซ (7) โมดูลตรวจจับแรงสั่นสะเทือน พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.76)

6.1.3.4 ผลการประเมินความเหมาะสมด้าน การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย ประกอบด้วย (1) แจ้งเตือนผ่านไลน์แอพพลิเคชั่น (2) การประเมินและควบคุมความเสี่ยง (3) ระบบจัดการรายงาร พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.76, S.D. = 0.50)

6.1.3.5 ผลการประเมินความเหมาะด้าน เว็บเซิร์ฟเวอร์และดาด้าเบสเซิร์เวอร์ พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.70, S.D. = 0.67)

6.1.3.6 ผลการประเมินความเหมาะสมด้าน หลักการทำงานของสถาปัตยกรรมระบบ ประกอบด้วย (1) หลักการทำงานของระบบ (2) ความเหมาะสมของอุปกรณ์ตรวจจับ (3) ความเหมาะสมของระบบการแจ้งเตือน (4) ความเหมาะสมของระบบจัดเก็บข้อมูล พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.70, S.D. = 0.50)

6.1.4 สรุปผลการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ แบ่งออกเป็น 2 ส่วน ประเมินโดยผู้เชี่ยวชาญ จำนวน 10 ท่าน มีดังนี้

6.1.4.1 ผลการประเมินการออกแบบระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ที่มีความสัมพันธ์ทั้งหมด 6 ส่วน ประกอบด้วย 1. ผู้ที่เกี่ยวข้องกับระบบ 2. ไอโอทีดีไวท์สำหรับการตรวจจับบุคคลและวัตถุ 3. โมดูลย่อยของระบบ 4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย 5. เว็บเซิร์ฟเวอร์และดาด้าเบสเซิร์เวอร์ 6. หลักการทำงานของระบบ ซึ่งมีการประเมินใน 6 ด้าน พบว่าในภาพรวมอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ = 4.94, S.D. = 0.17) ซึ่งแต่ละด้านมีรายละเอียดดังนี้

6.1.4.1.1 ผลการประเมินความเหมาะสมด้าน ผู้ที่เกี่ยวข้องกับ ประกอบด้วย (1) ผู้บริหารระบบ (2) ผู้บริหารสถานศึกษา (3) เจ้าหน้าที่รักษาความปลอดภัย (4) ผู้ใช้งานระบบ พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุดพบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.80, S.D. = 0.41)

6.1.4.1.2 ผลการประเมินความเหมาะสมด้าน ไอโอทีดีไวท์สำหรับการตรวจจับบุคคลและวัตถุ ประกอบด้วย (1) กล้องตรวจจับใบหน้า (2) บัตร RFID (3) กล้องตรวจจับป้ายทะเบียน (4) เซนเซอร์ตรวจจับควัน (5) เซนเซอร์ตรวจจับความร้อน (6) เซนเซอร์ตรวจจับก๊าซ (7)เซนเซอร์ตรวจจับแรงสั่นสะเทือน พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.50, S.D. = 0.70)

6.1.4.1.3 ผลการประเมินความเหมาะสมด้าน โมดูลย่อยของระบบ ประกอบด้วย (1) โมดูลตรวจจับใบหน้า (2) โมดูลสแกนบัตร (3) โมดูลตรวจจับป้ายทะเบียน (4) โมดูลตรวจจับควัน (5) โมดูลตรวจจับความร้อน (6) โมดูลตรวจจับก๊าซ (7) โมดูลตรวจจับแรงสั่นสะเทือน พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19)

6.1.4.1.4 ผลการประเมินความเหมาะสมด้าน การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย ประกอบด้วย (1) แจ้งเตือนผ่านไลน์แอพพลิเคชั่น (2) การประเมินและควบคุมความเสี่ยง (3) ระบบจัดการรายงาร พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19)

6.1.4.1.5 ผลการประเมินความเหมาะด้าน เว็บเซิร์ฟเวอร์และดาด้าเบสเซิร์ฟเวอร์ พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19)

6.1.4.1.6 ผลการประเมินความเหมาะสมด้าน หลักการทำงานของสถาปัตยกรรมระบบ ประกอบด้วย (1) หลักการทำงานของระบบ (2) ความเหมาะสมของอุปกรณ์ตรวจจับ (3) ความเหมาะสมของระบบการแจ้งเตือน (4) ความเหมาะสมของระบบจัดเก็บข้อมูล พบว่ามีค่าเฉลี่ยระดับความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.93, S.D. = 0.19)

6.1.4.2 ผลการประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ซึ่งมีการประเมินใน 4 ด้าน พบว่าในภาพรวมอยู่ในระดับ ความเหมาะสมมากที่สุด ($\bar{X}$ =4.63, S.D. =0.48) ซึ่งแต่ละด้านมีรายละเอียดดังนี้

6.1.4.2.1 ผลการประเมินประสิทธิภาพด้านโมดูลย่อย(Module Test) ของระบบ ประกอบด้วย 1. โมดูลการวางระบบโครงสร้างพื้นฐาน (Infrastructure Management System : IMS) 2. โมดูลระบบตรวจจับใบหน้า (Face Detection System) 3. โมดูลระบบแสกนบัตร (RFID System) 4. โมดูลตรวจจับป้ายทะเบียนรถ (License Plate Detection) 5. โมดูลตรวจจับความร้อน (Heat Detection System) 6. โมดูลตรวจจับควัน (Smoke Detection System) 7. โมดูลตรวจจับก๊าซ (Gas Detection System) 8. โมดูลตรวจจับแรงสั่นสะเทือน (Vibration Detection System) 9. โมดูลการแจ้งเตือน (Notification) 10. โมดูลการประเมินและควบคุมความเสี่ยง (Risk Assessment & Control) พบว่าในภาพรวมอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ =4.61, S.D. =0.57)

6.1.4.2.2 ผลการประเมินประสิทธิภาพด้านการทำงานของระบบทั้งหมด (System Test) ประกอบด้วย 1. ความสามารถในการพิสูจน์ตัวตน (Authentication) 2. ความสามารถของระบบจัดเก็บข้อมูล 3. ความสามารถของความสัมพันธ์ในแต่ละระบบงานย่อยในการใช้ข้อมูลร่วมกัน 4. ความสามารถในการลดเวลาและทรัพยากรในการทำงาน 5. ความครบถ้วนของฟังก์ชันการทำงานของระบบ 6. ความสามารถเชื่อมต่อประสาน (Plug) ส่วนเพิ่มเติม 7. มีแนวโน้มในการปรับปรุงระบบได้ง่ายและรวดเร็ว พบว่าในภาพรวมอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ =4.70, S.D. =0.40)

6.1.4.2.3 ผลการประเมินประสิทธิภาพด้านการใช้งานระบบ (Usability Test) ประกอบด้วย 1. ความง่ายและความสะดวกในการใช้งานระบบ 2. ความเหมาะสมของตำแหน่งการจัดวางส่วนต่าง ๆ บนจอภาพ 3. การแบ่งเมนูของระบบสามารถเข้าใจได้ง่าย 4. ความชัดเจนของข้อความที่แสดงบนจอภาพ 5. ความเหมาะสมของตัวอักษรเกี่ยวกับขนาด สี ความชัดเจน ง่าย ต่อการอ่าน 6. ความเหมาะสมของปริมาณข้อมูลที่นำเสนอในแต่ละหน้าจอ 7. ความเหมาะสมในการตอบสนองระบบในภาพรวม พบว่าในภาพรวมอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ =4.58, S.D. =0.48)

6.1.4.2.4 ผลการประเมินประสิทธิภาพด้านความปลอดภัยของระบบ (Security Test) ประกอบด้วย 1. การตรวจสอบสิทธิ์ในการเข้าใช้งานของผู้ใช้ระบบ 2. การแจ้งเตือนเมื่อพบข้อผิดพลาดในการเข้าใช้งาน 3. ความเหมาะสมในการรักษาความปลอดภัยของระบบ โดยภาพรวมพบว่าในภาพรวมอยู่ในระดับความเหมาะสมมากที่สุด ($\bar{X}$ =4.66, S.D. =0.47)

6.1.5 สรุปผลการศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยกลุ่มตัวอย่างได้จากการเลือกแบบเจาะจง จำนวน 50 คน ประกอบด้วยผู้บริหาร ครู อาจารย์ บุคคลกรทางการศึกษาจากสถานศึกษาทั้งในระบบและนอกระบบในเขตพื้นที่การศึกษาจังหวัดชายแดนภาคใต้ ประกอบด้วย นราธิวาส ยะลา ปัตตานี การศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ประกอบด้วย 2 ส่วน ดังนี้

6.1.5.1 ผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ จากผู้ใช้ระบบ พบว่า มีความเหมาะสมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.94, S.D. = 0.17) ที่ประกอบด้วย 1) การวางระบบโครงสร้างพื้นฐาน 2) ระบบตรวจจับใบหน้า 3) ระบบสแกนบัตร 4) ตรวจจับป้ายทะเบียนรถ 5) ตรวจจับความร้อน 6) ตรวจจับควัน 7) ตรวจจับก๊าซ 8) ตรวจจับแรงสั่นสะเทือน 9) การแจ้งเตือน 10) การประเมินและควบคุมความเสี่ยง 11) ภาพรวมของผลการใช้ระบบ

6.1.5.2 ความพึงพอใจของผู้ใช้ต่อการใช้งานระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ พบว่า ผู้ใช้มีความพึงพอใจอยู่ในระดับมากที่สุด เนื่องจากผู้ใช้ระบบเกิดความสะดวกต่อการใช้งานระบบ กระบวนการทำงานของระบบที่ไม่ซับซ้อน สามารถเข้าถึงข้อมูลได้ง่ายด้วยเทคโนโลยีไร้สายที่ผู้ใช้ระบบส่วนใหญ่มักคุ้นชินกับการทำงานในชีวิตประจำวัน ผู้ใช้มีความตระหนักเนื่องจากนโยบายและการให้ความสำคัญเกี่ยวกับรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้ใช้มีความรู้สึกถึงความปลอดภัยเพิ่มขึ้น เนื่องจากระบบมีการแจ้งเตือนความมั่นคงปลอดภัยทำให้ผู้ใช้สามารถวิเคราะห์และตัดสินใจได้ทันทวงทีในการวางแผนการเดินทางไปยังสถานที่เมื่อเกิดเหตุการณ์ความไม่ปลอดภัย

6.2 อภิปรายผล

จากการการวิเคราะห์และสังเคราะห์เอกสารงานวิจัยที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสูงสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ การสอบถามกลุ่มตัวอย่างประกอบด้วยผู้บริหาร ครู อาจารย์ บุคลากรทางการศึกษา จนนำไปสู่การพัฒนาระบบการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ตลอดจนผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ สามารถอภิปรายผลตามวัตถุประสงค์ของการวิจัย โดยมีรายละเอียดดังนี้

6.2.1 การวิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ในส่วนนี้ผู้วิจัยทำการศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยประกอบด้วย ระเบียบ และ มาตรการทางด้านการรักษาความปลอดภัยสำหรับสถานศึกษา เป็นเกณฑ์มาตรฐานหนึ่งที่ได้กำหนดขึ้นจากหน่วยงานของรัฐบาลที่แสดงให้เห็นถึงแนวทางการรักษาความปลอดภัยสำหรับสถานศึกษา ประกอบด้วย 3 ส่วนคือ การรักษาความมั่นคงปลอดภัยเกี่ยวกับบุคคล การรักษาความมั่นคงปลอดภัยเกี่ยวกับสถานที่ และ การป้องกันและแก้ไขปัญหาด้านความไม่สงบ ซึ่งมีความเกี่ยวข้องกับกระบวนการรักษาความมั่นคงปลอดภัย ซึ่งแบ่งออกเป็น 4 ระบบ คือ 1) ระบบยืนยันตัวตน 2) ระบบควบคุมการเข้า-ออกยานพาหนะ 3) ระบบตรวจจับและแจ้งเตือนภัยภายในอาคาร และ 4) ระบบฐานข้อมูลด้านความมั่นคง ในส่วนของเทคโนโลยีเชื่อมโยงใช้การตรวจจับด้วย กล้องตรวจจับ เซนเซอร์ และ บัตรอาร์เอฟไอดี โดยใช้กับโมดูลทั้ง 7 ส่วน ได้แก่ 1) โมดูลตรวจจับใบหน้า 2) โมดูลสแกนบัตร 3) โมดูลตรวจจับทะเบียนรถ 4) โมดูลตรวจจับควันไฟ 5) โมดูลตรวจจับความร้อน 6) โมดูลตรวจจับก๊าซ 7) โมดูลตรวจจับแรงสั่นสะเทือน ซึ่งสารสนเทศที่ได้จากโมดูลทั้ง 7 จะอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิคส์หรือหลักฐานดิจิทัล (Digital Forensic) ที่ประกอบด้วย 3 ส่วน คือ 1) การรวบรวมพยานหลักฐาน 2) การวิเคราะห์เพื่อประเมินความเสี่ยง 3) การรายงานความมั่นคงปลอดภัยการพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

6.2.2 การพัฒนาแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ อยู่ในระดับมากที่สุด โดยแบ่งออกเป็น 4 มิติ ประกอบด้วย 1. มิติด้านการรักษาความปลอดภัยสำหรับสถานศึกษา 2. มิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา 3. มิติด้านการบริหารจัดการข้อมูล 4. มิติด้านการตรวจสอบหลักฐานดิจิทัล ซึ่งมีรายละเอียดการประเมินดังนี้

6.2.3 การออกแบบสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ อยู่ในระดับมากที่สุด ประกอบด้วย 1. ผู้ที่เกี่ยวข้องกับระบบ (Stakeholders) 2. ไอโอทีดีไวซ์ สำหรับการตรวจจับบุคคลและวัตถุ 3. โมดูลย่อยของระบบ 4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย 5. เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server) 6. หลักการทำงานของสถาปัตยกรรมระบบ

6.2.4 การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ อยู่ในระดับมากที่สุด

ประกอบด้วย 1. โมดูลตรวจจับใบหน้า 2. โมดูลสแกนบัตร 3. โมดูลตรวจจับป้ายทะเบียน 4. โมดูลตรวจจับควันไฟ 5. โมดูลตรวจจับความร้อน 6. โมดูลตรวจจับก๊าซ 7. โมดูลตรวจจับแรงสั่นสะเทือน

6.2.5 การศึกษาผลการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ อยู่ในระดับมากที่สุดเนื่องจากผู้บริหาร ผู้ใช้ระบบ มีความรู้ความเข้าใจในการใช้งานระบบ ผู้ใช้ระบบเกิดความสะดวกต่อการใช้งานระบบ โดยมีกระบวนการทำงานของระบบที่ไม่ซับซ้อน สามารถเข้าถึงข้อมูลได้ง่ายด้วยเทคโนโลยีไร้สายที่ผู้ใช้ระบบส่วนใหญ่มักคุ้นชินกับการทำงานในชีวิตประจำวัน ผู้ใช้มีความตระหนักเนื่องจากนโยบายและการให้ความสำคัญเกี่ยวกับรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้ใช้มีความรู้สึกถึงความปลอดภัยเพิ่มขึ้น เนื่องจากระบบมีการแจ้งเตือนความมั่นคงปลอดภัย ทำให้ผู้ใช้สามารถวิเคราะห์และตัดสินใจได้ทันทวงทีในการวางแผนการเดินทางไปยังสถานที่เมื่อเกิดเหตุการณ์ความไม่ปลอดภัย

6.2.6 ผลการนำระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ทำให้สถานศึกษาเพิ่มประสิทธิภาพทางด้านการป้องกันและรักษาความมั่นคงปลอดภัย ระบบสามารถทำการตรวจสอบและบันทึกกระบวนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา ไม่ว่าจะเป็นการรักษาความปลอดภัยสำหรับบุคคล การรักษาความปลอดภัยสำหรับสถานที่ การป้องกันและแก้ไขปัญหาด้านผลกระบทจาการสู้รบและความไม่สงบ ทำให้สถานศึกษามีความพร้อมในการรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้นได้ ซึ่งสถานณ์การณ์ในจังหวัดชายแดนภาคใต้อยู่ในระดับความเสียงสูงที่หน่วยงานจำเป็นต้องมีการป้องกันภัยจากเหตุการณ์การก่อความไม่สงบ โดยความขัดแย้งที่เกิดขึ้นย่อมส่งผลกระทบต่อกระบวนการทำงานขององค์กร หน่วยงานหรือสถานศึกษา รวมไปถึง นักเรียน นักศึกษา ครู อาจารย์ บุคลากร ผู้ปกครอง และประชาชนรอบข้าง ซึ่งเมือเกิดเหตุการณ์ดังกล่าว ไม่ว่าจะเป็นภาครัฐ หรือ ภาคเอกชน ก็ได้พยายามในการแก้ไขปัญหาอย่างต่อนี้เพื่อยุติความขัดแย้ง แต่ทั้งนี้ การนำระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มาใช้สามารถเข้ามาช่วยป้องกันและแก้ไขปัญหาดังกล่าวได้ ส่งผลต่อการลดความเสี่ยงทางด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาได้อย่างมีประสิทธิภาพ

6.3 ข้อเสนอแนะ

ผลจากการวิจัยเรื่อง การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ มีข้อเสนอแนะสำหรับการวิจัย ดังนี้

6.3.1 พัฒนาโมดูลการรับข้อมูลจากการให้ข้อมูลข่าวสารที่เป็นประโยชน์ต่อการรักษาความปลอดภัยเพื่อนำเข้าสู่ระบบรักษาความมั่นคงปลอดภัย

6.3.2 พัฒนาระบบรักษาความมั่นคงปลอดภัย เป็นแอพพลิเคชัน (Application) ทั้งระบบปฏิบัติการแอนดรอยด์ (Android) และ ระบบปฏิบัติการไอโอเอส (IOS)

6.3.3 พัฒนาให้ระบบรักษาความมั่นคงปลอดภัยสามารถเชื่อมโยงด้วยระบบดาวเทียมเพื่อเพิ่มประสิทธิภาพการทำงานของระบบให้สูงขึ้น

6.3.4 พัฒนาระบบให้รองรับการเปลี่ยนแปลงของบัตรสมาร์ทการ์ด เช่น บัตรนักเรียน นักศึกษา บุคลากร เจ้าหน้าที่ ให้เป็นบัตรสามาร์ทการ์ด หรือ Smart Card : IoT

6.3.5 พัฒนาการเชื่อมต่อระบบรักษาความมั่นคงปลอดภัยเพื่อให้สามารถเชื่อมต่อกับระบบหน่วยงานภายในและหน่วยงานภายนอก ทั้งนี้หากระบบได้รับการพัฒนาเพิ่มเติม จะทำให้ระบบสามารถเชื่อมโยงและติดต่อสื่อสารร่วมกัน ส่งผลให้การสื่อสารเชื่อมต่อร่วมกับหน่วยงานทั้งภายในและภายนอกได้อย่างทันท่วงที เพื่อการสนับสนุนการตัดสินใจและแก้ไขปัญหาด้านความมั่นคงปลอดภัยได้อยางมีประสิทธิภาพ

บรรณานุกรม

ภาษาไทย

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2545). [ออนไลน์]. กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสารระยะ พ.ศ. 2554-2563 ของประเทศไทย ICT2020. [สืบค้นวันที่ 7 มิถุนายน 2560] จาก http://ict.rid.go.th/main/images/th/public-doc/doc/ict2020_book.pdf

กลุ่มด้วยใจ. (2561). [ออนไลน์]. รายงานสถานการณ์เด็กในจังหวัดชายแดนภาคใต้ประจำปี 2560. [สืบค้นวันที่ 7 มิถุนายน 2561]" จาก https://deepsouthwatch.org/sites/default/files/archives/docs/dj_children_in_southern_conflict_2017_edited_clean.pdf

กัลยา วานิชย์บัญชา. (2554). หลักสถิติ. กรุงเทพมหานคร : โรงพิมพ์แห่งจุฬาลงกรณ์หมาวิทยาลัย.

ฉัตรศิริ ปิยะพิมลสิทธิ์. (2554). [ออนไลน์]. ค่าเฉลี่ยเลขคณิต. [สืบค้นวันที่ 9 พฤษภาคม 2559]. จาก http://www.watpon.com/Elearning/stat8.htm

ชาติกาย วิเรชรัตน์. (2558). [ออนไลน์]. ทำความเข้าใจเรื่อง internet of Things (IoT) เทรนด์ที่หลายคนกำลังพูดถึง. [สืบค้นวันที่ 25 กันยายน 2560]. จาก http://goo.gl/hgRYBa

ต่วนนูรีซันน์ สุริยะ. (2559). "อินเทอร์เน็ตออฟธิงส์กับการบริหารจัดการห้องเรียนอัจฉริยะ." วารสารการอาชีวะและเทคนิคศึกษา. ปีที่ 6 ฉบับที่ 11 : 26-31.

พระราชบัญญัติ การรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2551. (2551). [ออนไลน์]. การรักษาความมั่นคงภายในราชอาณาจักร. [สืบค้นวันที่ 25 กันยายน 2560]. จาก https://www.ocsc.go.th/sites/default/files/attachment/page/stabitity-2551.pdf

รุ่ง แก้วแดง. (2548). สงครามและสันติสุข @ ชายแดนภาคใต้. กรุงเทพมหานคร : มติชน.

ศูนย์เฝ้าระวังสถานการณ์ภาคใต้. (2561). [ออนไลน์]. ฐานข้อมูลเหตุการณ์ชายแดนใต้. [สืบค้นวันที่ 25 กันยายน 2560]. จาก https://deepsouthwatch.org/en/node/

ศูนย์เฝ้าระวังสถานการณ์ภาคใต้. (2561). [ออนไลน์]. รายงานสถานการณ์ ความขัดแย้งรุนแรงในชายแดนใต้. [สืบค้นวันที่ 25 กันยายน 2560]. จาก https://deepsouthwatch.org/th/node/11899

ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2560). [ออนไลน์]. ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐาน. [สืบค้นวันที่ 25 กันยายน 2560]. จาก www.etda.or.th

ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2560). [ออนไลน์]. ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน Version 1.0. [สืบค้นวันที่ 25 กันยายน 2560]. จาก www.thicert.or.th

สำนักข่าวกรองแห่งชาติ. (2553). [ออนไลน์]. มาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน. [สืบค้นวันที่ 25 กันยายน 2560]. จาก http://www.edupol.org/eduOrganize/eLearning/generalStaff/doc/group09/05/04.pdf

สำนักงานสภาความมั่นคงแห่งชาติ. (2558). [ออนไลน์]. นโยบายการบริหารและการพัฒนาจังหวัดชายแดนภาคใต้ พ.ศ 2560 – 2562. [สืบค้นวันที่ 25 กันยายน 2560]. จาก http://www.nsc.go.th/

สำนักงานสภาความมั่นคงแห่งชาติ. (2558). [ออนไลน์]. นโยบายความมั่นคงแห่งชาติ พ.ศ. 2548-2564. [สืบค้นวันที่ 25 กันยายน 2560]. จาก http://www.nsc.go.th/Download1/policy58.pdf

สำนักนายกรัฐมนตรี. (2552). [ออนไลน์]. ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552. [สืบค้นวันที่ 25 กันยายน 2560]. จาก https://www.secnia.go.th/

สำนักอำนวยการ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน. (2556). [ออนไลน์]. คู่มือแนวทางปฏิบัติและมาตรการรักษาความปลอดภัยของสถานศึกษา ฉบับปรับปรุง พ.ศ. 2556. [สืบค้นวันที่ 25 กันยายน 2560]. จาก http://www.phichai.ac.th/home/5.pdf

อรฉัตร จิตต์โสภักตร์ม และจตุพล เบญจประกายรัตน์ชัยพิทกัษ์. (2558). ระบบตรวจจับใบหน้าและติดตามบุคคลผ่านกล้องวงจรปิด. กรุงเทพฯ : คณะวศิวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาษาอังกฤษ

Alessio, Walter, Valerio and Antonio. (2016). “Integration of Cloud Computingand Internet of Things: a Survey.” Future Generation Computer Systems. [cited 2016]. Available from : URL : http://dx.doi.org/10.1016/j.future.2015.09.021

Al-Fuqaha, A., et al. (2015). [serial online]. “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications.” IEEE Communications Surveys Tutorials. [cited 2016]. Available from : URL : doi:10.1109/COMST.2015.2444095. ISSN 1553-877X.

Ashton, K. (2009). [serial online]. “That ‘Internet of Things’ Thing.” RFiD Journal. [cited 2017]. Available from : URL : https://www.rfidjournal.com/articles/view?4986

Asimakopoulou. (2013). [serial online]. “The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments.” Springer-Verlag Berlin Heidelberg. [cited 2016]. Available from : URL : https://doi.org/10.1007/978-3-642-34952-2_4

Bessis, N., et al. (2013). [serial online]. Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence. [cited 2016]. Available from : URL : https://www.springer.com/gp/book/9783642349515

Casey, E. (2011). Digital Evidence and Computer Crime. (Third Edition). Waltham : Academic Press Publication.

Eoghan Casey. (2010). [online]. Handbook of Digital Forensics and Investigation. [cited 2016]. Available from : URL : https://doi.org/10.1016/C2009-0-01683-3

Evdokimov, S., et al. (2010). “RFID and the Internet of Things : Technology Applications, and Security Challenges.” Foundations and Trends in Technology, Information and Operations Management. Vol.4 No.2 : 105-185

Fatma Ozmen, Ceyhun Dur and Tulin Akgul. (2010). “School security problems and the ways of tackling them.” Procedia - Social and Behavioral Sciences. Vol.2010 No.2 : 5377-5383.

G. Cristian Gonzalez et al. (2017). “Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes.” Future Generation Computer Systems. Vol.76 : 301-313.

Gonzalez, R. C. and R. E. Woods. (2002). Digital Image Processing. New Jersey : Prentice-Hall, Inc.

Jason Sentell. (2014). [online]. Barcodes and the Internet of Things. [cited 2016]. Available from : URL : http://www.waspbarcode.com/buzz/barcodes-internet-things/

Jeannette Chin, Vic Callaghan. (2013). [serial online]. "Educational Living Labs; A novel Internet-of-Things based Approach to Teaching and Research." 2013 9th International Conference on Intelligent Environments. [cited 2017]. Available from : URL : DOI 10.1109/IE.2013.48

John Edwards. (2015). [online]. Internet of Things breathes new life into RFID technology. [cited 2016]. Available from : URL : http://goo.gl/Ouhg9E

Kathy Gilsinan. (2014). [online]. Terrorist Attacks on Schools Have Soared in the Past 10 Years. [cited 2016]. Available from : URL : https://www.theatlantic.com/international/archive/2014/12/terrorist-attacks-on-schools-have-soared-in-the-past-10-years/383825/

Laykin, E. (2013). Investigative Computer Forensics. Canada : Simultaneously.

Maros, L. and R, Jozef. (2017). "Smart city, Safety and Security. International scientific conference on sustainable." Modern and safe transport. Procedia Engineering. Vol.2017 No.192 : 522-527.

Molloy, D. (2015). Exploring Beaglebone tools and techniques for building with embedded linux. USA : John Wiley & Sons,Inc.

Gasparik, M and Solek, P. (2014). [serial online]. "Design the robot as security system in the home." Procedia Engineering. Vol.2014 No.96 : 126-130.

Paul Timm., et al. (2015). School Security How to Build and strengthen a School Safety Program. Waltham, USA : Elsvier Inc.

Pietikainen, M. and L. F. Pau. (1996). Machine Vision for Advanced Production. New York : World Scientific.

R. Nunes-Vaz. (2014). "Designing physical security for complex infrastructures." International journal of critical infrastructure protection. Vol.2014 No.7 : 178-192.

Sentell, J. (2014). [online]. Barcodes and the internet of Things. [cited 2016]. Available from : URL : http://goo.gl/tlfL5s

Shane Buckley. (2014). [online]. Industries Entrepreneurs Can Disrupt With the Internet of Things. [cited 2015]. Available from : URL : http://www.entrepreneur.com/article/241001

Sonka, M., Hlavac, V., and Boyle, R. (2014). [online]. Image Processing, Analysis, and Machine Vision. Cengage Learning. [cited 2016]. Available from : URL : http://user.engineering.uiowa.edu/~sonka/ps-files/cfai.pdf

Strommer, E., Hillukkala, M. and Ylisaukko-oja, A. (2007). "Ultra-low Power Sensors with Near Field Communication for Mobile Applications." The Intemational Federation for Information Processing. Vol.48 : 131-142.

Thomas L. Norman. (2012). [online]. Risk Analysis and Security Countermeasure Selection 1st Edition. [cited 2015]. Available from : URL : https://www.elsevier.com/books/school-security/timm/978-0-12-407811-6

Want, Roy, Bill, N., Schilit and Scott Jenson. (2015). "Enabling the Internet of Things." IEEE. Vol.48 No.1 : 28-35.

Wolff Olins. (2012). [online]. The Internet of Things. [cited 2016]. Available from : URL : http:// archive.wolffolin.com/blog/16357411549/this-the-first-future-patrol-a-monthly-series

Xu Xingmei, Zhou Jing and Wang He. (2013). "Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things." in 2013 3rd International Conference on Computer Science and Network Technology. China : Curran Associates, Inc. : (825-828).

ภาคผนวก ก

รายนามผู้เชี่ยวชาญ

รายนามผู้เชี่ยวชาญ

1. ผศ.ดร.ศรัณ ณงค์กูล
   ตำแหน่ง อาจารย์ประจำสาขาวิชาเทคโนโลยีไฟฟ้าอุตสาหกรรม
   สังกัด มหาวิทยาลัยราชภัฏสงขลา
2. ดร.กันตภณ มะหาหมัด
   ตำแหน่ง รองคณบดีฝ่ายวิชาการคณะเทคโนโลยีอุตสาหกรรม
   สังกัด มหาวิทยาลัยราชภัฏสงขลา
3. ดร.วัจนารัตน์ ควรดี
   ตำแหน่ง อาจารย์ประจำสาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี
   สังกัด มหาวิทยาลัยราชภัฏสุรินทร์
4. ดร. ธนะวัชร จริยะภูมิ
   ตำแหน่ง ประธานสาขาวิชาคอมพิวเตอร์ธุรกิจ คณะบริหารธุรกิจ
   สังกัด มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
5. ผู้ช่วยศาสตราจารย์ ดร. สมศักดิ์ เตชะโกสิต
   ตำแหน่ง อาจารย์กลุ่มสาระการเรียนรู้วิทยาศาตร์และเทคโนโลยี(วิทยาศาสตร์)
   สังกัด โรงเรียนสาธิตแห่งมหาวิทยาลัยเกษตรศาสตร์ ศูนย์วิจัยและพัฒนาการศึกษา
6. ดร.อนุชิต อนุพันธ์
   ตำแหน่ง อาจารย์ประจำโปรแกรมวิชาคอมพิวเตอร์ศึกษา คณะคุรุศาสตร์
   สังกัด มหาวิทยาลัยราชภัฏศรีสะเกษ
7. ดร.สุริยะ พุ่มเฉลิม
   ตำแหน่ง หัวหน้าสาขาวิชาคอมพิวเตอร์ธุรกิจ คณะวิทยาศาสตร์และเทคโนโลยี
   สังกัด มหาวิทยาลัยเซาธ์อีสบางกอกมหาวิทยาลัยสวนดุสิต
8. ดร.นาวิน คงรักษา
   ตำแหน่ง รองคณบดีคณะวิทยาศาสตร์และเทคโนด
   สังกัด มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
9. ดร.จักรกฤษณ์ เปรมสมิทธ์
   ตำแหน่ง อาจารย์ประจำวิทยาลัยเทคโนโลยีอุตสาหกรรม
   สังกัด มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

10. ดร.กวิตา ปานล้ำเลิศ
    ตำแหน่ง อาจารย์ประจำคณะวิทยาการจัดการ
    สังกัด มหาวิทยาลัยสวนดุสิต
11. ดร.สุดารัตน์ ศรีมา
    ตำแหน่ง รองผู้อำนวยการฝ่ายวิชาการ (มัธยม)
    สังกัด โรงเรียนสาธิตมหาวิทยาลัยราชภัฏสวนสุนันทา
12. ดร.จารุมน หนูคง
    ตำแหน่ง รองผู้อำนวยการฝ่ายวิชาการ
    สังกัด มหาวิทยาลัยราชภัฏสวนสุนันทา
13. ผศ.ดร.วีระชัย แสงฉาย
    ตำแหน่ง คณบดี คณะเทคโนโลยีอุตสาหกรรม
    สังกัด มหาวิทยาลัยราชภัฏสงขลา
14. ว่าที่ร้อยตรี ดร.ชาครีย์ คะนอง
    ตำแหน่ง ผู้อำนวยการโรงเรียนบ้านตะโละไกรทอง
    สังกัด โรงเรียนบ้านตะโละไกรทอง จังหวัด ปัตตานี

ภาคผนวก ข

เครื่องมือที่ใช้ในการวิจัย

- แบบสอบถามสำหรับวิเคราะห์สภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบ
- แบบประเมินการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้
- แบบประเมินคุณลักษณะระบบรักษาความปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้
- แบบประเมินองค์ประกอบของคุณลักษณะระบบรักษาความปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้
- แบบประเมินแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้
- แบบประเมินสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้
- แบบประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้
- แบบประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

แบบสอบเพื่อวิเคราะห์สภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

การวิจัยนี้เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยมีวัตถุประสงค์เพื่อ **วิเคราะห์การรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้**

แบบสอบถามฉบับนี้แบ่งออกเป็น 3 ขั้นตอน ประกอบด้วย

ตอนที่ 1 ว่าด้วยข้อมูลสถานภาพทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 การวิเคราะห์สภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบ และ

ตอนที่ 3 ว่าด้วยข้อเสนอแนะอื่น ๆ

<u>ตอนที่ 1</u> ข้อมูลสถานภาพทั่วไปของผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ลงใน ☐ หน้าข้อความที่ตรงกับสภาพความเป็นจริงของท่าน และเติมข้อความให้สมบูรณ์

1.เพศ ☐1.ชาย ☐2. หญิง

2.อายุ ☐1.20-29 ปี ☐2. 30-39 ปี

☐3. 40-49 ปี ☐4. 50 ปีขึ้นไป

3.วุฒิการศึกษา ☐1. ปริญญาตรี ☐2. ปริญญาโท

☐3. ปริญญาเอก ☐4. อื่น ๆ (ระบุ).....

4.ตำแหน่ง ☐1. ผู้บริหาร ☐2. ครู อาจารย์ ☐3.บุคลากรสายสนับสนุน

5.สถานที่ทำงาน .....

6.ระยะเวลาการทำงาน ☐1. 1-5 ปี ☐2. 6-10 ปี

☐3. 11-15 ปี ☐4. 15 ปีขึ้นไป

<u>ตอนที่ 2</u> **การวิเคราะห์สภาพปัญหาและศึกษาความต้องการในการพัฒนาระบบ**

ประเด็นคำถาม	ข้อคิดเห็น/ข้อเสนอแนะของผู้เชี่ยวชาญ
ด้านที่ 1. การรักษาความปลอดภัยเกี่ยวกับบุคค (Personal security)	
1.1 การตรวจสอบประวัติและพฤติกรรมบุคคล	
1.2 การควบคุมและบันทึกเวลาการเข้า – ออก ของบุคคล	
ด้านที่ 2. การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Place security)	
2.1 ระบบตรวจจับและแจ้งเตือนภัย	
2.2 ระบบแจ้งเตือนมวลชนผ่านข้อความโทรศัพท์มือถือ	
2.3 ระบบควบคุมยานพาหนะเข้า – ออก	
2.4 กล้องโทรทัศน์วงจรปิด	
ด้าน 3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ (Prevention of war and its environment consequence)	
3.1 การประสานความร่วมมือกับหน่วยงานด้านความมั่นคง	-
3.2 ฐานข้อมูลด้านความมั่นคง	-

<u>ตอนที่ 3</u> ข้อเสนอแนะอื่น ๆ

<u>คำชี้แจง</u> โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับวิเคราะห์สภาพปัญหาและความต้องการในการพัฒนาระบบรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

แบบประเมินการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วยคำถามเกี่ยวกับการรักษาความปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยท่านสามารถพิจารณารายละเอียดตามเอกสารที่ส่งมาด้วย

โปรดทำเครื่องหมาย √ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณาดังนี้

5 หมายถึง มีความเหมาะสมมากที่สุด
4 หมายถึง มีความเหมาะสมมาก
3 หมายถึง มีความเหมาะสมปานกลาง
2 หมายถึง มีความเหมาะสมน้อย
1 หมายถึง มีความเหมาะสมน้อยที่สุด

แบบประเมินการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อผู้ประเมิน.....

ตำแหน่ง.....

สถานที่ทำงาน.....

ตอนที่ 2 แบบประเมินการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ระดับความเหมาะสม**					**ข้อเสนอแนะ**
	5	**4**	**3**	**2**	**1**	
1. การรักษาความปลอดภัยเกี่ยวกับบุคคล						
1.1 การตรวจสอบประวัติและพฤติกรรมบุคคล						
1.2 การควบคุมและบันทึกเวลาการเข้า – ออกของบุคคล						
2. การรักษาความปลอดภัยเกี่ยวกับสถานที่						
2.1 ระบบตรวจจับและแจ้งเตือนภัย						
2.2 ระบบแจ้งเตือนมวลชนผ่านข้อความโทรศัพท์มือถือ						
2.3 ระบบควบคุมยานพาหนะเข้า - ออก						
3. การป้องกันและแก้ไขปัญหาด้านความไม่สงบ						
3.1 การประสานความร่วมมือกับหน่อยงานด้านความมั่นคง						
3.2 ฐานข้อมูลด้านความมั่นคง						

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

คำชี้แจง โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

.....

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

แบบประเมินคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่ง เพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วยคำถามเกี่ยวกับคุณลักษณะของการรักษาความปลอดภัย โดยท่านสามารถพิจารณารายละเอียดตามเอกสารที่ส่งมาด้วย

โปรดทำเครื่องหมาย √ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณาดังนี้

5 หมายถึง มีความเหมาะสมมากที่สุด
4 หมายถึง มีความเหมาะสมมาก
3 หมายถึง มีความเหมาะสมปานกลาง
2 หมายถึง มีความเหมาะสมน้อย
1 หมายถึง มีความเหมาะสมน้อยที่สุด

แบบประเมินคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 แบบประเมินคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อผู้ประเมิน.....

ตำแหน่ง.....

สถานที่ทำงาน..... .....

ตอนที่ 2 แบบประเมินคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ระดับความเหมาะสม**					**ข้อเสนอแนะ**
	5	**4**	**3**	**2**	**1**	
1. ระบบยืนยันตัวตน						
1.1 บัตรเข้าออก						
1.2 ระบบตรวจจับใบหน้า						
2. ระบบควบคุมการเข้า - ออก ยานพาหนะ						
2.1 บัตรเข้าออก						
2.2 ระบบอ่านป้ายทะเบียนรถ						
2.3 ระบบควบคุมยานพาหนะเข้า - ออก						
3. ระบบตรวจจับและแจ้งเตือนภายในอาคาร						
3.1 ตรวจจับควันไฟ						
3.2 ตรวจจับความร้อน						
3.3 ตรวจจับก๊าซ						
3.4 ตรวจจับแรงสั่นสะเทือน						
4. ระบบฐานข้อมูลด้านความมั่นคง						
4.1 ระบบแจ้งเตือนผู้ต้องสงสัย						
4.2 ระบบแจ้งเตือนรถต้องสงสัย						

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

คำชี้แจง โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับคุณลักษณะของการรักษาความมั่นคงปลอดภัย

.....

.....

.....

.....

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

แบบประเมินองค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินองค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชาย แดนภาคใต้ ประกอบด้วยคำถามเกี่ยวกับคุณลักษณะของการรักษาความปลอดภัย โดยท่านสามารถพิจารณารายละเอียดตามเอกสารที่ส่งมาด้วย

โปรดทำเครื่องหมาย √ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณาดังนี้

5 หมายถึง มีความเหมาะสมมากที่สุด
4 หมายถึง มีความเหมาะสมมาก
3 หมายถึง มีความเหมาะสมปานกลาง
2 หมายถึง มีความเหมาะสมน้อย
1 หมายถึง มีความเหมาะสมน้อยที่สุด

แบบประเมินองค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 แบบประเมินองค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อผู้ประเมิน.....

ตำแหน่ง.....

สถานที่ทำงาน.....

ตอนที่ 2 แบบประเมินองค์ประกอบของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชาย แดนภาคใต้

รายการประเมิน	**ระดับความเหมาะสม**					**ข้อเสนอแนะ**
	5	**4**	**3**	**2**	**1**	
1. องค์ประกอบด้านการรักษาความมั่นคงปลอดภัย						
2. องค์ประกอบด้านเทคโนโลยีเชื่อมโยงสรรพสิ่ง (The Internet of Things: IoT)						
2.1 กล้องตรวจจับ (Camera Sensors)						
2.2 บัตรอาร์เอฟไอดี (RFID)						
2.3 เซนเซอร์ตรวจจับ (Sensors Detector)						
3. องค์ประกอบด้านการแสดงผลการแจ้งเตือน โดยเลือกใช้ Application Line ในการแจ้งความมั่นคงปลอดภัย						
4. องค์ประกอบด้านการตรวจสอบหลักฐานดิจิทัล (Digital Forensic)						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
4.1 Data Acquisition การรวบรวมพยานหลักฐาน						
4.2 Analysis การวิเคราะห์เพื่อประเมินความเสี่ยง						
4.3 Reporting การรายงานความมั่นคงปลดภัยสูงสำหรับสถานศึกษา						
คุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้						

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

คำชี้แจง โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับองค์ประกอบหลักของคุณลักษณะของการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

.....

.....

.....

.....

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

แบบประเมินแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วยคำถามเกี่ยวกับมิติและองค์ประกอบของแบบจำลอง โดยท่านสามารถพิจารณษรายละเอียดตามเอกสารที่ส่งมาด้วย

โปรดทำเครื่องหมาย √ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณาดังนี้

5 หมายถึง มีความเหมาะสมมากที่สุด
4 หมายถึง มีความเหมาะสมมาก
3 หมายถึง มีความเหมาะสมปานกลาง
2 หมายถึง มีความเหมาะสมน้อย
1 หมายถึง มีความเหมาะสมน้อยที่สุด

แบบประเมินแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 แบบประเมินแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อผู้ประเมิน.....

ตำแหน่ง.....

สถานที่ทำงาน..... .....

ตอนที่ 2 แบบประเมินแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ระดับความเหมาะสม**					**ข้อเสนอแนะ**
	5	4	3	2	1	
1. มิติด้านการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา						
1.1 การรักษาความปลอดภัยเกี่ยวกับบุคคล						
1.2 การรักษาความปลอดภัยเกี่ยวกับสถานที่						
1.3 การป้องกันและแก้ไขปัญหาด้านความไม่สงบ						
2. มิติด้านเทคโนโลยีสารสนเทศที่สนับสนุนการรักษาความมั่นคงปลอดภัยสำหรับสถานศึกษา						
2.1 เทคโนโลยีเชื่อมโยงสรรพสิ่ง						
2.2 ระบบตรวจจับและรู้จำ						
2.3 ระบบจัดการฐานข้อมูล						
2.4 ระบบจัดการรายงาน						
2.5 ระบบแสดงผลข้อมูล						
2.6 ระบบแจ้งเตือน						
3. มิติด้านการบริหารจัดการข้อมูล						
3.1 การแจ้งเตือน (Application Line)						
3.2 การรายงานความเสี่ยง (Dash Board)						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
3.3 การบำรุงรักษาและตรวจสอบ (Maintain & Improve)						
4.มิติด้านการตรวจสอบหลักฐานดิจิทัล						
4.1 การรวบรวมพยานหลักฐาน Data Acquisition						
4.2 การวิเคราะห์เพื่อประเมินความเสี่ยง Analysis						
4.3 การรายงานความมั่งคงปลอดภัย Reporting						

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

คำชี้แจง โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

.....

.....

.....

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

แบบประเมินสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่ง เพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินสถาปัตยกรรมรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วยคำถามเกี่ยวองค์ประกอบของสถาปัตยกรรมระบบ โดยท่านสามารถพิจารณษรายละเอียดตามเอกสารที่ส่งมาด้วย

โปรดทำเครื่องหมาย √ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณาดังนี้

5 หมายถึง มีความเหมาะสมมากที่สุด
4 หมายถึง มีความเหมาะสมมาก
3 หมายถึง มีความเหมาะสมปานกลาง
2 หมายถึง มีความเหมาะสมน้อย
1 หมายถึง มีความเหมาะสมน้อยที่สุด

แบบประเมินสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 แบบประเมินสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อผู้ประเมิน.....

ตำแหน่ง.....

สถานที่ทำงาน.....

ตอนที่ 2 แบบประเมินสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ระดับความเหมาะสม**					**ข้อเสนอแนะ**
	5	**4**	**3**	**2**	**1**	
1. ผู้ที่เกี่ยวข้องกับระบบ (Stakeholders)						
1.1 ผู้บริหารระบบ (Administrators)						
1.2 ผู้บริหารสถานศึกษา (CEO)						
1.3 เจ้าหน้าที่รักษาความปลอดภัย (Staff)						
1.4 ผู้ใช้งานระบบ (Users)						
2. ไอโอทีดีไวซ์ สำหรับการตรวจจับบุคคลและวัตถุ						
2.1 กล้องตรวจจับใบหน้า						
2.2 บัตร RFID						
2.3 กล้องตรวจจับป้ายทะเบียน						
2.4 เซนเซอร์ตรวจจับควัน						
2.5 เซนเซอร์ตรวจจับความร้อน						
2.6 เซนเซอร์ตรวจจับก๊าซ						
2.7 เซนเซอร์ตรวจจับแรงสั่นสะเทือน						
3. โมดูลย่อยของระบบ						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
3.1 โมดูลตรวจจับใบหน้า						
3.2 โมดูลสแกนบัตร						
3.3 โมดูลตรวจจับป้ายทะเบียนรถ						
3.4 โมดูลตรวจจับควันไฟ						
3.5 โมดูลตรวจจับความร้อน						
3.6 โมดูลตรวจจับก๊าซ						
3.7 โมดูลตรวจจับแรงสั่นสะเทือน						
4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย						
4.1 แจ้งเตือนผ่านไลน์แอพพลิเคชั่น Application Line						
4.2 การประเมินและควบคุมความเสี่ยง Dashboard						
4.3 ระบบจัดการรายงาน Report Management System						
5. เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)						
5.1 เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)						
6. หลักการทำงานของสถาปัตยกรรมระบบ						
6.1 หลักการทำงานของระบบ						
6.2 ความเหมาะสมของอุปกรณ์ตรวจจับ						
6.3 ความเหมาะสมของระบบการแจ้งเตือน						
6.4 ความเหมาะสมของระบบจัดเก็บข้อมูล						

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

คำชี้แจง โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับสถาปัตยกรรมระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

.....

.....

.....

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

แบบประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วยคำถามเกี่ยวกับการออกแบบระบบ โดยท่านสามารถพิจารณษรายละเอียดตามเอกสารที่ส่งมาด้วย

โปรดทำเครื่องหมาย √ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณาดังนี้

5 หมายถึง มีความเหมาะสมมากที่สุด
4 หมายถึง มีความเหมาะสมมาก
3 หมายถึง มีความเหมาะสมปานกลาง
2 หมายถึง มีความเหมาะสมน้อย
1 หมายถึง มีความเหมาะสมน้อยที่สุด

แบบประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 แบบประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อผู้ประเมิน.....

ตำแหน่ง.....

สถานที่ทำงาน.....

ตอนที่ 2 แบบประเมินระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ระดับความเหมาะสม**					**ข้อเสนอแนะ**
	5	**4**	**3**	**2**	**1**	
1. ผู้ที่เกี่ยวข้องกับระบบ (Stakeholders)						
1.1 ผู้บริหารระบบ (Administrators)						
1.2 ผู้บริหารสถานศึกษา (CEO)						
1.3 เจ้าหน้าที่รักษาความปลอดภัย (Staff)						
1.4 ผู้ใช้งานระบบ (Users)						
1.5 บุคคลากรภายนอกด้านการรักษาความปลอดภัยสำหรับสถานศึกษา						
2. ไอโอทีดีไวซ์ สำหรับการตรวจจับบุคคลและวัตถุ						
2.1 กล้องตรวจจับใบหน้า						
2.2 บัตร RFID						
2.3 กล้องตรวจจับป้ายทะเบียน						
2.4 เซนเซอร์ตรวจจับควัน						
2.5 เซนเซอร์ตรวจจับความร้อน						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
2.6 เซนเซอร์ตรวจจับก๊าซ						
2.7 เซนเซอร์ตรวจจับแรงสั่นสะเทือน						
2.8 ความสะดวกในการปรับเปลี่ยนหรือเพิ่มอุปกรณ์ในอนาคตที่จะสนับสนุนการทำงานของระบบ						
3. โมดูลย่อยของระบบรักษาความมั่นคงปลอดภัย HISMSystem						
3.1 โมดูลตรวจจับใบหน้า						
3.2 โมดูลสแกนบัตร						
3.3 โมดูลตรวจจับป้ายทะเบียนรถ						
3.4 โมดูลตรวจจับควันไฟ						
3.5 โมดูลตรวจจับความร้อน						
3.6 โมดูลตรวจจับก๊าซ						
3.7 โมดูลตรวจจับแรงสั่นสะเทือน						
3.8 ความสะดวกในการเพิ่มขยายโมดูลในอนาคตที่จะสนับสนุนการทำงานของระบบ						
4. การแจ้งเตือนและการรายงานผลความมั่นคงปลอดภัย						
4.1 แจ้งเตือนผ่านไลน์แอพพลิเคชั่น Application Line						
4.2 การประเมินและควบคุมความเสี่ยง Dashboard						
4.3 ระบบจัดการรายงาน Report Management System						
4.4 ความสะดวกในการเพิ่มส่วนการแจ้งเตือนและรายงานผล						
5. เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)						
5.1 เว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ (Web Server and Database Server)						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
5.2 ความสะดวกในการเพิ่ม ขยาย หรือปรับปรุงเว็บเซิร์ฟเวอร์และดาต้าเบสเซิร์ฟเวอร์ เพื่อรองรับการทำงานในอนาคตได้						
6. หลักการทำงานของสถาปัตยกรรมระบบ						
6.1 หลักการทำงานของระบบ						
6.2 ความเหมาะสมของอุปกรณ์ตรวจจับ						
6.3 ความเหมาะสมของระบบการแจ้งเตือน						
6.4 ความเหมาะสมของระบบจัดเก็บข้อมูล						
6.5 ความสะดวกในการเพื่อ ขยาย หรือปรับปรุงการทำงานของระบบ						
6.6 มีแนวโน้มในการปรับปรุงระบบได้ง่ายและรวดเร็ว						

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

คำชี้แจง โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับแบบจำลองการรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

.....

.....

.....

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

แบบประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ชื่องานวิจัย การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.ปณิตา วรรณพิรุณ
รองศาสตราจารย์ ดร.ปรัชญนันท์ นิลสุข

ผู้วิจัย นางต่วนนูรีซันน์ สุริยะ
สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา
คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

คำชี้แจง

แบบประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ประกอบด้วยคำถามเกี่ยวกับการออกแบบระบบ โดยท่านสามารถพิจารณษรายละเอียดตามเอกสารที่ส่งมาด้วย

โปรดทำเครื่องหมาย √ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่าน โดยมีเกณฑ์ในการพิจารณาดังนี้

5 หมายถึง มีความเหมาะสมมากที่สุด
4 หมายถึง มีความเหมาะสมมาก
3 หมายถึง มีความเหมาะสมปานกลาง
2 หมายถึง มีความเหมาะสมน้อย
1 หมายถึง มีความเหมาะสมน้อยที่สุด

แบบประเมินประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ ผู้วิจัยแบ่งการประเมินออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 แบบประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

ตอนที่ 1 ข้อมูลทั่วไป

ชื่อผู้ประเมิน.....

ตำแหน่ง.....

สถานที่ทำงาน.....

ตอนที่ 2 แบบประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

รายการประเมิน	**ระดับความเหมาะสม**					**ข้อเสนอแนะ**
	5	**4**	**3**	**2**	**1**	
1. การประเมินโมดูลยอ่ย (Module Test) -ของระบบ						
1.1 โมดูลการวางระบบโครงสร้างพื้นฐาน (Infrastructure Management System: IMS						
1.1.1 ความสามารถในการเพิ่มข้อมูล						
1.1.2 ความสามารถในการลบข้อมูล						
1.1.3 ความสามารถในการปรับปรุงข้อมูล						
1.1.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.1.5 ความสามารถในการจัดเก็บข้อมูล						
1.1.6 ความเหมาะสมของข้อมูลในโมดูล						
1.2 โมดูลระบบตรวจจับใบหน้า (Face Detection System)						
1.2.1 ความสามารถในการเพิ่มข้อมูล						
1.2.2 ความสามารถในการลบข้อมูล						
1.2.3 ความสามารถในการปรับปรุงข้อมูล						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
1.2.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.2.5 ความสามารถในการจัดเก็บข้อมูล						
1.2.6 ความเหมาะสมของข้อมูลในโมดูล						
1.3 โมดูลระบบสแกนบัตร (RFID System)						
1.3.1 ความสามารถในการเพิ่มข้อมูล						
1.3.2 ความสามารถในการลบข้อมูล						
1.3.3 ความสามารถในการปรับปรุงข้อมูล						
1.3.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.3.5 ความสามารถในการจัดเก็บข้อมูล						
1.3.6 ความเหมาะสมของข้อมูลในโมดูล						
1.4 โมดูลระบบตรวจจับป้ายทะเบียน (License Plate Detection System)						
1.4.1 ความสามารถในการเพิ่มข้อมูล						
1.4.2 ความสามารถในการลบข้อมูล						
1.4.3 ความสามารถในการปรับปรุงข้อมูล						
1.4.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.4.5 ความสามารถในการจัดเก็บข้อมูล						
1.4.6 ความเหมาะสมของข้อมูลในโมดูล						
1.5 โมดูลระบบตรวจจับความร้อน (Heat Detection System)						
1.5.1 ความสามารถในการเพิ่มข้อมูล						
1.5.2 ความสามารถในการลบข้อมูล						
1.5.3 ความสามารถในการปรับปรุงข้อมูล						
1.5.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.5.5 ความสามารถในการจัดเก็บข้อมูล						
1.5.6 ความเหมาะสมของข้อมูลในโมดูล						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
1.6 โมดูลระบบตรวจจับควัน (Smoke Detection System)						
1.6.1 ความสามารถในการเพิ่มข้อมูล						
1.6.2 ความสามารถในการลบข้อมูล						
1.6.3 ความสามารถในการปรับปรุงข้อมูล						
1.6.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.6.5 ความสามารถในการจัดเก็บข้อมูล						
1.6.6 ความเหมาะสมของข้อมูลในโมดูล						
1.7 โมดูลระบบตรวจจับก๊าซ (Gas Detection System)						
1.7.1 ความสามารถในการเพิ่มข้อมูล						
1.7.2 ความสามารถในการลบข้อมูล						
1.7.3 ความสามารถในการปรับปรุงข้อมูล						
1.7.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.7.5 ความสามารถในการจัดเก็บข้อมูล						
1.7.6 ความเหมาะสมของข้อมูลในโมดูล						
1.8 โมดูลระบบตรวจจับแรงสั่นสะเทือน (Vibration Detection System)						
1.8.1 ความสามารถในการเพิ่มข้อมูล						
1.8.2 ความสามารถในการลบข้อมูล						
1.8.3 ความสามารถในการปรับปรุงข้อมูล						
1.8.4 ความสามารถในการสืบค้นข้อมูลตามเงื่อนไข						
1.8.5 ความสามารถในการจัดเก็บข้อมูล						
1.8.6 ความเหมาะสมของข้อมูลในโมดูล						
1.9 โมดูลการแจ้งเตือน (Notification)						
1.9.1 ความสามารถในการแสดงผล						
1.9.2 ความเหมาะสมของข้อมูลในโมดูล						
1.10 โมดูลการประเมินและควบคุมความเสี่ยง (Risk Assessment & Control)						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
1.10.1 ความสามารถในการแสดงผล						
1.10.2 ความเหมาะสมของข้อมูลในโมดูล						
2. การประเมินการทำงานของระบบทั้งหมด (System Test)						
2.1 ความสามาถในการพิสูจน์ตัวตน (Authentication)						
2.2 ความสามารถของระบบจัดเก็บข้อมูล						
2.3 ความสามารถของความสัมพันธ์ในแต่ละระบบงานย่อยในการใช้ข้อมูลร่วมกัน						
2.4 ความสามารถในการลดเวลาและทรัพยากรในการทำงาน						
2.5 คววามครบถ้วนของฟังก์ชันการทำงานของระบบ						
2.6 ความสามารถเชื่อมต่อประสาน (Plug) ส่วนเพิ่มเติม						
2.7 มีแนวโน้มในการปรับปรุงระบบได้ง่ายและรวดเร็ว						
3 การประเมินการใช้งานระบบ (Usability Test)						
3.1 ความง่ายและความสะดวกในการใช้งานระบบ						
3.2 ความเหมาะสมของตำแหน่งการจัดวางส่วนต่าง ๆ บนจอภาพ						
3.3 การแบ่งเมนูของระบบสารมารถเข้าใจได้ง่าย						
3.4 ความชัดเจนของข้อความที่แสดงบนจอภาพ						
3.5 ความเหมาะสมของตัวอักษรเกี่ยวกับขนาด สี ความชัดเจน ง่ายต่อการอ่าน						
-3.6 ความเหมาะสมของปริมาณข้อมูลที่นำเสนอในแต่ละหน้าจอ						
3.7 ความเหมาะสมในการตอบสนองระบบในภาพรวม						

รายการประเมิน	ระดับความเหมาะสม					ข้อเสนอแนะ
	5	4	3	2	1	
4. การประเมินความปลอดภัยของระบบ (Security Test)						
4.1 การตรวจสอบสิทธิ์ในการเข้าใช้งานของผู้ใช้ระบบ						
4.2 การแจ้งเตือนเมื่อพบข้อผิดพลาดในการเข้าใช้งาน						
4.3 ความเหมาะสมในการรักษาความปลอดภัยของระบบโดยภาพรวม						

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ

คำชี้แจง โปรดแสดงความคิดเห็นของท่านเพิ่มเติม (ถ้ามี) เพื่อเป็นประโยชน์ในการปรับปรุงข้อมูลสำหรับการพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

.....

.....

.....

ลงชื่อ .....ผู้ประเมิน

(.....)

...../...../.....

โทรศัพท์/อีเมล.....

ผู้วิจัยขอขอบคุณท่านเป็นอย่างสูงที่ให้ความอนุเคราะห์ตอบแบบประเมินงานวิจัยนี้

ภาคผนวก ค

คู่มือการใช้งานระบบ

คู่มือการใช้งานระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

1. ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

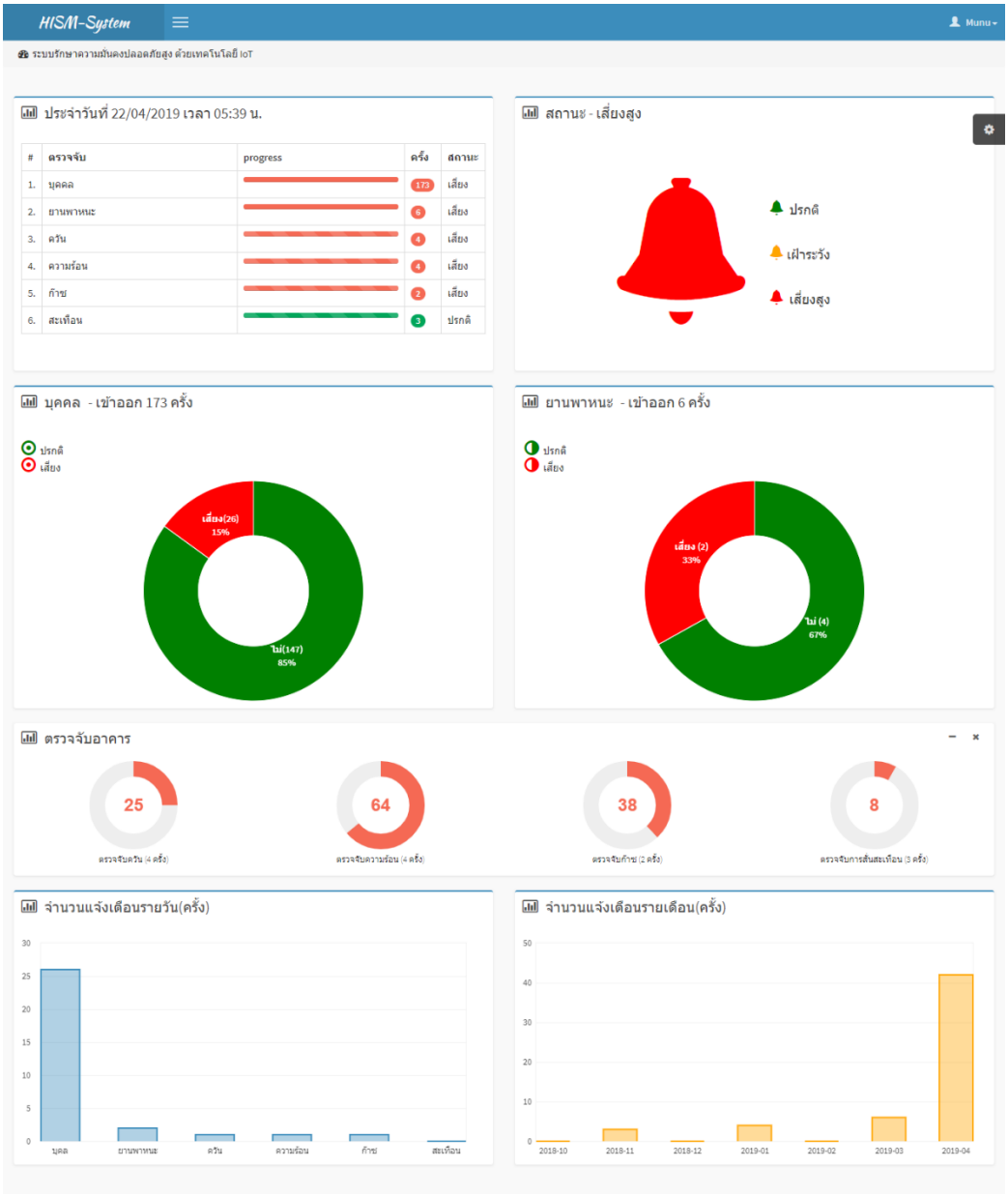
ระบบบริหารจัดการรักษาความมั่นคงปลอดภัยสูง (HISMS) คือ ระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ โดยผู้ใช้สามารถเข้าถึงระบบได้จากอุปกรณ์คอมพิวเตอร์ได้ทุกชนิด เช่น คอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์แท็บเล็ต หรือ สมาร์ทโฟน เป็นต้น โดยระบบเชื่อมโยงกับระบบเครือข่ายอินเทอร์เน็ตเพื่อเป็นเครื่องมือติดต่อสื่อสาร ระหว่างกันได้ด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่ง หรือ Internet of Things: IoT

2. การเข้าใช้งานระบบ HISMS

ผู้ใช้งานสามารถเข้าใช้งานหน้าหลักระบบ OMILS
ได้ที่ URL : http://www.hismsystem.com/

3. การใช้งานระบบ OMILS

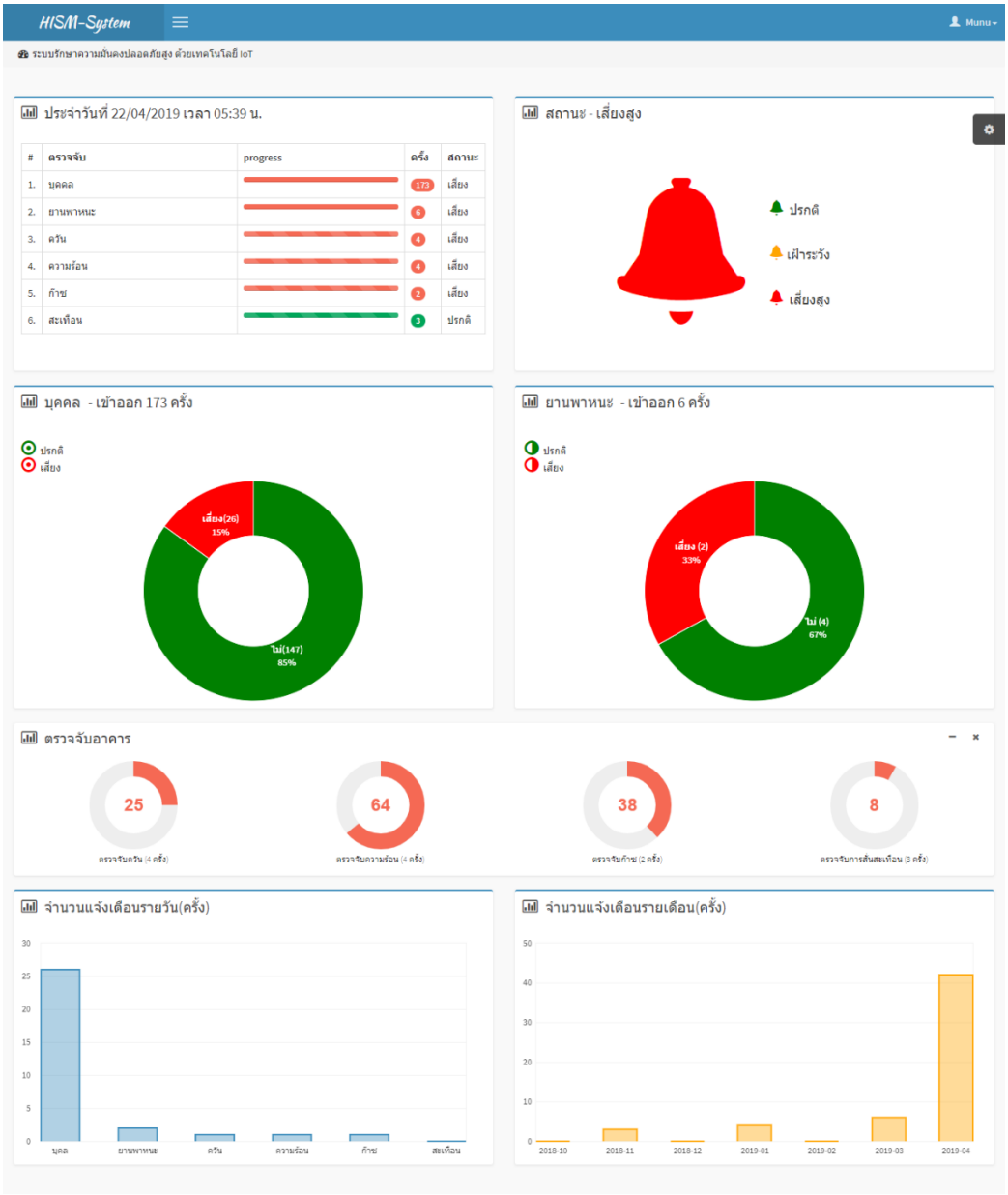
เมื่อเข้าสู่ระบบหรือเว็บไซต์ http://www.hismsystem.com/ จะปรากฏหน้าจอหลักประกอบไปด้วย หน้าจอแสดงผลการวิเคราะห์ความเสี่ยง (Dashboard) หน้าจอแสดงรายละเอียดของระบบ และคำแนะการใช้ระบบอย่างละเอียด ดังภาพที่ ค-1



ภาพที่ ค-1 หน้าจอหลัก

การเข้าใช้งานระบบ HISS แบ่งออกเป็น 2 ส่วน คือ ส่วนของผู้ใช้ทั่วไป และส่วนของผู้ดูแลระบบ รายละเอียดประกอบด้วย

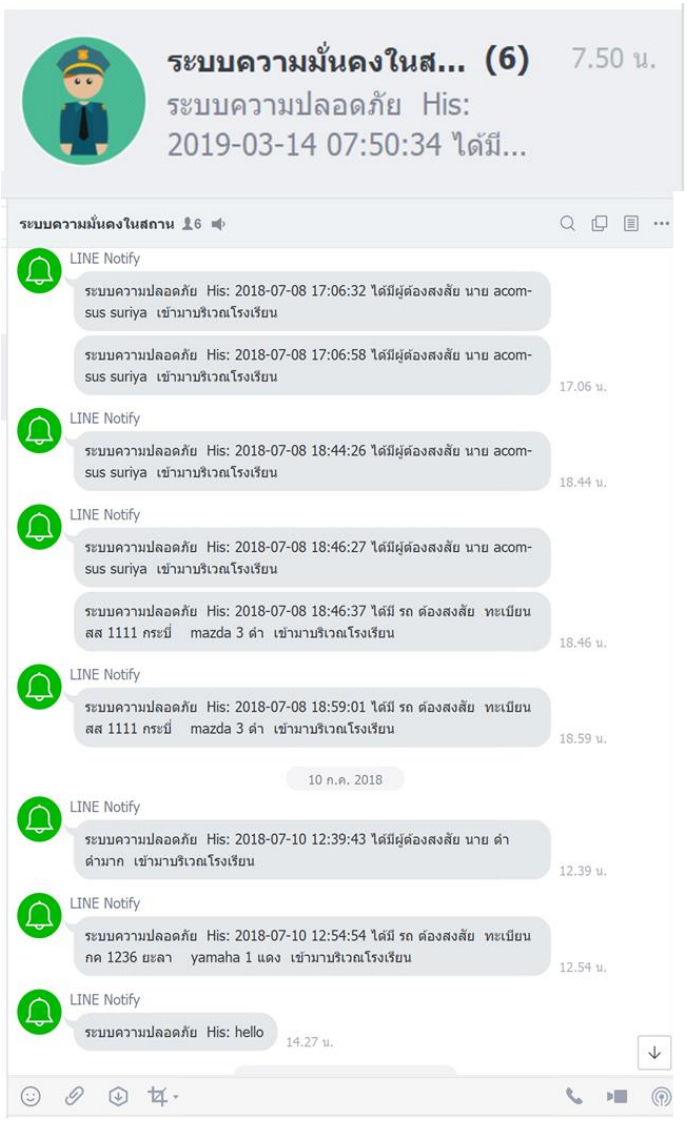
1. ส่วนของผู้ใช้ทั่วไป



ภาพที่ ค-2 หน้าจอหลักเข้าสู่ระบบ HISMS

จากภาพที่ ค-2 ผู้ใช้ทั่วไปสามารถเข้าสู้หน้าเว็บไซต์ http://www.hismsystem.com/ เพื่อต้องการตรวจสอบสถานะความมั่นคงปลอดภัยของสถานศึกษา โดยผู้ใช้ทั่วไปสามารถเข้าสู้เว็บไซต์ได้ทันทีโดยไม่ต้องเข้าสู้ระบบ (Login) จากนั้นจะปรากฏหน้าจอแสดงผลการวิเคราะห์ความเสี่ยง (Dashboard) ด้านสถานะความมั่นคงปลอดภัยของสถานศึกษา โดยแสดงในรูปแบบของข้อมูลสรุป ซึ่งมีการกำหนดการแสดงสถานะด้วยแทบที่เขียว หมายถึงความปกติ และ แทบสีแดง หมายถึงความ

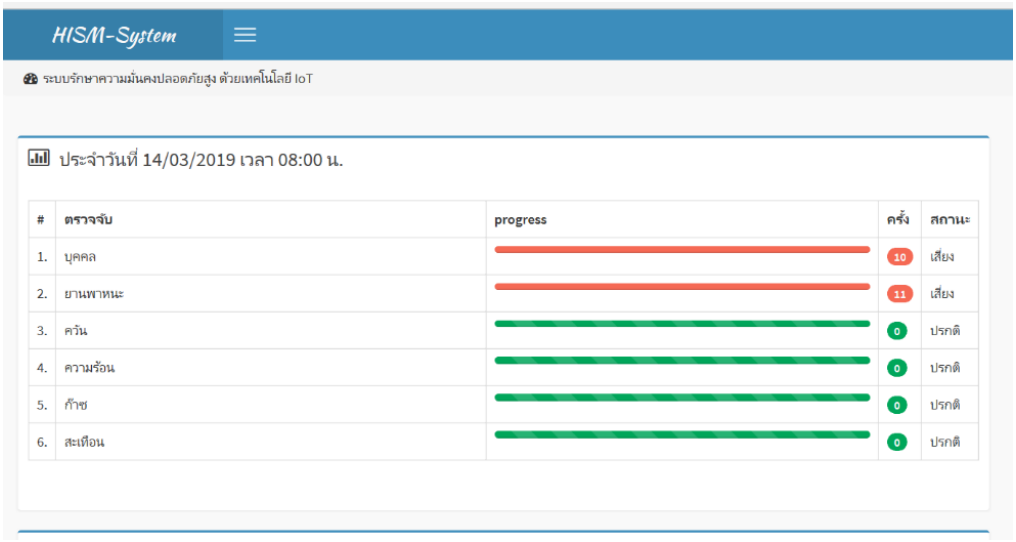
เสี่ยงที่ระบบจะทำการแจ้งเตือน โดยข้อมูลของระบบจะทำการประมวลผลแบบทันทีทันใด และทำการแจ้งเตือนสถานะความเสี่ยงผ่านทางหน้าจอแสดงผล และ Line Notification เพื่อแจ้งเตือนข้อมูลที่เป็นความเสี่ยงหรือความไม่ปลอดภัยที่อาจเกิดขึ้นกับสถานศึกษาที่มีระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้ รายละเอียดด้านสถานะความเสี่ยงหรือความไม่ปลอดภัยประกอบด้วย



ภาพที่ ค-3 หน้าจอแสดงผลการแจ้งเตือนความเสี่ยงหรือความผิดปกติที่ไม่ปลอดภัยผ่านทาง Line Notification

จากภาพที่ ค-3 แสดงผลการแจ้งเตือนความเสี่ยงหรือความผิดปกติที่ไม่ปลอดภัยผ่านทาง Line Notification ซึ่งเป็นแอพพลิเคชั่นแจ้งเตือนสำหรับผู้ใช้ที่เป็นสมาชิกกลุ่ม สามารถได้รับข้อมูลการแจ้ง

เตือนจากระบบ HISMS ได้แบบทันที่ทันใด โดยข้อมูลการแจ้งเตือนจะประกอบไปด้วยการแจ้งเตือนความปลอดภัยในแต่ละประเภทที่ระบบ HISMS สามารถทำการตรวจจับหรือตรวจพบข้อมูลที่เป็นความผิดปกติที่ถูกกำหนดไว้ในระบบ HISMS

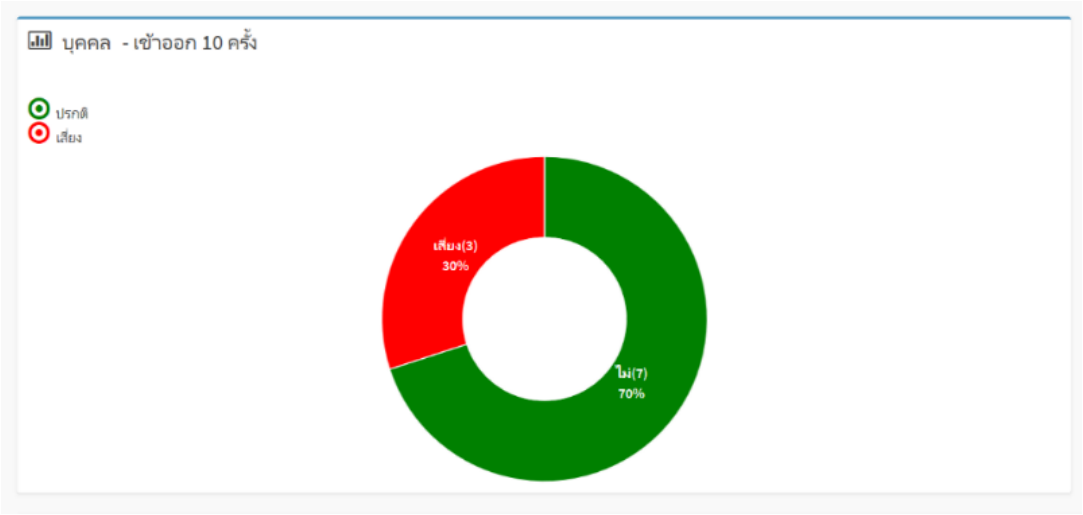


ภาพที่ ค-4 หน้าจอแสดงข้อมูลสรุปรายงานความเสี่ยงประจำวัน

จากภาพที่ ค-4 แสดงข้อมูลสรุปรายงานความเสี่ยงประจำวัน ในรูปแบบของ Dashboard ซึ่งระบบจะทำการสรุปข้อมูลประจำวันโดยแสดงตามรายการตรวจจับความปลอดภัย ซึ่งแสดงข้อมูลความปกติปลอดภัยด้วยแทบที่ เขียว และแสดงข้อมูลความผิดปกติหรือความเสี่ยงด้วยแทบที่ แดง ประกอบด้วยการตรวจจับบุคคล ยานพาหนะ ควันไฟ ความร้อน ก๊าซ และ แรงสั่นสะเทือน

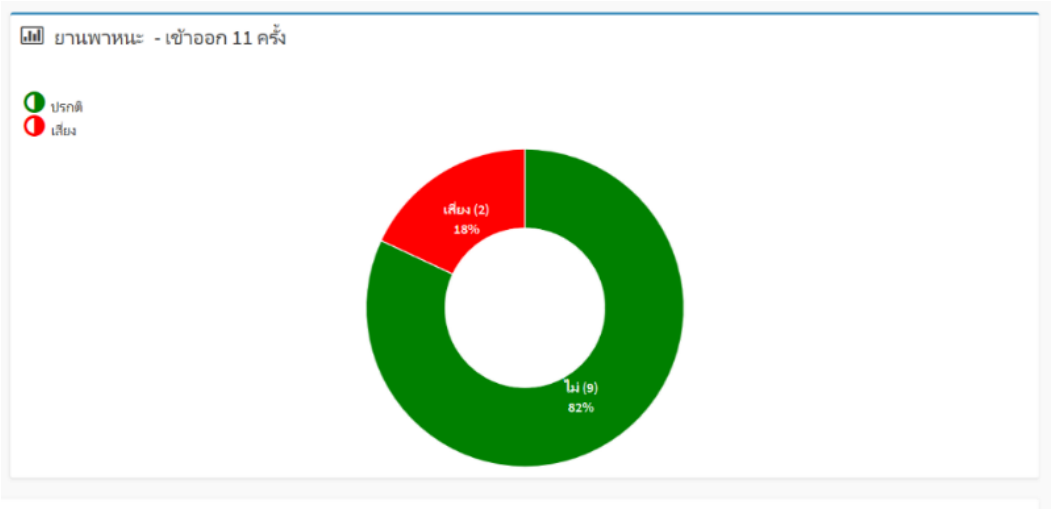
ภาพที่ ค-5 หน้าจอแสดงสถานะการแจ้งเตือนความเสี่ยงของระบบ

จากภาพที่ ค-5 แสดงข้อมูลสถานะความเสี่ยงภาพรวมของระบบ HISMS ในรูปแบบของ Dashboard โดยใช้สัญลักษณ์แจ้งเตือน ประกอบด้วย 1) แทบสีเขียว หมายถึง ความปกติของระบบที่ยังไม่ได้ตรวจผิดความผิดปกติ 2) แทบที่เหลือง หมายถึง เฝ้าระวัง ซึ่งระบบมีการตรวจจับความผิดปกติของระบบที่อยู่ในระดับต้องเฝ้าระวังที่อาจเกิดจากการตรวจจับอาคารที่อยู่ในระดับใกล้ถึงความผิดปกติ 3) แทบสีแดง หมายถึง เสี่ยงสูง ระบบจะดำเนินการแจ้งเตือนทันที่เมื่อระบบสามารถตรวจจับบุคคล ยานพาหนะ ต้องสงสัยที่ถูกบันทึกไว้ในระบบฐานข้อมูล และการตรวจจับปริมาณวัตถุควันไฟ ความร้อน ก๊าซ แรงสั่นสะเทือน ที่เกินระดับความปลอดภัย



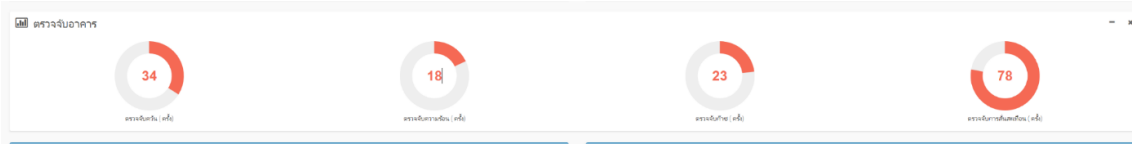
ภาพที่ ค-6 หน้าจอแสดงข้อมูลบุคคลเข้า - ออก ประจำวัน

จากภาพที่ ค-6 แสดงข้อมูลบุคคลเข้า - ออก ประจำวันในรูปแบบของ Dashboard ซึ่งระบบจะแสดงข้อมูลความปกติปลอดภัยด้วยแทบที่ เขียว และแสดงข้อมูลความผิดปกติหรือความเสี่ยงด้วยแทบที่ แดง



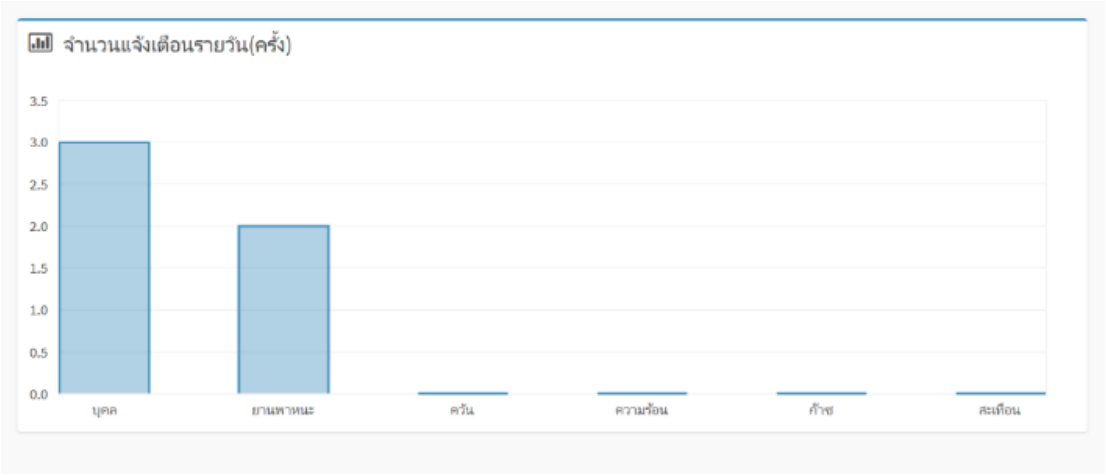
ภาพที่ ค-7 หน้าจอแสดงข้อมูลยานพาหนะเข้า - ออก ประจำวัน

จากภาพที่ ค-6 แสดงข้อมูลยานพาหนะเข้า - ออก ประจำวันในรูปแบบของ Dashboard ซึ่งระบบ จะแสดงข้อมูลความปกติปลอดภัยด้วยแทบที่ เขียว และแสดงข้อมูลความผิดปกติหรือความเสี่ยงด้วยแทบที่ แดง



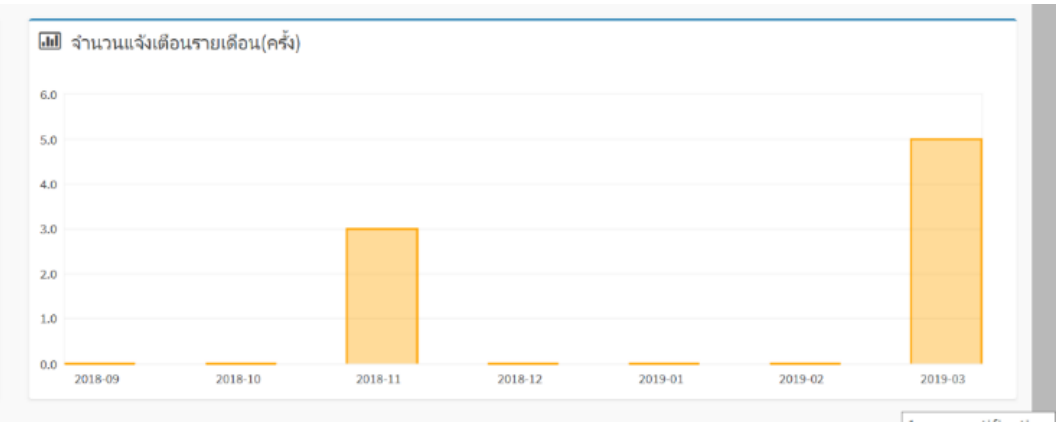
ภาพที่ ค-8 หน้าจอแสดงข้อมูลการตรวจจับภายในอาคารสถานที่ประจำวัน

จากภาพที่ ค-8 แสดงข้อมูลการตรวจจับภายในอาคารสถานที่ ประจำวันในรูปแบบของ Dashboard ซึ่งระบบ จะแสดงข้อมูลจำนวนครั้งที่ระบบสามารถทำการตรวจจับปริมารวัตถุที่เกิดค่าความผิดปกติ ประกอบด้วยการตรวจจับปริมาณ ควันไฟ ความร้อน ก๊าซ และ แรงสั่นสะเทือน แสดงปริมาณการตรวจจับด้วยแทบที่สีแดง



ภาพที่ ค-9 หน้าจอแสดงรายงานสรุปการแจ้งเตือนรายวัน

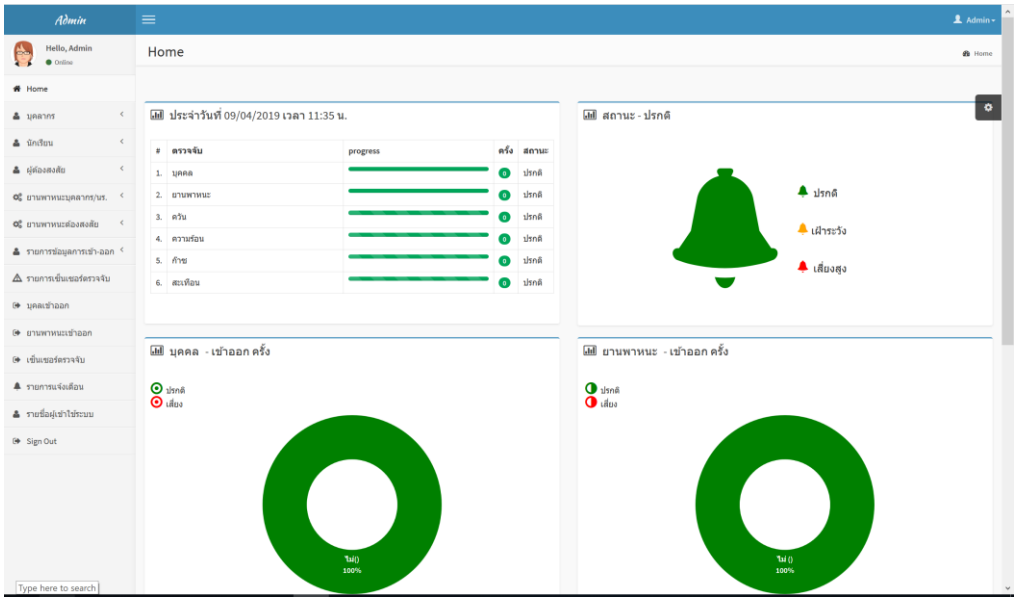
จากภาพที่ ค-4 แสดงข้อมูลสรุปรายงานจำนวนการแจ้งเตือนรายวัน โดยแสดงในรูปแบบของ Dashboard ลักษณะแผนภูมิ ซึ่งระบบจะทำการสรุปข้อมูลจำนวนการแจ้งเตือนความเสี่ยงหรือความไม่ปลอดภัยประจำเดือน เป็นจำนวนครั้งที่ระบบได้ทำการตรวจจับและแจ้งเตือน ซึ่งประกอบด้วยจำนวนการแจ้งเตือนประจำวันเป็นจำนวนครั้ง ประกอบด้วย การแจ้งเตือน บุคคล ยานพาหนะ ควัน ไฟ ความร้อน ก๊าซ และแสงสั่นสะเทือน



ภาพที่ ค-10 หน้าจอแสดงรายงานสรุปประจำเดือน

จากภาพที่ ค-10 แสดงข้อมูลรายงานสรุปจำนวนการแจ้งเตือนประจำเดือน โดยแสดงในรูปแบบของ Dashboard ลักษณะแผนภูมิ ซึ่งระบบจะทำการสรุปข้อมูลจำนวนการแจ้งเตือนความเสี่ยงหรือความไม่ปลอดภัยประจำเดือน เป็นจำนวนครั้งที่ระบบได้ทำการตรวจจับและแจ้งเตือนของแต่ละเดือนว่ามีการแจ้งเตือนทั้งหมดกี่ครั้ง

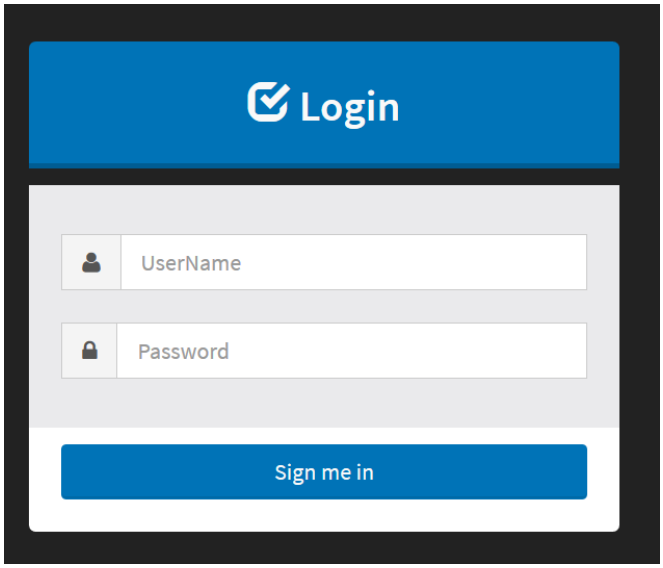
2. ส่วนของผู้ดูแลระบบ



ภาพที่ ค-11 เครื่องมือสำหรับการบริหารและจัดการข้อมูลสารสนเทศของระบบ

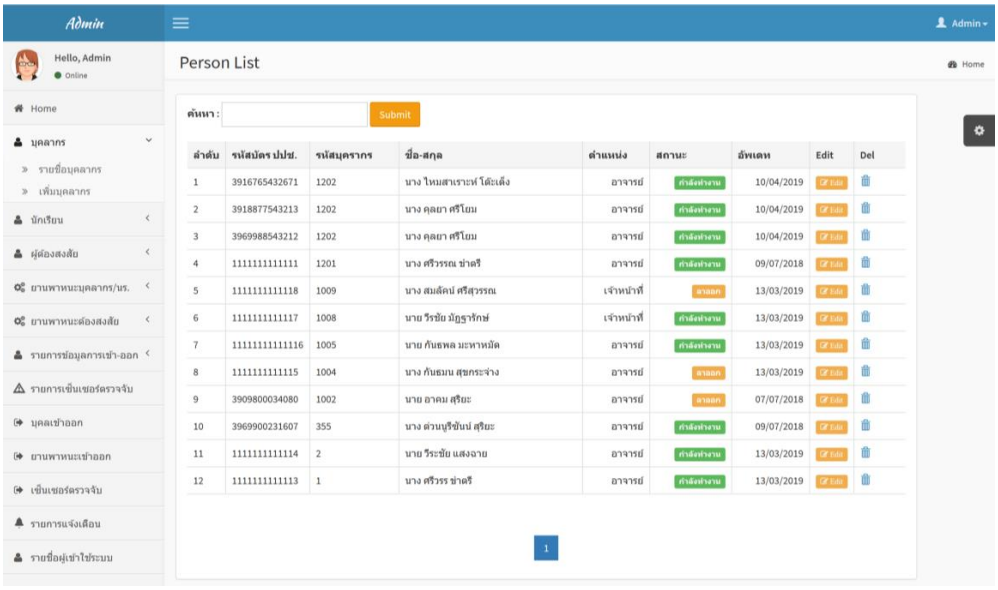
จากภาพที่ ค-11 เครื่องมือสำหรับการบริหารและจัดการข้อมูลสารสนเทศของระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับ

สถานศึกษาในจังหวัดชายแดนภาคใต้ โดยผู้ดูแลระบบสามารถเข้าสู่เว็บไซต์ ผู้ใช้ทั่วไปสามารถเข้าสู่หน้าเว็บไซต์ http://www.hismsystem.com/ เพื่อดำเนินการบริหารและจัดการข้อมูลสารสนเทศของระบบ และ สามารถตรวจสอบสถานะความมั่นคงปลอดภัยของสถานศึกษา โดยผู้ดูแลระบบเข้าสู่เว็บไซต์และทำการเข้าสู่ระบบ (Login) จากนั้นจะปรากฏหน้าจอแสดงผลสำหรับการบริหารและจัดการข้อมูลสารสนเทศของระบบผลการวิเคราะห์ความเสี่ยง (Dashboard) และข้อมูลด้านสถานะความมั่นคงปลอดภัยของสถานศึกษา



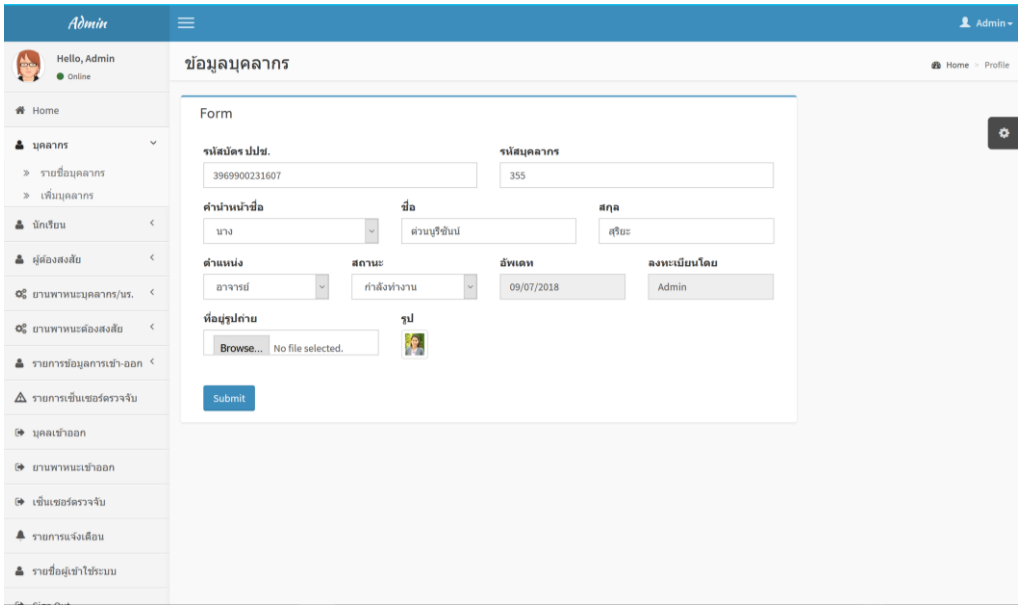
ภาพที่ ค-12 หน้าจอเข้าสู่ระบบ (Loging)

จากภาพที่ ค-12 หน้าเข้าสู่ระบบเพื่อทำการ Login เข้าสู่ระบบ HISMS โดยผู้เข้าใช้ระบบสามารถเข้าสู่ระบบตามสิทธิการเข้าใช้ระบบที่ถูกกำหนดไว้



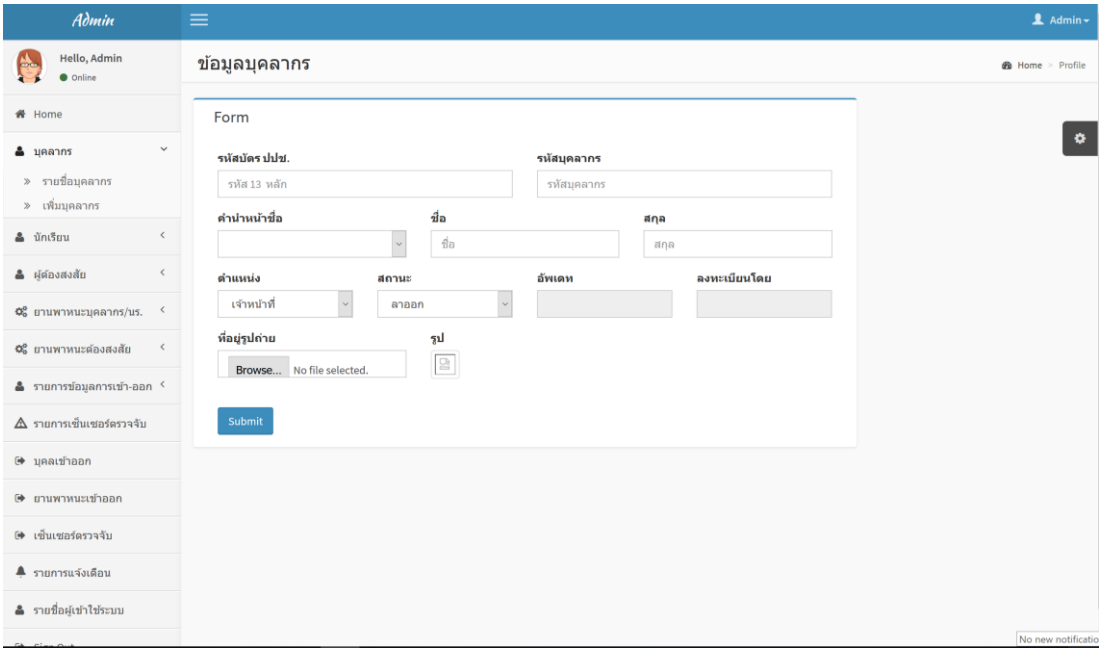
ภาพที่ ค-13 หน้าจอแสดงรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS

จากภาพที่ ค-13 แสดงหน้าจอรายรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS ประกอบไปด้วยข้อมูลส่วนบุคลากรรวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดัง**ภาพที่ ค-**14



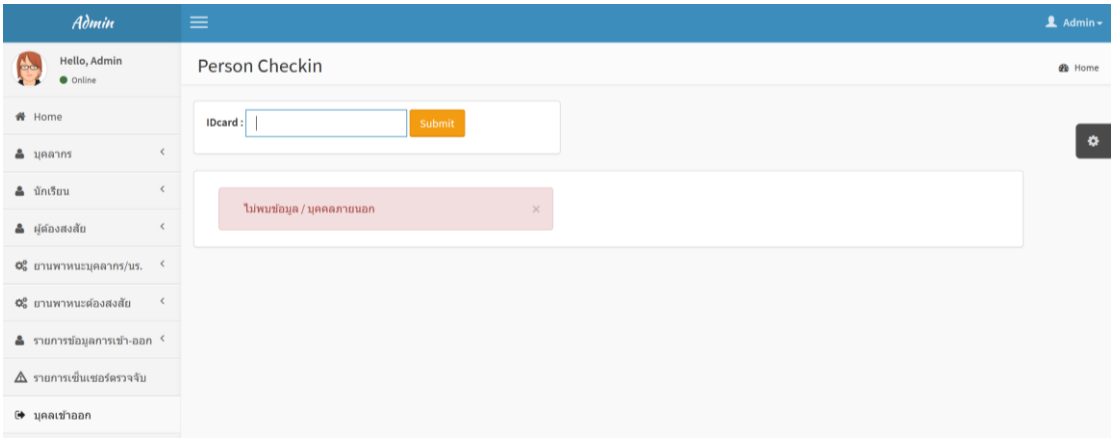
ภาพที่ ค-14 หน้าจอแสดงรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษา ที่ใช้งานระบบ HISMS เพิ่มเติม

จากภาพที่ ค-14 หน้าจอแสดงรายละเอียดข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS เพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้

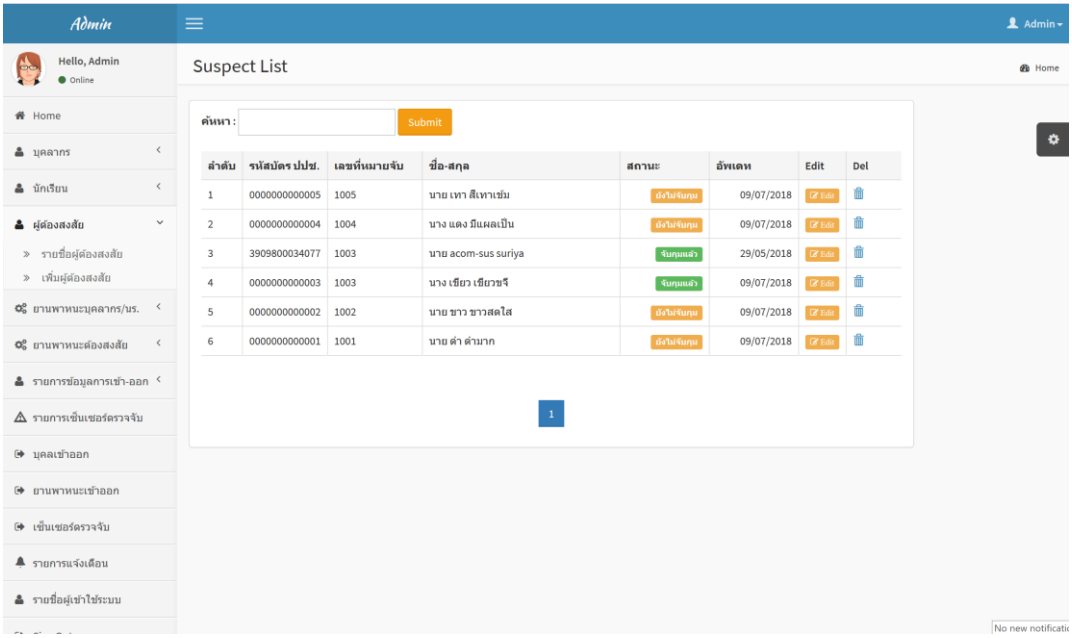


ภาพที่ ค-15 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS

จากภาพที่ ค-15 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลบุคลากรภายในของสถานศึกษาที่ใช้งานระบบ HISMS ผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ

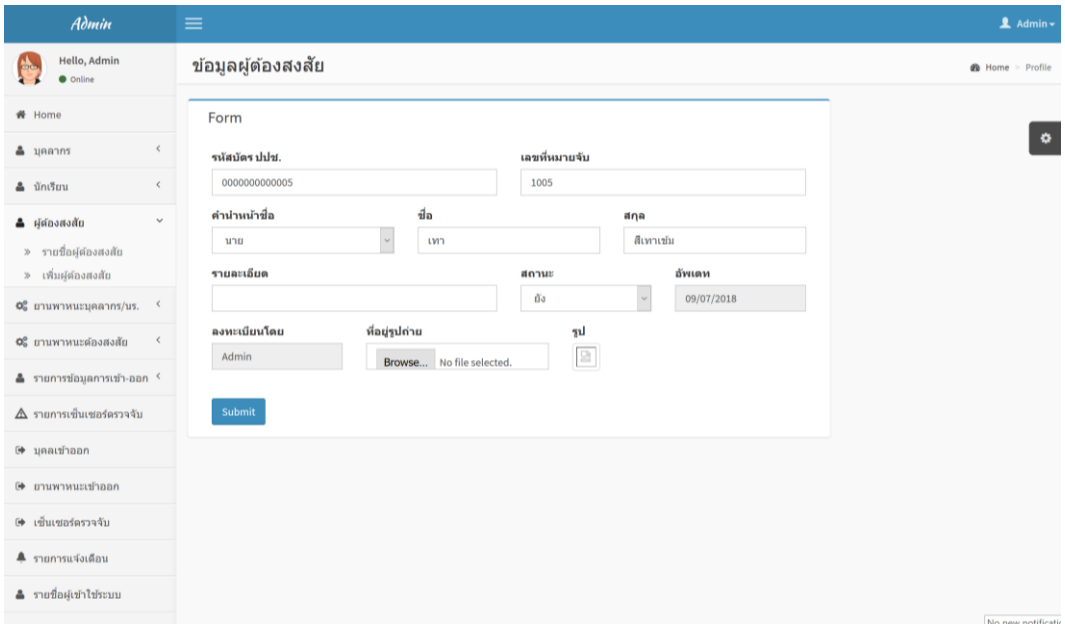


ภาพที่ ค-16 หน้าจอการค้นหาข้อมูลบุคคล



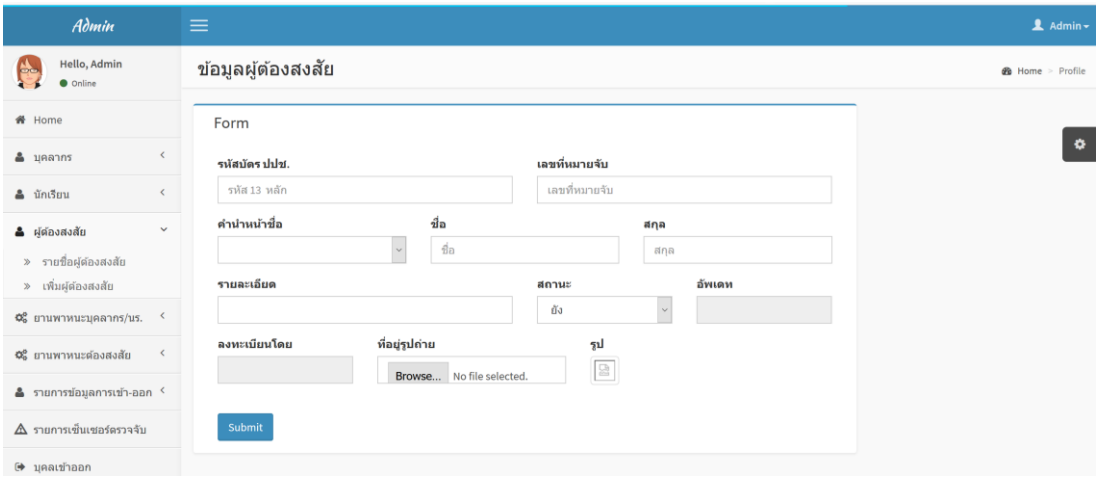
ภาพที่ ค-17 หน้าจอแสดงรายละเอียดข้อมูลผู้ต้องสงสัย

จากภาพที่ ค-17 แสดงหน้าจอรายรายละเอียดข้อมูลผู้ต้องสงสัยที่ถูกจัดเก็บข้อมูลไว้ในระบบฐานข้อมูล HISMS ประกอบไปด้วยรายละเอียดข้อมูลผู้ต้องสงสัยรวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดังภาพที่ ค-18



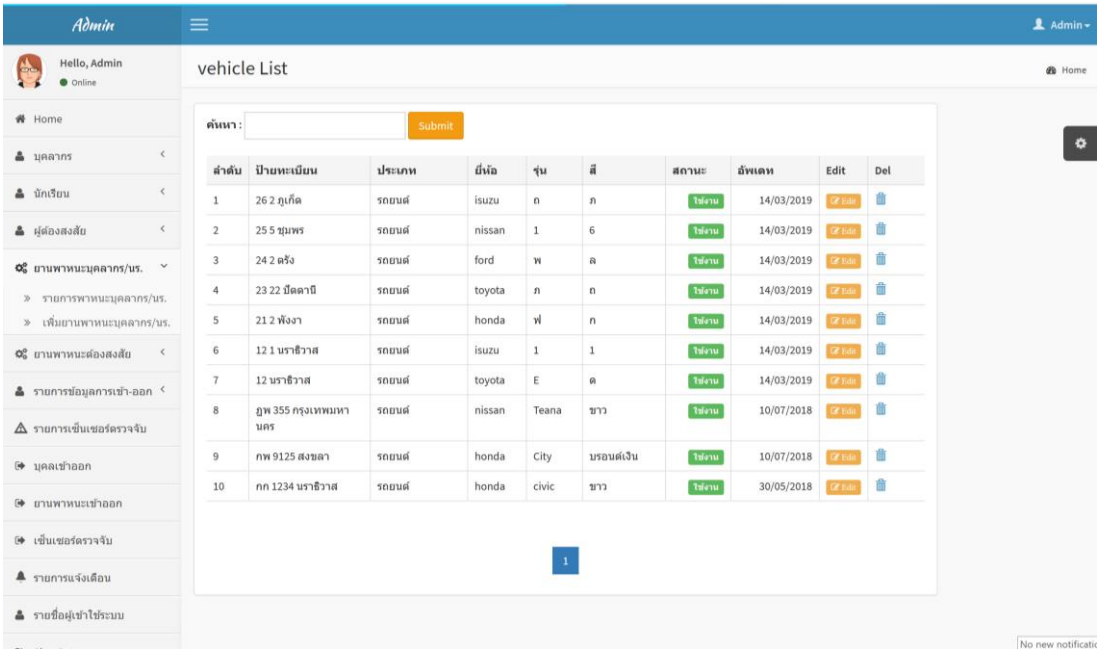
ภาพที่ ค-18 หน้าจอแสดงรายละเอียดข้อมูลผู้ต้องสงสัยเพิ่มเติม

จากภาพที่ ค-18 หน้าจอแสดงรายละเอียดข้อมูลผู้ต้องสงสัย เพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้



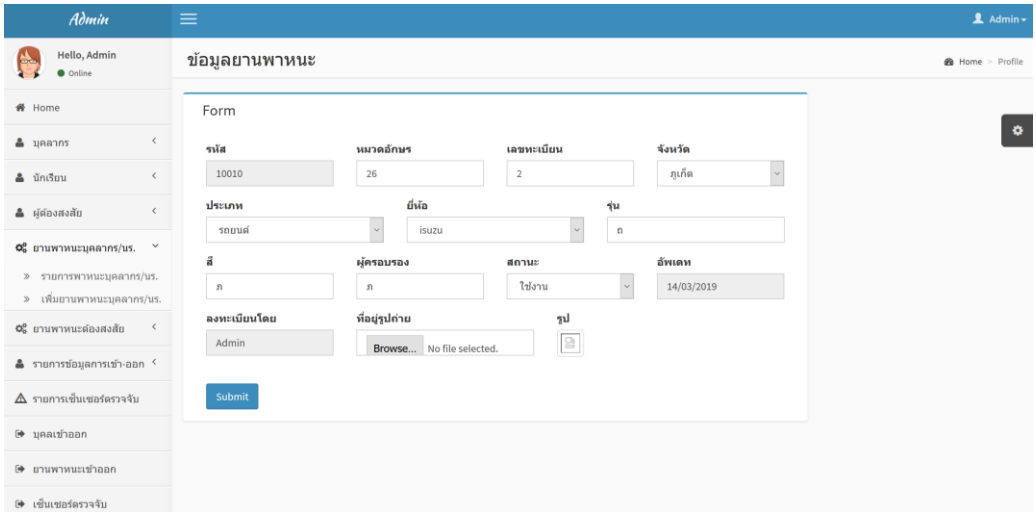
ภาพที่ ค-19 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลผู้ต้องสงสัย

จากภาพที่ ค-19 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลผู้ต้องสงสัย ซึ่งผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ



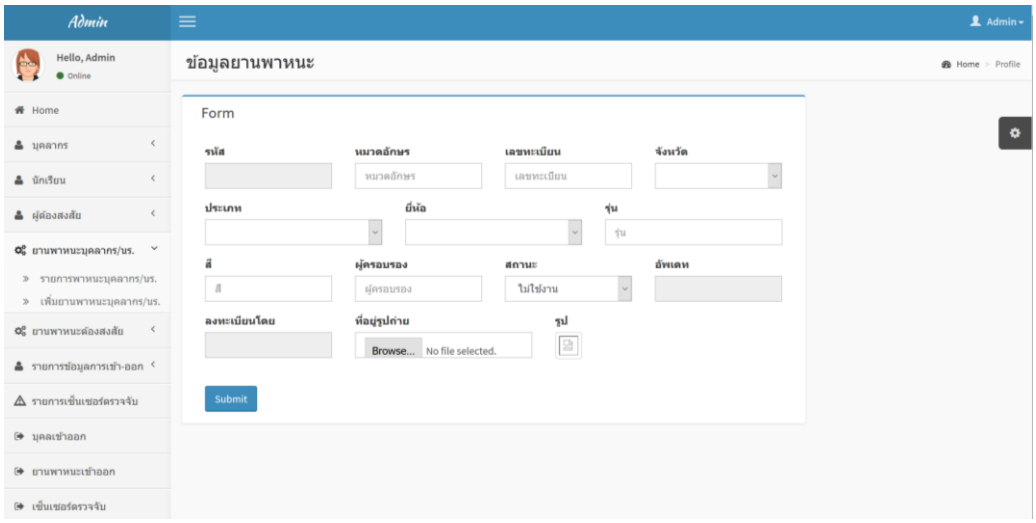
ภาพที่ ค-20 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะบุคลากรภายในและนักเรียนนักศึกษาของสถานศึกษาที่ใช้งานระบบ HISMS

จากภาพที่ ค-20 แสดงหน้าจอแสดงรายละเอียดข้อมูลยานพาหนะบุคลากรภายในและนักเรียนนักศึกษาของสถานศึกษาที่ใช้งานระบบ HISMS ประกอบไปด้วยข้อมูลรายละเอียดของยานพาหนะรวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดังภาพที่ ค-20



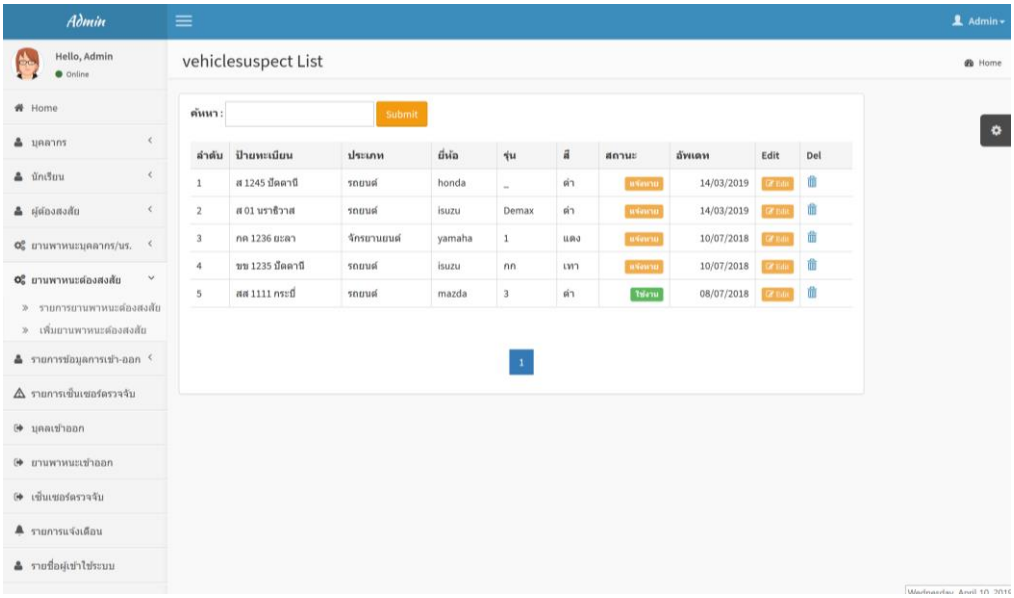
ภาพที่ ค-21 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะเพิ่มเติม

จากภาพที่ ค-21 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะเพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้



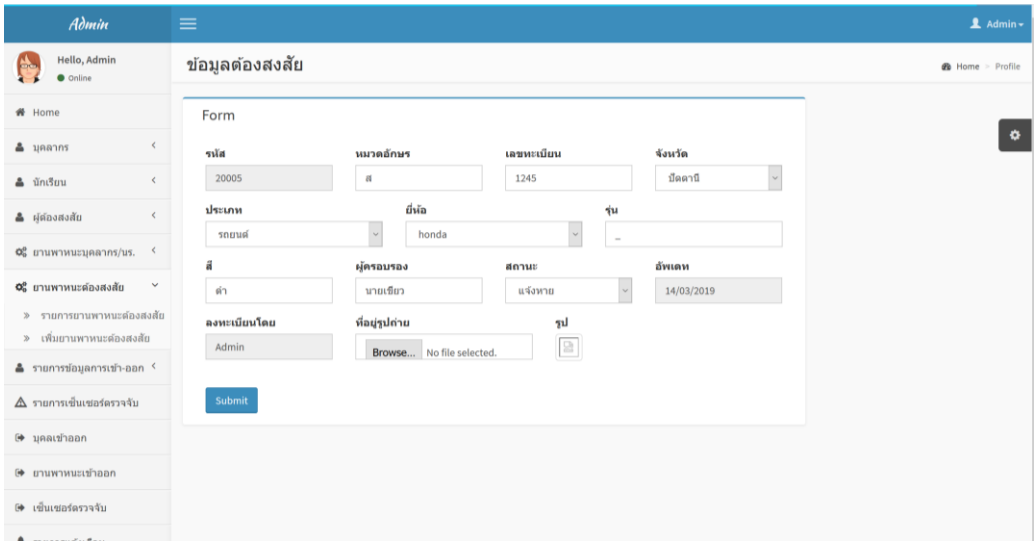
ภาพที่ ค-22 หน้าจอแสดงรายละเอียดการเพิ่มยานพาหนะ

จากภาพที่ ค-22 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลยานพาหนะ ซึ่งผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ



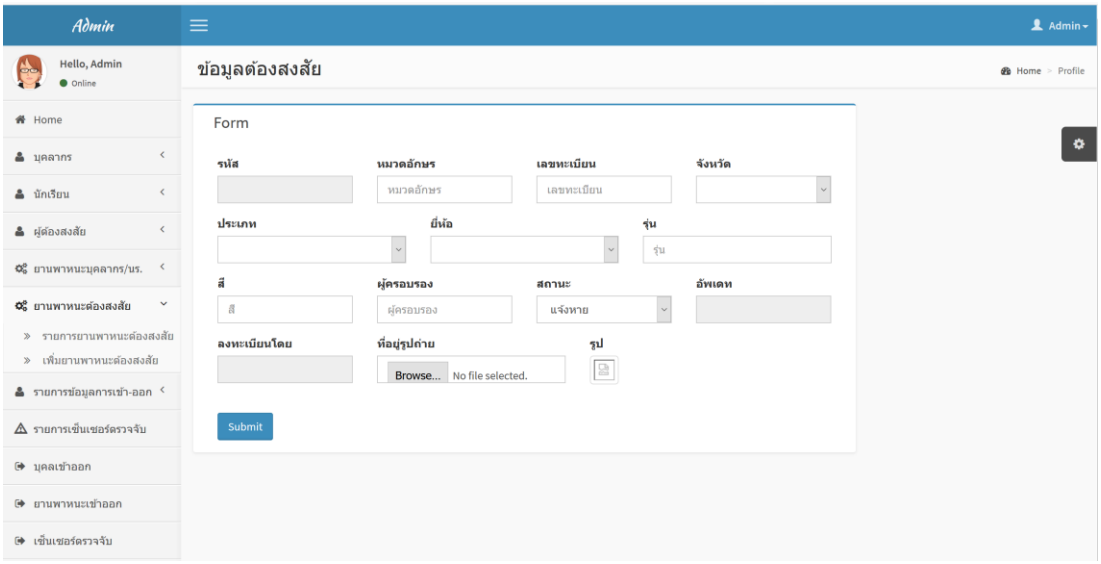
ภาพที่ ค-23 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัย

จากภาพที่ ค-23 แสดงหน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัย ประกอบไปด้วยข้อมูลรายละเอียดของยานพาหนะรวมถึงรูปภาพ ซึ่งผู้ดูแลระบบสามารถ ทำการ เพิ่ม แก้ไข และ ลบข้อมูลได้ ผ่านทางเมนูปรับปรุงข้อมูล (Edit) ภายในระบบ แสดงดังภาพที่ ค-23



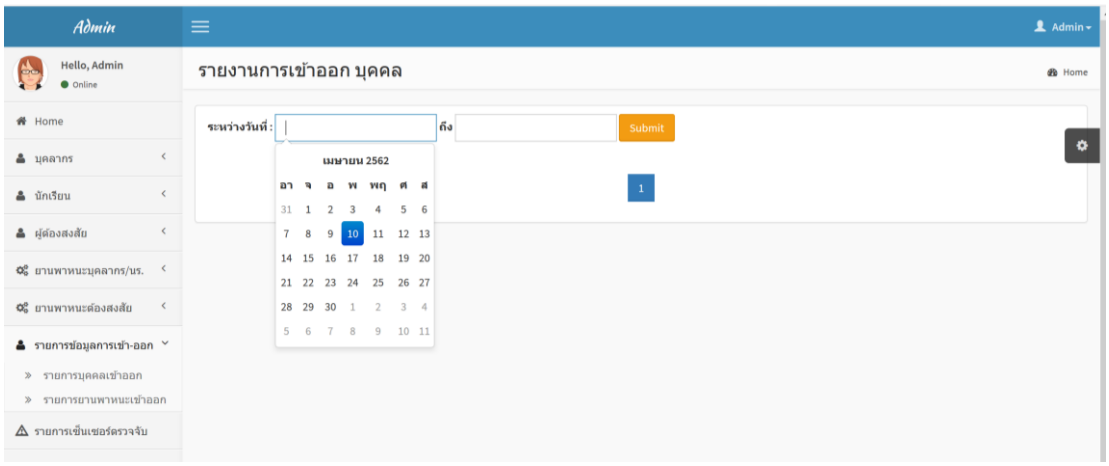
ภาพที่ ค-24 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัยเพิ่มเติม

จากภาพที่ ค-24 หน้าจอแสดงรายละเอียดข้อมูลยานพาหนะต้องสงสัยเพิ่มเติม ผู้ดูแลระบบสามารถทำการ ปรับปรุงแก้ไขข้อมูลดังกล่าวได้



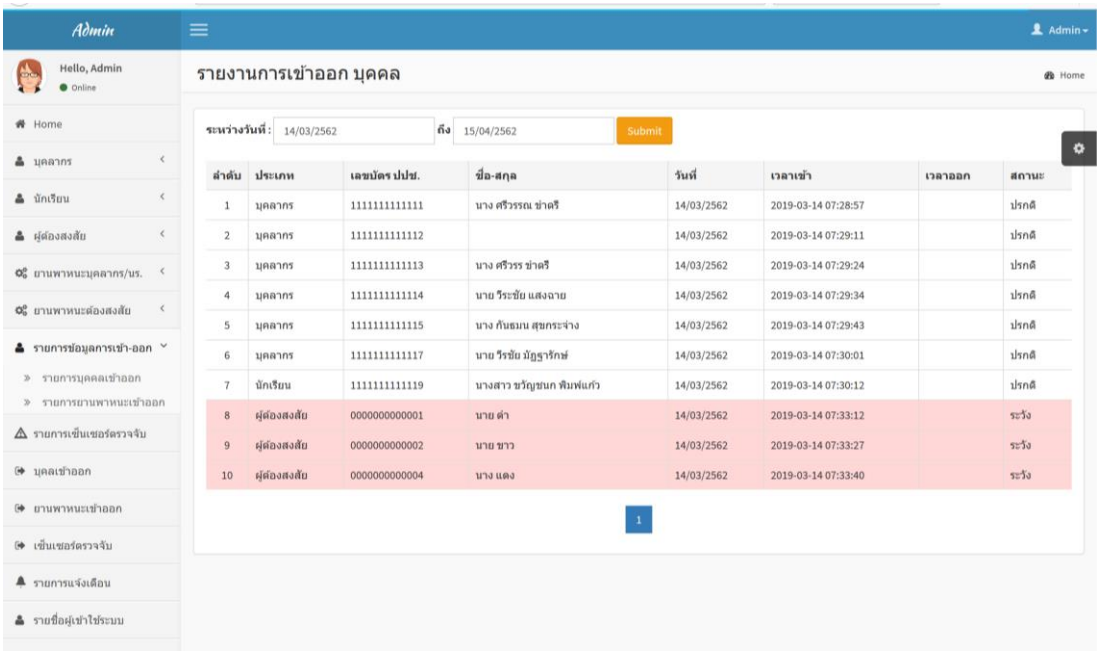
ภาพที่ ค-25 หน้าจอแสดงรายละเอียดการเพิ่มยานพาหนะต้องสงสัย

จากภาพที่ ค-25 หน้าจอแสดงรายละเอียดการเพิ่มข้อมูลยานพาหนะต้องสงสัย ซึ่งผู้ดูแลระบบสามารถทำการ เพิ่มข้อมูลดังกล่าวได้ และ บันทึกเข้าสู่ระบบ



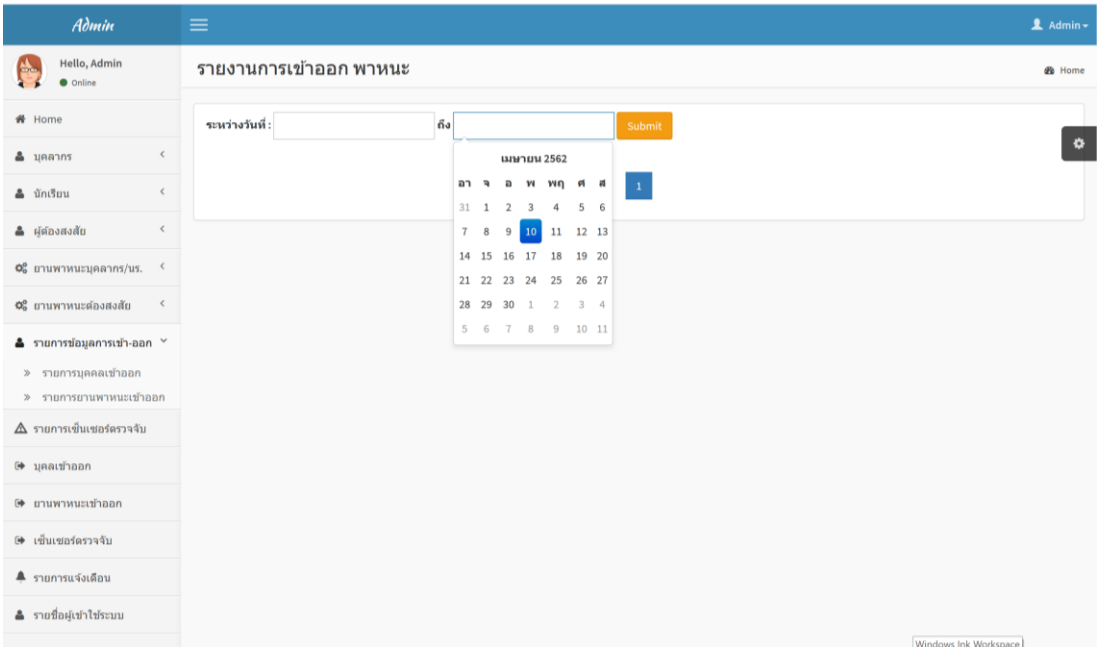
ภาพที่ ค-26 หน้าจอแสดงรายการค้นหารายงานข้อมูลบุคคลเข้าออก

จากภาพที่ ค-26 หน้าจอแสดงรายการค้นหารายงานข้อมูลบุคคลเข้าออก สามารถค้นหาข้อมูลจำนวนบุคคลเข้าออกโดยแสดงเป็นรายงานสรุปดัง**ภาพที่ ค-**26



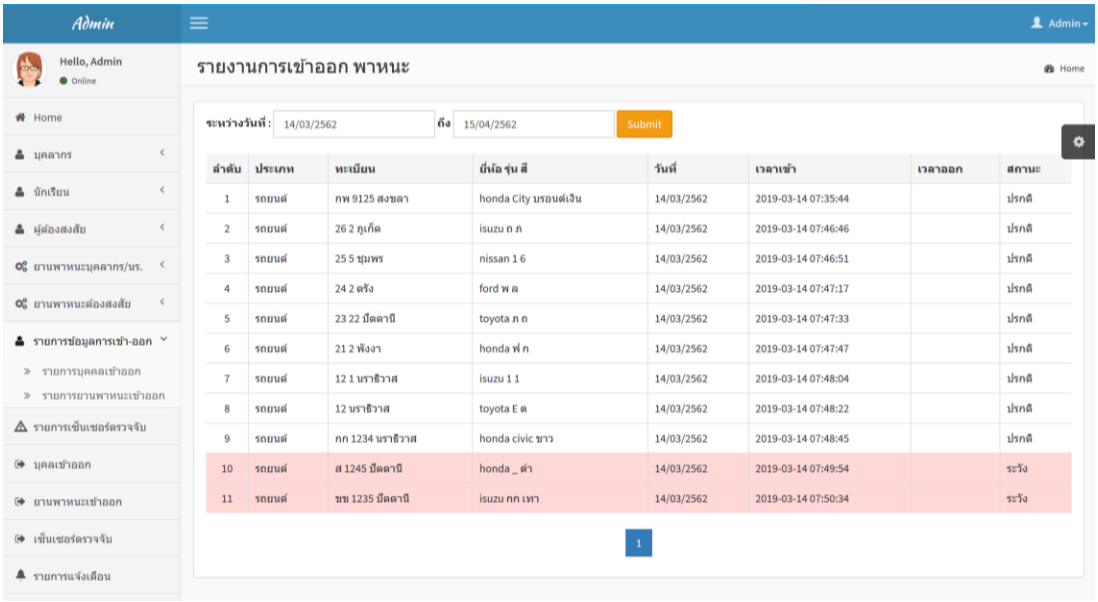
ภาพที่ ค-27 หน้าจอแสดงรายงานการค้นหาข้อมูลบุคคลเข้าออก

จากภาพที่ ค-27 หน้าจอแสดงรายงานค้นหาข้อมูลบุคคลเข้าออก สามารถแสดงรายงานสรุปวันที่ เวลาเข้าออก และ สถานะของบุคคลเข้าออกได้



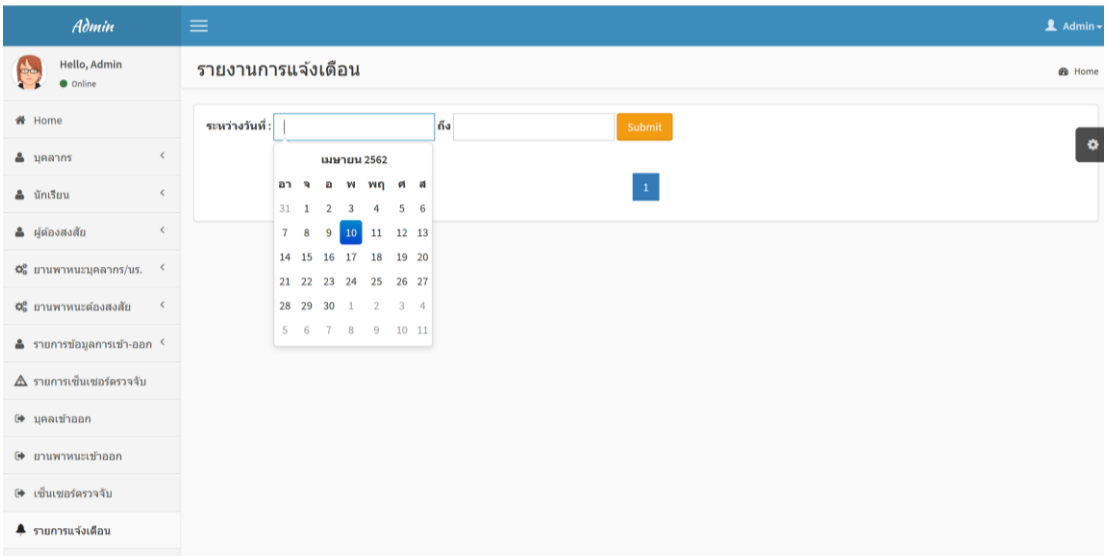
ภาพที่ ค-28 หน้าจอแสดงรายการค้นหารายงานข้อมูลยานพาหนะเข้าออก

จากภาพที่ ค-28 หน้าจอแสดงรายการค้นหารายงานข้อมูลยานพาหนะเข้าออก สามารถค้นหาข้อมูลจำนวนยานพาหนะเข้าออกโดยแสดงเป็นรายงานสรุปดังภาพที่ ค-28



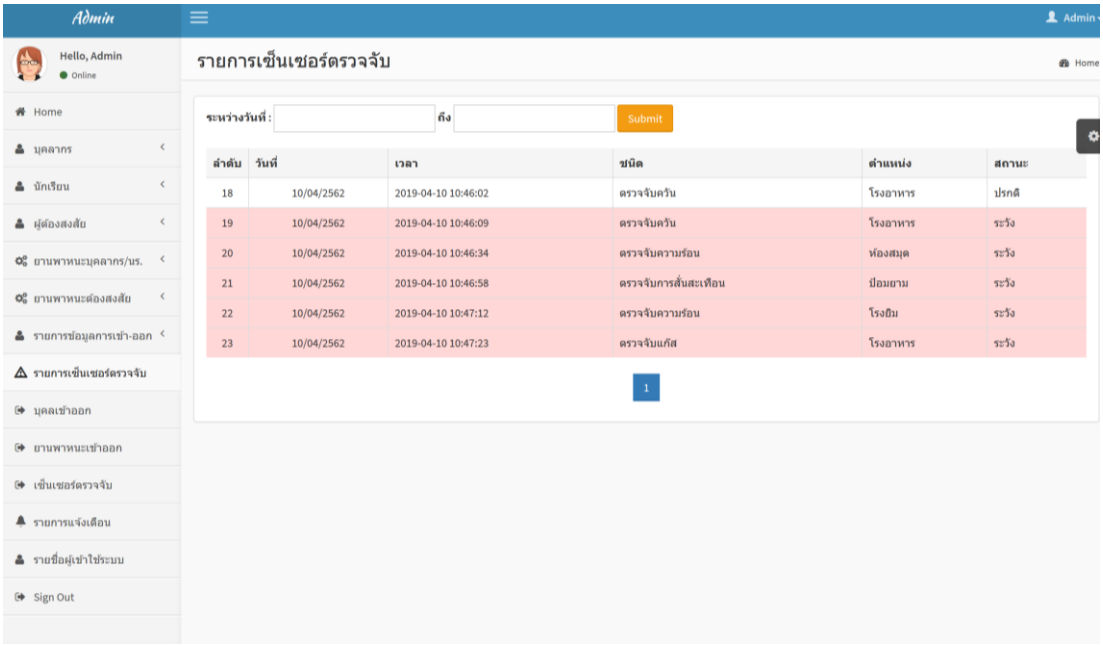
ภาพที่ ค-29 หน้าจอแสดงรายงานการค้นหาข้อมูลบุคคลเข้าออก

จากภาพที่ ค-29 หน้าจอแสดงรายงานค้นหาข้อมูลยานพาหนะเข้าออก สามารถแสดงรายงานสรุปวันที่ เวลาเข้าออก และ สถานะของยานพาหนะเข้าออกได้



ภาพที่ ค-30 หน้าจอแสดงรายการค้นหารายงานข้อมูลการแจ้งเตือนอาคารสถานที่

จากภาพที่ ค-30 หน้าจอแสดงรายการค้นหารายงานข้อมูลการแจ้งเตือนอาคารสถานที่ สามารถค้นหาข้อมูลอาคารสถานที่ ประเภทการตรวจจับ จำนวนครั้ง และสถานะความเสี่ยงของอาคารสถานที่โดยแสดงเป็นรายงานสรุปดังภาพที่ ค-31



ภาพที่ ค-31 หน้าจอแสดงรายงานการค้นหาข้อมูลบุคคลเข้าออก

จากภาพที่ ค-31 หน้าจอแสดงรายงานค้นหาข้อมูลายงานข้อมูลการแจ้งเตือนอาคารสถานที่ สามารถค้นหาข้อมูลอาคารสถานที่ได้

ภาคผนวก ง

บทความวิจัยเผยแพร่

ใบประกาศนียบัตรการนำเสนองานวิจัยในงานประชุมวิชาการระดับนานาชาติ

2019 ICSCT

Certificate

OF PARTICIPATION

THIS CERTIFICATE IS PRESENTED TO

Tuannurisan Suriya

King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand

Paper ID: CT043

Paper Title: Conceptual Framework of High Security System Using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province

for giving your oral presentation at 2019 8th International Conference on Software and Computing Technologies (ICSCT 2019) as an author during April 5-7, 2019 in Hong Kong.

IAP

Session Chair
ICSCT 2019

หนังสือตอบรับการนำเสนองานวิจัยในงานประชุมวิชาการระดับนานาชาติ

Acceptance Notification of Full Paper

2019 8th International Conference on Software and Computing Technologies

(Annual meeting of JCP | April 5-7, 2019, Hong Kong)

http://www.icsct.org/

ICSCT JCP ISSN: 1796-203X

Supported by

Journal of Computers

Paper ID#: CT043

Title of full Paper: Conceptual Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province

Dear Tuannurisan Suriya , Panita Wannapiroon, and Prachyanun Nilsook,

Congratulations! We're pleased to inform you that your full paper above has passed the blind review of the conference technical committees and has been accepted for both publication and oral presentation at the conference 2019 8th International Conference on Software and Computing Technologies (ICSCT 2019), Hong Kong during April 5-7, 2019.

Your paper will be published in **International Journal of Future Computer and Communication** (IJFCC, ISSN: 2010-3751), which will be indexed by Google Scholar, Crossref, Electronic Journals Library, EI (INSPEC, IET), etc.

Registration Instructions

Please follow the six steps below to guarantee your registration will be completed on time.

1. Revise your paper according to the review comments in the attachment carefully.

2. Prepare your final revised paper by following the template.
http://www.ijfcc.org/IJFCC_template.doc

3. Complete and Sign the Copyright Form.
http://www.ijfcc.org/IJFCC.Copyright.doc

4. Download and complete the Registration Form.
http://www.icsct.org/Regform_Author.doc

5. Finish the payment of Registration fee (The information can be found in the Registration form)

6. Send your Final Revised Paper, Signed Copyright Form, Filled Registration Form (Both .doc and .pdf format), Scanned Payment Proof to us at icsct2017@iacsitp.com by Registration Deadline (Before March 10, 2019)

Note:

- If you pay by Credit Card through the online payment system, please fill your confirmation number in the registration form after your make the payment.
- If you pay by bank transfer, please scan the payment slip as the payment proof for checking.

If you have any problem, please feel free to contact us via icsct2017@iacsitp.com for assistance. For the most updated information about the conference, please check the conference website at http://www.icsct.org/index.html. The conference schedule will be available on the conference website in March, 2019.

Note: The conference organizer will not provide the accommodation during the conference, so we suggest you make early reservation at the conference hotel or other hotels nearby.

Again, congratulations. We look forward to seeing you in Hong Kong.

Yours sincerely,

Nancy Y. Liu
JCP Editorial Office
Executive Director
Tel.: +86-28-86512185; Email: nancy@iap.com
JCP Website: http://www.jcomputers.us/ | JCP Email: jcp@iap.org

บทความวิจัยเผยแพร่ในงานประชุมวิชาการระดับนานาชาติ

Conceptual Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province

Tuannurisan Suriya , Panita Wannapiroon, and Prachyanun Nilsook

Abstract— **The purpose of this study to designed Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province. The research procedures were divided into two phases: 1) designing a framework Conceptual Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province. 2) evaluation the appropriateness of the framework. The samples are 5 experts selected by purposive sampling. The research instrument used in this study were as follows: 1) the framework for a High Security system and 2) the appropriateness measurement of High Security system. The data is analyzed by means and standardized deviations statistically.**

The research findings were as follows:

1) The Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province consisted of 4 components as followed: 1) Internet of Things, 2) High Integrated Security Management System, 3) Notification System, and 4) Digital Forensic

2) The results of the evaluation of a Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province. as absolutely appropriate in overall ($\overline{X}$ =4.66, S.D.=0.28).

Index Terms— **High Security system, Internet of Thing, Digital Forensic, Educational Institutions, Southern Border Province.**

I. Introduction

"National Security Policy 2015 - 2021" is the national policy set by the National Security Council. This is a guideline for maintaining the interests and security of the nation to keep up with the changing situation and to solve more diverse problems. It aims to address issues that affect the core of the country with the emphasis on maintaining the core institutions of the nation, to harmony people in the nation and to create a peaceful environment in the southern border provinces. Moreover, it aims to promote security and prevent or mitigate the effects of threats. [1] National Security Policy 2015 - 2021 has set policy priorities that drive the policy into two parts: 1) it is an important policy to strengthen the core of national security which aims to strengthen the security base and strengthen the peace environment in the southern border provinces and 2) It is a general national security policy to build the immunity of society at all levels for addressing the issues and threats, to reduce the risk of the effects of security threats. In addition, it has to be prepared to prevent and solve the problem of all security, to have a strong national defenses and to strengthen the international environment conducive to the preservation of national interests. The security policy is set out in fifth policy which aims to strengthen the capacity to prevent and address transnational threats. It consists of 4 parts: 1) to develop strong system, mechanisms and measures for the prevention and resolution of transnational terrorism and crime. Moreover, to strengthen the capacity of government agencies, especially the news and the legal system to be strengthened, and promote cooperation and coordination between government agencies to unity. 2) To take action to prevent and address all forms of terrorism focused on mitigating factors and conditions that contribute to terrorism and every person or group of people supporting terrorism who use the territory of Thailand as a refuge, an area that seeks to support terrorism or a violent or terrorist area. All of these focus on the protection and security of the urban area. 3) To support and develop the international cooperation at all levels, including international organizations, under the ASEAN framework for the prevention and resolution of transnational terrorism and crime, and to raise the appropriate of Thailand's position on terrorism. 4) To raise the conscious and awareness in the issues of terrorism and transnational crime to the private sector, the public sector and civil society. Furthermore, to build a strong network in cooperation with the government to protect all forms of transnational threats. [2]

The unrest situation happen in three provinces of southern Thailand: Pattani, Yala, Narathiwat and the six districts of Songkhla such as Sadao, Chana, Nathawee, Hat Yai and Saba Yoi. It is caused by the conflict in the southern border provinces, which is the problem of national security. There are various forms of terrorism, including assaults on government officers and the public, ambush, arson of government offices, schools and shops, bullying and bombing. [3] This situation is serious and continuous. It creates skepticism and misery to people's lives in the area, and it also results in significant losses in the public and government sector: physical, mental, life and property, which affect the overall development of the country, social, economic and political.

Educational Institutions in the southern border provinces are one of the targets that insurgents want to attack. Based on terrorist attacks on schools and schools around the world, it appears that schools in Thailand ranked second in attack inferior to Pakistan. [4] Researchers from Maryland University have collected information on the topic "Terrorist Attacks" during the period from 1970 to 2013 to study the

intent of the school. It was found that at that time, there were 3,400 attacks in 110 countries. Pakistan has the highest number of terrorist attacks of 724 times. While Thailand has statistics collected by the Ministry of Education along with the Security Department, it found that the burning of schools in the southern border provinces from 2004 to 2019 had 325 state schools burned; there were 314 security cases and 11 general crime cases. The 109 teachers were killed and 130 got injured, and under the age of 15, there were 81 children died and 445 injured.[5]

Security is a non-threatening condition, out of a dangerous situation or could be harmful to life and property. The body is free from accidents, and the property without damages. Those are what all people want. At present, the living conditions of people in the society have two problems. The first is social problems and natural disasters such as storms, floods, lightning strikes, earthquakes, landslides and fire. Second, the dangers from human actions are disclosure offenses such as riots, insurgencies, and attacks by opponents, and non-disclosure offenses such as theft, espionage, sabotage and terrorism. [6] Most finding ways to prevent or avoid all dangers and increasing security is using technology equipment to help alert the danger at some level. Because of the development of information and communication technology, computer technology and software, computers are rapidly advancing and the ability of various technologies is introduced. It is used to facilitate the daily operation of human communication. Besides, it can present information to users anywhere and anytime to perform various tasks or support decision making promptly. This will lead to full use of information and communication technology in living, and to develop a digital society in accordance with international standards, which aims to develop a vision to step into smart society or Smart Thailand. Smart Thailand is placed under the Information Technology and Communication Policy Framework to 2020. It is the objectives of the Master Plan for Information and Communication Technology (No. 3) of Thailand in 2014-2020, and based on the development of information and communication technology.[7]

With the rapid expansion of mobile devices in the present and the potential in the future as Gartner [8] expectation, it is predicted that the future technology in 2020 will expand and the internet can be accessed by devices increasing to 26-30 billion. Moreover, collaboration with information technology which applies mobile devices allows personal users in the present can access the information, technology, and connect with others easily. Moreover, IoT can be done easily as well so this is the opportunity to extend the potential in the development of system for the thoroughness and speed and allow devices to communicate each other or Internet of Things (IoT). It is the ecosystem that contains things which can communicate and connect others via communication protocol both wired and wireless. Things have the method to identify themselves, know the context of the environment, have the interaction, and work together [9]. This is the concept invented by Kevin Ashton in 1999 which have the infrastructure that can connect to the internet by sensor to communicate to each other [10] to be components in the development of security system which contains intelligent device control for risk location and area where need security in controlling the unrest situation and to receive security information in forms of digital information which can be analyzed, investigated, and reported immediately.

In the present, digital devices are essential for people living in the present so much until it can be said that they are part of our life. These digital devices may be parts of lawsuits. [11] Police officers need to search for evidence to investigate the offender which called Digital evidence. This process is called Digital Forensics which is the collection and preparation of related information from computers for legal proceedings. Analysis of evidence from computers is a process to get evidence from electronic media and store evidence. Implementation according to the investigation process needs to be conformed to an accepted standard. The basis of processes related to digital evidence investigation starts from 1. Evidence acquisition, 2. Evidence storage, 3. Evidence analysis, and 4. Report to court. [12]

Under the unrest situation in southern border provinces which intensifies by various factors, the security in southern border provinces especially educational institutions which are targets that insurgents want to attack. From statistics of attacks on schools and educational institutions around the world by terrorists, schools in Thailand is the 2nd place that attacked after Pakistan [4] From this, the author has a purposes to study the conceptual framework to develop high security conceptual framework by Internet of Thing for educational institutions to investigate digital evidence of educational institutions in southern border provinces to be the prototype system of the development of high security system by Internet of Thing to investigate digital evidence of educational institutions in southern border provinces.

In this paper, we propose a Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province. and To serve as a tool to Development of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

II. PURPOSE OR THE RESEARCH

The purposes of the research are:

1) To design a High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

2) To evaluate a High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

III. SCOPE OF THE RESEARCH

1) Population

Population is the experts in the field of security system, information technology, and internet of thing.

2) Sample Groups

Samples are 5 experts in the field of security system, information technology, and internet of thing chosen by purposive sampling. They are highly-experienced experts in these fields for at least 5 years.

3)Variables of the research

Independent variable is the High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

Dependent variable is the appropriateness of the High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

IV. RESEARCH FRAMEWORK

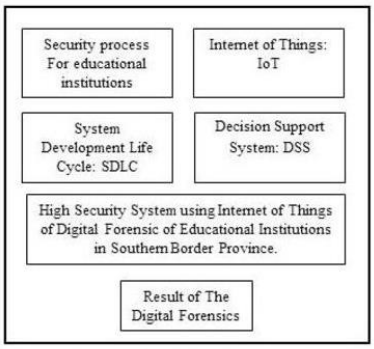


Fig. 1. The Research Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

V. METHODOLOGY

The Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province can be divided into two phases:

1) Design the framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

i) Design the framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

ii) Propose the framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province to the advisor for further examination and revision and

iii) Create an instrument for assessing the appropriateness of the framework High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province.

2) Assessment of the appropriateness of the framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province as the following:-

i) Propose the designed the framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province. to the 5 experts for assessing the appropriateness and

ii)Analyze the output data by using appropriateness measurement scale based on 5-point Likert Scale as well as means ($\overline{X}$) statistics

1.00-1.49 means the assessment topic is absolutely inappropriate

1.50-2.49 means the assessment topic is inappropriate

2.50-3.49 means the assessment topic is neutral

3.50-4.49 means the assessment topic is appropriate

4.50-5.00 means the assessment topic is absolutely appropriate

VI. RESULT

Stage 1 The Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province or HISMS is composed of 4 key components which are

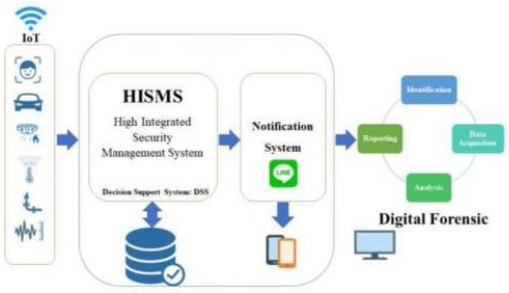


Fig. 2. The framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province. (HISMS)

From Figure 2, high-security conceptual framework High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province consists of 4 parts as follows;

Part Internet of Thing: IoT or technology to connect things invented by Kevin Ashton in 1999 who needs electronic devices has the infrastructure which can connect internet and communicate with each other [10]. Therefore, using IoT is a prototype to design security system by IoT in educational institutions in southern border provinces where have the security problems because they are defined as risky area which need some processes to prevent and solve the unrest problems in the area according to policy of National Council for Peace and Order and the government under the framework of solving problems and developing plan (NCPO), the development and problem solution of southern border provinces to lead to Thailand 4.0, the model to drive Thailand to wealth, stability and sustainability to reform the economic structure of the country to "Value-Based Economy" or innovation-driven economy by assigning the development of digital internet technology which connect devices and artificial intelligence. [13]

IoT technology can be used to communicate with each other by using sensors to communicate. The system consists of camera sensor for detection of face and license plate (RFID), card scanning (sensor), and detection of temperature, smoke, and gas to be the intermediary of internet communication for identification of persons, license plate, and the amount of temperature, smoke, and gas. Therefore, it can classify or identify the type of information which will be used as the input in Part 2 or HISMS system which can be accessed anywhere anytime from every device.

Part 2 High Integrated Security Management System (HISMS) is high security database management system which is the main objective of this study that will develop High Security System using Internet of Things of Digital Forensic. This system can be used via IoT device in Part 1 and do the in-depth analysis and data management by Decision Support System.

Part 3 Notification System is the notification system for the result of security system of educational institutions in southern border provinces by using Line Application to present the notification of the system. This is the smartphone application that can access the notification anytime and anywhere.

Part 4 Digital Forensics or digital evidence investigation is the process of data analysis to investigate digital evidence. This consists of 4 sequences as follows; 1) Identification, 2) Data Acquisition, 3) Analysis to evaluate the risk, and 4) Reporting of high security for educational institutions.[14]

Stage 2 The result of appropriateness measurement of the framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province

TABLE I: THE ASSESSMENT RESULT OF FRAMEWORK OF HIGH SECURITY SYSTEM

Assessment Topics	$\bar{x}$	S.D.	Assessment Result
The framework of security system	4.63	.31	absolutely appropriate
The suitability of IoT devices in term of supporting the system	*4.60*	*.30*	absolutely appropriate
The suitability of Application Line for notification system	4.80	.40	appropriate
The suitability of digital forensic management	4.80	.40	absolutely appropriate
Workflow of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province	4.70	.46	absolutely appropriate
Appropriate use a framework Appropriate use a framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province	4.70	.46	absolutely appropriate
Total	**4.70**	**.38**	**absolutely appropriate**

Following TABLE I, the framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province is rated as absolutely appropriate in overall ($\bar{x}$ =4.70, S.D.=0.38). Considering each item, every item was at absolutely appropriate level.

VII. CONCLUSION

This article presents the design framework which focuses on the connection with the concept of IoT (Internet of Thing) which is the main objective of the study that will develop the High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province. The system will be based on information technology device which electronic devices' potential is developed in the present to able to communicate to each other according to the concept of Internet of Things (IoT) which invented by Kevin Ashton in 1999 who wants electronic devices have the infrastructure to connect the internet. Therefore, devices can communicate with each other [10]. Therefore, using IoT is a prototype to design security system by IoT in educational institutions in southern border provinces where have the security problems because they are defined as risky area which need some processes to prevent and solve the unrest problems in the area according to policy of National Council for Peace and Order and the government under the framework of solving problems and developing plan (NCPO), the development and problem solution of southern border provinces (Office of the Secretary of the Steering Committee for the Solving of Southern Border Problems, 2016) to lead to Thailand 4.0, the model to drive Thailand to wealth, stability and sustainability to reform the economic structure of the country to "Value-Based Economy" or innovation-driven economy by assigning the development of digital internet technology which connect devices and artificial intelligence.[1]

Therefore, using IoT is a prototype to design security system by IoT in educational institutions in southern border provinces where have the security problems because they are defined as risky area which need some processes to prevent and solve the unrest problems in the area according to policy of National Council for Peace and Order and the government under the framework of solving problems and developing plan (NCPO), the development and problem solution of southern border provinces [15] to lead to Thailand 4.0, the model to drive Thailand to wealth, stability and sustainability to reform the economic structure of the country to "Value-Based Economy" or innovation-driven economy by assigning the development of digital internet technology which connect devices and artificial intelligence with the satiable country development.

ACKNOWLEDGMENT

This research received a partial thesis research grant for graduate students from the Graduate College at King Mongkut"s University of Technology North Bangkok.

REFERENCES

(Periodical style)

[1] Office of the national Thailand. *Security Council. Management policy and development in the southern border 2018-2019* Available: http://www.nsc.go.th/

[2] National Economic and Social Development Board. *20 years national strategy, future Thailand For stability and prosperity.*

[3] Baker, C. & Pasuk, P. (2005), *A History of Thailand, Cambridge University Press*, New York.

[4] Kathy Gilsinan. *Terrorist Attacks on Schools Have Soared in The Past 10 Years.* Dec 17, 2014 Available: https://www.theatlantic.com/international/archive/2014/12/terrorist-attacks-on-schools-have-soared-in-the-past-10-years/383825/

[5] Ministry of Education, *Report on the situation of children in the southern border provinces*. Jan13,2019 Available: https://deepsouthwatch.org/sites/default/files/archives/docs/dj_children_in_southern_conflict_2017_edited_clean.pdf

[6] Andie L. Knutson, *The Concept of Personal Security The Journal of Social Psychology,* Department of Psychology, Princeton University 1954,40, 219-236

[7] Ministry of Information and Communication Technology.(Feb.2014). SMART THAILAND 2020. [Online]. Available: http://www.smartthailand2020.co

[8] Gartner, *Gartner predicts five big data trends that will dominate 2016.* [Online]. Available: http://bigdata-madesimple.com/gartner-predictsfive-big-data-trends-that-will-dominate-2016/

[9] Nectec. NETPIE: *Internet of Things* [online]. Available: http://www.nectec.or.th/innovation/innovationsoftware/netpie.html

[10] Kevin Ashton, *That 'Internet of Things' Thing.* [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[11] M.Harbawi,A.Varol,Animproveddigitalevidenceacquisitionmodelfor the Internet of Things forensic I: A theoretical framework, in:2017 5th InternationalSymposiumonDigitalForensicandSecurity,ISDFS,IEEE,2017,pp.1–6. http://dx.doi.org/10.1109/ISDFS.2017.7916508.

[12] Darren Quick, Kim-Kwang Raymond Choo, Digital forensic intelligence: Data subsets and open source intelligence (DFINT+OSINT): a timely and cohesive mix, Future Gener. Comput. Syst. 78 (2018) 558–567. http://dx.doi.org/10.1016/j.future.2016.12.032.

[13] B.B.Zarpelão,R.S.Miani,C.T.Kawakani,S.C.deAlvarenga,Asurveyofintrusion detectioninInternetofThings,J.Netw.Comput.Appl.84(2017)25–37.http: //dx.doi.org/10.1016/j.jnca.2017.02.009.

[14] S.Watson,A.Dehghantanha, Digitalforensics: themissingpieceof the Internet of Thingspromise, Comput. Fraud & Secur.2016(6)(2016)5–8.http://dx.doi.org/10.1016/S1361-3723(15)30045-2.

[15] A. Dehghantanha, K. Franke, Privacy-respecting digital investigation, in:Proceedings of 2014 Twelfth Annual International Conference on Privacy, Security and Trust, PST, 2014, pp. 129–138. http://dx.doi.org/10.1109/PST. 2014.6890932.

Tuannurisan Suriya is a Ph.D. candidate in Information and Communication Technology for Education, Faculty of Technical Education, King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand.
(e-mail: tuannurisan.su@skru.ac.th)

Panita Wannapiroon is an associate professor at the Division of Information and Communication Technology for Education, Faculty of Technical Education, King Mongkut's University of Technology, North Bangkok (KMUTNB), Thailand. Presently, she works in the field of ICT in education. She is a member of Professional Societies in the Apec Learning Community Builders, Thailand (ALCoB), and Association for Educational Technology of Thailand (AETT). (e-mail: panitaw@kmutnb.ac.th)

Prachyanun Nilsook is an associate professor at the Division of Information and Communication Technology for Education, King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand. He currently works in the field of ICT for education. He is a member of Professional Societies in the Association for Educational Technology of Thailand (AETT).
(e-mail: prachyanunn@kmutnb.ac.th)

ICSCT 2019 & ICCRI 2019
Table of Contents

Software and Computing Technologies

Control, Robotics and Informatics

ประวัติผู้วิจัย

ชื่อ : นางต่วนนูรีซันน์ สุริยะ

ชื่อวิทยานิพนธ์ : การพัฒนาระบบรักษาความมั่นคงปลอดภัยสูงด้วยเทคโนโลยีเชื่อมโยงสรรพสิ่งเพื่อการตรวจสอบหลักฐานดิจิทัลสำหรับสถานศึกษาในจังหวัดชายแดนภาคใต้

สาขาวิชา : เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา

ประวัติการศึกษา

พ.ศ. 2549 สำเร็จการศึกษาระดับปริญญาตรี หลักสูตรวิทยาศาสตรบัณฑิต (วท.บ.) สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์

พ.ศ. 2553 สำเร็จการศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต (วท.ม.) สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์

ประวัติการทำงาน

พ.ศ. 2550 - 2551 อาจารย์ สาขาวิชาคอมพิวเตอร์ธุรกิจ วิทยาลัยพาณิชยการหาดใหญ่

พ.ศ. 2553 - ปัจจุบัน อาจารย์ประจำหลักสูตร โปรแกรมวิชาอุตสาหกรรมและเทคโนโลยี คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏสงขลา

ผลงานวิชาการ

Tuannurisan Suriya , Panita Wannapiroon, and Prachyanun Nilsook (2019). "Conceptual Framework of High Security System using Internet of Things of Digital Forensic of Educational Institutions in Southern Border Province." In International Conference on Software and Computing Technologies ICSCT 2019 8th April 5-7, 2019. Hong Kong.

ต่วนนูรีซันน์ สุริยะ, กันต์ธมน สุขกระจ่าง และ ธนะรัตน์ รัตนกูล (2562). "ปัจจัยในการคัดเลือกระบบประมวลผลแบบกลุ่มเมฆของกิจการพัฒนาระบบสารสนเทศโดยวิธีวิเคราะห์เชิงลำดับขั้น." ใน การประชุมวิชาการระดับชาติเทคโนโลยีภาคใต้วิจัยครั้งที่ 9 ประจำปี 2562. นครศรีธรรมราช.

Weerachai Sangchay, Phatcharee Phoempoon, Tanarat Rattanakool,kantamon Sukkrajang, Kulaya Sriyoum, Phuthithon Tugtian,Tuannurisan Suriya, and Salakjit Nilboworn. (2018). "Enhanced antibacterial activity under UV irradiation of WO3-dopedTiO2 thin films." In During the 5th Rajabhat

University National and International Research and Academic Conference. 2-5 December 2018. Phetchaburi : Thailand

ต่วนนูรีซันน์ สุริยะ. (2559). “อินเทอร์เน็ตออฟธิงส์กับการบริหารจัดการห้องเรียนอัจฉริยะ.” วารสารการอาชีวะและเทคนิคศึกษา. ปีที่ 6 ฉบับที่ 11 มกราคม-มิถุนายน : 26-31.

ต่วนนูรีซันน์ สุริยะ, บุณิกา จันทร์เกตุ, กันต์ธมน สุขกระจ่าง และ ธนะรัตน์ รัตนกูล. (2558). “การศึกษาสมรรถนะหลักของบุคลากรที่ปฏิบัติงานฝ่ายกองการศึกษา กรณีศึกษาองค์การบริหารส่วนตำบลเกาะหมาก จังหวัดพัทลุง.” ใน การประชุมหาดใหญ่วิชาการระดับชาติ ครั้งที่ 6 มหาวิทยาลัยหาดใหญ่. จัดหวัดสงขลา, 1,319-1,325.

ต่วนนูรีซันน์ สุริยะ, ไพศาล คงเรือง, นิพนธ์ มณีโชติ และ ศรีวรรณ ขำตรี. (2558). ภาวการณ์มีงานทำของบัณฑิต คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏสงขลา. ใน การประชุมหาดใหญ่วิชาการระดับชาติ ครั้งที่ 6 มหาวิทยาลัยหาดใหญ่. จังหวัดสงขลา, 1,208-1,215.

ต่วนนูรีซันน์ สุริยะ, ธนะรัตน์ รัตนกูล และ กันต์ธมน สุขกระจ่าง. (2558). “การประเมินพฤติกรรมความปลอดภัยของผู้ปฏิบัติงานกับคอมพิวเตอร์ในสำนักงาน กรณีศึกษาคณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏสงขลา.” ใน การประชุมหาดใหญ่วิชาการระดับชาติ ครั้งที่ 6 มหาวิทยาลัยหาดใหญ่. จัดหวัดสงขลา, 1,442-1,753.

ต่วนนูรีซันน์ สุกิจจานันท์ และ วัชรวลี ตั้งคุปตานนท์. (2553). “ระบบตรวจสอบหมายจับออนไลน์บนอุปกรณ์สื่อสารเคลื่อนที่” ใน การประชุมวิชาการระดับประเทศด้านเทคโนโลยีสารสนเทศ ครั้งที่ 3 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. กรุงเทพมหานคร.

กันต์ธมน สุขกระจ่าง, ศรีวรรณ ขำตรี, ธนะรัตน์ รัตนกูล และต่วนนูรีซันน์ สุริยะ (2555). “การศึกษาการบริหารจัดการความปลอดภัยตามแนวคิดของพนักงาน กรณีศึกษา: โรงผลิตอาหารสัตว์ ABC จำกัด.” ใน การประชุมวิชาการข่ายงานวิศวกรรมอุตสาหการประจำปี 2555. เพชรบุรี.