สถาบันวิทยาลัยชุมชน
INSTITUTE OF COMMUNITY COLLEGES

วิทยาลัยชุมชนสตูล
SATUN COMMUNITY COLLEGE

แนวปฏิบัติที่ดี

การเสริมสร้าง ความมั่นคงปลอดภัย ทางไซเบอร์ขององค์กร



วิทยาลัยชุมชนสตูล

กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

คำนำ

ปัจจุบันเทคโนโลยีดิจิทัลมีบทบาทสำคัญต่อการบริหารจัดการองค์กร การจัดการเรียนการสอน และการให้บริการทางการศึกษา ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) จึงเป็นประเด็นสำคัญที่หน่วยงานต้องให้ความใส่ใจ เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ รักษาความถูกต้องครบถ้วนของข้อมูล และสร้างความพร้อมในการใช้งานระบบสารสนเทศอย่างต่อเนื่อง

วิทยาลัยชุมชนสตูลตระหนักถึงความสำคัญดังกล่าว จึงให้ความสำคัญกับการพัฒนาและดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ใช้สนับสนุนการดำเนินงานขององค์กร ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server โดยในปีงบประมาณ พ.ศ. 2568 ได้ดำเนินมาตรการด้านเทคนิค อาทิ การใช้ระบบ Firewall การติดตั้งใบรับรอง SSL การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ให้มีประสิทธิภาพและรองรับอุปกรณ์ที่หลากหลาย ต่อเนื่องถึงปีงบประมาณ พ.ศ. 2569 ที่ให้ความสำคัญกับการทบทวนองค์ความรู้และการแลกเปลี่ยนเรียนรู้ด้านการดูแลข้อมูลและการป้องกันภัยคุกคามทางไซเบอร์ผ่านกระบวนการจัดการความรู้ (Knowledge Management: KM)

แนวปฏิบัติที่ดี เรื่อง การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร จัดทำขึ้นเพื่อรวบรวมแนวคิด กระบวนการดำเนินงาน มาตรการรักษาความปลอดภัย ตลอดจนองค์ความรู้และประสบการณ์จากการปฏิบัติงานของบุคลากร เพื่อใช้เป็นแนวทางในการพัฒนาระบบสารสนเทศและส่งเสริมวัฒนธรรมการใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัย รวมทั้งเป็นพื้นฐานในการปรับปรุงการดำเนินงานของวิทยาลัยให้มีประสิทธิภาพและต่อเนื่อง

วิทยาลัยชุมชนสตูลหวังเป็นอย่างยิ่งว่า รายงานฉบับนี้จะเป็นประโยชน์ต่อผู้บริหาร บุคลากร และผู้เกี่ยวข้องในการนำองค์ความรู้และแนวปฏิบัติไปประยุกต์ใช้ เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์และสนับสนุนการพัฒนาองค์กรสู่การเป็นองค์กรดิจิทัลอย่างยั่งยืน

วิทยาลัยชุมชนสตูล
27 กรกฎาคม 2569

สารบัญ

เรื่อง **หน้า**

คำนำ ก
สารบัญ ข
บทที่ 1 บทนำ 1
บทที่ 2 แนวคิดและหลักการด้านความมั่นคงปลอดภัยทางไซเบอร์ 8
บทที่ 3 กระบวนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ 26
บทที่ 4 แนวปฏิบัติที่ดีของวิทยาลัยชุมชนสตูล 43
บทที่ 5 ผลการดำเนินงานและผลลัพธ์ 59
บทที่ 6 ปัจจัยความสำเร็จและการพัฒนาต่อยอด 71
เอกสารอ้างอิง 86
ภาคผนวก 88
ภาคผนวก ก 89
- การถอดความรู้จากผู้รู้ในหน่วยงาน (Tacit Knowledge to Explicit Knowledge)

แนวปฏิบัติที่ดี การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

บทที่ 1 บทนำ

1.1 ความเป็นมาและความสำคัญ

ปัจจุบันเทคโนโลยีดิจิทัลและระบบสารสนเทศมีบทบาทสำคัญต่อการบริหารจัดการองค์กรภาครัฐและสถาบันการศึกษา โดยเฉพาะการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารงาน การจัดการเรียนการสอน การจัดเก็บและประมวลผลข้อมูล การสื่อสารภายในองค์กร ตลอดจนการให้บริการข้อมูลแก่ประชาชนและผู้มีส่วนเกี่ยวข้อง การประยุกต์ใช้เทคโนโลยีดังกล่าวช่วยเพิ่มประสิทธิภาพในการปฏิบัติงาน ลดขั้นตอนการดำเนินงาน และสนับสนุนการบริหารจัดการให้มีความรวดเร็วและเป็นระบบมากยิ่งขึ้น อย่างไรก็ตาม การพึ่งพาระบบเทคโนโลยีสารสนเทศยังส่งผลให้องค์กรต้องเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งอาจส่งผลกระทบต่อข้อมูล ระบบเครือข่าย และความต่อเนื่องในการดำเนินงานขององค์กร

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) เป็นกระบวนการและมาตรการที่ใช้ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งที่เกิดจากปัจจัยภายในและภายนอกองค์กร ครอบคลุมการปกป้องระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมประยุกต์ และข้อมูลสารสนเทศจากการเข้าถึง การใช้ การเปลี่ยนแปลง การเปิดเผย หรือการทำลายโดยไม่ได้รับอนุญาต ตลอดจนการป้องกันเหตุการณ์ที่อาจทำให้ระบบไม่สามารถให้บริการได้ตามปกติ โดยมีเป้าหมายสำคัญเพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ ซึ่งเป็นหลักการพื้นฐานของการรักษาความมั่นคงปลอดภัยสารสนเทศ (International Organization for Standardization [ISO], 2022)

ภัยคุกคามทางไซเบอร์ในปัจจุบันมีรูปแบบและวิธีการที่หลากหลาย เช่น การโจมตีระบบเครือข่าย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การหลอกลวงผ่านอีเมลหรือเว็บไซต์ปลอม (Phishing) การแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) การเรียกค่าไถ่ข้อมูล (Ransomware) และการโจมตีที่ทำให้ระบบไม่สามารถให้บริการได้ (Denial of Service) นอกจากนี้ ความเสี่ยงยังอาจเกิดจากการตั้งค่าระบบที่ไม่เหมาะสม การใช้ซอฟต์แวร์ที่ไม่ได้รับการปรับปรุง การกำหนดสิทธิ์การเข้าถึงที่ไม่รัดกุม และความผิดพลาดจากพฤติกรรมการใช้งานของบุคลากร ปัจจัยเหล่านี้อาจก่อให้เกิดความเสียหายต่อข้อมูลส่วนบุคคล ข้อมูลทางราชการ และระบบงานที่มีความสำคัญต่อการดำเนินงานขององค์กร

การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์จึงจำเป็นต้องดำเนินการอย่างเป็นระบบ โดยไม่จำกัดเฉพาะการติดตั้งเครื่องมือหรือเทคโนโลยีเพื่อป้องกันภัยคุกคามเท่านั้น แต่ต้องครอบคลุมการกำกับดูแล การประเมินความเสี่ยง การกำหนดมาตรการป้องกัน การตรวจจับเหตุการณ์ผิดปกติ การตอบสนองต่อเหตุการณ์ และการฟื้นฟูระบบภายหลังเกิดเหตุ ทั้งนี้ National Institute of Standards and Technology (NIST) ได้พัฒนากรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือ NIST Cybersecurity Framework (CSF) 2.0 เพื่อใช้เป็นแนวทางบริหารจัดการความเสี่ยงทางไซเบอร์สำหรับองค์กรทุกประเภท ประกอบด้วย 6 หน้าที่หลัก ได้แก่ การกำกับดูแล (Govern) การระบุความเสี่ยง (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการฟื้นฟู (Recover) ซึ่งสามารถนำมาประยุกต์ใช้ให้เหมาะสมกับบริบทและระดับความพร้อมของแต่ละองค์กร (Pascoe, Quinn, & Scarfone, 2024)

นอกจากนี้ การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ยังมีความเกี่ยวข้องกับกฎหมายและมาตรฐานที่สำคัญ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งกำหนด

หลักการและมาตรการเกี่ยวกับการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งกำหนดหลักเกณฑ์เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล และมาตรฐาน ISO/IEC 27001:2022 ซึ่งเป็นมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่ให้ความสำคัญกับการประเมินและจัดการความเสี่ยง การกำหนดมาตรการควบคุม และการปรับปรุงระบบอย่างต่อเนื่อง

วิทยาลัยชุมชนสตูลเป็นสถาบันการศึกษาที่นำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการบริหารจัดการและการดำเนินงานตามภารกิจขององค์กร ทั้งด้านการบริหารงาน การจัดการศึกษา การบริหารงานบุคคล การจัดการเอกสาร และการเผยแพร่ข้อมูลข่าวสาร โดยมีระบบสารสนเทศที่เกี่ยวข้องกับการดำเนินงาน ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ของวิทยาลัย และระบบ Server ซึ่งเป็นองค์ประกอบสำคัญของการจัดเก็บ ประมวลผล และให้บริการข้อมูล การดูแลรักษาความปลอดภัยของระบบเหล่านี้จึงมีความสำคัญต่อการรักษาความถูกต้องของข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการสนับสนุนให้การดำเนินงานของวิทยาลัยเป็นไปอย่างต่อเนื่อง

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลได้ดำเนินมาตรการด้านเทคนิคเพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีการใช้ระบบ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก การใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ให้รองรับการใช้งานผ่านอุปกรณ์ที่หลากหลาย พร้อมปรับปรุงโครงสร้างเมนูให้ผู้ใช้งานสามารถเข้าถึงข้อมูลได้สะดวกยิ่งขึ้น การดำเนินงานดังกล่าวเป็นการพัฒนาระบบเทคโนโลยีสารสนเทศควบคู่กับการรักษาความปลอดภัยของข้อมูลและการให้บริการดิจิทัลขององค์กร

ต่อมาในปีงบประมาณ พ.ศ. 2569 วิทยาลัยได้ให้ความสำคัญกับการทบทวนองค์ความรู้และแนวปฏิบัติด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์ โดยเชื่อมโยงกับกระบวนการจัดการความรู้ (Knowledge Management: KM) เพื่อรวบรวมองค์ความรู้จากการปฏิบัติงาน ส่งเสริมการแลกเปลี่ยนเรียนรู้ และสร้างความตระหนักรู้แก่บุคลากรเกี่ยวกับการใช้งานระบบสารสนเทศอย่างปลอดภัย ตลอดจนสนับสนุนการนำองค์ความรู้ไปประยุกต์ใช้ในการดูแลและพัฒนาระบบสารสนเทศให้สอดคล้องกับบริบทของวิทยาลัย

จากความสำคัญดังกล่าว วิทยาลัยชุมชนสตูลจึงจัดทำรายงานแนวปฏิบัติที่ดี เรื่อง **การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร** เพื่อรวบรวมแนวคิด หลักการ มาตรการ และกระบวนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนองค์ความรู้และประสบการณ์จากการดูแลระบบสารสนเทศของวิทยาลัย โดยมุ่งเน้นการพัฒนาระบบป้องกันภัยคุกคาม การบริหารจัดการความเสี่ยง การดูแลรักษาข้อมูล และการส่งเสริมความรู้ความเข้าใจแก่บุคลากร เพื่อใช้เป็นแนวทางในการพัฒนาการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นระบบและต่อเนื่อง อันจะนำไปสู่การสร้างความเชื่อมั่นในการใช้เทคโนโลยีสารสนเทศและสนับสนุนการพัฒนาวิทยาลัยชุมชนสตูลสู่การเป็นองค์กรดิจิทัลที่มีความมั่นคงปลอดภัย

1.2 วัตถุประสงค์ของการดำเนินงาน

การจัดทำแนวปฏิบัติที่ดี เรื่อง การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร มีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อศึกษาและรวบรวมองค์ความรู้ แนวคิด และหลักการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับการดำเนินงานของวิทยาลัยชุมชนสตูล

2. เพื่อพัฒนาและเสริมสร้างมาตรการรักษาความมั่นคงปลอดภัยของระบบเว็บไซต์ ระบบเครือข่าย Server และระบบสารสนเทศที่ใช้สนับสนุนภารกิจของวิทยาลัย
3. เพื่อส่งเสริมกระบวนการบริหารจัดการความเสี่ยงและการป้องกันภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อข้อมูลและระบบสารสนเทศขององค์กร
4. เพื่อส่งเสริมการจัดการความรู้และการแลกเปลี่ยนประสบการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ระหว่างบุคลากร
5. เพื่อสร้างความรู้ ความเข้าใจ และความตระหนักรู้แก่บุคลากรเกี่ยวกับการใช้งานระบบสารสนเทศ การดูแลข้อมูล และการป้องกันภัยคุกคามทางไซเบอร์
6. เพื่อจัดทำแนวทางการดำเนินงานและการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถนำไปประยุกต์ใช้และปรับปรุงได้อย่างต่อเนื่อง

1.3 เป้าหมายและขอบเขตการดำเนินงาน

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูลกำหนดเป้าหมายให้ครอบคลุมการดูแลระบบสารสนเทศ การบริหารจัดการข้อมูล และการพัฒนาความรู้ของบุคลากร โดยมุ่งเน้นการป้องกันความเสี่ยงและสนับสนุนให้ระบบเทคโนโลยีสารสนเทศสามารถรองรับการดำเนินงานขององค์กรได้อย่างเหมาะสม ทั้งนี้ กำหนดเป้าหมายและขอบเขตการดำเนินงาน ดังนี้

1.3.1 เป้าหมายการดำเนินงาน

การดำเนินงานมีเป้าหมายสำคัญ 3 ด้าน ได้แก่

1) ด้านระบบเทคโนโลยีสารสนเทศ

มุ่งเน้นการดูแลและพัฒนาระบบเครือข่าย เว็บไซต์ Server และระบบสารสนเทศที่ใช้ในการบริหารจัดการของวิทยาลัย โดยให้ความสำคัญกับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเข้ารหัสข้อมูล การปรับปรุงระบบ และการดูแลความพร้อมใช้งานของระบบสารสนเทศ

2) ด้านการบริหารจัดการความมั่นคงปลอดภัย

มุ่งเน้นการกำหนดแนวทางการดูแลรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ การควบคุมสิทธิ์การเข้าถึง การตรวจสอบการทำงานของระบบ การบำรุงรักษา และการจัดเตรียมแนวทางรับมือกับเหตุการณ์ผิดปกติที่อาจเกิดขึ้น

3) ด้านบุคลากรและการจัดการความรู้

มุ่งเน้นการพัฒนาความรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ การส่งเสริมพฤติกรรมการใช้งานระบบสารสนเทศอย่างปลอดภัย การแลกเปลี่ยนประสบการณ์ และการรวบรวมองค์ความรู้เพื่อใช้เป็นแนวทางในการปฏิบัติงานของบุคลากร

1.3.2 ขอบเขตด้านเนื้อหา

การดำเนินงานครอบคลุมเนื้อหาสำคัญ ดังนี้

1) แนวคิดและหลักการพื้นฐานเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
2) หลักการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล (CIA Triad)
3) การวิเคราะห์ภัยคุกคามและการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์
4) การใช้มาตรการทางเทคนิคเพื่อป้องกันภัยคุกคาม เช่น Firewall และการเข้ารหัสการสื่อสารผ่านเว็บไซต์ด้วย SSL/TLS

5) การปรับปรุงและดูแลระบบเว็บไซต์ ระบบเครือข่าย และ Server
6) การดูแลระบบสารสนเทศที่ใช้สนับสนุนภารกิจของวิทยาลัย
7) การจัดการความรู้ การถ่ายทอด และการแลกเปลี่ยนองค์ความรู้ด้าน Cybersecurity
8) การติดตาม ตรวจสอบ และพัฒนาแนวทางรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง

1.3.3 ขอบเขตด้านระบบสารสนเทศ

ครอบคลุมระบบสารสนเทศที่วิทยาลัยใช้สนับสนุนการบริหารจัดการและการดำเนินงาน ได้แก่

- ระบบ ICCS-PORTAL
- ระบบ E-Office
- ระบบ E-HR.ICCS
- ระบบ SMART ERPG
- เว็บไซต์วิทยาลัยชุมชนสตูล
- ระบบ Server และโครงสร้างพื้นฐานที่เกี่ยวข้อง

1.3.4 ขอบเขตด้านกลุ่มเป้าหมาย

กลุ่มเป้าหมายในการดำเนินงานประกอบด้วย ผู้บริหาร บุคลากรสายวิชาการ บุคลากรสายสนับสนุน ผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศ และบุคลากรที่เกี่ยวข้องกับการใช้ การจัดเก็บ และการบริหารจัดการข้อมูลของวิทยาลัย

1.3.5 ขอบเขตด้านระยะเวลา

การจัดทำรายงานครอบคลุมการดำเนินงาน 2 ปีงบประมาณ ได้แก่

- **ปีงบประมาณ พ.ศ. 2568** เน้นการดำเนินมาตรการด้านเทคนิคและการพัฒนาระบบสารสนเทศ ประกอบด้วย การใช้ Firewall การใช้ใบรับรอง SSL การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ให้รองรับการใช้งานผ่านอุปกรณ์ที่หลากหลาย
- **ปีงบประมาณ พ.ศ. 2569** เน้นการทบทวนองค์ความรู้และแนวปฏิบัติด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์ โดยเชื่อมโยงกับกระบวนการจัดการความรู้ เพื่อส่งเสริมการแลกเปลี่ยนเรียนรู้และการนำองค์ความรู้ไปใช้ในการพัฒนาการดำเนินงานของวิทยาลัย

การกำหนดขอบเขตดังกล่าวเป็นกรอบในการรวบรวม วิเคราะห์ และนำเสนอข้อมูลการดำเนินงาน โดยแยกผลการดำเนินงานที่เกิดขึ้นจริงออกจากแนวทางการพัฒนาที่อยู่ระหว่างการดำเนินการหรือกำหนดไว้เป็นเป้าหมายในอนาคต

1.4 ระบบสารสนเทศที่สำคัญของวิทยาลัยชุมชนสตูล

วิทยาลัยชุมชนสตูลนำระบบเทคโนโลยีสารสนเทศมาใช้สนับสนุนการบริหารจัดการและการดำเนินงานตามภารกิจขององค์กร โดยระบบสารสนเทศมีบทบาทในการจัดเก็บ ประมวลผล เผยแพร่ และแลกเปลี่ยนข้อมูลระหว่างผู้บริหาร บุคลากร นักศึกษา และผู้มีส่วนเกี่ยวข้อง ระบบสารสนเทศที่สำคัญประกอบด้วยระบบงานภายใน ระบบบริหารจัดการ และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ซึ่งต้องได้รับการดูแลรักษาความมั่นคงปลอดภัยให้เหมาะสมกับลักษณะการใช้งานและประเภทของข้อมูล

จากข้อมูลระบบสารสนเทศที่เผยแพร่บนเว็บไซต์ของวิทยาลัยชุมชนสตูล พบว่ามีระบบงานที่เกี่ยวข้องกับการบริหารโครงการตามพันธกิจ งานทะเบียน วัดผลและประเมินการศึกษา ระบบจัดการ

หลักสูตร ระบบประกันคุณภาพการศึกษา ระบบการเงินและพัสดุ ระบบคลังข้อมูลด้านการบริหารงานบุคคล ระบบสารสนเทศเพื่อผู้บริหาร งานจัดการเรียนการสอน และระบบ E-Office ICCS เป็นต้น

สำหรับการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร สามารถจำแนกระบบสารสนเทศและโครงสร้างพื้นฐานที่เกี่ยวข้องได้ดังนี้

ตารางที่ 1.1 ระบบสารสนเทศที่สำคัญของวิทยาลัยชุมชนสตูล

ลำดับ	ระบบสารสนเทศ	ลักษณะการใช้งานและความสำคัญ
1	ICCS-PORTAL	ระบบสนับสนุนการบริหารจัดการและการติดตามผลการดำเนินงานขององค์กร ใช้ประกอบการรวบรวมและบริหารจัดการข้อมูลที่เกี่ยวข้องกับภารกิจของวิทยาลัย
2	E-Office	ระบบสำนักงานอิเล็กทรอนิกส์สำหรับสนับสนุนงานสารบรรณ การรับ–ส่งเอกสาร และการดำเนินงานด้านเอกสารภายในองค์กร
3	E-HR.ICCS	ระบบสารสนเทศด้านการบริหารงานบุคคล สนับสนุนการจัดเก็บและบริหารจัดการข้อมูลที่เกี่ยวข้องกับบุคลากร
4	SMART ERPG	ระบบสนับสนุนการบริหารจัดการและการดำเนินงานขององค์กร โดยเกี่ยวข้องกับข้อมูลและกระบวนการทำงานตามภารกิจ
5	เว็บไซต์วิทยาลัยชุมชนสตูล	ช่องทางเผยแพร่ข้อมูล ข่าวสาร ประชาสัมพันธ์ หลักสูตร และข้อมูลการให้บริการแก่ผู้เรียน บุคลากร และประชาชน
6	ระบบ Server	โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่รองรับการจัดเก็บ ประมวลผล และให้บริการระบบงานและข้อมูลขององค์กร

ที่มา: ข้อมูลระบบสารสนเทศของวิทยาลัยชุมชนสตูล และข้อมูลการดำเนินงานด้านเทคโนโลยีสารสนเทศที่ใช้ประกอบการจัดทำรายงาน

ระบบสารสนเทศแต่ละประเภทมีลักษณะการใช้งานและระดับความสำคัญแตกต่างกัน จึงจำเป็นต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยให้เหมาะสมกับข้อมูลและกระบวนการทำงาน โดยสามารถจำแนกประเด็นการดูแลรักษาความปลอดภัยได้ดังนี้

1) การรักษาความปลอดภัยด้านการเข้าถึงข้อมูล

ระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลการบริหารงาน ข้อมูลบุคลากร และข้อมูลการศึกษาจำเป็นต้องมีการกำหนดบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงตามบทบาทหน้าที่ เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมทั้งควรมีการทบทวนบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงอย่างเหมาะสม

2) การรักษาความถูกต้องครบถ้วนของข้อมูล

ข้อมูลที่จัดเก็บและประมวลผลในระบบสารสนเทศจำเป็นต้องได้รับการป้องกันจากการเปลี่ยนแปลง แก้ไข หรือลบโดยไม่ได้รับอนุญาต โดยควรกำหนดสิทธิ์ในการบันทึกและแก้ไขข้อมูลตามหน้าที่ มีการตรวจสอบความถูกต้องของข้อมูล และจัดเก็บประวัติการเปลี่ยนแปลงตามความเหมาะสม

3) การรักษาความปลอดภัยของการสื่อสาร

เว็บไซต์และระบบที่มีการรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตจำเป็นต้องมีมาตรการเข้ารหัสการสื่อสาร เพื่อป้องกันการดักอ่านหรือแก้ไขข้อมูลระหว่างการรับส่ง โดยใช้โปรโตคอลที่มีความปลอดภัยและใบรับรองดิจิทัลที่ถูกต้อง

4) การรักษาความปลอดภัยของระบบเครือข่ายและ Server

ระบบเครือข่ายและ Server เป็นโครงสร้างพื้นฐานที่รองรับการทำงานของระบบสารสนเทศ จึงต้องมีการควบคุมการเชื่อมต่อ การจำกัดสิทธิ์ผู้ดูแลระบบ การปรับปรุงซอฟต์แวร์ การตรวจสอบการทำงาน และการสำรองข้อมูล เพื่อป้องกันความเสียหายและลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัย

5) การรักษาความต่อเนื่องในการให้บริการ

ระบบสารสนเทศที่สนับสนุนภารกิจของวิทยาลัยควรได้รับการดูแลให้สามารถใช้งานได้อย่างต่อเนื่อง โดยมีการตรวจสอบสถานะระบบ การบำรุงรักษาอุปกรณ์ การสำรองข้อมูล และการเตรียมแนวทางฟื้นฟูระบบเมื่อเกิดเหตุการณ์ผิดปกติ

การดูแลระบบสารสนเทศดังกล่าวจึงเป็นองค์ประกอบสำคัญของการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูล โดยต้องอาศัยการดำเนินงานร่วมกันระหว่างผู้บริหาร ผู้รับผิดชอบระบบ และบุคลากรผู้ใช้งาน เพื่อให้การใช้เทคโนโลยีสารสนเทศเป็นไปอย่างปลอดภัยและสอดคล้องกับภารกิจขององค์กร

1.5 ประโยชน์ที่คาดว่าจะได้รับ

การดำเนินงานตามแนวปฏิบัติที่ดี เรื่อง การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร คาดว่าจะก่อให้เกิดประโยชน์ต่อการบริหารจัดการระบบสารสนเทศ การพัฒนาบุคลากร และการดำเนินงานของวิทยาลัยชุมชนสตูล ดังนี้

1. ด้านการพัฒนาระบบเทคโนโลยีสารสนเทศ

วิทยาลัยมีแนวทางในการดูแลและพัฒนาความมั่นคงปลอดภัยของระบบเครือข่าย เว็บไซต์ Server และระบบสารสนเทศที่ใช้สนับสนุนภารกิจขององค์กรอย่างเป็นระบบ สามารถนำไปใช้ประกอบการกำหนดมาตรการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม

2. ด้านการรักษาความปลอดภัยของข้อมูล

มีแนวทางในการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล รวมถึงการควบคุมสิทธิ์การเข้าถึง การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการดูแลข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่เกี่ยวข้อง

3. ด้านประสิทธิภาพการบริหารจัดการองค์กร

ระบบสารสนเทศได้รับการดูแลและพัฒนาให้สนับสนุนการบริหารจัดการ การปฏิบัติงาน และการให้บริการทางการศึกษาได้อย่างเหมาะสม ช่วยส่งเสริมความต่อเนื่องในการดำเนินงานและลดความเสี่ยงที่อาจเกิดจากความขัดข้องของระบบ

4. ด้านการพัฒนาศักยภาพบุคลากร

บุคลากรมีแนวทางในการพัฒนาความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ การใช้งานระบบสารสนเทศอย่างปลอดภัย การดูแลข้อมูล และการปฏิบัติตนเมื่อพบเหตุการณ์ผิดปกติ ซึ่งเป็นพื้นฐานสำคัญของการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ในองค์กร

5. ด้านการจัดการความรู้และการถ่ายทอดองค์ความรู้

เกิดการรวบรวม จัดระบบ และถ่ายทอดองค์ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์จากประสบการณ์การปฏิบัติงานของบุคลากร สามารถนำไปจัดทำเป็นคู่มือ แนวปฏิบัติ และแหล่งเรียนรู้สำหรับการพัฒนางานด้านเทคโนโลยีสารสนเทศของวิทยาลัย

6. ด้านการบริหารจัดการความเสี่ยง

วิทยาลัยมีกรอบแนวทางในการระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ สามารถนำไปใช้ประกอบการกำหนดมาตรการควบคุมและการติดตามตรวจสอบระบบสารสนเทศอย่างต่อเนื่อง

7. ด้านการพัฒนาองค์กรสู่ดิจิทัล

วิทยาลัยมีพื้นฐานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ที่เชื่อมโยงกับการบริหารจัดการองค์กรดิจิทัล ส่งเสริมความเชื่อมั่นในการใช้เทคโนโลยีสารสนเทศ และสนับสนุนการดำเนินงานตามภารกิจของวิทยาลัยอย่างมีประสิทธิภาพและยั่งยืน

บทที่ 2 แนวคิดและหลักการด้านความมั่นคงปลอดภัยทางไซเบอร์

การเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์เป็นองค์ประกอบสำคัญของการบริหารจัดการองค์กรในยุคดิจิทัล เนื่องจากระบบสารสนเทศและข้อมูลอิเล็กทรอนิกส์เป็นทรัพยากรที่มีความสำคัญต่อการดำเนินงานของหน่วยงาน ทั้งด้านการบริหารจัดการ การให้บริการ การจัดเก็บข้อมูล และการติดต่อสื่อสาร การรักษาความมั่นคงปลอดภัยจึงต้องครอบคลุมทั้งการป้องกันระบบและข้อมูล การบริหารจัดการความเสี่ยง การตรวจสอบและเฝ้าระวัง ตลอดจนการตอบสนองและฟื้นฟูระบบเมื่อเกิดเหตุการณ์ผิดปกติ

สำหรับวิทยาลัยชุมชนสตูล การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์มีความเกี่ยวข้องกับระบบสารสนเทศที่ใช้สนับสนุนภารกิจขององค์กร ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server ตลอดจนบุคลากรที่มีหน้าที่เกี่ยวข้องกับการบริหารจัดการและใช้งานระบบดังกล่าว การกำหนดแนวทางรักษาความปลอดภัยจึงจำเป็นต้องอาศัยหลักการทางวิชาการ มาตรฐานสากล และกฎหมายที่เกี่ยวข้อง เพื่อให้สามารถนำไปประยุกต์ใช้ในการดำเนินงานได้อย่างเหมาะสม

2.1 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

ความหมายของความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง การดำเนินมาตรการเพื่อป้องกัน ควบคุม ตรวจจับ ตอบสนอง และฟื้นฟูระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสื่อสารอิเล็กทรอนิกส์ และข้อมูลที่เกี่ยวข้องจากภัยคุกคามหรือการกระทำที่อาจก่อให้เกิดความเสียหาย โดยมีวัตถุประสงค์เพื่อรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน และคุณสมบัติด้านความปลอดภัยอื่นที่เกี่ยวข้องกับระบบสารสนเทศ

National Institute of Standards and Technology (NIST) อธิบายความมั่นคงปลอดภัยทางไซเบอร์ว่าเป็นการป้องกันความเสียหาย การคุ้มครอง และการฟื้นฟูระบบคอมพิวเตอร์และระบบสื่อสารอิเล็กทรอนิกส์ รวมถึงข้อมูลที่อยู่ภายในระบบ เพื่อให้เกิดความพร้อมใช้งาน ความถูกต้องครบถ้วน การพิสูจน์ตัวตน การรักษาความลับ และการไม่สามารถปฏิเสธความรับผิดชอบต่อการกระทำทางอิเล็กทรอนิกส์ได้

ส่วนความมั่นคงปลอดภัยสารสนเทศ (Information Security) เป็นแนวคิดที่มุ่งคุ้มครองข้อมูลและระบบสารสนเทศจากการเข้าถึง การใช้ การเปิดเผย การรบกวน การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต เพื่อรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล

ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยสารสนเทศมีความสัมพันธ์กันอย่างใกล้ชิด โดยความมั่นคงปลอดภัยทางไซเบอร์ให้ความสำคัญกับการป้องกันและจัดการความเสี่ยงที่เกิดขึ้นในสภาพแวดล้อมดิจิทัลและระบบเครือข่าย ขณะที่ความมั่นคงปลอดภัยสารสนเทศครอบคลุมการคุ้มครองข้อมูลในทุกรูปแบบ ทั้งข้อมูลอิเล็กทรอนิกส์ เอกสาร และข้อมูลที่จัดเก็บในสื่อประเภทต่าง ๆ

ดังนั้น การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรจึงไม่ได้จำกัดอยู่เพียงการติดตั้งโปรแกรมป้องกันไวรัสหรืออุปกรณ์รักษาความปลอดภัยเท่านั้น แต่ยังรวมถึงการกำหนดนโยบาย การควบคุมสิทธิ์การเข้าถึง การบริหารจัดการข้อมูล การพัฒนาบุคลากร และการกำหนดกระบวนการรับมือกับเหตุการณ์ด้านความปลอดภัยอย่างเป็นระบบ

ความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ต่อองค์กร

ความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญต่อการดำเนินงานขององค์กรในหลายด้าน ดังนี้

1. การคุ้มครองข้อมูลและสารสนเทศ

ข้อมูลเป็นทรัพยากรสำคัญขององค์กร ทั้งข้อมูลการบริหารงาน ข้อมูลบุคลากร ข้อมูลนักศึกษา ข้อมูลทางการเงิน และข้อมูลการดำเนินงาน การรักษาความปลอดภัยช่วยลดความเสี่ยงจากการเข้าถึง การเปิดเผย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

2. การรักษาความต่อเนื่องในการดำเนินงาน

ระบบสารสนเทศเป็นเครื่องมือสนับสนุนภารกิจขององค์กร หากเกิดเหตุการณ์ที่ทำให้ระบบไม่สามารถใช้งานได้ อาจส่งผลกระทบต่อการบริหารจัดการ การปฏิบัติงาน และการให้บริการ การจัดให้มีมาตรการป้องกัน การสำรองข้อมูล และการฟื้นฟูระบบจึงมีความสำคัญต่อการรักษาความต่อเนื่องขององค์กร

3. การสร้างความเชื่อมั่นในการใช้บริการดิจิทัล

การรักษาความปลอดภัยของระบบสารสนเทศช่วยสร้างความเชื่อมั่นให้แก่ผู้บริหาร บุคลากร นักศึกษา และประชาชนที่เข้ามาใช้บริการ โดยเฉพาะระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร

4. การลดความเสี่ยงและผลกระทบจากภัยคุกคาม

การกำหนดมาตรการป้องกันและการตรวจสอบระบบอย่างต่อเนื่องช่วยลดโอกาสเกิดเหตุการณ์ผิดปกติ และช่วยให้องค์กรสามารถตรวจพบและจัดการกับความเสี่ยงได้อย่างเหมาะสม

5. การสนับสนุนการปฏิบัติตามกฎหมายและมาตรฐาน

องค์กรที่มีการจัดเก็บ ใช้ หรือประมวลผลข้อมูลส่วนบุคคลจำเป็นต้องคำนึงถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมายและข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง การกำหนดมาตรการรักษาความปลอดภัยจึงเป็นส่วนหนึ่งของการบริหารจัดการองค์กรที่มีความรับผิดชอบ

องค์ประกอบของการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์

การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ต้องอาศัยองค์ประกอบหลายด้านที่ทำงานสัมพันธ์กัน โดยสามารถจำแนกได้เป็น 3 องค์ประกอบสำคัญ ได้แก่

1. ด้านบุคลากร (People)

บุคลากรเป็นผู้ใช้งานและผู้ดูแลระบบสารสนเทศ จึงมีบทบาทสำคัญต่อการรักษาความปลอดภัยขององค์กร การสร้างความตระหนักรู้เกี่ยวกับภัยคุกคาม การใช้รหัสผ่านอย่างปลอดภัย การระมัดระวังการเปิดเผยข้อมูล และการรายงานเหตุการณ์ผิดปกติ เป็นแนวทางสำคัญในการลดความเสี่ยงจากความผิดพลาดของผู้ใช้งาน

2. ด้านกระบวนการ (Process)

เป็นการกำหนดนโยบาย ระเบียบ ข้อปฏิบัติ และขั้นตอนการดำเนินงานด้านความปลอดภัย เช่น การกำหนดสิทธิ์การเข้าถึง การตรวจสอบระบบ การสำรองข้อมูล การจัดการเหตุการณ์ผิดปกติ และการทบทวนมาตรการรักษาความปลอดภัยให้เหมาะสมกับสภาพแวดล้อมขององค์กร

3. ด้านเทคโนโลยี (Technology)

เป็นการนำเครื่องมือและระบบเทคโนโลยีมาใช้ในการป้องกันและควบคุมความเสี่ยง เช่น Firewall ระบบป้องกันมัลแวร์ ระบบเข้ารหัสข้อมูล ใบรับรองดิจิทัล ระบบตรวจสอบการใช้งาน และระบบสำรองข้อมูล

องค์ประกอบทั้งสามด้านมีความสัมพันธ์และต้องดำเนินการควบคู่กัน การมีเทคโนโลยีที่ทันสมัยเพียงอย่างเดียวไม่สามารถรับประกันความปลอดภัยได้ หากไม่มีการกำหนดกระบวนการควบคุมและการสร้างความตระหนักรู้แก่บุคลากร

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์

National Institute of Standards and Technology ได้จัดทำกรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือ NIST Cybersecurity Framework 2.0 เพื่อเป็นแนวทางสำหรับองค์กรในการทำความเข้าใจ ประเมิน จัดลำดับความสำคัญ และบริหารจัดการความเสี่ยงทางไซเบอร์ โดยสามารถประยุกต์ใช้ได้กับองค์กรทุกขนาดและทุกประเภท (Pascoe, Quinn, & Scarfone, 2024)

กรอบดังกล่าวประกอบด้วย 6 หน้าที่หลัก ดังนี้



ที่มา: Pascoe, Quinn, and Scarfone (2024), NIST CSF 2.0

กรอบ NIST CSF 2.0 สามารถนำมาใช้เป็นแนวทางในการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูล โดยเชื่อมโยงการกำกับดูแล การสำรวจระบบสารสนเทศ การใช้มาตรการป้องกัน การตรวจสอบระบบ การรับมือกับเหตุการณ์ และการฟื้นฟูระบบเข้าด้วยกัน ทั้งนี้ การนำกรอบดังกล่าวมาใช้ต้องพิจารณาความพร้อม ทรัพยากร และลักษณะการดำเนินงานของวิทยาลัยเป็นสำคัญ

2.2 หลักการรักษาความมั่นคงปลอดภัยของข้อมูล (CIA Triad)

หลักการ CIA Triad เป็นกรอบแนวคิดพื้นฐานของการรักษาความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วยองค์ประกอบ 3 ประการ ได้แก่ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาความพร้อมใช้งาน (Availability) ซึ่งเป็นหลักการที่ใช้กำหนดมาตรการควบคุมและประเมินความปลอดภัยของข้อมูลและระบบสารสนเทศ (NIST, n.d.; ISO, 2022)

หลักการทั้งสามมีความสัมพันธ์กันและเป็นพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยของระบบสารสนเทศ โดยสามารถอธิบายได้ดังนี้

2.2.1 การรักษาความลับ (Confidentiality)

การรักษาความลับ หมายถึง การควบคุมให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะบุคคล หน่วยงาน หรือกระบวนการที่ได้รับอนุญาตเท่านั้น โดยมีวัตถุประสงค์เพื่อป้องกันการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลที่มีความสำคัญต่อองค์กร (NIST, n.d.)

การรักษาความลับมีความสำคัญต่อระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ข้อมูลบุคลากร ข้อมูลนักศึกษา ข้อมูลทางการเงิน และเอกสารภายในองค์กร เนื่องจากข้อมูลเหล่านี้อาจส่งผลกระทบต่อสิทธิของบุคคลและการดำเนินงานของหน่วยงาน หากถูกเปิดเผยแก่ผู้ไม่มีสิทธิ์

แนวทางการรักษาความลับของข้อมูลประกอบด้วย

1) กำหนดบัญชีผู้ใช้งานและรหัสผ่านสำหรับเข้าสู่ระบบ
2) กำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทและหน้าที่รับผิดชอบ
3) ใช้หลักการให้สิทธิ์เท่าที่จำเป็น (Principle of Least Privilege)
4) ใช้การเข้ารหัสข้อมูลเมื่อมีการจัดเก็บหรือส่งผ่านข้อมูลที่มีความสำคัญ
5) จำกัดการเผยแพร่และส่งต่อข้อมูลส่วนบุคคลเฉพาะกรณีที่มีความจำเป็นและมีฐานทางกฎหมายรองรับ
6) ตรวจสอบและทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานอย่างสม่ำเสมอ
7) ยกเลิกหรือปรับเปลี่ยนสิทธิ์การเข้าถึงเมื่อบุคลากรเปลี่ยนหน้าที่หรือสิ้นสุดการปฏิบัติงาน

การประยุกต์ใช้กับวิทยาลัยชุมชนสตูล

ระบบ E-HR.ICCS ซึ่งเกี่ยวข้องกับการบริหารงานบุคคล และระบบ E-Office ซึ่งใช้สนับสนุนการรับ–ส่งและจัดเก็บเอกสารอิเล็กทรอนิกส์ เป็นระบบที่ควรให้ความสำคัญกับการกำหนดสิทธิ์ผู้ใช้งาน การจำกัดการเข้าถึงข้อมูล และการควบคุมการเผยแพร่เอกสาร เพื่อป้องกันการเปิดเผยข้อมูลที่ไม่เหมาะสม ส่วนระบบ ICCS-PORTAL และ SMART ERPG ควรมีการกำหนดสิทธิ์ให้สอดคล้องกับบทบาทของผู้ใช้งานแต่ละกลุ่ม

2.2.2 การรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity)

การรักษาความถูกต้องครบถ้วน หมายถึง การคุ้มครองข้อมูลให้มีความถูกต้อง สมบูรณ์ และเชื่อถือได้ โดยป้องกันการเปลี่ยนแปลง แก้ไข หรือลบข้อมูลโดยไม่ได้รับอนุญาต รวมทั้งรักษาความถูกต้องของข้อมูลตลอดกระบวนการจัดเก็บ ประมวลผล และส่งผ่านข้อมูล (NIST, n.d.)

การรักษาความถูกต้องครบถ้วนของข้อมูลมีความสำคัญต่อการบริหารจัดการองค์กร เนื่องจากข้อมูลที่ผิดพลาดหรือถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการตัดสินใจ การรายงานผลการดำเนินงาน และการให้บริการของหน่วยงาน

แนวทางการรักษาความถูกต้องครบถ้วนของข้อมูลประกอบด้วย

1) กำหนดสิทธิ์ในการบันทึก แก้ไข และลบข้อมูลให้เหมาะสมกับหน้าที่
2) ตรวจสอบความถูกต้องของข้อมูลก่อนนำเข้าสู่ระบบ
3) จัดเก็บบันทึกประวัติการเข้าใช้งานและการเปลี่ยนแปลงข้อมูล (Audit Log)
4) ใช้กลไกตรวจสอบความถูกต้องของข้อมูล เช่น Hash Function หรือ Digital Signature ตามลักษณะงาน
5) กำหนดขั้นตอนการอนุมัติการแก้ไขข้อมูลที่มีความสำคัญ

6) สำรองข้อมูลและเก็บรักษาข้อมูลต้นฉบับตามความเหมาะสม
7) ตรวจสอบความถูกต้องของข้อมูลเป็นระยะ

การประยุกต์ใช้กับวิทยาลัยชุมชนสตูล

ระบบ ICCS-PORTAL และ SMART ERPG ซึ่งใช้สนับสนุนการบริหารจัดการข้อมูลขององค์กร จำเป็นต้องมีการควบคุมการบันทึกและแก้ไขข้อมูลให้เหมาะสมกับหน้าที่ของผู้ใช้งาน รวมทั้งควรมีการตรวจสอบข้อมูลก่อนนำไปใช้ประกอบการรายงานและการตัดสินใจ สำหรับระบบ E-Office ควรให้ความสำคัญกับความถูกต้องของเอกสารอิเล็กทรอนิกส์และการจัดเก็บประวัติการดำเนินงาน

2.2.3 การรักษาความพร้อมใช้งานของข้อมูล (Availability)

การรักษาความพร้อมใช้งาน หมายถึง การทำให้ข้อมูล ระบบสารสนเทศ และบริการทางเทคโนโลยีสามารถเข้าถึงและใช้งานได้อย่างทันเวลาและเชื่อถือได้ เมื่อผู้ใช้งานที่ได้รับอนุญาตมีความจำเป็นต้องใช้ข้อมูลหรือระบบ

การรักษาความพร้อมใช้งานมีความสำคัญต่อระบบสารสนเทศที่สนับสนุนภารกิจขององค์กร เนื่องจากความขัดข้องของระบบ การโจมตีทางไซเบอร์ ความเสียหายของอุปกรณ์ หรือเหตุการณ์ที่ทำให้ข้อมูลสูญหาย อาจส่งผลกระทบต่อการบริหารจัดการและการให้บริการ
แนวทางการรักษาความพร้อมใช้งานประกอบด้วย

1) ตรวจสอบสถานะการทำงานของระบบเครือข่ายและ Server อย่างสม่ำเสมอ
2) บำรุงรักษาอุปกรณ์และระบบสารสนเทศตามรอบระยะเวลาที่กำหนด
3) สำรองข้อมูลตามความสำคัญและความจำเป็นของระบบ
4) จัดเก็บข้อมูลสำรองแยกจากระบบหลักและควบคุมสิทธิ์การเข้าถึง
5) ทดสอบกระบวนการกู้คืนข้อมูลและระบบ
6) จัดทำแผนรองรับเหตุการณ์ที่อาจทำให้ระบบหยุดชะงัก
7) กำหนดผู้รับผิดชอบและช่องทางการแจ้งเหตุเมื่อระบบไม่สามารถให้บริการได้

การประยุกต์ใช้กับวิทยาลัยชุมชนสตูล

ระบบ Server และเว็บไซต์ของวิทยาลัยเป็นองค์ประกอบสำคัญในการรองรับการให้บริการข้อมูลและระบบสารสนเทศ จึงควรมีการตรวจสอบสถานะการทำงาน การบำรุงรักษา และการสำรองข้อมูลอย่างเหมาะสม รวมถึงการกำหนดแนวทางฟื้นฟูระบบเมื่อเกิดเหตุขัดข้อง เพื่อสนับสนุนให้การดำเนินงานของวิทยาลัยสามารถดำเนินต่อไปได้

ตารางสรุปหลักการ CIA Triad

ตารางที่ 2.1 หลักการรักษาความมั่นคงปลอดภัยของข้อมูล

องค์ประกอบ	ความหมาย	ความเสี่ยงที่เกี่ยวข้อง	แนวทางควบคุม
Confidentiality	การรักษาความลับของข้อมูล	การเปิดเผยข้อมูลหรือการเข้าถึงโดยไม่ได้รับอนุญาต	กำหนดสิทธิ์ ใช้รหัสผ่าน และเข้ารหัสข้อมูล
Integrity	การรักษาความถูกต้องครบถ้วน	การแก้ไขหรือลบข้อมูลโดยไม่ได้รับอนุญาต	ควบคุมการแก้ไข ตรวจสอบข้อมูล และจัดเก็บ Log
Availability	การรักษาความพร้อมใช้งาน	ระบบหยุดชะงักหรือข้อมูลสูญหาย	บำรุงรักษาระบบ สำรองข้อมูล และทดสอบกู้คืน

ที่มา: ประยุกต์จาก NIST (n.d.) และ ISO/IEC 27001:2022

หลักการ CIA Triad เป็นกรอบพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยของระบบสารสนเทศ โดยการดำเนินงานต้องคำนึงถึงองค์ประกอบทั้งสามด้านควบคู่กัน เนื่องจากการให้ความสำคัญกับด้านใดด้านหนึ่งมากเกินไปอาจส่งผลกระทบต่อการใช้งานหรือการบริหารจัดการระบบโดยรวม

2.3 ภัยคุกคามและความเสี่ยงทางไซเบอร์

2.3.1 ความหมายของภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือเหตุการณ์ที่มีศักยภาพก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ระบบเครือข่าย ข้อมูล หรือบริการดิจิทัล โดยอาจเกิดจากบุคคล กลุ่มบุคคล โปรแกรมประสงค์ร้าย หรือปัจจัยอื่นที่ส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

ภัยคุกคามอาจเกิดขึ้นจากภายนอกองค์กร เช่น การโจมตีผ่านเครือข่ายอินเทอร์เน็ต การหลอกลวงทางอิเล็กทรอนิกส์ และการแพร่กระจายของมัลแวร์ หรืออาจเกิดจากภายในองค์กร เช่น การกำหนดสิทธิ์ไม่เหมาะสม การใช้งานข้อมูลโดยไม่ระมัดระวัง และความผิดพลาดจากการปฏิบัติงาน

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่เนื้อหาพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งครอบคลุมภัยคุกคามและการโจมตีทางสารสนเทศ การหลอกลวงทางสังคม ระบบเครือข่าย Firewall การพิสูจน์ตัวตน การสำรองข้อมูล การจัดการเหตุการณ์ และความปลอดภัยของซอฟต์แวร์และเว็บไซต์ (ThaiCERT, ม.ป.ป.)

2.3.2 ความหมายของความเสี่ยงทางไซเบอร์

ความเสี่ยงทางไซเบอร์ (Cybersecurity Risk) หมายถึง ความเป็นไปได้ที่ภัยคุกคามจะใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนของระบบสารสนเทศ จนก่อให้เกิดผลกระทบต่อข้อมูล ระบบงาน ทรัพย์สิน หรือการดำเนินงานขององค์กร

การประเมินความเสี่ยงต้องพิจารณาปัจจัยสำคัญ ได้แก่

1) **ภัยคุกคาม (Threat):** เหตุการณ์หรือการกระทำที่อาจก่อให้เกิดความเสียหาย
2) **ช่องโหว่ (Vulnerability):** จุดอ่อนของระบบ กระบวนการ หรือบุคลากรที่อาจถูกนำไปใช้ในการโจมตี
3) **โอกาสเกิดเหตุการณ์ (Likelihood):** ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น
4) **ผลกระทบ (Impact):** ระดับความเสียหายที่อาจเกิดขึ้นต่อข้อมูล ระบบ และภารกิจขององค์กร

การบริหารความเสี่ยงจึงเป็นกระบวนการที่ต้องดำเนินการอย่างเป็นระบบ ตั้งแต่การระบุความเสี่ยง การวิเคราะห์และประเมินระดับความเสี่ยง การกำหนดมาตรการควบคุม และการติดตามทบทวนผลการดำเนินงาน

2.3.3 ประเภทของภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์สามารถจำแนกตามลักษณะการโจมตีและผลกระทบต่อระบบสารสนเทศได้ดังนี้

1. มัลแวร์ (Malware)

มัลแวร์เป็นโปรแกรมหรือซอฟต์แวร์ที่ถูกออกแบบมาเพื่อกระทำการที่เป็นอันตรายต่อระบบคอมพิวเตอร์และข้อมูล เช่น การขโมยข้อมูล การทำลายไฟล์ การติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต หรือการเปิดช่องให้ผู้โจมตีเข้าควบคุมอุปกรณ์

มัลแวร์มีหลายประเภท ได้แก่ Virus, Worm, Trojan, Spyware และ Ransomware ซึ่งแต่ละประเภทมีวิธีการทำงานและผลกระทบแตกต่างกัน

2. การหลอกลวงทางอิเล็กทรอนิกส์ (Phishing)

Phishing เป็นการใช้ข้อความ อีเมล เว็บไซต์ หรือช่องทางสื่อสารอิเล็กทรอนิกส์เพื่อหลอกให้ผู้ใช้งานเปิดเผยข้อมูลสำคัญ เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน ข้อมูลส่วนบุคคล หรือรหัสยืนยันตัวตน ผู้โจมตีมักปลอมแปลงเป็นบุคคลหรือหน่วยงานที่ผู้รับมีความคุ้นเคย เพื่อสร้างความน่าเชื่อถือและกระตุ้นให้ดำเนินการตามคำขอ

3. มัลแวร์เรียกค่าไถ่ (Ransomware)

Ransomware เป็นมัลแวร์ที่มุ่งเข้ารหัสไฟล์หรือข้อมูลของผู้ใช้งานหรือองค์กร เพื่อทำให้ไม่สามารถเข้าถึงข้อมูลได้ตามปกติ และอาจมีการเรียกร้องค่าไถ่เพื่อแลกกับการกู้คืนข้อมูล บางรูปแบบยังมีการขโมยข้อมูลออกไปและข่มขู่ว่าจะเผยแพร่ข้อมูลดังกล่าว

4. การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access)

เป็นการเข้าสู่ระบบหรือข้อมูลโดยไม่มีสิทธิ์หรือเกินขอบเขตที่ได้รับอนุญาต อาจเกิดจากการใช้รหัสผ่านที่ถูกขโมย การใช้บัญชีผู้ใช้งานร่วมกัน การกำหนดสิทธิ์ไม่เหมาะสม หรือการใช้ช่องโหว่ของระบบเพื่อเข้าถึงทรัพยากรสารสนเทศ

5. การโจมตีเพื่อทำให้ระบบไม่สามารถให้บริการได้ (Denial of Service: DoS/DDoS)

เป็นการโจมตีโดยส่งคำขอหรือปริมาณข้อมูลจำนวนมากไปยังระบบเป้าหมาย เพื่อใช้ทรัพยากรของระบบจนไม่สามารถให้บริการผู้ใช้งานตามปกติได้ กรณีที่ใช้แหล่งโจมตีหลายจุดพร้อมกันเรียกว่า Distributed Denial of Service (DDoS)

6. การโจมตีผ่านช่องโหว่ของซอฟต์แวร์ (Software Vulnerability Exploitation)

เป็นการใช้ประโยชน์จากข้อบกพร่องหรือช่องโหว่ของระบบปฏิบัติการ โปรแกรมประยุกต์ เว็บไซต์ หรือองค์ประกอบของระบบ เพื่อเข้าถึงข้อมูล เปลี่ยนแปลงการทำงาน หรือควบคุมระบบโดยไม่ได้รับอนุญาต

7. การหลอกลวงทางสังคม (Social Engineering)

เป็นวิธีการหลอกลวงที่ใช้จิตวิทยาและพฤติกรรมของมนุษย์เป็นช่องทางในการโจมตี เช่น การแอบอ้างเป็นผู้บริหาร เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ หรือบุคคลที่น่าเชื่อถือ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลหรือดำเนินการบางอย่างที่อาจก่อให้เกิดความเสียหาย

8. ความผิดพลาดจากผู้ใช้งาน (Human Error)

เป็นความผิดพลาดที่เกิดจากการปฏิบัติงานหรือการใช้งานระบบสารสนเทศ เช่น การส่งข้อมูลผิดผู้รับ การเปิดเผยรหัสผ่าน การลบข้อมูลโดยไม่ตั้งใจ การใช้สื่อบันทึกข้อมูลที่ไม่ปลอดภัย หรือการคลิกลิงก์ที่มีความเสี่ยง

ตารางที่ 2.2 ประเภทภัยคุกคามทางไซเบอร์และผลกระทบ

ประเภทภัยคุกคาม	ลักษณะการโจมตี	ผลกระทบที่อาจเกิดขึ้น
Malware	แทรกซึมโปรแกรมประสงค์ร้ายเข้าสู่ระบบ	ข้อมูลเสียหายและระบบทำงานผิดปกติ
Phishing	หลอกลวงให้เปิดเผยข้อมูลหรือรหัสผ่าน	บัญชีผู้ใช้งานถูกยึดครอง
Ransomware	เข้ารหัสไฟล์และเรียกค่าไถ่	ไม่สามารถเข้าถึงข้อมูลได้

ประเภทภัยคุกคาม	ลักษณะการโจมตี	ผลกระทบที่อาจเกิดขึ้น
Unauthorized Access	เข้าถึงระบบโดยไม่มีสิทธิ์	ข้อมูลรั่วไหลหรือถูกเปลี่ยนแปลง
DoS/DDoS	ส่งคำขอจำนวนมากเพื่อรบกวนระบบ	เว็บไซต์หรือบริการหยุดชะงัก
Software Vulnerability	ใช้ช่องโหว่ของโปรแกรมหรือระบบ	ระบบถูกโจมตีหรือควบคุม
Social Engineering	ใช้การหลอกลวงทางจิตวิทยา	บุคลากรเปิดเผยข้อมูลสำคัญ
Human Error	ความผิดพลาดจากการใช้งาน	ข้อมูลสูญหายหรือส่งต่อผิดพลาด

ที่มา: ประมวลจาก NIST และ ThaiCERT (NIST, n.d.; ThaiCERT, ม.ป.ป.)

2.3.4 ปัจจัยที่ก่อให้เกิดความเสี่ยงทางไซเบอร์

ปัจจัยที่ก่อให้เกิดความเสี่ยงทางไซเบอร์สามารถจำแนกได้เป็น 4 ด้าน ดังนี้

1. ปัจจัยด้านเทคโนโลยี

เกิดจากระบบคอมพิวเตอร์ ซอฟต์แวร์ เครือข่าย หรืออุปกรณ์ที่มีช่องโหว่ การตั้งค่าระบบไม่เหมาะสม การใช้ซอฟต์แวร์ที่ไม่ได้รับการปรับปรุง หรือการขาดระบบสำรองข้อมูล

2. ปัจจัยด้านบุคลากร

เกิดจากการขาดความรู้ความเข้าใจด้านความปลอดภัย การใช้รหัสผ่านที่คาดเดาได้ง่าย การเปิดเผยข้อมูลโดยไม่ระมัดระวัง หรือการหลงเชื่อข้อความและเว็บไซต์หลอกลวง

3. ปัจจัยด้านกระบวนการบริหารจัดการ

เกิดจากการขาดนโยบายหรือแนวปฏิบัติด้านความปลอดภัย การไม่กำหนดผู้รับผิดชอบที่ชัดเจน การไม่ทบทวนสิทธิ์ผู้ใช้งาน และการไม่มีแผนรับมือเมื่อเกิดเหตุการณ์ผิดปกติ

4. ปัจจัยด้านสภาพแวดล้อมภายนอก

เกิดจากภัยคุกคามที่มาจากเครือข่ายภายนอก การโจมตีจากบุคคลหรือกลุ่มผู้ไม่หวังดี เหตุขัดข้องของระบบสาธารณูปโภค และเหตุการณ์ที่ส่งผลกระทบต่อการให้บริการของระบบสารสนเทศ

2.3.5 แนวทางการประเมินความเสี่ยงทางไซเบอร์

การประเมินความเสี่ยงทางไซเบอร์เป็นกระบวนการพิจารณาโอกาสเกิดเหตุการณ์และระดับผลกระทบ เพื่อจัดลำดับความสำคัญของความเสี่ยงและกำหนดมาตรการควบคุมที่เหมาะสม โดยมีขั้นตอนดังนี้

1) ระบุทรัพย์สินสารสนเทศที่ต้องได้รับการคุ้มครอง
2) ระบุภัยคุกคามและช่องโหว่ที่อาจส่งผลกระทบต่อระบบ
3) วิเคราะห์โอกาสเกิดเหตุการณ์และระดับผลกระทบ
4) ประเมินระดับความเสี่ยงและจัดลำดับความสำคัญ
5) กำหนดมาตรการควบคุมและแนวทางจัดการความเสี่ยง
6) ติดตามและทบทวนผลการดำเนินงานอย่างต่อเนื่อง

การประเมินความเสี่ยงสามารถใช้เกณฑ์ระดับความเสี่ยง เช่น ต่ำ ปานกลาง สูง และสูงมาก โดยพิจารณาจากโอกาสเกิดเหตุและผลกระทบ ทั้งนี้ ต้องกำหนดเกณฑ์คะแนนและความหมายของแต่ละระดับให้ชัดเจนก่อนนำไปใช้จริง (NIST, 2012)

ตารางที่ 2.3 ตัวอย่างการจำแนกความเสี่ยงทางไซเบอร์ของระบบสารสนเทศ

ระบบ/ทรัพยากร	ความเสี่ยงที่ควรประเมิน	ผลกระทบที่อาจเกิดขึ้น
ICCS-PORTAL	การเข้าถึงหรือแก้ไขข้อมูลโดยไม่มีสิทธิ์	ข้อมูลการบริหารจัดการคลาดเคลื่อน
E-Office	การเปิดเผยเอกสารหรือการเข้าถึงเอกสารโดยไม่ได้รับอนุญาต	ข้อมูลภายในองค์กรรั่วไหล
E-HR.ICCS	การเข้าถึงข้อมูลบุคลากรโดยไม่มีสิทธิ์	ข้อมูลส่วนบุคคลถูกเปิดเผย
SMART ERPG	การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต	ข้อมูลการดำเนินงานไม่ถูกต้อง
เว็บไซต์วิทยาลัย	การโจมตีเว็บไซต์หรือแก้ไขเนื้อหา	การเผยแพร่ข้อมูลผิดพลาดและบริการหยุดชะงัก
Server	ช่องโหว่ของระบบหรือการเข้าถึงโดยไม่ได้รับอนุญาต	ระบบงานและข้อมูลได้รับผลกระทบ

2.4 แนวทางการป้องกันและรักษาความปลอดภัยระบบสารสนเทศ

การป้องกันและรักษาความปลอดภัยระบบสารสนเทศเป็นกระบวนการกำหนดมาตรการเพื่อคุ้มครองระบบคอมพิวเตอร์ เครือข่าย โปรแกรมประยุกต์ และข้อมูลจากภัยคุกคามที่อาจส่งผลกระทบต่อการดำเนินงานขององค์กร โดยต้องครอบคลุมมาตรการด้านเทคนิค การบริหารจัดการ และการพัฒนาบุคลากร เพื่อให้ระบบสารสนเทศมีความปลอดภัยและสามารถให้บริการได้อย่างต่อเนื่อง

แนวทางการป้องกันและรักษาความปลอดภัยระบบสารสนเทศสามารถจำแนกเป็น 10 ด้าน ดังนี้

2.4.1 การรักษาความปลอดภัยระบบเครือข่าย (Network Security)

การรักษาความปลอดภัยระบบเครือข่ายเป็นการกำหนดมาตรการควบคุมและป้องกันการรับส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีจากภายนอก และการใช้ทรัพยากรเครือข่ายในลักษณะที่อาจก่อให้เกิดความเสียหาย

มาตรการสำคัญประกอบด้วย

1) ติดตั้งและกำหนดค่า Firewall เพื่อควบคุมการรับส่งข้อมูลระหว่างเครือข่าย
2) กำหนดกฎการอนุญาตและปฏิเสธการเชื่อมต่อตามความจำเป็น
3) จำกัดการเปิดใช้งานพอร์ตและบริการที่ไม่จำเป็น
4) แบ่งแยกเครือข่ายตามลักษณะการใช้งานและระดับความสำคัญของระบบ
5) ตรวจสอบการเชื่อมต่อและบันทึกเหตุการณ์การใช้งานเครือข่าย
6) ปรับปรุงอุปกรณ์เครือข่ายและซอฟต์แวร์ให้เป็นปัจจุบัน
7) กำหนดมาตรการรักษาความปลอดภัยสำหรับการเชื่อมต่อเครือข่ายไร้สาย

Firewall เป็นเครื่องมือสำคัญในการควบคุมการรับส่งข้อมูลตามกฎที่กำหนด อย่างไรก็ตาม การใช้ Firewall ควรดำเนินการร่วมกับมาตรการอื่น เช่น การควบคุมสิทธิ์ผู้ใช้งาน การตรวจสอบระบบ และการปรับปรุงช่องโหว่ เพื่อให้การรักษาความปลอดภัยมีความครอบคลุมมากขึ้น

2.4.2 การรักษาความปลอดภัยเว็บไซต์และเว็บแอปพลิเคชัน (Website and Web Application Security)

เว็บไซต์และเว็บแอปพลิเคชันเป็นช่องทางสำคัญในการให้บริการและเผยแพร่ข้อมูลขององค์กร การรักษาความปลอดภัยจึงต้องครอบคลุมทั้งระบบเว็บไซต์ โปรแกรมประยุกต์ ฐานข้อมูล และการเชื่อมต่อกับระบบอื่น

มาตรการสำคัญประกอบด้วย

1) ใช้ใบรับรองดิจิทัลและโปรโตคอล TLS เพื่อเข้ารหัสการรับส่งข้อมูลผ่าน HTTPS
2) ปรับปรุงระบบจัดการเว็บไซต์และองค์ประกอบซอฟต์แวร์ให้เป็นปัจจุบัน
3) ตรวจสอบช่องโหว่ของเว็บไซต์และเว็บแอปพลิเคชัน
4) กำหนดสิทธิ์ผู้ดูแลเว็บไซต์ตามหน้าที่รับผิดชอบ
5) ป้องกันการเข้าถึงหน้าจัดการระบบโดยไม่ได้รับอนุญาต
6) สำรองข้อมูลเว็บไซต์และฐานข้อมูลอย่างสม่ำเสมอ
7) ตรวจสอบไฟล์และเนื้อหาที่เผยแพร่บนเว็บไซต์
8) จัดเก็บบันทึกการเข้าใช้งานและการเปลี่ยนแปลงข้อมูล

การพัฒนาเว็บไซต์ควรคำนึงถึงความปลอดภัยตั้งแต่ขั้นตอนการออกแบบ พัฒนา ทดสอบ และนำระบบไปใช้งาน โดยสามารถอ้างอิงแนวทาง Website Security Guideline ของ ThaiCERT เพื่อประกอบการกำหนดมาตรการรักษาความปลอดภัยเว็บไซต์ของหน่วยงาน

2.4.3 การควบคุมสิทธิ์และการพิสูจน์ตัวตน (Access Control and Authentication)

การควบคุมสิทธิ์การเข้าถึงเป็นกระบวนการกำหนดขอบเขตการใช้งานระบบและข้อมูลให้เหมาะสมกับบทบาทหน้าที่ของบุคลากร เพื่อป้องกันการเข้าถึงหรือใช้ข้อมูลเกินกว่าสิทธิ์ที่ได้รับอนุญาต แนวทางดำเนินงานประกอบด้วย

1) กำหนดบัญชีผู้ใช้งานเป็นรายบุคคล ไม่ใช้บัญชีร่วมกันโดยไม่จำเป็น
2) กำหนดสิทธิ์การเข้าถึงตามบทบาทหน้าที่ (Role-Based Access Control)
3) ใช้หลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege)
4) กำหนดหลักเกณฑ์การตั้งรหัสผ่านที่มีความปลอดภัย
5) ใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับระบบที่รองรับและมีความเสี่ยงเหมาะสม
6) ทบทวนสิทธิ์การใช้งานเมื่อมีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่
7) ยกเลิกบัญชีผู้ใช้งานเมื่อหมดความจำเป็น
8) ตรวจสอบประวัติการเข้าสู่ระบบและการใช้งานที่ผิดปกติ

การควบคุมสิทธิ์ที่เหมาะสมช่วยลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และสนับสนุนการตรวจสอบความรับผิดชอบในการใช้ระบบสารสนเทศ

2.4.4 การเข้ารหัสข้อมูล (Data Encryption)

การเข้ารหัสข้อมูลเป็นกระบวนการแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้โดยง่าย หากไม่มีรหัสหรือกุญแจที่ถูกต้องสำหรับถอดรหัส มีวัตถุประสงค์เพื่อรักษาความลับของข้อมูลและลดความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

การเข้ารหัสข้อมูลสามารถแบ่งตามลักษณะการใช้งานได้ 2 ประเภท ได้แก่

1. การเข้ารหัสข้อมูลขณะรับส่ง (Data in Transit)

เป็นการเข้ารหัสข้อมูลระหว่างการส่งผ่านเครือข่าย เช่น การใช้ HTTPS ร่วมกับ TLS เพื่อป้องกันการดักอ่านและการเปลี่ยนแปลงข้อมูลระหว่างการสื่อสาร

2. การเข้ารหัสข้อมูลขณะจัดเก็บ (Data at Rest)

เป็นการเข้ารหัสข้อมูลที่จัดเก็บอยู่ในอุปกรณ์หรือระบบฐานข้อมูล เช่น Server คอมพิวเตอร์ และสื่อบันทึกข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลเมื่ออุปกรณ์หรือสื่อจัดเก็บตกอยู่ในความครอบครองของบุคคลที่ไม่มีสิทธิ์

การเข้ารหัสข้อมูลต้องมีการบริหารจัดการกุญแจเข้ารหัสอย่างเหมาะสม รวมถึงการกำหนดผู้รับผิดชอบ การจัดเก็บ และการป้องกันการเปิดเผยกุญแจดังกล่าว

2.4.5 การปรับปรุงระบบและจัดการช่องโหว่ (Patch and Vulnerability Management)

การปรับปรุงระบบเป็นกระบวนการดูแลซอฟต์แวร์ ระบบปฏิบัติการ โปรแกรมประยุกต์ และอุปกรณ์ที่เกี่ยวข้องให้มีความทันสมัยและได้รับการแก้ไขข้อบกพร่องด้านความปลอดภัยอย่างเหมาะสม

แนวทางดำเนินงานประกอบด้วย

1) สำรวจระบบปฏิบัติการและซอฟต์แวร์ที่ใช้งานในองค์กร
2) ตรวจสอบสถานะการสนับสนุนและการอัปเดตของซอฟต์แวร์
3) ติดตามประกาศแจ้งเตือนช่องโหว่ด้านความปลอดภัย
4) จัดลำดับความสำคัญของช่องโหว่ตามระดับความเสี่ยง
5) ดำเนินการติดตั้งโปรแกรมปรับปรุงหรือแก้ไขช่องโหว่
6) ทดสอบการทำงานของระบบหลังการปรับปรุง
7) บันทึกประวัติการปรับปรุงและผลการตรวจสอบ

การจัดการช่องโหว่อย่างต่อเนื่องช่วยลดโอกาสที่ผู้ไม่หวังดีจะใช้ประโยชน์จากข้อบกพร่องของระบบในการเข้าถึงหรือควบคุมข้อมูลและระบบสารสนเทศ

2.4.6 การสำรองและกู้คืนข้อมูล (Data Backup and Recovery)

การสำรองข้อมูลเป็นกระบวนการจัดทำสำเนาข้อมูลจากระบบหลักเพื่อใช้ในการกู้คืนเมื่อเกิดเหตุการณ์ที่ทำให้ข้อมูลสูญหาย เสียหาย หรือไม่สามารถเข้าถึงได้ตามปกติ

แนวทางการสำรองและกู้คืนข้อมูลประกอบด้วย

1) จำแนกข้อมูลตามความสำคัญและความจำเป็นในการใช้งาน
2) กำหนดรอบระยะเวลาการสำรองข้อมูล
3) จัดเก็บข้อมูลสำรองแยกจากระบบหลัก
4) จำกัดสิทธิ์การเข้าถึงข้อมูลสำรอง
5) ป้องกันข้อมูลสำรองจากการถูกแก้ไขหรือลบโดยไม่ได้รับอนุญาต
6) ตรวจสอบความสมบูรณ์ของข้อมูลสำรอง
7) ทดสอบการกู้คืนข้อมูลและระบบตามระยะเวลาที่กำหนด
8) จัดทำขั้นตอนการฟื้นฟูระบบเมื่อเกิดเหตุการณ์ผิดปกติ

การสำรองข้อมูลควรพิจารณาระยะเวลาที่ยอมรับได้ในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาของข้อมูลที่ยอมรับได้ในการสูญหาย (Recovery Point Objective: RPO) เพื่อกำหนดระดับการสำรองและการฟื้นฟูให้เหมาะสมกับความสำคัญของระบบ

2.4.7 การตรวจสอบและเฝ้าระวังระบบ (Monitoring and Logging)

การตรวจสอบและเฝ้าระวังระบบเป็นกระบวนการติดตามการทำงานของระบบสารสนเทศและตรวจจับเหตุการณ์ผิดปกติ เพื่อให้สามารถระบุปัญหาและดำเนินการแก้ไขได้อย่างเหมาะสม มาตรการสำคัญประกอบด้วย

1) จัดเก็บบันทึกเหตุการณ์การใช้งานระบบ (System Log)
2) ตรวจสอบการเข้าสู่ระบบและการใช้งานบัญชีผู้ดูแลระบบ
3) ติดตามการเปลี่ยนแปลงของข้อมูลและการตั้งค่าระบบ
4) ตรวจสอบการเชื่อมต่อเครือข่ายที่ผิดปกติ
5) กำหนดแนวทางแจ้งเตือนเมื่อพบเหตุการณ์ที่มีความเสี่ยง
6) จำกัดสิทธิ์การเข้าถึงและป้องกันการแก้ไข Log โดยไม่ได้รับอนุญาต
7) เก็บรักษาหลักฐานตามระยะเวลาที่เหมาะสมกับข้อกำหนดขององค์กร

ข้อมูลบันทึกเหตุการณ์เป็นหลักฐานสำคัญสำหรับการตรวจสอบย้อนหลัง การวิเคราะห์สาเหตุ และการดำเนินการตอบสนองเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

2.4.8 การรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response)

การรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยเป็นกระบวนการจัดการเมื่อเกิดเหตุการณ์ที่อาจกระทบต่อข้อมูล ระบบเครือข่าย หรือการดำเนินงานขององค์กร โดยมีวัตถุประสงค์เพื่อจำกัดความเสียหาย ลดผลกระทบ และฟื้นฟูระบบให้กลับมาใช้งานได้ตามปกติ

กระบวนการรับมือเหตุการณ์ประกอบด้วย

1) **การเตรียมความพร้อม:** กำหนดผู้รับผิดชอบ ช่องทางการแจ้งเหตุ และขั้นตอนการดำเนินงาน
2) **การตรวจพบและวิเคราะห์:** ตรวจสอบเหตุการณ์และประเมินระดับผลกระทบ
3) **การควบคุมเหตุการณ์:** จำกัดการแพร่กระจายหรือการเข้าถึงระบบที่ได้รับผลกระทบ
4) **การกำจัดสาเหตุ:** แก้ไขช่องโหว่หรือองค์ประกอบที่ก่อให้เกิดเหตุการณ์
5) **การฟื้นฟูระบบ:** กู้คืนข้อมูลและระบบให้สามารถกลับมาใช้งานได้
6) **การทบทวนหลังเกิดเหตุ:** วิเคราะห์สาเหตุและกำหนดมาตรการป้องกันไม่ให้เกิดเหตุซ้ำ

การดำเนินงานต้องมีการบันทึกรายละเอียดเหตุการณ์ วันเวลา ผู้เกี่ยวข้อง ผลกระทบ และวิธีการแก้ไข เพื่อใช้เป็นข้อมูลในการตรวจสอบและพัฒนามาตรการรักษาความปลอดภัย

2.4.9 การสร้างความตระหนักรู้แก่บุคลากร (Security Awareness)

บุคลากรเป็นส่วนสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากการใช้งานระบบสารสนเทศในชีวิตประจำวันอาจก่อให้เกิดความเสี่ยงได้ หากขาดความรู้และความระมัดระวัง การสร้างความตระหนักรู้ควรครอบคลุมประเด็นต่อไปนี้

1) การจำแนกอีเมลและข้อความหลอกลวง
2) การตรวจสอบความน่าเชื่อถือของเว็บไซต์และลิงก์ก่อนเข้าใช้งาน
3) การตั้งและรักษาความปลอดภัยของรหัสผ่าน
4) การไม่เปิดเผยรหัสผ่านหรือรหัส OTP แก่บุคคลอื่น
5) การป้องกันข้อมูลส่วนบุคคลและข้อมูลภายในองค์กร

6) การใช้งานอุปกรณ์และเครือข่ายอย่างปลอดภัย
7) การแจ้งเหตุเมื่อพบความผิดปกติของระบบ
8) การปฏิบัติตามนโยบายและแนวทางรักษาความปลอดภัยขององค์กร

การส่งเสริมความรู้ควรดำเนินการผ่านการอบรม การประชาสัมพันธ์ การจัดทำคู่มือ และการแลกเปลี่ยนเรียนรู้ เพื่อให้บุคลากรสามารถนำความรู้ไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างเหมาะสม

2.4.10 การบริหารจัดการความปลอดภัยตามวงจรการพัฒนาอย่างต่อเนื่อง

การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นกระบวนการที่ต้องดำเนินการอย่างต่อเนื่อง เนื่องจากเทคโนโลยี รูปแบบการใช้งาน และภัยคุกคามมีการเปลี่ยนแปลงอยู่เสมอ องค์กรจึงควรนำแนวคิดวงจรคุณภาพ PDCA (Plan–Do–Check–Act) มาใช้เป็นแนวทางในการพัฒนาระบบ ดังนี้

ขั้นตอน	ความหมาย	แนวทางดำเนินงาน
Plan	การวางแผน	สำรวจระบบ วิเคราะห์ความเสี่ยง และกำหนดมาตรการ
Do	การดำเนินงาน	ติดตั้ง ปรับปรุง และดำเนินมาตรการรักษาความปลอดภัย
Check	การตรวจสอบ	ตรวจสอบระบบ ประเมินผล และรวบรวมหลักฐาน
Act	การปรับปรุง	แก้ไขข้อบกพร่องและพัฒนาแนวทางให้เหมาะสม

ที่มา: ประยุกต์ใช้แนวคิดการปรับปรุงอย่างต่อเนื่องร่วมกับหลักการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศตาม ISO/IEC 27001:2022

ตารางที่ 2.4 สรุปแนวทางการป้องกันและรักษาความปลอดภัยระบบสารสนเทศ

ด้านการดำเนินงาน	มาตรการสำคัญ	วัตถุประสงค์
Network Security	Firewall และการควบคุมเครือข่าย	ป้องกันการเชื่อมต่อที่ไม่ได้รับอนุญาต
Website Security	HTTPS/TLS และการปรับปรุงเว็บไซต์	ป้องกันความเสี่ยงในการใช้งานเว็บไซต์
Access Control	บัญชีผู้ใช้และการกำหนดสิทธิ์	ควบคุมการเข้าถึงข้อมูล
Data Encryption	การเข้ารหัสข้อมูล	รักษาความลับของข้อมูล
Patch Management	การปรับปรุงซอฟต์แวร์	ลดช่องโหว่ของระบบ
Backup and Recovery	การสำรองและกู้คืนข้อมูล	รักษาความพร้อมใช้งาน
Monitoring and Logging	การตรวจสอบและจัดเก็บ Log	ตรวจจับและตรวจสอบเหตุการณ์
Incident Response	การรับมือเหตุการณ์	ลดผลกระทบและฟื้นฟูระบบ
Security Awareness	การพัฒนาความรู้บุคลากร	ลดความเสี่ยงจากพฤติกรรมผู้ใช้งาน
Continuous Improvement	การพัฒนาอย่างต่อเนื่อง	ยกระดับมาตรการรักษาความปลอดภัย

แนวทางดังกล่าวสามารถนำไปใช้เป็นกรอบในการดูแลระบบสารสนเทศของวิทยาลัยชุมชนสตูล โดยกำหนดมาตรการตามระดับความสำคัญของระบบ ประเภทข้อมูล และความเสี่ยงที่เกี่ยวข้อง ทั้งนี้ การเลือกใช้มาตรการแต่ละประเภทต้องสอดคล้องกับทรัพยากรและความพร้อมของหน่วยงาน

2.5 กฎหมายและมาตรฐานที่เกี่ยวข้อง

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรจำเป็นต้องคำนึงถึงกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง เพื่อให้การบริหารจัดการระบบสารสนเทศและข้อมูลเป็นไปตามหลักเกณฑ์ด้านความปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล และการใช้เทคโนโลยีสารสนเทศอย่างมีความรับผิดชอบ

สำหรับวิทยาลัยชุมชนสตูล กฎหมายและมาตรฐานที่เกี่ยวข้องกับการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์สามารถจำแนกได้ดังนี้

2.5.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นกฎหมายที่กำหนดหลักเกณฑ์และมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยมีวัตถุประสงค์เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

สาระสำคัญของกฎหมายประกอบด้วยการกำหนดหน่วยงานและกลไกการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดลักษณะภัยคุกคามทางไซเบอร์ การกำหนดมาตรการป้องกันและรับมือ รวมถึงการกำหนดหน้าที่ของหน่วยงานที่เกี่ยวข้องในการดำเนินการตามหลักเกณฑ์และกรอบมาตรฐานที่กำหนด

กฎหมายดังกล่าวมีความเกี่ยวข้องกับการดำเนินงานของหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยเฉพาะการจัดทำแนวทางป้องกันและรับมือภัยคุกคามทางไซเบอร์ ทั้งนี้ การพิจารณาหน้าที่ตามกฎหมายต้องคำนึงถึงสถานะและประเภทของหน่วยงานตามบทบัญญัติที่เกี่ยวข้อง ไม่ใช่ทุกหน่วยงานจะมีหน้าที่และข้อกำหนดในระดับเดียวกัน (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

ความเชื่อมโยงกับวิทยาลัยชุมชนสตูล

การดำเนินงานของวิทยาลัยสามารถนำหลักการตามกฎหมายมาใช้เป็นกรอบในการพัฒนามาตรการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยง การเตรียมความพร้อมรับมือเหตุการณ์ และการจัดทำแนวปฏิบัติในการดูแลระบบ โดยต้องพิจารณาข้อกำหนดที่ใช้บังคับกับสถานะของวิทยาลัยตามกฎหมายและประกาศที่เกี่ยวข้อง

2.5.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล และกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

สาระสำคัญของกฎหมายประกอบด้วย

1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องมีฐานทางกฎหมายรองรับ
2) การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์และขอบเขตที่กฎหมายกำหนด
3) ต้องมีการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

4) ต้องมีการควบคุมการเข้าถึงและป้องกันการใช้หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
5) ต้องมีแนวทางดำเนินการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลตามหลักเกณฑ์และระยะเวลาที่กฎหมายกำหนด
6) ต้องคำนึงถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายบัญญัติ

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลมีความสำคัญต่อการดำเนินงานขององค์กรที่มีการจัดเก็บและใช้ข้อมูลบุคลากร นักศึกษา และบุคคลที่เกี่ยวข้อง โดยต้องป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

ความเชื่อมโยงกับวิทยาลัยชุมชนสตูล

วิทยาลัยมีการใช้ระบบสารสนเทศเพื่อสนับสนุนการบริหารงานบุคคล การบริหารจัดการเอกสาร และการดำเนินงานทางการศึกษา ซึ่งอาจมีการประมวลผลข้อมูลส่วนบุคคลของบุคลากร นักศึกษา และผู้เกี่ยวข้อง ดังนั้น การดูแลระบบ E-HR.ICCS, E-Office และระบบอื่นที่มีข้อมูลส่วนบุคคลจึงต้องคำนึงถึงการกำหนดสิทธิ์การเข้าถึง การจำกัดการใช้ข้อมูลตามวัตถุประสงค์ การรักษาความปลอดภัยของข้อมูล และการจัดการเหตุละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

2.5.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม เป็นกฎหมายที่กำหนดความผิดและบทลงโทษเกี่ยวกับการกระทำต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ โดยครอบคลุมการกระทำที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบและข้อมูล

สาระสำคัญของกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่

1) การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ
2) การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ
3) การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ
4) การทำให้ข้อมูลคอมพิวเตอร์เสียหาย ถูกทำลาย หรือเปลี่ยนแปลงโดยมิชอบ
5) การรบกวนหรือทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ
6) การเผยแพร่หรือนำเข้าข้อมูลคอมพิวเตอร์ในลักษณะที่กฎหมายกำหนดให้เป็นความผิด

กฎหมายดังกล่าวมีความเกี่ยวข้องกับการกำหนดแนวทางการใช้งานระบบสารสนเทศขององค์กร การควบคุมสิทธิ์การเข้าถึง การจัดเก็บบันทึกการใช้งาน และการป้องกันการกระทำที่อาจส่งผลกระทบต่อระบบคอมพิวเตอร์และข้อมูลของหน่วยงาน

ความเชื่อมโยงกับวิทยาลัยชุมชนสตูล

การใช้งานระบบสารสนเทศของวิทยาลัยจำเป็นต้องกำหนดแนวปฏิบัติสำหรับผู้ใช้งานและผู้ดูแลระบบ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่มีสิทธิ์ การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต และการใช้ระบบคอมพิวเตอร์ในลักษณะที่ก่อให้เกิดความเสียหาย รวมทั้งควรมีการจัดเก็บหลักฐานการใช้งานระบบตามความเหมาะสมและข้อกำหนดที่เกี่ยวข้อง

2.5.4 มาตรฐาน ISO/IEC 27001:2022

ISO/IEC 27001:2022 เป็นมาตรฐานสากลด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ซึ่งกำหนดข้อกำหนดสำหรับการจัดตั้ง การดำเนินงาน การรักษา และการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยใช้กระบวนการบริหารจัดการความเสี่ยงเป็นพื้นฐาน (International Organization for Standardization, 2022)

มาตรฐานดังกล่าวให้ความสำคัญกับองค์ประกอบสำคัญ ได้แก่

1. บริบทขององค์กร (Context of the Organization)

การทำความเข้าใจบริบทขององค์กร ผู้มีส่วนได้ส่วนเสีย และขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

2. ภาวะผู้นำ (Leadership)

การกำหนดนโยบาย บทบาทหน้าที่ และความรับผิดชอบของผู้บริหารและบุคลากรที่เกี่ยวข้อง

3. การวางแผน (Planning)

การระบุและประเมินความเสี่ยง ตลอดจนการกำหนดเป้าหมายด้านความมั่นคงปลอดภัยสารสนเทศ

4. การสนับสนุน (Support)

การจัดสรรทรัพยากร การพัฒนาความรู้ความสามารถ และการสื่อสารข้อมูลที่เกี่ยวข้องกับระบบบริหารจัดการ

5. การดำเนินงาน (Operation)

การนำแผนและมาตรการควบคุมความเสี่ยงไปปฏิบัติจริง

6. การประเมินผลการดำเนินงาน (Performance Evaluation)

การติดตาม ตรวจสอบ วิเคราะห์ และประเมินประสิทธิผลของระบบบริหารจัดการ

7. การปรับปรุง (Improvement)

การแก้ไขข้อบกพร่องและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

ความเชื่อมโยงกับวิทยาลัยชุมชนสตูล

วิทยาลัยสามารถใช้หลักการของ ISO/IEC 27001:2022 เป็นกรอบอ้างอิงในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยเริ่มจากการสำรวจระบบสารสนเทศ การประเมินความเสี่ยง การกำหนดมาตรการควบคุม การตรวจสอบผลการดำเนินงาน และการปรับปรุงระบบอย่างต่อเนื่อง ทั้งนี้ การนำมาตรฐานมาใช้อ้างอิงไม่ได้หมายความว่าวิทยาลัยได้รับการรับรองมาตรฐาน ISO/IEC 27001 แล้ว

2.5.5 NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework 2.0 เป็นกรอบแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ จัดทำโดย National Institute of Standards and Technology และเผยแพร่เมื่อวันที่ 26 กุมภาพันธ์ ค.ศ. 2024 โดยออกแบบให้สามารถประยุกต์ใช้กับองค์กรทุกประเภท ทุกขนาด และทุกระดับความพร้อมในการบริหารจัดการความเสี่ยงทางไซเบอร์ (Pascoe et al., 2024)

กรอบดังกล่าวประกอบด้วย 6 หน้าที่หลัก ได้แก่

หน้าที่	ความหมาย	การประยุกต์ใช้กับองค์กร
Govern	การกำกับดูแล	กำหนดนโยบายและผู้รับผิดชอบด้าน Cybersecurity
Identify	การระบุความเสี่ยง	สำรวจระบบและประเมินความเสี่ยง
Protect	การป้องกัน	ใช้ Firewall ควบคุมสิทธิ์และเข้ารหัสข้อมูล
Detect	การตรวจจับ	ตรวจสอบ Log และเฝ้าระวังระบบ
Respond	การตอบสนอง	จัดการและควบคุมเหตุการณ์ผิดปกติ
Recover	การฟื้นฟู	กู้คืนข้อมูลและระบบให้กลับมาใช้งานได้

กรอบ NIST CSF 2.0 สามารถนำมาใช้ประกอบการวางแผนและกำหนดแนวทางดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูล โดยเชื่อมโยงการดำเนินงานด้านเทคนิคกับการบริหารจัดการและการพัฒนาบุคลากร เพื่อให้การป้องกันและรับมือภัยคุกคามครอบคลุมทุกกระบวนการ

2.5.6 แนวทางและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

นอกจากกฎหมายและมาตรฐานสากลแล้ว ประเทศไทยยังมีหน่วยงานที่รับผิดชอบในการกำหนดแนวทางส่งเสริม และเผยแพร่ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT)

หน่วยงานดังกล่าวได้เผยแพร่เอกสารและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น

1) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
2) แนวปฏิบัติพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่และการรั่วไหลของข้อมูล
3) แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline)
4) แนวทางการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
5) แนวทางการแจ้งและรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์
6) แนวทางด้านความมั่นคงปลอดภัยสำหรับระบบคลาวด์

เอกสารเหล่านี้เป็นแหล่งอ้างอิงสำหรับการกำหนดมาตรการด้านความปลอดภัย การป้องกันภัยคุกคาม และการพัฒนาระบบสารสนเทศให้มีความเหมาะสมกับบริบทของหน่วยงาน

ตารางที่ 2.5 สรุปกฎหมายและมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

กฎหมาย/มาตรฐาน	สาระสำคัญ	ความเชื่อมโยงกับการดำเนินงาน
พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์	การกำหนดแนวทางดูแลและรับมือภัยคุกคาม

กฎหมาย/มาตรฐาน	สาระสำคัญ	ความเชื่อมโยงกับการดำเนินงาน
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	การคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความปลอดภัย	การดูแลข้อมูลบุคลากรและนักศึกษา
พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม	การกำหนดความผิดเกี่ยวกับระบบและข้อมูลคอมพิวเตอร์	การควบคุมการเข้าถึงและการใช้งานระบบ
ISO/IEC 27001:2022	ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	การประเมินความเสี่ยงและการปรับปรุงระบบ
NIST CSF 2.0	กรอบการบริหารจัดการความเสี่ยงทางไซเบอร์ 6 หน้าที่	การกำหนดกระบวนการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟู
แนวทางของ ThaiCERT	แนวปฏิบัติด้านเว็บไซต์ มัลแวร์ และการจัดการเหตุการณ์	การพัฒนามาตรการป้องกันและรับมือภัยคุกคาม

ที่มา: ประมวลจากกฎหมายไทย มาตรฐาน ISO/IEC 27001:2022, NIST CSF 2.0 และเอกสารเผยแพร่ของ ThaiCERT

สรุปท้ายบท

ความมั่นคงปลอดภัยทางไซเบอร์เป็นองค์ประกอบสำคัญของการบริหารจัดการองค์กรดิจิทัล โดยมีพื้นฐานจากการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลตามหลัก CIA Triad การดำเนินงานจำเป็นต้องคำนึงถึงภัยคุกคามและความเสี่ยงที่อาจเกิดขึ้นจากเทคโนโลยี บุคลากร กระบวนการบริหารจัดการ และสภาพแวดล้อมภายนอกองค์กร ตลอดจนกำหนดมาตรการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูระบบอย่างเป็นระบบ

สำหรับวิทยาลัยชุมชนสตูล แนวคิดและหลักการดังกล่าวเป็นพื้นฐานในการพัฒนาการดูแลระบบ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server โดยสามารถประยุกต์ใช้มาตรการทางเทคนิคควบคู่กับการบริหารจัดการความเสี่ยง การปฏิบัติตามกฎหมายที่เกี่ยวข้อง และการพัฒนาความรู้ของบุคลากร เพื่อสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ให้มีความต่อเนื่องและสอดคล้องกับภารกิจขององค์กร

บทที่ 3 กระบวนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นกระบวนการบริหารจัดการระบบสารสนเทศอย่างเป็นระบบ โดยครอบคลุมการสำรวจและวิเคราะห์ทรัพยากรสารสนเทศ การประเมินความเสี่ยง การกำหนดมาตรการป้องกัน การตรวจสอบและบำรุงรักษาระบบ ตลอดจนการจัดการความรู้และการสร้างความตระหนักรู้แก่บุคลากร เพื่อให้ระบบสารสนเทศสามารถดำเนินงานได้อย่างปลอดภัย มีความน่าเชื่อถือ และรองรับภารกิจขององค์กรได้อย่างต่อเนื่อง

การดำเนินงานดังกล่าวสามารถประยุกต์ใช้กรอบ NIST Cybersecurity Framework 2.0 ซึ่งประกอบด้วย 6 หน้าที่หลัก ได้แก่ Govern (การกำกับดูแล) Identify (การระบุความเสี่ยง) Protect (การป้องกัน) Detect (การตรวจจับ) Respond (การตอบสนอง) และ Recover (การฟื้นฟู) เพื่อใช้เป็นแนวทางในการวางแผน ดำเนินงาน ติดตาม และพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ให้ครอบคลุมทั้งด้านเทคโนโลยี กระบวนการ และบุคลากร (Pascoe, Quinn, & Scarfone, 2024)

สำหรับวิทยาลัยชุมชนสตูล กระบวนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์มีความเชื่อมโยงกับการดูแลระบบสารสนเทศที่ใช้สนับสนุนการบริหารจัดการและการให้บริการ ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server โดยมีข้อมูลการดำเนินงานในปีงบประมาณ พ.ศ. 2568 เกี่ยวกับการใช้ Firewall การใช้ใบรับรอง SSL การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ รวมถึงการทบทวนองค์ความรู้และแนวปฏิบัติด้านความปลอดภัยในปีงบประมาณ พ.ศ. 2569

เนื้อหาในบทนี้จึงนำเสนอหลักการและขั้นตอนการดำเนินงานที่เกี่ยวข้อง เพื่อใช้เป็นกรอบในการอธิบายแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูล โดยแยกหลักการดำเนินงานออกจากผลการปฏิบัติที่มีหลักฐานยืนยันอย่างชัดเจน

3.1 การสำรวจและวิเคราะห์ระบบสารสนเทศขององค์กร

การสำรวจและวิเคราะห์ระบบสารสนเทศเป็นขั้นตอนพื้นฐานของการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากองค์กรจำเป็นต้องทราบว่ามีทรัพยากรสารสนเทศประเภทใดอยู่ภายใต้ความรับผิดชอบ มีการใช้งานอย่างไร มีข้อมูลประเภทใดถูกจัดเก็บหรือประมวลผล และมีความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานในลักษณะใด การสำรวจระบบอย่างเป็นระบบช่วยให้สามารถกำหนดขอบเขตการรักษาความปลอดภัย จัดลำดับความสำคัญของทรัพยากร และวางแผนมาตรการควบคุมได้อย่างเหมาะสม

ตามแนวทาง NIST Cybersecurity Framework 2.0 การระบุทรัพย์สินและทำความเข้าใจบริบทขององค์กรเป็นส่วนสำคัญของหน้าที่ Identify ซึ่งมุ่งให้หน่วยงานสามารถระบุทรัพยากรที่ต้องได้รับการคุ้มครอง รวมถึงระบบงาน ข้อมูล ผู้ใช้งาน และความสัมพันธ์ระหว่างองค์ประกอบต่าง ๆ เพื่อใช้เป็นข้อมูลประกอบการบริหารจัดการความเสี่ยง (Pascoe et al., 2024)

3.1.1 วัตถุประสงค์ของการสำรวจระบบสารสนเทศ

การสำรวจและวิเคราะห์ระบบสารสนเทศมีวัตถุประสงค์สำคัญ ดังนี้

1) เพื่อรวบรวมข้อมูลเกี่ยวกับระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรมประยุกต์ และ Server ที่ใช้ในการดำเนินงานขององค์กร
2) เพื่อจำแนกประเภทและระดับความสำคัญของข้อมูลที่จัดเก็บและประมวลผลในระบบสารสนเทศ

3) เพื่อระบุผู้รับผิดชอบ ผู้ดูแลระบบ และกลุ่มบุคลากรที่มีสิทธิ์ใช้งานระบบ
4) เพื่อศึกษาความสัมพันธ์และการเชื่อมโยงระหว่างระบบสารสนเทศต่าง ๆ
5) เพื่อระบุจุดที่อาจก่อให้เกิดความเสี่ยงหรือส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบ
6) เพื่อใช้ข้อมูลจากการสำรวจเป็นพื้นฐานในการประเมินความเสี่ยงและกำหนดมาตรการรักษาความปลอดภัย

3.1.2 ขอบเขตการสำรวจระบบสารสนเทศ

การสำรวจระบบสารสนเทศควรครอบคลุมองค์ประกอบสำคัญ 5 ด้าน ดังนี้

1. ด้านระบบงานและโปรแกรมประยุกต์ (Application Systems)

เป็นการสำรวจระบบโปรแกรมที่องค์กรนำมาใช้สนับสนุนภารกิจ เช่น ระบบบริหารจัดการ ระบบสารบรรณอิเล็กทรอนิกส์ ระบบบริหารงานบุคคล ระบบการเงิน และระบบเผยแพร่ข้อมูล โดยพิจารณาหน้าที่ของระบบ ข้อมูลที่เกี่ยวข้อง ผู้ใช้งาน และผู้รับผิดชอบ

2. ด้านข้อมูลและสารสนเทศ (Data and Information)

เป็นการสำรวจประเภทข้อมูลที่องค์กรจัดเก็บ ใช้ และประมวลผล เช่น ข้อมูลบุคลากร ข้อมูลนักศึกษา ข้อมูลการบริหารงาน ข้อมูลทางการเงิน และเอกสารอิเล็กทรอนิกส์ โดยพิจารณาความสำคัญ ความลับ ความถูกต้อง และความจำเป็นในการใช้งาน

3. ด้านอุปกรณ์และโครงสร้างพื้นฐาน (IT Infrastructure)

เป็นการสำรวจอุปกรณ์และทรัพยากรทางเทคโนโลยี เช่น Server เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์จัดเก็บข้อมูล และระบบสำรองข้อมูล เพื่อให้ทราบสถานะการใช้งานและความจำเป็นในการบำรุงรักษา

4. ด้านระบบเครือข่ายและการเชื่อมต่อ (Network and Connectivity)

เป็นการสำรวจโครงสร้างเครือข่ายภายในและภายนอกองค์กร การเชื่อมต่ออินเทอร์เน็ต ระบบเครือข่ายไร้สาย การกำหนดค่า Firewall และช่องทางการเข้าถึงระบบสารสนเทศจากภายนอก

5. ด้านบุคลากรและการบริหารจัดการ (People and Management)

เป็นการสำรวจผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และผู้เกี่ยวข้องกับการจัดการข้อมูล รวมถึงบทบาทหน้าที่ ความรับผิดชอบ และสิทธิ์ในการเข้าถึงระบบสารสนเทศ

3.1.3 การสำรวจระบบสารสนเทศของวิทยาลัยชุมชนสตูล

วิทยาลัยชุมชนสตูลมีการใช้ระบบสารสนเทศเพื่อสนับสนุนการบริหารจัดการ การปฏิบัติงาน และการให้บริการ โดยระบบสำคัญที่อยู่ในขอบเขตการศึกษาของรายงานประกอบด้วย ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server ซึ่งแต่ละระบบมีลักษณะการใช้งานและความสำคัญแตกต่างกัน

การสำรวจระบบดังกล่าวควรพิจารณาหน้าที่ของระบบ ประเภทข้อมูล ผู้ใช้งาน และประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง ดังตารางต่อไปนี้

ตารางที่ 3.1 ระบบสารสนเทศที่สำคัญของวิทยาลัยชุมชนสตูลและประเด็นการสำรวจ

ระบบสารสนเทศ	ลักษณะการใช้งาน	ประเด็นที่ต้องสำรวจด้านความปลอดภัย
ICCS-PORTAL	สนับสนุนการบริหารจัดการและการติดตามผลการดำเนินงาน	การกำหนดสิทธิ์ การเข้าถึงข้อมูล และความถูกต้องของข้อมูล
E-Office	สนับสนุนการรับ–ส่งและจัดการเอกสารอิเล็กทรอนิกส์	การรักษาความลับเอกสาร การกำหนดสิทธิ์ และประวัติการใช้งาน
E-HR.ICCS	สนับสนุนการบริหารจัดการข้อมูลบุคลากร	การคุ้มครองข้อมูลส่วนบุคคลและการควบคุมสิทธิ์
SMART ERPG	สนับสนุนการบริหารจัดการและการปฏิบัติงานตามภารกิจ	การควบคุมการเข้าถึงและความถูกต้องของข้อมูล
เว็บไซต์วิทยาลัย	เผยแพร่ข่าวสาร ประชาสัมพันธ์ และข้อมูลของวิทยาลัย	ความปลอดภัยของเว็บไซต์ การเข้ารหัส และการควบคุมผู้ดูแล
Server	รองรับการจัดเก็บ ประมวลผล และให้บริการระบบสารสนเทศ	ความปลอดภัยของระบบปฏิบัติการ การปรับปรุงซอฟต์แวร์ การสำรองข้อมูล และการเข้าถึง

3.1.4 ขั้นตอนการสำรวจและวิเคราะห์ระบบสารสนเทศ

การสำรวจระบบสารสนเทศสามารถดำเนินการตามขั้นตอนดังนี้

ขั้นตอนที่ 1 การรวบรวมข้อมูลระบบสารสนเทศ

รวบรวมข้อมูลจากทะเบียนครุภัณฑ์ เอกสารการดูแลระบบ คู่มือการใช้งาน ข้อมูลผู้ดูแลระบบ รายการซอฟต์แวร์ และข้อมูลโครงสร้างเครือข่าย รวมถึงข้อมูลจากหน่วยงานที่เกี่ยวข้อง

ขั้นตอนที่ 2 การจัดทำทะเบียนทรัพย์สินสารสนเทศ

จัดทำรายการทรัพย์สินสารสนเทศที่อยู่ภายใต้ความรับผิดชอบขององค์กร โดยระบุชื่อระบบ ประเภททรัพยากร ที่ตั้ง ผู้รับผิดชอบ และระดับความสำคัญ

ขั้นตอนที่ 3 การจำแนกประเภทข้อมูล

จำแนกข้อมูลตามลักษณะและระดับความสำคัญ เช่น ข้อมูลทั่วไป ข้อมูลภายใน ข้อมูลส่วนบุคคล และข้อมูลที่มีความสำคัญต่อการบริหารงาน เพื่อกำหนดมาตรการควบคุมที่เหมาะสม

ขั้นตอนที่ 4 การวิเคราะห์ความเชื่อมโยงของระบบ

ตรวจสอบการเชื่อมโยงระหว่างระบบสารสนเทศ เครือข่าย ฐานข้อมูล และผู้ใช้งาน เพื่อระบุจุดที่อาจส่งผลกระทบต่อระบบอื่นเมื่อเกิดเหตุการณ์ผิดปกติ

ขั้นตอนที่ 5 การจัดทำรายงานผลการสำรวจ

สรุปข้อมูลระบบสารสนเทศ สถานะการใช้งาน ประเด็นที่ต้องควบคุม และข้อกำหนดด้านความปลอดภัย เพื่อใช้เป็นข้อมูลประกอบการประเมินความเสี่ยงและกำหนดมาตรการป้องกัน

3.1.5 เอกสารและหลักฐานประกอบการสำรวจ

การสำรวจระบบสารสนเทศควรมีเอกสารประกอบเพื่อใช้ในการตรวจสอบและติดตามผล ได้แก่

1) ทะเบียนทรัพย์สินสารสนเทศขององค์กร
2) รายการระบบสารสนเทศและรายละเอียดการใช้งาน
3) แผนผังโครงสร้างระบบเครือข่าย
4) รายชื่อผู้ดูแลระบบและผู้รับผิดชอบ
5) รายการบัญชีผู้ใช้งานและสิทธิ์การเข้าถึง
6) รายการซอฟต์แวร์และระบบปฏิบัติการ
7) รายงานการตรวจสอบและบำรุงรักษาระบบ
8) รายงานการสำรองและกู้คืนข้อมูล
9) เอกสารการกำหนดมาตรการรักษาความปลอดภัย

ผลจากการสำรวจและวิเคราะห์ระบบสารสนเทศจะเป็นฐานข้อมูลสำคัญสำหรับการประเมินความเสี่ยง การกำหนดมาตรการควบคุม และการจัดลำดับความสำคัญในการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

3.2 การประเมินความเสี่ยงและกำหนดมาตรการป้องกัน

การประเมินความเสี่ยงเป็นกระบวนการวิเคราะห์ความเป็นไปได้ที่ภัยคุกคามจะก่อให้เกิดความเสียหายต่อระบบสารสนเทศ โดยพิจารณาร่วมกับช่องโหว่ของระบบ โอกาสเกิดเหตุการณ์ และระดับผลกระทบที่อาจเกิดขึ้น การประเมินความเสี่ยงช่วยให้องค์กรสามารถจัดลำดับความสำคัญของปัญหาและเลือกมาตรการควบคุมที่เหมาะสมกับระดับความเสี่ยง

NIST Special Publication 800-30 Revision 1 กำหนดแนวทางการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยครอบคลุมการเตรียมการประเมิน การดำเนินการประเมิน และการติดตามความเสี่ยงอย่างต่อเนื่อง (NIST, 2012)

3.2.1 วัตถุประสงค์ของการประเมินความเสี่ยง

1) เพื่อระบุภัยคุกคามและช่องโหว่ที่อาจส่งผลกระทบต่อระบบสารสนเทศ
2) เพื่อวิเคราะห์โอกาสเกิดเหตุการณ์และระดับความเสียหาย
3) เพื่อจัดลำดับความสำคัญของความเสี่ยง
4) เพื่อกำหนดมาตรการควบคุมและป้องกันให้เหมาะสมกับระบบ
5) เพื่อสนับสนุนการตัดสินใจในการจัดสรรทรัพยากรด้านความปลอดภัย
6) เพื่อใช้เป็นข้อมูลในการติดตามและปรับปรุงมาตรการรักษาความปลอดภัย

3.2.2 องค์ประกอบในการประเมินความเสี่ยง

การประเมินความเสี่ยงทางไซเบอร์ต้องพิจารณาองค์ประกอบสำคัญ ดังนี้

1. ทรัพย์สินสารสนเทศ (Information Assets)

หมายถึง ข้อมูล ระบบสารสนเทศ อุปกรณ์ เครือข่าย โปรแกรม และทรัพยากรอื่นที่มีคุณค่าต่อการดำเนินงานขององค์กร

2. ภัยคุกคาม (Threats)

หมายถึง เหตุการณ์หรือการกระทำที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศ เช่น การโจมตีทางเครือข่าย มัลแวร์ การหลอกลวงทางอิเล็กทรอนิกส์ และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

3. ช่องโหว่ (Vulnerabilities)

หมายถึง จุดอ่อนของระบบ เทคโนโลยี กระบวนการ หรือบุคลากรที่อาจถูกใช้เป็นช่องทางในการโจมตีหรือก่อให้เกิดความเสียหาย

4. โอกาสเกิดเหตุการณ์ (Likelihood)

หมายถึง ความเป็นไปได้ที่ภัยคุกคามจะเกิดขึ้นหรือใช้ประโยชน์จากช่องโหว่ของระบบ

5. ผลกระทบ (Impact)

หมายถึง ระดับความเสียหายที่อาจเกิดขึ้นต่อข้อมูล ระบบสารสนเทศ การบริหารจัดการ และการให้บริการขององค์กร

3.2.3 กระบวนการประเมินความเสี่ยง

การประเมินความเสี่ยงสามารถดำเนินการตามขั้นตอนต่อไปนี้

1) **กำหนดขอบเขตการประเมิน** โดยระบุระบบสารสนเทศและทรัพยากรที่ต้องได้รับการประเมิน
2) **ระบุภัยคุกคาม** โดยพิจารณาประเภทภัยคุกคามที่อาจเกิดขึ้นกับแต่ละระบบ
3) **ระบุช่องโหว่** โดยตรวจสอบจุดอ่อนด้านเทคนิค การกำหนดค่า และกระบวนการทำงาน
4) **วิเคราะห์โอกาสเกิดเหตุการณ์** โดยพิจารณาประวัติการเกิดเหตุ ลักษณะระบบและมาตรการควบคุมที่มีอยู่
5) **วิเคราะห์ผลกระทบ** โดยพิจารณาความเสียหายต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล
6) **จัดระดับความเสี่ยง** โดยนำผลการวิเคราะห์โอกาสเกิดและผลกระทบมาพิจารณาร่วมกัน
7) **กำหนดมาตรการจัดการความเสี่ยง** โดยเลือกวิธีควบคุม ลด โอน หรือยอมรับความเสี่ยงตามความเหมาะสม
8) **ติดตามและทบทวนผล** เพื่อให้มาตรการสามารถรองรับการเปลี่ยนแปลงของระบบและภัยคุกคามได้

3.2.4 การกำหนดระดับความเสี่ยง

การกำหนดระดับความเสี่ยงสามารถใช้การประเมินแบบเมทริกซ์ โดยพิจารณาคะแนนโอกาสเกิดเหตุการณ์และคะแนนผลกระทบ ดังนี้

ตารางที่ 3.2 เกณฑ์การประเมินโอกาสเกิดเหตุการณ์

คะแนน	ระดับ	คำอธิบาย
1	น้อยมาก	มีโอกาสเกิดเหตุการณ์น้อยมาก
2	น้อย	มีโอกาสเกิดเหตุการณ์ค่อนข้างต่ำ
3	ปานกลาง	มีโอกาสเกิดเหตุการณ์ในระดับปานกลาง
4	สูง	มีโอกาสเกิดเหตุการณ์ค่อนข้างสูง
5	สูงมาก	มีโอกาสเกิดเหตุการณ์สูงมาก

ตารางที่ 3.3 เกณฑ์การประเมินผลกระทบ

คะแนน	ระดับ	คำอธิบาย
1	น้อยมาก	กระทบต่อการดำเนินงานเพียงเล็กน้อย
2	น้อย	เกิดผลกระทบจำกัดและแก้ไขได้ง่าย
3	ปานกลาง	กระทบต่อการปฏิบัติงานบางส่วน
4	สูง	กระทบต่อระบบหรือการให้บริการที่สำคัญ
5	สูงมาก	กระทบต่อข้อมูลสำคัญหรือทำให้ภารกิจหลักหยุดชะงัก

ตารางที่ 3.4 เกณฑ์การแปลผลระดับความเสี่ยงตัวอย่าง

คะแนนรวม	ระดับความเสี่ยง	แนวทางจัดการ
1–4	ต่ำ	ควบคุมตามมาตรการปกติและติดตาม
5–9	ปานกลาง	กำหนดมาตรการลดความเสี่ยงและติดตาม
10–16	สูง	จัดทำแผนแก้ไขและกำหนดผู้รับผิดชอบ
17–25	สูงมาก	ให้ความสำคัญเร่งด่วนและกำหนดมาตรการควบคุม

ที่มา: ตัวอย่างเกณฑ์สำหรับใช้ประกอบการประเมินความเสี่ยงขององค์กร โดยต้องกำหนดและรับรองเกณฑ์การประเมินก่อนนำไปใช้จริง

3.2.5 การกำหนดมาตรการป้องกันความเสี่ยง

เมื่อประเมินระดับความเสี่ยงแล้ว องค์กรต้องกำหนดมาตรการควบคุมให้เหมาะสมกับประเภทของความเสี่ยง โดยสามารถแบ่งเป็น 4 แนวทาง ได้แก่

1. **การหลีกเลี่ยงความเสี่ยง (Risk Avoidance):** ยุติหรือปรับเปลี่ยนกิจกรรมที่มีความเสี่ยงสูงเกินกว่าจะยอมรับได้
2. **การลดความเสี่ยง (Risk Mitigation):** กำหนดมาตรการควบคุมเพื่อลดโอกาสเกิดเหตุหรือผลกระทบ
3. **การถ่ายโอนความเสี่ยง (Risk Sharing/Transfer):** จัดให้มีการแบ่งปันหรือถ่ายโอนความรับผิดชอบบางส่วนตามสัญญาหรือกลไกที่เหมาะสม
4. **การยอมรับความเสี่ยง (Risk Acceptance):** ยอมรับความเสี่ยงที่เหลืออยู่ภายใต้การพิจารณาและอนุมัติของผู้มีอำนาจ

3.2.6 ตัวอย่างการวิเคราะห์ความเสี่ยงของระบบสารสนเทศวิทยาลัยชุมชนสตูล

ตารางที่ 3.5 ตัวอย่างการวิเคราะห์ความเสี่ยงและมาตรการควบคุม

ระบบสารสนเทศ	ความเสี่ยงที่ควรพิจารณา	มาตรการป้องกันที่เหมาะสม
ICCS-PORTAL	การเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	กำหนดสิทธิ์และตรวจสอบประวัติการใช้งาน
E-Office	การเปิดเผยเอกสารอิเล็กทรอนิกส์	ควบคุมสิทธิ์และการเผยแพร่เอกสาร
E-HR.ICCS	การรั่วไหลของข้อมูลบุคลากร	จำกัดสิทธิ์และป้องกันข้อมูลส่วนบุคคล

ระบบสารสนเทศ	ความเสี่ยงที่ควรพิจารณา	มาตรการป้องกันที่เหมาะสม
SMART ERPG	การเปลี่ยนแปลงข้อมูลโดยไม่มีอำนาจ	กำหนดผู้รับผิดชอบและตรวจสอบข้อมูล
เว็บไซต์วิทยาลัย	การโจมตีเว็บไซต์และช่องโหว่ของโปรแกรม	ใช้ HTTPS/TLS ปรับปรุงระบบ และตรวจสอบเว็บไซต์
Server	การเข้าถึงโดยไม่ได้รับอนุญาตและระบบหยุดชะงัก	ใช้ Firewall ปรับปรุงระบบ สำรองข้อมูล และตรวจสอบ Log

3.2.7 การติดตามและทบทวนความเสี่ยง

การประเมินความเสี่ยงไม่ใช่กระบวนการที่ดำเนินการเพียงครั้งเดียว แต่ต้องมีการทบทวนเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ การติดตั้งซอฟต์แวร์ใหม่ การเปลี่ยนแปลงโครงสร้างเครือข่าย การเปลี่ยนผู้รับผิดชอบ หรือเมื่อเกิดเหตุการณ์ด้านความปลอดภัย

3.3 การพัฒนาระบบป้องกันภัยคุกคามทางไซเบอร์

การพัฒนาระบบป้องกันภัยคุกคามทางไซเบอร์เป็นกระบวนการนำมาตรการด้านเทคโนโลยีและการบริหารจัดการมาใช้เพื่อลดความเสี่ยงต่อระบบสารสนเทศ โดยมุ่งเน้นการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีระบบเครือข่าย การรั่วไหลของข้อมูล และการหยุดชะงักของบริการดิจิทัล

การพัฒนาระบบป้องกันต้องสอดคล้องกับลักษณะการใช้งานและระดับความสำคัญของระบบ โดยพิจารณาทั้งการป้องกันในระดับเครือข่าย เว็บไซต์ Server ฐานข้อมูล และบัญชีผู้ใช้งาน

3.3.1 การรักษาความปลอดภัยระบบเครือข่ายด้วย Firewall

Firewall เป็นระบบรักษาความปลอดภัยเครือข่ายที่ทำหน้าที่ควบคุมการรับส่งข้อมูลระหว่างเครือข่ายตามกฎที่กำหนด โดยสามารถอนุญาตหรือปฏิเสธการเชื่อมต่อจากต้นทางไปยังปลายทางตามเงื่อนไข เช่น หมายเลข IP พอร์ต โปรโตคอล และลักษณะของการเชื่อมต่อ

มาตรการดำเนินงานประกอบด้วย

1) กำหนดขอบเขตเครือข่ายที่ต้องได้รับการป้องกัน
2) กำหนดกฎการอนุญาตและปฏิเสธการเชื่อมต่อ
3) จำกัดพอร์ตและบริการที่ไม่จำเป็น
4) ควบคุมการเชื่อมต่อจากเครือข่ายภายนอก
5) ตรวจสอบบันทึกการรับส่งข้อมูลและเหตุการณ์ผิดปกติ
6) ทบทวนและปรับปรุงกฎ Firewall ให้เหมาะสมกับการใช้งาน
7) จำกัดสิทธิ์การเข้าถึงหน้าจัดการ Firewall

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีข้อมูลการดำเนินงานเกี่ยวกับการใช้ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก ซึ่งเป็นมาตรการด้านเทคนิคที่เกี่ยวข้องกับการควบคุมการเชื่อมต่อและการรักษาความปลอดภัยของระบบเครือข่าย

3.3.2 การรักษาความปลอดภัยเว็บไซต์ด้วยใบรับรองดิจิทัลและ HTTPS/TLS

การรักษาความปลอดภัยเว็บไซต์เป็นการกำหนดมาตรการเพื่อป้องกันการเข้าถึงและการเปลี่ยนแปลงเว็บไซต์โดยไม่ได้รับอนุญาต รวมถึงการคุ้มครองข้อมูลที่รับส่งระหว่างผู้ใช้งานกับเว็บไซต์

ใบรับรองดิจิทัล (Digital Certificate) ใช้สำหรับยืนยันตัวตนของเว็บไซต์และสนับสนุนการสร้างการเชื่อมต่อที่เข้ารหัสผ่านโปรโตคอล TLS โดยเว็บไซต์ที่ใช้ HTTPS จะช่วยลดความเสี่ยงจากการดักอ่านหรือแก้ไขข้อมูลระหว่างการรับส่ง

มาตรการสำคัญประกอบด้วย

1) ติดตั้งใบรับรองดิจิทัลที่ออกโดยผู้ให้บริการที่เชื่อถือได้
2) กำหนดให้เว็บไซต์ใช้ HTTPS
3) ตรวจสอบอายุและสถานะของใบรับรอง
4) ปรับปรุงระบบเว็บไซต์และส่วนประกอบซอฟต์แวร์
5) ควบคุมบัญชีผู้ดูแลเว็บไซต์
6) สำรองข้อมูลเว็บไซต์และฐานข้อมูล
7) ตรวจสอบความผิดปกติของเว็บไซต์และการเปลี่ยนแปลงไฟล์

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีข้อมูลการใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ ซึ่งเป็นมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยในการรับส่งข้อมูล โดยการดำเนินงานทางเทคนิคควรใช้โปรโตคอล TLS รุ่นที่มีความปลอดภัยและได้รับการสนับสนุนในปัจจุบัน

3.3.3 การปรับปรุงรหัสโปรแกรมและระบบ Server

ระบบ Server เป็นโครงสร้างพื้นฐานที่รองรับการจัดเก็บ ประมวลผล และให้บริการระบบสารสนเทศ การรักษาความปลอดภัยจึงต้องครอบคลุมทั้งระบบปฏิบัติการ ซอฟต์แวร์ โปรแกรมประยุกต์ ฐานข้อมูล และการกำหนดค่าระบบ

มาตรการสำคัญประกอบด้วย

1) ตรวจสอบและปรับปรุงรหัสโปรแกรมเพื่อแก้ไขข้อบกพร่อง
2) ตรวจสอบช่องโหว่ของระบบปฏิบัติการและซอฟต์แวร์
3) ติดตั้งโปรแกรมปรับปรุงความปลอดภัยตามความเหมาะสม
4) ปิดบริการและพอร์ตที่ไม่จำเป็น
5) จำกัดสิทธิ์บัญชีผู้ดูแลระบบ
6) เปลี่ยนหรือยกเลิกรหัสผ่านเริ่มต้น
7) สำรองข้อมูลและจัดเตรียมแนวทางกู้คืนระบบ
8) ตรวจสอบ Log และสถานะการทำงานของ Server
9) บันทึกประวัติการเปลี่ยนแปลงและปรับปรุงระบบ

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีข้อมูลการปรับปรุงรหัสโปรแกรมของ Server ซึ่งเป็นส่วนหนึ่งของการพัฒนาระบบและดูแลความปลอดภัยของโครงสร้างพื้นฐานสารสนเทศ

3.3.4 การพัฒนาเว็บไซต์ให้มีความปลอดภัยและรองรับการใช้งาน

การพัฒนาเว็บไซต์ขององค์กรต้องคำนึงถึงความปลอดภัยของระบบควบคู่กับประสิทธิภาพและความสะดวกในการเข้าถึงข้อมูล โดยต้องรองรับการใช้งานผ่านอุปกรณ์ที่หลากหลาย เช่น คอมพิวเตอร์ แท็บเล็ต และโทรศัพท์เคลื่อนที่

แนวทางดำเนินงานประกอบด้วย

1) ปรับโครงสร้างเว็บไซต์และเมนูให้เข้าถึงข้อมูลได้สะดวก
2) พัฒนาเว็บไซต์ให้รองรับการแสดงผลบนอุปกรณ์ที่หลากหลาย
3) ควบคุมสิทธิ์การจัดการเนื้อหาเว็บไซต์

4) ป้องกันการส่งข้อมูลผ่านช่องทางที่ไม่มีการเข้ารหัส
5) ตรวจสอบความถูกต้องของข้อมูลก่อนเผยแพร่
6) ปรับปรุงระบบและซอฟต์แวร์ที่เกี่ยวข้อง
7) ตรวจสอบการทำงานของเว็บไซต์หลังการปรับปรุง
8) จัดเก็บข้อมูลสำรองและเตรียมแนวทางกู้คืนเว็บไซต์

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีข้อมูลการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย พร้อมปรับโครงสร้างเมนูเพื่อให้เข้าถึงข้อมูลได้สะดวก การดำเนินงานดังกล่าวเกี่ยวข้องกับการพัฒนาคุณภาพการให้บริการสารสนเทศผ่านเว็บไซต์ขององค์กร

3.3.5 การพัฒนามาตรการป้องกันในระดับผู้ใช้งาน

การป้องกันภัยคุกคามไม่ได้จำกัดเฉพาะอุปกรณ์เครือข่ายและระบบ Server เท่านั้น แต่ยังครอบคลุมบัญชีผู้ใช้งานและอุปกรณ์ที่บุคลากรใช้ปฏิบัติงาน

มาตรการประกอบด้วย

1) กำหนดบัญชีผู้ใช้งานรายบุคคล
2) กำหนดหลักเกณฑ์การตั้งรหัสผ่าน
3) ใช้การยืนยันตัวตนหลายปัจจัยในระบบที่รองรับ
4) จำกัดสิทธิ์การเข้าถึงตามบทบาทหน้าที่
5) ป้องกันการติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต
6) ตรวจสอบและปรับปรุงโปรแกรมป้องกันมัลแวร์
7) กำหนดแนวทางการใช้งานอุปกรณ์จัดเก็บข้อมูลภายนอก
8) สร้างความตระหนักเกี่ยวกับอีเมลและลิงก์ที่มีความเสี่ยง

3.3.6 การบูรณาการมาตรการป้องกันกับระบบสารสนเทศของวิทยาลัย

มาตรการป้องกันภัยคุกคามทางไซเบอร์ต้องมีการเชื่อมโยงระหว่างระบบเครือข่าย เว็บไซต์ Server และระบบสารสนเทศที่ใช้ในการปฏิบัติงาน เพื่อให้สามารถดูแลความปลอดภัยได้อย่างครอบคลุม

ตารางที่ 3.6 มาตรการป้องกันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับวิทยาลัยชุมชนสตูล

องค์ประกอบ	มาตรการด้านความปลอดภัย	หลักฐานที่ใช้ตรวจสอบ
ระบบเครือข่าย	การใช้ Firewall	ภาพหน้าจอการตั้งค่าและเอกสารการดูแลระบบ
เว็บไซต์	การใช้ใบรับรองดิจิทัลและ HTTPS/TLS	รายละเอียดใบรับรองและผลตรวจสอบเว็บไซต์
Server	การปรับปรุงรหัสโปรแกรมและระบบ	บันทึกการปรับปรุงและรายงานการตรวจสอบ
เว็บไซต์วิทยาลัย	การพัฒนาโครงสร้างและการแสดงผล	ภาพก่อนและหลังการพัฒนาและรายงานการทดสอบ
บัญชีผู้ใช้งาน	การกำหนดสิทธิ์และควบคุมการเข้าถึง	ทะเบียนผู้ใช้งานและเอกสารกำหนดสิทธิ์
ข้อมูลสารสนเทศ	การสำรองและกู้คืนข้อมูล	บันทึกการสำรองและผลทดสอบกู้คืน

3.4 การตรวจสอบและบำรุงรักษาระบบสารสนเทศ

การตรวจสอบและบำรุงรักษาระบบสารสนเทศเป็นกระบวนการติดตามสถานะการทำงานของระบบ ตรวจสอบความผิดปกติ ป้องกันการเสื่อมสภาพของอุปกรณ์ และแก้ไขข้อบกพร่องที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบงาน การดำเนินงานดังกล่าวช่วยให้สามารถค้นพบปัญหาได้ตั้งแต่ระยะเริ่มต้น ลดความเสี่ยงจากระบบหยุดชะงัก และสนับสนุนการให้บริการขององค์กรอย่างต่อเนื่อง

ตามกรอบ NIST CSF 2.0 การตรวจสอบและบำรุงรักษาระบบมีความเกี่ยวข้องกับหน้าที่ Protect, Detect, Respond และ Recover เนื่องจากครอบคลุมการป้องกัน การตรวจจับเหตุการณ์ การจัดการปัญหา และการฟื้นฟูระบบให้กลับมาใช้งานได้ตามปกติ (Pascoe et al., 2024)

3.4.1 วัตถุประสงค์ของการตรวจสอบและบำรุงรักษา

1) เพื่อตรวจสอบสถานะการทำงานของระบบสารสนเทศและอุปกรณ์ที่เกี่ยวข้อง
2) เพื่อค้นหาความผิดปกติและช่องโหว่ที่อาจส่งผลกระทบต่อความปลอดภัย
3) เพื่อป้องกันปัญหาที่อาจทำให้ระบบหยุดชะงัก
4) เพื่อรักษาความถูกต้องและความพร้อมใช้งานของข้อมูล
5) เพื่อให้ระบบและซอฟต์แวร์ได้รับการปรับปรุงตามความจำเป็น
6) เพื่อจัดเก็บหลักฐานและประวัติการบำรุงรักษา
7) เพื่อสนับสนุนการวางแผนฟื้นฟูระบบเมื่อเกิดเหตุการณ์ผิดปกติ

3.4.2 การตรวจสอบระบบเครือข่ายและอุปกรณ์รักษาความปลอดภัย

การตรวจสอบระบบเครือข่ายมีวัตถุประสงค์เพื่อประเมินสถานะการเชื่อมต่อและความปลอดภัยของอุปกรณ์ที่รองรับการรับส่งข้อมูลภายในองค์กร

รายการตรวจสอบประกอบด้วย

1) ตรวจสอบสถานะการทำงานของอุปกรณ์เครือข่าย
2) ตรวจสอบการเชื่อมต่ออินเทอร์เน็ตและระบบเครือข่ายภายใน
3) ตรวจสอบการตั้งค่า Firewall
4) ตรวจสอบกฎการอนุญาตและปฏิเสธการเชื่อมต่อ
5) ตรวจสอบพอร์ตและบริการที่เปิดใช้งาน
6) ตรวจสอบบันทึกการเชื่อมต่อที่ผิดปกติ
7) ตรวจสอบการเปลี่ยนแปลงการตั้งค่าอุปกรณ์
8) ปรับปรุงเฟิร์มแวร์และซอฟต์แวร์ของอุปกรณ์ตามความเหมาะสม

3.4.3 การตรวจสอบเว็บไซต์และใบรับรองดิจิทัล

การตรวจสอบเว็บไซต์เป็นกระบวนการติดตามความพร้อมใช้งานและความปลอดภัยของเว็บไซต์ โดยต้องตรวจสอบทั้งการแสดงผล การทำงานของระบบ การเชื่อมต่อ และความถูกต้องของข้อมูล

รายการตรวจสอบประกอบด้วย

1) ตรวจสอบสถานะการเข้าถึงเว็บไซต์
2) ตรวจสอบการทำงานของหน้าเว็บไซต์และเมนูต่าง ๆ
3) ตรวจสอบใบรับรองดิจิทัลและวันหมดอายุ
4) ตรวจสอบการเชื่อมต่อผ่าน HTTPS/TLS
5) ตรวจสอบระบบจัดการเนื้อหาและโปรแกรมที่เกี่ยวข้อง
6) ตรวจสอบบัญชีผู้ดูแลเว็บไซต์

7) ตรวจสอบการเปลี่ยนแปลงไฟล์และเนื้อหาที่เผยแพร่
8) สำรองข้อมูลเว็บไซต์และฐานข้อมูล

3.4.4 การตรวจสอบและบำรุงรักษา Server

การบำรุงรักษา Server เป็นกระบวนการตรวจสอบและดูแลอุปกรณ์และซอฟต์แวร์ที่รองรับระบบสารสนเทศ เพื่อรักษาความพร้อมใช้งานและลดความเสี่ยงจากข้อบกพร่องทางเทคนิค

รายการตรวจสอบประกอบด้วย

1) ตรวจสอบสถานะการทำงานของ Server
2) ตรวจสอบพื้นที่จัดเก็บข้อมูลและการใช้ทรัพยากรระบบ
3) ตรวจสอบระบบปฏิบัติการและซอฟต์แวร์
4) ติดตั้งโปรแกรมปรับปรุงด้านความปลอดภัย
5) ตรวจสอบสิทธิ์บัญชีผู้ดูแลระบบ
6) ตรวจสอบบันทึกเหตุการณ์ของระบบ
7) ตรวจสอบระบบสำรองข้อมูล
8) ทดสอบการกู้คืนข้อมูลตามแผน
9) บันทึกผลการบำรุงรักษาและการแก้ไขปัญหา

3.4.5 การสำรองและทดสอบการกู้คืนข้อมูล

การสำรองข้อมูลเป็นมาตรการสำคัญในการลดความเสียหายจากเหตุการณ์ข้อมูลสูญหาย ระบบขัดข้อง การโจมตีด้วยมัลแวร์ หรือความผิดพลาดจากการปฏิบัติงาน โดยองค์กรต้องกำหนดความถี่ในการสำรองข้อมูลตามระดับความสำคัญของข้อมูลและระบบ

แนวทางการดำเนินงานประกอบด้วย

- กำหนดประเภทข้อมูลที่ต้องสำรอง
- กำหนดรอบระยะเวลาและผู้รับผิดชอบการสำรองข้อมูล
- จัดเก็บข้อมูลสำรองแยกจากระบบหลัก
- จำกัดสิทธิ์การเข้าถึงข้อมูลสำรอง
- ตรวจสอบความสมบูรณ์ของไฟล์สำรอง
- ทดสอบการกู้คืนข้อมูล
- จัดทำบันทึกผลการสำรองและกู้คืนข้อมูล

การทดสอบกู้คืนข้อมูลเป็นขั้นตอนที่จำเป็น เนื่องจากการมีไฟล์สำรองเพียงอย่างเดียวไม่ได้ยืนยันว่าข้อมูลสามารถนำกลับมาใช้งานได้จริง การทดสอบจึงต้องตรวจสอบทั้งความครบถ้วนของข้อมูลและความสามารถในการนำระบบกลับมาให้บริการ

3.4.6 การตรวจสอบบันทึกเหตุการณ์ (Log Monitoring)

การจัดเก็บและตรวจสอบบันทึกเหตุการณ์เป็นมาตรการสำคัญสำหรับการติดตามการใช้งานระบบและการตรวจสอบย้อนหลัง โดยข้อมูลที่ควรจัดเก็บประกอบด้วย

1) ประวัติการเข้าสู่ระบบและออกจากระบบ
2) ประวัติการเข้าถึงระบบของบัญชีผู้ดูแล
3) ประวัติการเปลี่ยนแปลงการตั้งค่าระบบ
4) ประวัติการแก้ไขหรือเปลี่ยนแปลงข้อมูลที่สำคัญ
5) ประวัติการเชื่อมต่อเครือข่าย

6) เหตุการณ์ผิดปกติที่ระบบตรวจพบ
7) ประวัติการดำเนินการแก้ไขปัญหา

ข้อมูล Log ควรมีการควบคุมสิทธิ์การเข้าถึง ป้องกันการแก้ไขโดยไม่ได้รับอนุญาต และกำหนดระยะเวลาการจัดเก็บให้สอดคล้องกับความจำเป็นและข้อกำหนดที่เกี่ยวข้อง

3.4.7 การจัดทำแผนตรวจสอบและบำรุงรักษาระบบ

การตรวจสอบและบำรุงรักษาควรมีการวางแผนอย่างเป็นระบบ โดยกำหนดรายการตรวจสอบ ความถี่ ผู้รับผิดชอบ และหลักฐานที่ต้องจัดเก็บ

ตารางที่ 3.7 ตัวอย่างแผนการตรวจสอบและบำรุงรักษาระบบสารสนเทศ

รายการตรวจสอบ	ความถี่ตัวอย่าง	ผู้รับผิดชอบ	หลักฐาน
ตรวจสอบสถานะเว็บไซต์	รายเดือน	ผู้ดูแลเว็บไซต์	รายงานตรวจสอบ
ตรวจสอบใบรับรอง HTTPS/TLS	รายเดือนและก่อนหมดอายุ	ผู้ดูแลระบบ	รายละเอียดใบรับรอง
ตรวจสอบ Firewall	รายเดือนและเมื่อมีการเปลี่ยนแปลง	ผู้ดูแลเครือข่าย	บันทึกการตรวจสอบ
ตรวจสอบ Server	รายเดือน	ผู้ดูแลระบบ	รายงานสถานะ Server
ตรวจสอบการปรับปรุงซอฟต์แวร์	ตามรอบและเมื่อมีประกาศสำคัญ	ผู้ดูแลระบบ	บันทึกการปรับปรุง
สำรองข้อมูล	ตามระดับความสำคัญของข้อมูล	ผู้ดูแลระบบ	รายงาน Backup
ทดสอบการกู้คืนข้อมูล	ตามแผนที่กำหนด	ผู้ดูแลระบบ	รายงานผลการทดสอบ
ตรวจสอบบัญชีผู้ใช้งาน	รายไตรมาสและเมื่อมีการเปลี่ยนแปลงบุคลากร	ผู้ดูแลระบบและหน่วยงานเจ้าของระบบ	รายการสิทธิ์ผู้ใช้งาน

3.4.8 การจัดการเหตุการณ์ผิดปกติและการฟื้นฟูระบบ

เมื่อพบเหตุการณ์ผิดปกติที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องมีกระบวนการรับแจ้ง ตรวจสอบ วิเคราะห์ และดำเนินการแก้ไข โดยมีขั้นตอนสำคัญดังนี้

1) รับแจ้งเหตุและบันทึกข้อมูลเบื้องต้น
2) ตรวจสอบประเภทและขอบเขตของเหตุการณ์
3) ประเมินผลกระทบต่อระบบและข้อมูล
4) ดำเนินการควบคุมเหตุการณ์เพื่อลดความเสียหาย
5) แก้ไขสาเหตุและช่องโหว่ที่เกี่ยวข้อง
6) กู้คืนระบบและข้อมูล
7) ตรวจสอบการทำงานหลังการกู้คืน
8) จัดทำรายงานสรุปเหตุการณ์และแนวทางป้องกันการเกิดซ้ำ

กระบวนการดังกล่าวช่วยให้หน่วยงานสามารถจัดการเหตุการณ์ด้านความปลอดภัยได้อย่างเป็นระบบ และมีข้อมูลสำหรับปรับปรุงมาตรการป้องกันในระยะต่อไป

3.5 การจัดการความรู้และการสร้างความตระหนักรู้แก่บุคลากร

การจัดการความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นกระบวนการรวบรวม วิเคราะห์ จัดระบบ ถ่ายทอด และนำองค์ความรู้ไปใช้ในการปฏิบัติงาน เพื่อให้บุคลากรมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามและแนวทางรักษาความปลอดภัยของระบบสารสนเทศ สามารถปฏิบัติงานได้อย่างถูกต้อง และมีส่วนร่วมในการป้องกันความเสี่ยงขององค์กร

การจัดการความรู้มีความสำคัญเนื่องจากภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงอยู่เสมอ บุคลากรจึงจำเป็นต้องได้รับการพัฒนาความรู้และทักษะให้สอดคล้องกับรูปแบบการใช้งานเทคโนโลยีและความเสี่ยงที่เกิดขึ้น

สำหรับวิทยาลัยชุมชนสตูล การดำเนินงานด้านการจัดการความรู้ในปีงบประมาณ พ.ศ. 2569 มีการเชื่อมโยงการทบทวนองค์ความรู้และแนวปฏิบัติด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ขององค์กร เพื่อส่งเสริมการนำความรู้ไปประยุกต์ใช้ในการดูแลระบบสารสนเทศและสร้างความตระหนักรู้แก่บุคลากร

3.5.1 วัตถุประสงค์ของการจัดการความรู้ด้าน Cybersecurity

1) เพื่อรวบรวมองค์ความรู้และประสบการณ์ด้านการดูแลระบบสารสนเทศขององค์กร
2) เพื่อจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ให้เป็นระบบ
3) เพื่อถ่ายทอดความรู้จากผู้ดูแลระบบและผู้มีประสบการณ์ไปสู่บุคลากรที่เกี่ยวข้อง
4) เพื่อพัฒนาความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์
5) เพื่อส่งเสริมพฤติกรรมการใช้งานระบบสารสนเทศอย่างปลอดภัย
6) เพื่อสร้างฐานความรู้สำหรับใช้ในการแก้ไขปัญหาและพัฒนาระบบอย่างต่อเนื่อง

3.5.2 กระบวนการจัดการความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การจัดการความรู้สามารถดำเนินการตามกระบวนการจัดการความรู้ 7 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 การบ่งชี้ความรู้ (Knowledge Identification)

กำหนดหัวข้อความรู้ที่จำเป็นต่อการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ เช่น การดูแลเว็บไซต์ การใช้ Firewall การรักษาความปลอดภัย Server การจัดการรหัสผ่าน การสำรองข้อมูล และการป้องกันภัยคุกคามทางอิเล็กทรอนิกส์

ขั้นตอนที่ 2 การสร้างและแสวงหาความรู้ (Knowledge Creation and Acquisition)

รวบรวมองค์ความรู้จากผู้ดูแลระบบ บุคลากรผู้ปฏิบัติงาน เอกสารทางเทคนิค คู่มือการใช้งาน มาตรฐานสากล และแหล่งความรู้ที่เชื่อถือได้ เพื่อนำมาใช้ประกอบการพัฒนาองค์ความรู้ขององค์กร

ขั้นตอนที่ 3 การจัดการความรู้ให้เป็นระบบ (Knowledge Organization)

จำแนกและจัดหมวดหมู่ข้อมูลตามประเภทความรู้ เช่น ความรู้ด้านระบบเครือข่าย ความรู้ด้านเว็บไซต์ ความรู้ด้าน Server ความรู้ด้านการคุ้มครองข้อมูล และความรู้ด้านการรับมือเหตุการณ์

ขั้นตอนที่ 4 การประมวลและกลั่นกรองความรู้ (Knowledge Refinement)

ตรวจสอบความถูกต้อง ความทันสมัย และความเหมาะสมขององค์ความรู้ โดยพิจารณาความสอดคล้องกับระบบที่ใช้งานจริงและมาตรฐานด้านความปลอดภัยที่เกี่ยวข้อง

ขั้นตอนที่ 5 การเข้าถึงความรู้ (Knowledge Access)

จัดทำช่องทางให้บุคลากรสามารถเข้าถึงองค์ความรู้ เช่น คู่มือ เอกสารอิเล็กทรอนิกส์ เว็บไซต์ภายใน และฐานข้อมูลความรู้ขององค์กร

ขั้นตอนที่ 6 การแบ่งปันและแลกเปลี่ยนความรู้ (Knowledge Sharing)

ดำเนินกิจกรรมแลกเปลี่ยนเรียนรู้ระหว่างผู้ดูแลระบบและบุคลากร เพื่อถ่ายทอดประสบการณ์ ปัญหาที่พบ วิธีการป้องกัน และแนวทางแก้ไขปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

ขั้นตอนที่ 7 การเรียนรู้และนำความรู้ไปใช้ (Learning and Utilization)

นำองค์ความรู้ที่ได้ไปประยุกต์ใช้ในการปฏิบัติงาน เช่น การตรวจสอบเว็บไซต์ การใช้งานระบบสารสนเทศอย่างปลอดภัย การป้องกันการเปิดเผยข้อมูล และการรายงานเหตุการณ์ผิดปกติ พร้อมติดตามผลการนำความรู้ไปใช้

3.5.3 การถ่ายทอดความรู้จากผู้มีประสบการณ์สู่บุคลากร

การถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ควรให้ความสำคัญกับความรู้ 2 ประเภท ได้แก่

1. ความรู้ที่ฝังอยู่ในตัวบุคคล (Tacit Knowledge)

เป็นความรู้ที่เกิดจากประสบการณ์และการปฏิบัติงานของบุคลากร เช่น ประสบการณ์ในการแก้ไขปัญหาเว็บไซต์ การดูแล Server การตั้งค่า Firewall และการตรวจสอบความผิดปกติของระบบ ซึ่งอาจไม่สามารถถ่ายทอดผ่านเอกสารได้ทั้งหมด

2. ความรู้ที่ชัดแจ้ง (Explicit Knowledge)

เป็นความรู้ที่สามารถจัดทำเป็นเอกสาร คู่มือ ขั้นตอนการปฏิบัติงาน แผนผังระบบ และแนวปฏิบัติที่สามารถเผยแพร่และนำไปใช้งานได้

การจัดการความรู้จึงควรดำเนินการโดยรวบรวมประสบการณ์จากผู้มีความรู้และผู้ปฏิบัติงาน แล้วนำมาวิเคราะห์และเรียบเรียงเป็นองค์ความรู้ที่สามารถถ่ายทอดให้บุคลากรอื่นนำไปใช้ได้

ตัวอย่างหัวข้อความรู้ที่สามารถนำมาถ่ายทอด ได้แก่

- แนวทางการดูแลและตรวจสอบระบบ Firewall
- ขั้นตอนการตรวจสอบใบรับรอง SSL/TLS
- แนวทางการปรับปรุงและดูแล Server
- วิธีการตรวจสอบเว็บไซต์และแก้ไขปัญหาเบื้องต้น
- การสำรองและกู้คืนข้อมูล
- การจัดการบัญชีผู้ใช้งานและรหัสผ่าน
- การตรวจสอบอีเมลและข้อความหลอกลวง
- การรายงานเหตุการณ์ผิดปกติทางไซเบอร์

3.5.4 การสร้างความตระหนักรู้แก่บุคลากร

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นการพัฒนาความรู้ ความเข้าใจ และพฤติกรรมการใช้งานเทคโนโลยีอย่างปลอดภัย โดยบุคลากรทุกกลุ่มควรมีความรู้พื้นฐานที่เหมาะสมกับหน้าที่และความรับผิดชอบ

เนื้อหาการพัฒนาความรู้ควรครอบคลุมประเด็นดังต่อไปนี้

1. การรักษาความปลอดภัยของบัญชีผู้ใช้งาน

ให้บุคลากรเข้าใจหลักการตั้งรหัสผ่านที่ปลอดภัย การไม่ใช้รหัสผ่านซ้ำโดยไม่จำเป็น และการไม่เปิดเผยรหัสผ่านหรือรหัสยืนยันตัวตนแก่ผู้อื่น

2. การป้องกันอีเมลและข้อความหลอกลวง

ให้บุคลากรสามารถสังเกตอีเมลและข้อความที่มีความผิดปกติ ตรวจสอบผู้ส่ง และหลีกเลี่ยงการเปิดไฟล์หรือลิงก์ที่ไม่น่าเชื่อถือ

3. การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

ให้บุคลากรเข้าใจการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสม รวมถึงการป้องกันการส่งข้อมูลให้บุคคลที่ไม่มีสิทธิ์

4. การใช้งานระบบสารสนเทศอย่างปลอดภัย

ให้บุคลากรปฏิบัติตามแนวทางการใช้งานระบบขององค์กร ไม่ติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต และไม่ใช้บัญชีของบุคคลอื่นเข้าสู่ระบบ

5. การแจ้งเหตุการณ์ผิดปกติ

ให้บุคลากรทราบช่องทางการรายงานเมื่อพบเหตุการณ์ เช่น ระบบทำงานผิดปกติ การได้รับอีเมลต้องสงสัย การสูญหายของอุปกรณ์ หรือการพบความผิดปกติในการเข้าถึงข้อมูล

3.5.5 รูปแบบการจัดกิจกรรมแลกเปลี่ยนเรียนรู้

การจัดกิจกรรมแลกเปลี่ยนเรียนรู้สามารถดำเนินการได้หลายรูปแบบ ดังนี้

1. **การประชุมแลกเปลี่ยนเรียนรู้:** ให้ผู้ดูแลระบบและบุคลากรร่วมแลกเปลี่ยนประสบการณ์ ปัญหา และแนวทางแก้ไข
2. **การอบรมเชิงปฏิบัติการ:** ถ่ายทอดความรู้เกี่ยวกับการป้องกันภัยคุกคามและการใช้งานระบบอย่างปลอดภัย
3. **การจัดทำคู่มือ:** จัดทำเอกสารแสดงขั้นตอนการปฏิบัติงานและแนวทางดูแลระบบ
4. **การสาธิตการปฏิบัติงาน:** ถ่ายทอดวิธีการตรวจสอบระบบ การสำรองข้อมูล และการจัดการเหตุการณ์
5. **การเรียนรู้ผ่านสื่อดิจิทัล:** เผยแพร่บทเรียน สื่อประชาสัมพันธ์ และเอกสารความรู้ผ่านช่องทางออนไลน์
6. **การถอดบทเรียน:** รวบรวมประสบการณ์จากการปฏิบัติงานและจัดทำเป็นแนวปฏิบัติที่สามารถนำไปใช้ซ้ำได้

3.5.6 การประเมินผลการจัดการความรู้และการสร้างความตระหนักรู้

การประเมินผลควรพิจารณาทั้งกระบวนการดำเนินงาน ผลผลิต และผลลัพธ์ เพื่อให้ทราบว่าการจัดการความรู้สามารถสร้างความเข้าใจและส่งเสริมการนำความรู้ไปใช้ในการปฏิบัติงานได้มากน้อยเพียงใด

ตารางที่ 3.8 ตัวชี้วัดการจัดการความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

ประเด็นการประเมิน	ตัวชี้วัด	วิธีการประเมิน	หลักฐาน
การรวบรวมความรู้	จำนวนองค์ความรู้ที่รวบรวม	ตรวจสอบเอกสาร	ทะเบียนองค์ความรู้
การจัดทำคู่มือ	จำนวนคู่มือหรือแนวปฏิบัติ	ตรวจสอบเอกสาร	คู่มือและเอกสาร KM
การแลกเปลี่ยนเรียนรู้	จำนวนกิจกรรมที่ดำเนินการ	ตรวจสอบกิจกรรม	กำหนดการและรายงาน
การมีส่วนร่วม	จำนวนบุคลากรที่เข้าร่วม	ตรวจสอบรายชื่อ	ใบลงทะเบียน
ความรู้ความเข้าใจ	คะแนนความรู้ก่อนและหลังการเรียนรู้	แบบทดสอบ Pre-test/Post-test	ผลการประเมิน
ความตระหนักรู้	ระดับความตระหนักด้าน Cybersecurity	แบบประเมิน	ผลการประเมิน
การนำความรู้ไปใช้	จำนวนหรือสัดส่วนบุคลากรที่นำความรู้ไปใช้	แบบติดตามผลและการสัมภาษณ์	รายงานติดตามผล
การพัฒนาต่อยอด	จำนวนแนวปฏิบัติที่ได้รับการปรับปรุง	ตรวจสอบเอกสาร	รายงานการปรับปรุง

3.5.7 การจัดเก็บองค์ความรู้และการพัฒนาฐานความรู้ขององค์กร

การจัดเก็บองค์ความรู้เป็นขั้นตอนสำคัญในการรักษาองค์ความรู้ขององค์กรให้สามารถนำกลับมาใช้ได้อย่างต่อเนื่อง โดยควรจัดทำระบบจัดเก็บที่มีโครงสร้างชัดเจนและสามารถค้นคืนข้อมูลได้สะดวก

องค์ความรู้ที่ควรจัดเก็บ ได้แก่

1) คู่มือการดูแลระบบสารสนเทศ
2) คู่มือการใช้งาน Firewall
3) เอกสารการดูแลเว็บไซต์และใบรับรองดิจิทัล
4) แนวทางการปรับปรุงและบำรุงรักษา Server
5) ขั้นตอนการสำรองและกู้คืนข้อมูล
6) แนวทางการจัดการบัญชีผู้ใช้งาน
7) แนวทางการป้องกันภัยคุกคามทางไซเบอร์
8) รายงานการตรวจสอบและแก้ไขปัญหา
9) รายงานการแลกเปลี่ยนเรียนรู้และถอดบทเรียน
10) เอกสารการปรับปรุงแนวปฏิบัติด้านความปลอดภัย

การจัดเก็บความรู้ควรมีการกำหนดผู้รับผิดชอบ วันที่จัดทำ วันที่ทบทวน และสถานะของเอกสาร เพื่อให้มั่นใจว่าองค์ความรู้ที่นำไปใช้งานมีความถูกต้องและเป็นปัจจุบัน

3.5.8 การนำองค์ความรู้ไปพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง

การนำองค์ความรู้ไปใช้เป็นขั้นตอนสำคัญของการจัดการความรู้ โดยต้องเชื่อมโยงองค์ความรู้ที่ได้รับจากการแลกเปลี่ยนเรียนรู้เข้ากับการปฏิบัติงานจริง เพื่อให้บุคลากรสามารถนำความรู้ไปใช้ในการดูแลระบบสารสนเทศและป้องกันภัยคุกคามได้อย่างเหมาะสม

แนวทางการดำเนินงานประกอบด้วย

1) นำองค์ความรู้จากผู้ดูแลระบบมาจัดทำเป็นคู่มือและแนวปฏิบัติ
2) นำแนวปฏิบัติไปใช้ในการดูแลเว็บไซต์ ระบบเครือข่าย และ Server
3) ถ่ายทอดความรู้เกี่ยวกับการป้องกันภัยคุกคามให้บุคลากรที่เกี่ยวข้อง
4) ติดตามปัญหาและอุปสรรคจากการนำความรู้ไปใช้
5) รวบรวมข้อเสนอแนะและประสบการณ์จากการปฏิบัติงาน
6) ปรับปรุงองค์ความรู้และเอกสารให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี
7) จัดเก็บองค์ความรู้ไว้เป็นฐานข้อมูลสำหรับการเรียนรู้ขององค์กร

กระบวนการดังกล่าวสอดคล้องกับหลักการปรับปรุงอย่างต่อเนื่องของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตาม ISO/IEC 27001:2022 และแนวทาง NIST CSF 2.0 ซึ่งให้ความสำคัญกับการนำผลการดำเนินงานและบทเรียนที่ได้รับกลับมาใช้ในการพัฒนาระบบบริหารจัดการความเสี่ยงทางไซเบอร์ (ISO, 2022; Pascoe et al., 2024)

สรุป

กระบวนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ประกอบด้วยการสำรวจและวิเคราะห์ระบบสารสนเทศ การประเมินความเสี่ยงและกำหนดมาตรการป้องกัน การพัฒนาระบบป้องกันภัยคุกคาม การตรวจสอบและบำรุงรักษาระบบ ตลอดจนการจัดการความรู้และการสร้างความตระหนักรู้แก่บุคลากร ซึ่งเป็นกระบวนการที่มีความสัมพันธ์และสนับสนุนซึ่งกันและกัน

สำหรับวิทยาลัยชุมชนสตูล การดำเนินงานดังกล่าวเชื่อมโยงกับการดูแลระบบสารสนเทศที่สำคัญ ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server โดยข้อมูลการดำเนินงานในปีงบประมาณ พ.ศ. 2568 แสดงให้เห็นถึงมาตรการด้านเทคนิคที่เกี่ยวข้องกับการใช้ Firewall การใช้ใบรับรอง SSL การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ ส่วนปีงบประมาณ พ.ศ. 2569 มีการเชื่อมโยงการทบทวนองค์ความรู้และแนวปฏิบัติด้านความปลอดภัยเข้ากับกระบวนการจัดการความรู้ขององค์กร

กระบวนการดังกล่าวสามารถใช้เป็นกรอบในการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัย โดยอาศัยการกำกับดูแล การระบุความเสี่ยง การป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟูระบบ ควบคู่กับการพัฒนาความรู้ของบุคลากรและการปรับปรุงมาตรการอย่างต่อเนื่อง เพื่อสนับสนุนการบริหารจัดการและการให้บริการของวิทยาลัยให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพ

บทที่ 4 แนวปฏิบัติที่ดีของวิทยาลัยชุมชนสตูล

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) เป็นส่วนสำคัญของการบริหารจัดการองค์กรในยุคดิจิทัล โดยเฉพาะหน่วยงานทางการศึกษาที่มีการใช้ระบบสารสนเทศเพื่อสนับสนุนการบริหารจัดการ การจัดการเรียนการสอน การบริหารงานบุคคล การจัดเก็บข้อมูล และการให้บริการแก่ผู้เรียนและประชาชน การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจึงต้องดำเนินการอย่างเป็นระบบครอบคลุมทั้งระบบเครือข่าย เว็บไซต์ โปรแกรมประยุกต์ Server และการใช้งานของบุคลากร

วิทยาลัยชุมชนสตูลให้ความสำคัญกับการดูแลและพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย โดยในปีงบประมาณ พ.ศ. 2568 มีการดำเนินมาตรการด้านเทคนิค ได้แก่ การใช้ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก การใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย พร้อมปรับโครงสร้างเมนูให้สามารถเข้าถึงข้อมูลได้สะดวก

ต่อมาในปีงบประมาณ พ.ศ. 2569 วิทยาลัยได้เชื่อมโยงการทบทวนองค์ความรู้และแนวปฏิบัติด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ (Knowledge Management: KM) เพื่อส่งเสริมการถ่ายทอดความรู้และสร้างความตระหนักรู้แก่บุคลากรในการใช้งานระบบสารสนเทศอย่างปลอดภัย

แนวปฏิบัติที่ดีในบทนี้จึงนำเสนอการดำเนินงานตามมาตรการที่มีข้อมูลรองรับ พร้อมอธิบายหลักการทางวิชาการ กระบวนการดำเนินงาน และแนวทางการจัดเก็บหลักฐาน เพื่อให้สามารถนำไปใช้เป็นองค์ความรู้ขององค์กรและเป็นพื้นฐานในการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง

4.1 การรักษาความปลอดภัยระบบเครือข่ายด้วย Firewall

การรักษาความปลอดภัยระบบเครือข่ายเป็นองค์ประกอบพื้นฐานของการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากระบบเครือข่ายเป็นช่องทางเชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ ระบบสารสนเทศ และเครือข่ายภายนอกองค์กร หากไม่มีมาตรการควบคุมที่เหมาะสม อาจทำให้เกิดความเสี่ยงจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต การโจมตีทางเครือข่าย และการนำข้อมูลออกไปใช้โดยมิชอบ

Firewall เป็นกลไกด้านความปลอดภัยที่ทำหน้าที่ควบคุมการรับส่งข้อมูลระหว่างเครือข่ายตามกฎที่กำหนด โดยพิจารณาจากเงื่อนไขต่าง ๆ เช่น หมายเลข IP ต้นทางและปลายทาง หมายเลขพอร์ต โปรโตคอล และลักษณะการเชื่อมต่อ เพื่ออนุญาตหรือปฏิเสธการรับส่งข้อมูลตามนโยบายความปลอดภัยขององค์กร

4.1.1 หลักการรักษาความปลอดภัยระบบเครือข่ายด้วย Firewall

การใช้ Firewall มีหลักการสำคัญคือการควบคุมการเชื่อมต่อเครือข่ายให้เป็นไปตามสิทธิ์และเงื่อนไขที่กำหนด โดยมุ่งลดโอกาสที่บุคคลหรือระบบที่ไม่ได้รับอนุญาตจะเข้าถึงทรัพยากรสารสนเทศขององค์กร

หลักการดำเนินงานประกอบด้วย

1) **การควบคุมการรับส่งข้อมูล:** กำหนดกฎการอนุญาตและปฏิเสธการเชื่อมต่อระหว่างเครือข่ายภายในและภายนอก
2) **การจำกัดการเข้าถึง:** เปิดใช้งานเฉพาะพอร์ตและบริการที่จำเป็นต่อภารกิจขององค์กร
3) **การควบคุมการเชื่อมต่อจากภายนอก:** กำหนดเงื่อนไขการเชื่อมต่อจากเครือข่ายภายนอกให้เหมาะสมกับระดับความเสี่ยง

4) **การตรวจสอบเหตุการณ์:** ตรวจสอบบันทึกการเชื่อมต่อเพื่อค้นหาพฤติกรรมที่ผิดปกติ

5) **การทบทวนกฎความปลอดภัย:** ตรวจสอบและปรับปรุงกฎ Firewall ให้สอดคล้องกับการเปลี่ยนแปลงของระบบเครือข่าย

4.1.2 การดำเนินงานของวิทยาลัยชุมชนสตูล

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีการดำเนินมาตรการด้านเทคนิคโดยใช้ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก ซึ่งเป็นการนำเครื่องมือด้านความปลอดภัยเครือข่ายมาใช้ควบคุมการเชื่อมต่อและลดความเสี่ยงจากการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

การดำเนินงานดังกล่าวเกี่ยวข้องกับการดูแลโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่รองรับการให้บริการระบบงานของวิทยาลัย โดยมีประเด็นสำคัญ ได้แก่

- การใช้ Firewall เป็นกลไกควบคุมการรับส่งข้อมูลเครือข่าย
- การป้องกันการเชื่อมต่อจากแหล่งที่ไม่ได้รับอนุญาตตามกฎที่กำหนด
- การสนับสนุนความปลอดภัยของระบบสารสนเทศที่ให้บริการผ่านเครือข่าย
- การลดความเสี่ยงจากภัยคุกคามที่อาศัยช่องทางการเชื่อมต่อเครือข่าย

4.1.3 กระบวนการดำเนินงานด้านการรักษาความปลอดภัยเครือข่าย

กระบวนการดูแลความปลอดภัยระบบเครือข่ายด้วย Firewall ประกอบด้วยขั้นตอนดังนี้

ขั้นตอนที่ 1 การสำรวจระบบเครือข่าย

ตรวจสอบโครงสร้างเครือข่าย อุปกรณ์ที่เชื่อมต่อ ระบบที่ให้บริการ และช่องทางการรับส่งข้อมูล เพื่อกำหนดขอบเขตการควบคุมความปลอดภัย

ขั้นตอนที่ 2 การกำหนดนโยบายการเชื่อมต่อ

กำหนดกฎการอนุญาตและปฏิเสธการเชื่อมต่อ โดยพิจารณาจากความจำเป็นในการใช้งานและระดับความเสี่ยงของระบบ

ขั้นตอนที่ 3 การใช้ Firewall ควบคุมเครือข่าย

นำ Firewall มาใช้เป็นกลไกควบคุมการรับส่งข้อมูลตามนโยบายที่กำหนด

ขั้นตอนที่ 4 การตรวจสอบการทำงาน

ตรวจสอบสถานะการทำงานของอุปกรณ์และบันทึกเหตุการณ์ เพื่อค้นหาความผิดปกติของการเชื่อมต่อ

ขั้นตอนที่ 5 การทบทวนและปรับปรุง

ทบทวนกฎการควบคุมการเชื่อมต่อเมื่อมีการเปลี่ยนแปลงระบบหรือพบความเสี่ยงใหม่ เพื่อให้มาตรการป้องกันมีความเหมาะสมกับสภาพแวดล้อมขององค์กร

4.1.4 แนวทางการจัดเก็บหลักฐานการดำเนินงาน

หลักฐานที่เกี่ยวข้องกับการใช้ Firewall ประกอบด้วย

1) ภาพถ่ายหรือภาพหน้าจออุปกรณ์ Firewall
2) เอกสารแสดงรายละเอียดการติดตั้งและการกำหนดค่า
3) รายการกฎการอนุญาตและปฏิเสธการเชื่อมต่อ
4) รายงานการตรวจสอบสถานะการทำงาน
5) บันทึกเหตุการณ์การเชื่อมต่อเครือข่าย
6) รายงานการปรับปรุงหรือบำรุงรักษาระบบ

ผลที่เกิดจากการดำเนินงาน: วิทยาลัยมีการนำ Firewall มาใช้เป็นมาตรการป้องกันภัยคุกคามจากภายนอก ซึ่งเป็นองค์ประกอบสำคัญในการควบคุมความปลอดภัยของระบบเครือข่าย และสนับสนุนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ใช้ในการดำเนินงานขององค์กร

4.2 การรักษาความปลอดภัยเว็บไซต์ด้วย SSL

เว็บไซต์เป็นช่องทางสำคัญในการเผยแพร่ข้อมูลข่าวสาร ประชาสัมพันธ์กิจกรรม และให้บริการข้อมูลแก่ผู้เรียน บุคลากร และประชาชนทั่วไป การรักษาความปลอดภัยเว็บไซต์จึงมีความสำคัญต่อการสร้างความน่าเชื่อถือขององค์กร รวมถึงการป้องกันความเสี่ยงจากการดักอ่านหรือเปลี่ยนแปลงข้อมูลระหว่างการรับส่งผ่านเครือข่าย

SSL (Secure Sockets Layer) เป็นชื่อของเทคโนโลยีการเข้ารหัสการสื่อสารที่ใช้ในอดีต ปัจจุบันมีการพัฒนาเป็น TLS (Transport Layer Security) ซึ่งเป็นมาตรฐานที่ใช้รักษาความปลอดภัยในการรับส่งข้อมูลผ่านเครือข่าย โดยเว็บไซต์ที่ใช้ HTTPS จะมีการเข้ารหัสการสื่อสารระหว่างเว็บเบราว์เซอร์ของผู้ใช้งานกับเว็บเซิร์ฟเวอร์

4.2.1 หลักการรักษาความปลอดภัยเว็บไซต์ด้วย SSL/TLS

การใช้ใบรับรองดิจิทัล (Digital Certificate) ร่วมกับโปรโตคอล TLS มีวัตถุประสงค์สำคัญในการรักษาความปลอดภัยของการสื่อสารผ่านเว็บไซต์ ได้แก่

1) **การยืนยันตัวตนของเว็บไซต์ (Authentication):** ใช้ใบรับรองดิจิทัลเพื่อยืนยันตัวตนของเว็บไซต์ตามข้อมูลที่ระบุในใบรับรอง
2) **การรักษาความลับของข้อมูล (Confidentiality):** เข้ารหัสข้อมูลระหว่างการรับส่ง เพื่อป้องกันบุคคลภายนอกดักอ่านข้อมูลได้โดยง่าย
3) **การรักษาความถูกต้องของข้อมูล (Integrity):** ใช้กลไกทางการเข้ารหัสเพื่อตรวจสอบและป้องกันการเปลี่ยนแปลงข้อมูลระหว่างการสื่อสาร

การใช้ HTTPS จึงเป็นมาตรการพื้นฐานที่ช่วยเพิ่มความปลอดภัยในการเข้าถึงเว็บไซต์โดยเฉพาะเว็บไซต์ที่มีการรับส่งข้อมูลหรือให้บริการแก่ผู้ใช้งานผ่านอินเทอร์เน็ต

4.2.2 การดำเนินงานของวิทยาลัยชุมชนสตูล

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีการใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ เป็นมาตรการทางเทคนิคที่มุ่งเพิ่มความปลอดภัยในการรับส่งข้อมูลระหว่างผู้ใช้งานกับเว็บไซต์ของวิทยาลัย

การดำเนินงานดังกล่าวช่วยสนับสนุนการรักษาความปลอดภัยของช่องทางการสื่อสารผ่านเว็บไซต์ โดยมีประเด็นสำคัญ ได้แก่

- การใช้ใบรับรองดิจิทัลสำหรับเว็บไซต์
- การเข้ารหัสข้อมูลระหว่างการเชื่อมต่อ
- การสนับสนุนความน่าเชื่อถือในการเข้าถึงเว็บไซต์
- การลดความเสี่ยงจากการดักอ่านหรือเปลี่ยนแปลงข้อมูลระหว่างการสื่อสาร

การใช้ใบรับรอง SSL เป็นมาตรการด้านการเข้ารหัสการสื่อสาร ไม่ได้หมายความว่าเว็บไซต์ได้รับการป้องกันจากการโจมตีทุกประเภท ดังนั้น การดูแลความปลอดภัยเว็บไซต์ยังจำเป็นต้องดำเนินการควบคู่กับการปรับปรุงซอฟต์แวร์ การควบคุมสิทธิ์ผู้ดูแล และการตรวจสอบช่องโหว่ของเว็บแอปพลิเคชัน

4.2.3 กระบวนการดูแลความปลอดภัยเว็บไซต์ด้วย SSL/TLS

1) ตรวจสอบชื่อโดเมนและระบบเว็บไซต์ที่ต้องการใช้งานใบรับรอง

2) จัดหาและติดตั้งใบรับรองดิจิทัลที่ออกโดยผู้ให้บริการที่เชื่อถือได้
3) กำหนดค่าเว็บเซิร์ฟเวอร์ให้รองรับ HTTPS และ TLS รุ่นที่ปลอดภัย
4) ตรวจสอบความถูกต้องของใบรับรองและการเชื่อมต่อ
5) กำหนดให้ผู้ใช้งานเข้าถึงเว็บไซต์ผ่าน HTTPS
6) ติดตามวันหมดอายุของใบรับรองและต่ออายุให้ทันกำหนด
7) ตรวจสอบการตั้งค่าเว็บไซต์และแก้ไขปัญหาที่เกี่ยวข้อง

4.2.4 แนวทางการจัดเก็บหลักฐาน

หลักฐานประกอบการดำเนินงาน ได้แก่

- รายละเอียดใบรับรองดิจิทัลของเว็บไซต์
- ภาพหน้าจอเว็บไซต์ที่แสดงการเชื่อมต่อ HTTPS
- รายงานผลการตรวจสอบใบรับรอง
- เอกสารการติดตั้งและกำหนดค่า TLS
- หลักฐานการต่ออายุใบรับรอง
- รายงานการตรวจสอบความปลอดภัยเว็บไซต์

ผลที่เกิดจากการดำเนินงาน: วิทยาลัยมีการใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ เป็นมาตรการที่สนับสนุนการรักษาความลับและความถูกต้องของข้อมูลระหว่างการรับส่ง และเพิ่มความน่าเชื่อถือของช่องทางการให้บริการข้อมูลผ่านเว็บไซต์

4.3 การปรับปรุงรหัสโปรแกรมและระบบ Server

Server เป็นองค์ประกอบสำคัญของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ทำหน้าที่รองรับการจัดเก็บ ประมวลผล และให้บริการข้อมูลแก่ระบบสารสนเทศต่าง ๆ ขององค์กร การรักษาความมั่นคงปลอดภัยของ Server จึงมีความสำคัญต่อการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การลดช่องโหว่ของระบบ และการรักษาความพร้อมใช้งานของบริการ

การปรับปรุงรหัสโปรแกรมและระบบ Server เป็นกระบวนการดูแลและพัฒนาระบบให้มีความถูกต้อง เหมาะสม และปลอดภัย โดยครอบคลุมการตรวจสอบรหัสโปรแกรม การแก้ไขข้อบกพร่อง การปรับปรุงซอฟต์แวร์ และการตรวจสอบการทำงานของระบบภายหลังการปรับปรุง

แนวทางดังกล่าวสอดคล้องกับหลักการ Secure Coding Practices ของ OWASP ซึ่งให้ความสำคัญกับการตรวจสอบข้อมูลนำเข้า การควบคุมสิทธิ์ การจัดการข้อผิดพลาด การจัดเก็บบันทึกเหตุการณ์ และการกำหนดค่าระบบให้มีความปลอดภัย (OWASP Foundation, n.d.)

4.3.1 หลักการปรับปรุงรหัสโปรแกรมและระบบ Server

การปรับปรุงรหัสโปรแกรมและระบบ Server ต้องคำนึงถึงองค์ประกอบด้านความปลอดภัยดังนี้

1. การตรวจสอบรหัสโปรแกรม (Code Review)

เป็นกระบวนการตรวจสอบความถูกต้องของรหัสโปรแกรม เพื่อค้นหาข้อผิดพลาด จุดอ่อน และรูปแบบการเขียนโปรแกรมที่อาจก่อให้เกิดช่องโหว่ โดยควรตรวจสอบการรับข้อมูลจากผู้ใช้งาน การประมวลผลข้อมูล การเชื่อมต่อฐานข้อมูล และการจัดการสิทธิ์การเข้าถึง

2. การแก้ไขข้อบกพร่องของโปรแกรม (Code Maintenance)

เป็นการปรับปรุงรหัสโปรแกรมให้สามารถทำงานได้อย่างถูกต้องและมีประสิทธิภาพ รวมถึงการแก้ไขข้อผิดพลาดที่อาจส่งผลกระทบต่อความปลอดภัยและการให้บริการของระบบ

3. การปรับปรุงซอฟต์แวร์ (Software Update)

เป็นการติดตั้งโปรแกรมปรับปรุงของระบบปฏิบัติการ เว็บเซิร์ฟเวอร์ ฐานข้อมูล และซอฟต์แวร์ที่เกี่ยวข้อง เพื่อแก้ไขข้อบกพร่องและลดความเสี่ยงจากช่องโหว่ที่มีการค้นพบ

4. การควบคุมสิทธิ์การเข้าถึง (Access Control)

กำหนดสิทธิ์การเข้าถึง Server ให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยจำกัดการใช้งานบัญชีผู้ดูแลระบบและบัญชีที่มีสิทธิ์สูงเท่าที่จำเป็น

5. การจัดเก็บบันทึกเหตุการณ์ (System Logging)

จัดเก็บข้อมูลการเข้าสู่ระบบ การเปลี่ยนแปลงการตั้งค่า และเหตุการณ์ผิดปกติ เพื่อใช้ตรวจสอบและวิเคราะห์ปัญหาที่เกิดขึ้น

4.3.2 การดำเนินงานของวิทยาลัยชุมชนสตูล

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีการดำเนินงานด้านเทคนิคเกี่ยวกับการปรับปรุงรหัสโปรแกรมของ Server เพื่อพัฒนาระบบและสนับสนุนการดูแลโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศขององค์กร

การดำเนินงานดังกล่าวเป็นส่วนหนึ่งของการดูแลระบบสารสนเทศที่รองรับการบริหารจัดการและการให้บริการของวิทยาลัย โดยมีสาระสำคัญเกี่ยวกับการปรับปรุงองค์ประกอบของระบบให้มีความเหมาะสมต่อการใช้งานและการดูแลรักษาในระยะยาว

การปรับปรุงรหัสโปรแกรมของ Server มีความเกี่ยวข้องกับกระบวนการพัฒนาระบบสารสนเทศในด้านต่าง ๆ ได้แก่

- การตรวจสอบและปรับปรุงรหัสโปรแกรม
- การแก้ไขข้อบกพร่องที่เกี่ยวข้องกับการทำงานของระบบ
- การพัฒนาความเหมาะสมของโปรแกรมที่ทำงานบน Server
- การสนับสนุนการทำงานของระบบสารสนเทศที่เกี่ยวข้อง
- การลดความเสี่ยงจากข้อผิดพลาดของโปรแกรม

ทั้งนี้ ข้อมูลการดำเนินงานที่มีอยู่ระบุการปรับปรุงรหัสโปรแกรมของ Server แต่ยังไม่มีรายละเอียดเชิงเทคนิคเกี่ยวกับจำนวนรายการที่ปรับปรุง ภาษาโปรแกรม เวอร์ชันซอฟต์แวร์ หรือผลการทดสอบช่องโหว่ จึงไม่นำข้อมูลดังกล่าวมาอ้างเป็นผลการตรวจสอบความปลอดภัยเชิงเทคนิค

4.3.3 กระบวนการปรับปรุงรหัสโปรแกรมและระบบ Server

การปรับปรุงระบบควรดำเนินการตามขั้นตอนที่เป็นระบบ ดังนี้

ขั้นตอนที่ 1 การสำรวจและตรวจสอบระบบเดิม

รวบรวมข้อมูลเกี่ยวกับ Server ระบบปฏิบัติการ โปรแกรมประยุกต์ ฐานข้อมูล และซอฟต์แวร์ที่เกี่ยวข้อง รวมถึงตรวจสอบสถานะการทำงานและข้อจำกัดของระบบ

ขั้นตอนที่ 2 การวิเคราะห์ปัญหาและข้อบกพร่อง

ตรวจสอบการทำงานของระบบและรหัสโปรแกรม เพื่อระบุข้อผิดพลาด จุดที่ต้องปรับปรุง และประเด็นที่อาจส่งผลกระทบต่อความปลอดภัย

ขั้นตอนที่ 3 การวางแผนปรับปรุง

กำหนดขอบเขตการปรับปรุง ผู้รับผิดชอบ ระยะเวลา และแนวทางสำรองข้อมูลก่อนดำเนินการ เพื่อป้องกันผลกระทบต่อระบบที่ให้บริการอยู่

ขั้นตอนที่ 4 การดำเนินการปรับปรุง

ดำเนินการแก้ไขรหัสโปรแกรมหรือปรับปรุงองค์ประกอบของระบบตามขอบเขตที่กำหนด โดยควรทดสอบในสภาพแวดล้อมที่เหมาะสมก่อนนำไปใช้งานจริง

ขั้นตอนที่ 5 การทดสอบหลังการปรับปรุง

ตรวจสอบความถูกต้องของโปรแกรม การทำงานของระบบ และความสามารถในการเชื่อมต่อกับระบบที่เกี่ยวข้อง รวมถึงตรวจสอบข้อผิดพลาดที่อาจเกิดขึ้นจากการปรับปรุง

ขั้นตอนที่ 6 การติดตามและจัดเก็บหลักฐาน

บันทึกรายละเอียดการปรับปรุง วันที่ดำเนินการ ผู้รับผิดชอบ ผลการทดสอบ และปัญหาที่พบ เพื่อใช้เป็นข้อมูลสำหรับการตรวจสอบย้อนหลัง

4.3.4 แนวทางการรักษาความปลอดภัยของ Server

เพื่อให้การดูแล Server มีความครอบคลุม ควรกำหนดมาตรการด้านความปลอดภัยเพิ่มเติม ดังนี้

1) ปรับปรุงระบบปฏิบัติการและซอฟต์แวร์ให้เป็นรุ่นที่ได้รับการสนับสนุน
2) กำหนดสิทธิ์การเข้าถึงตามหน้าที่และความจำเป็น
3) ปิดการใช้งานบริการและพอร์ตที่ไม่จำเป็น
4) เปลี่ยนรหัสผ่านเริ่มต้นและใช้การยืนยันตัวตนที่เหมาะสม
5) ตรวจสอบการเข้าสู่ระบบและการใช้งานบัญชีผู้ดูแล
6) สำรองข้อมูลสำคัญอย่างสม่ำเสมอ
7) ตรวจสอบพื้นที่จัดเก็บและทรัพยากรของระบบ
8) จัดเก็บ Log และตรวจสอบเหตุการณ์ผิดปกติ
9) ทดสอบการกู้คืนข้อมูลและระบบตามแผน
10) จัดทำเอกสารประวัติการบำรุงรักษาและการเปลี่ยนแปลงระบบ

4.3.5 แนวทางการจัดเก็บหลักฐานการดำเนินงาน

หลักฐานที่เกี่ยวข้องกับการปรับปรุงรหัสโปรแกรมและระบบ Server ประกอบด้วย

รายการหลักฐาน	รายละเอียด
รายงานการปรับปรุงระบบ	ระบุรายละเอียดและขอบเขตการปรับปรุง
ภาพหน้าจอการดำเนินงาน	แสดงขั้นตอนหรือผลการปรับปรุง
บันทึกการแก้ไขโปรแกรม	แสดงรายการรหัสโปรแกรมที่มีการเปลี่ยนแปลง
รายงานการทดสอบระบบ	แสดงผลการทดสอบหลังการปรับปรุง
รายงานการสำรองข้อมูล	แสดงการจัดทำข้อมูลสำรองก่อนดำเนินงาน
บันทึกการบำรุงรักษา	แสดงวันเวลาและผู้รับผิดชอบ

ผลที่เกิดจากการดำเนินงาน: วิทยาลัยมีการปรับปรุงรหัสโปรแกรมของ Server ในปีงบประมาณ พ.ศ. 2568 ซึ่งเป็นการดำเนินงานด้านการพัฒนาและดูแลระบบสารสนเทศ เพื่อสนับสนุนการทำงานของโครงสร้างพื้นฐานด้านเทคโนโลยีขององค์กร และเป็นส่วนหนึ่งของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

4.4 การพัฒนาเว็บไซต์ให้มีความปลอดภัยและรองรับการใช้งาน

เว็บไซต์เป็นช่องทางการสื่อสารและเผยแพร่ข้อมูลที่สำคัญของสถานศึกษา โดยทำหน้าที่ประชาสัมพันธ์ข่าวสาร กิจกรรม หลักสูตร และข้อมูลการให้บริการแก่ผู้เรียน บุคลากร และประชาชน การพัฒนาเว็บไซต์จึงต้องคำนึงถึงทั้งความปลอดภัยของระบบ ความถูกต้องของข้อมูล ความสะดวกในการเข้าถึง และความสามารถในการแสดงผลบนอุปกรณ์ที่หลากหลาย

การพัฒนาเว็บไซต์ที่มีคุณภาพควรดำเนินการควบคู่กันระหว่างการพัฒนาด้านเทคนิคและการออกแบบประสบการณ์ผู้ใช้งาน (User Experience: UX) โดยให้ความสำคัญกับโครงสร้างข้อมูล การจัดหมวดหมู่เนื้อหา การออกแบบเมนู และการรองรับการใช้งานผ่านอุปกรณ์ที่แตกต่างกัน

4.4.1 หลักการพัฒนาเว็บไซต์ให้มีความปลอดภัย

การพัฒนาเว็บไซต์ให้มีความปลอดภัยต้องพิจารณาองค์ประกอบสำคัญ ดังนี้

1. ความปลอดภัยของระบบเว็บไซต์

ต้องมีการปรับปรุงระบบเว็บไซต์ โปรแกรมประยุกต์ และส่วนประกอบซอฟต์แวร์ให้เหมาะสมกับการใช้งาน รวมถึงตรวจสอบช่องโหว่และกำหนดค่าระบบอย่างปลอดภัย

2. ความปลอดภัยของข้อมูล

ต้องมีมาตรการป้องกันข้อมูลจากการเข้าถึง การเปลี่ยนแปลง หรือการเปิดเผยโดยไม่ได้รับอนุญาต โดยเฉพาะข้อมูลส่วนบุคคลและข้อมูลภายในองค์กร

3. การควบคุมสิทธิ์ผู้ดูแลเว็บไซต์

กำหนดบัญชีผู้ดูแลเว็บไซต์และสิทธิ์การจัดการเนื้อหาให้เหมาะสมกับหน้าที่ของบุคลากร พร้อมตรวจสอบสิทธิ์เมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบ

4. การรักษาความปลอดภัยในการสื่อสาร

ใช้ HTTPS ร่วมกับ TLS เพื่อเข้ารหัสข้อมูลระหว่างผู้ใช้งานกับเว็บไซต์ และลดความเสี่ยงจากการดักอ่านข้อมูลระหว่างการสื่อสาร

5. การตรวจสอบและสำรองข้อมูล

ตรวจสอบการทำงานของเว็บไซต์และจัดให้มีการสำรองข้อมูล เพื่อรองรับการแก้ไขปัญหาและการกู้คืนระบบเมื่อเกิดเหตุการณ์ผิดปกติ

4.4.2 การดำเนินงานของวิทยาลัยชุมชนสตูล

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลมีการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย พร้อมปรับโครงสร้างเมนูเพื่อให้ผู้ใช้งานสามารถเข้าถึงข้อมูลได้สะดวกยิ่งขึ้น

การดำเนินงานดังกล่าวมีความสำคัญต่อการพัฒนาช่องทางการสื่อสารดิจิทัลของวิทยาลัย โดยมุ่งเน้นการปรับปรุงการแสดงผลและโครงสร้างการเข้าถึงข้อมูลให้สอดคล้องกับพฤติกรรมการใช้งานเทคโนโลยีของผู้เรียน บุคลากร และประชาชน

การพัฒนาเว็บไซต์ครอบคลุมประเด็นสำคัญ ได้แก่

1. การรองรับอุปกรณ์ที่หลากหลาย (Responsive Web Design)

เป็นการพัฒนาเว็บไซต์ให้สามารถปรับรูปแบบการแสดงผลตามขนาดหน้าจอของอุปกรณ์ เช่น คอมพิวเตอร์ แท็บเล็ต และโทรศัพท์เคลื่อนที่ เพื่อให้ผู้ใช้งานสามารถอ่านข้อมูลและเข้าถึงบริการได้อย่างเหมาะสม

2. การปรับปรุงโครงสร้างเมนูเว็บไซต์

เป็นการจัดหมวดหมู่ข้อมูลและปรับตำแหน่งเมนูให้มีความชัดเจน ช่วยให้ผู้ใช้งานค้นหาข้อมูลได้สะดวกและลดขั้นตอนในการเข้าถึงเนื้อหาที่ต้องการ

3. การพัฒนาการเข้าถึงข้อมูล

จัดวางเนื้อหาและองค์ประกอบเว็บไซต์ให้เหมาะสมกับลักษณะการใช้งาน โดยคำนึงถึงความชัดเจนของข้อมูลและความสะดวกในการใช้งาน

4. การดูแลความปลอดภัยของเว็บไซต์

เชื่อมโยงการพัฒนาเว็บไซต์กับมาตรการรักษาความปลอดภัย เช่น การใช้ใบรับรองดิจิทัล การควบคุมสิทธิ์ผู้ดูแล และการตรวจสอบระบบเว็บไซต์

4.4.3 กระบวนการพัฒนาเว็บไซต์

การพัฒนาเว็บไซต์สามารถดำเนินการตามขั้นตอนดังนี้

1) **การสำรวจเว็บไซต์เดิม:** ตรวจสอบโครงสร้างเว็บไซต์ เนื้อหา เมนู และการแสดงผลบนอุปกรณ์ต่าง ๆ

2) **การวิเคราะห์ความต้องการ:** ศึกษาความต้องการของผู้ใช้งานและกำหนดรูปแบบการนำเสนอข้อมูล

3) **การออกแบบโครงสร้างเว็บไซต์:** จัดหมวดหมู่ข้อมูล กำหนดเมนู และวางแผนการนำทาง

4) **การพัฒนาและปรับปรุงเว็บไซต์:** ปรับรูปแบบการแสดงผลและโครงสร้างเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย

5) **การตรวจสอบความปลอดภัย:** ตรวจสอบการเชื่อมต่อ HTTPS สิทธิ์ผู้ดูแล และความเหมาะสมของการตั้งค่าระบบ

6) **การทดสอบการใช้งาน:** ทดสอบการแสดงผลและการเข้าถึงข้อมูลผ่านอุปกรณ์ประเภทต่าง ๆ

7) **การเผยแพร่และติดตามผล:** นำเว็บไซต์ที่ปรับปรุงแล้วไปใช้งานและติดตามปัญหาที่เกิดขึ้น

4.4.4 แนวทางการพัฒนาเว็บไซต์ให้มีประสิทธิภาพ

การพัฒนาเว็บไซต์ขององค์กรควรคำนึงถึงองค์ประกอบดังต่อไปนี้

ด้านการพัฒนา	แนวทางดำเนินงาน
ด้านโครงสร้าง	จัดหมวดหมู่ข้อมูลและเมนูให้ชัดเจน
ด้านการแสดงผล	รองรับคอมพิวเตอร์ แท็บเล็ต และโทรศัพท์มือถือ
ด้านความปลอดภัย	ใช้ HTTPS/TLS และควบคุมสิทธิ์ผู้ดูแล
ด้านข้อมูล	ตรวจสอบความถูกต้องและความทันสมัยของเนื้อหา
ด้านการเข้าถึง	ออกแบบให้ผู้ใช้งานค้นหาข้อมูลได้สะดวก
ด้านการบำรุงรักษา	ตรวจสอบและปรับปรุงระบบอย่างต่อเนื่อง

4.4.5 แนวทางการจัดเก็บหลักฐานการดำเนินงาน

หลักฐานที่เกี่ยวข้องกับการพัฒนาเว็บไซต์ ประกอบด้วย

1) ภาพหน้าจอเว็บไซต์ก่อนและหลังการปรับปรุง
2) ภาพหน้าจอเว็บไซต์ที่แสดงผลบนอุปกรณ์ประเภทต่าง ๆ
3) เอกสารแสดงโครงสร้างเมนูและหมวดหมู่ข้อมูล
4) รายงานการพัฒนาและปรับปรุงเว็บไซต์
5) หลักฐานการใช้ใบรับรองดิจิทัล
6) รายงานการทดสอบเว็บไซต์
7) บันทึกการตรวจสอบและบำรุงรักษาระบบ

ผลที่เกิดจากการดำเนินงาน: วิทยาลัยมีการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลายและปรับโครงสร้างเมนูให้เข้าถึงข้อมูลได้สะดวกขึ้น เป็นการพัฒนาช่องทางการสื่อสารและการให้บริการข้อมูลขององค์กร ควบคู่กับมาตรการด้านความปลอดภัยของเว็บไซต์

4.5 การดูแลระบบสารสนเทศที่สำคัญของวิทยาลัย

ระบบสารสนเทศเป็นเครื่องมือสำคัญในการสนับสนุนการบริหารจัดการและการดำเนินงานของวิทยาลัยชุมชนสตูล โดยช่วยให้การจัดเก็บข้อมูล การประมวลผล การติดต่อสื่อสาร และการให้บริการสามารถดำเนินการผ่านระบบดิจิทัลได้อย่างมีประสิทธิภาพ

การดูแลระบบสารสนเทศจึงต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูลและระบบเป็นสำคัญ โดยครอบคลุมการควบคุมสิทธิ์การเข้าถึง การรักษาความถูกต้องของข้อมูล การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการรักษาความพร้อมใช้งานของระบบ

4.5.1 ระบบสารสนเทศที่สำคัญของวิทยาลัยชุมชนสตูล

จากข้อมูลการดำเนินงานของวิทยาลัยชุมชนสตูล มีระบบสารสนเทศสำคัญที่ใช้สนับสนุนภารกิจขององค์กร ดังนี้

1. ระบบ ICCS-PORTAL

เป็นระบบสารสนเทศที่ใช้สนับสนุนการบริหารจัดการและการติดตามผลการดำเนินงานของวิทยาลัย รวมถึงการรวบรวมข้อมูลตัวชี้วัดและผลการดำเนินงานตามภารกิจ การดูแลความปลอดภัยของระบบจึงต้องให้ความสำคัญกับการกำหนดสิทธิ์ผู้ใช้งาน การรักษาความถูกต้องของข้อมูล และการป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

2. ระบบ E-Office

เป็นระบบสารสนเทศที่สนับสนุนการบริหารจัดการเอกสารและการปฏิบัติงานด้านสารบรรณอิเล็กทรอนิกส์ การดูแลระบบต้องคำนึงถึงความลับของเอกสาร การกำหนดสิทธิ์ในการรับและส่งเอกสาร การตรวจสอบประวัติการดำเนินงาน และการจัดเก็บเอกสารให้สามารถเรียกใช้งานได้อย่างเหมาะสม

3. ระบบ E-HR.ICCS

เป็นระบบสารสนเทศที่เกี่ยวข้องกับการบริหารงานบุคคล ซึ่งอาจมีข้อมูลส่วนบุคคลและข้อมูลการปฏิบัติงานของบุคลากร การดูแลระบบจึงต้องให้ความสำคัญกับการจำกัดสิทธิ์การเข้าถึง การรักษาความลับของข้อมูล และการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4. ระบบ SMART ERPG

เป็นระบบสารสนเทศที่ใช้สนับสนุนการบริหารจัดการและการปฏิบัติงานขององค์กร การรักษาความปลอดภัยต้องคำนึงถึงการกำหนดสิทธิ์ตามบทบาทหน้าที่ การตรวจสอบความถูกต้องของข้อมูล และการป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

5. เว็บไซต์วิทยาลัยชุมชนสตูล

เป็นช่องทางเผยแพร่ข้อมูลข่าวสาร ประชาสัมพันธ์กิจกรรม และนำเสนอข้อมูลการดำเนินงานของวิทยาลัยแก่ผู้เรียน บุคลากร และประชาชนทั่วไป การดูแลเว็บไซต์ต้องให้ความสำคัญกับความปลอดภัยของเว็บเซิร์ฟเวอร์ การใช้ HTTPS การควบคุมสิทธิ์ผู้ดูแล และการตรวจสอบความถูกต้องของข้อมูลที่เผยแพร่

6. ระบบ Server

เป็นโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่รองรับการทำงานของระบบต่าง ๆ โดยเกี่ยวข้องกับการจัดเก็บ ประมวลผล และให้บริการข้อมูล การดูแล Server จึงต้องคำนึงถึงความปลอดภัยของระบบปฏิบัติการ ซอฟต์แวร์ การกำหนดสิทธิ์ การสำรองข้อมูล และการตรวจสอบสถานะการทำงาน

4.5.2 แนวทางการดูแลความมั่นคงปลอดภัยของระบบสารสนเทศ

การดูแลระบบสารสนเทศของวิทยาลัยสามารถกำหนดมาตรการตามลักษณะและความสำคัญของระบบ ดังนี้

1. การควบคุมสิทธิ์การเข้าถึงระบบ

กำหนดบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงตามบทบาทหน้าที่ เพื่อให้บุคลากรสามารถใช้งานข้อมูลและระบบได้เท่าที่จำเป็น โดยควรมีการทบทวนสิทธิ์เมื่อมีการเปลี่ยนแปลงหน้าที่หรือสิ้นสุดการปฏิบัติงาน

2. การรักษาความปลอดภัยของข้อมูล

กำหนดมาตรการป้องกันข้อมูลจากการสูญหาย การเปลี่ยนแปลง และการเปิดเผยโดยไม่ได้รับอนุญาต โดยเฉพาะข้อมูลส่วนบุคคล ข้อมูลบุคลากร ข้อมูลนักศึกษา และข้อมูลการบริหารจัดการของวิทยาลัย

3. การรักษาความพร้อมใช้งานของระบบ

ตรวจสอบสถานะการทำงานของระบบและโครงสร้างพื้นฐานที่เกี่ยวข้อง รวมถึงกำหนดแนวทางสำรองข้อมูลและฟื้นฟูระบบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อการให้บริการ

4. การตรวจสอบและติดตามการใช้งาน

จัดเก็บบันทึกการใช้งานและการเปลี่ยนแปลงข้อมูลที่สำคัญ เพื่อสนับสนุนการตรวจสอบย้อนหลังและการวิเคราะห์เหตุการณ์ผิดปกติ

5. การปรับปรุงระบบอย่างต่อเนื่อง

ตรวจสอบและปรับปรุงระบบสารสนเทศให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี ภัยคุกคาม และความต้องการในการใช้งานขององค์กร

4.5.3 ตารางแนวทางการดูแลความปลอดภัยของระบบสารสนเทศ

ตารางที่ 4.1 ระบบสารสนเทศและมาตรการดูแลความมั่นคงปลอดภัยของวิทยาลัยชุมชนสตูล

ระบบสารสนเทศ	ประเด็นสำคัญในการดูแล	แนวทางควบคุมความปลอดภัย
ICCS-PORTAL	ข้อมูลการบริหารและตัวชี้วัด	กำหนดสิทธิ์ ตรวจสอบข้อมูล และจัดเก็บประวัติการใช้งาน
E-Office	เอกสารอิเล็กทรอนิกส์	ควบคุมสิทธิ์การรับส่งและการเข้าถึงเอกสาร
E-HR.ICCS	ข้อมูลบุคลากร	จำกัดสิทธิ์และคุ้มครองข้อมูลส่วนบุคคล
SMART ERPG	ข้อมูลการบริหารจัดการ	กำหนดสิทธิ์และตรวจสอบการเปลี่ยนแปลงข้อมูล
เว็บไซต์วิทยาลัย	ข้อมูลเผยแพร่สาธารณะ	ใช้ HTTPS/TLS และควบคุมสิทธิ์ผู้ดูแลเว็บไซต์
Server	ระบบจัดเก็บและประมวลผลข้อมูล	ปรับปรุงระบบ สำรองข้อมูล และตรวจสอบเหตุการณ์

4.5.4 การกำหนดผู้รับผิดชอบในการดูแลระบบสารสนเทศ

การดูแลระบบสารสนเทศจำเป็นต้องกำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องให้ชัดเจน เพื่อให้การบริหารจัดการและการแก้ไขปัญหาสามารถดำเนินการได้อย่างเป็นระบบ

บทบาทหน้าที่ที่เกี่ยวข้องประกอบด้วย

1) **ผู้บริหาร:** กำหนดนโยบายและสนับสนุนทรัพยากรสำหรับการรักษาความมั่นคงปลอดภัยทางไซเบอร์
2) **ผู้ดูแลระบบสารสนเทศ:** ดูแลการทำงานของระบบ ตรวจสอบความผิดปกติ และดำเนินการบำรุงรักษาตามหน้าที่
3) **ผู้รับผิดชอบระบบงาน:** ดูแลข้อมูลและสิทธิ์การใช้งานตามภารกิจของระบบ
4) **บุคลากรผู้ใช้งาน:** ปฏิบัติตามแนวทางการใช้งานระบบสารสนเทศอย่างปลอดภัย และแจ้งเหตุเมื่อพบความผิดปกติ
5) **หน่วยงานที่เกี่ยวข้องกับการคุ้มครองข้อมูล:** สนับสนุนการดำเนินงานด้านข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมายที่เกี่ยวข้อง

4.5.5 การติดตามและประเมินผลการดูแลระบบสารสนเทศ

การติดตามและประเมินผลเป็นกระบวนการตรวจสอบว่ามาตรการรักษาความปลอดภัยที่กำหนดไว้ได้รับการนำไปใช้และสามารถสนับสนุนการดำเนินงานขององค์กรได้อย่างเหมาะสมหรือไม่ โดยสามารถกำหนดตัวชี้วัดได้ดังนี้

ประเด็นการประเมิน	ตัวชี้วัด	หลักฐาน
การควบคุมสิทธิ์	มีการทบทวนบัญชีผู้ใช้งานตามรอบที่กำหนด	ทะเบียนบัญชีผู้ใช้งาน
การดูแลระบบ	มีการตรวจสอบและบำรุงรักษาระบบ	รายงานการตรวจสอบ
การสำรองข้อมูล	มีการสำรองข้อมูลตามแผน	รายงาน Backup
การรักษาความปลอดภัยเว็บไซต์	สถานะใบรับรองและ HTTPS	รายงานตรวจสอบเว็บไซต์
การจัดการเหตุการณ์	มีการบันทึกและรายงานเหตุการณ์	รายงาน Incident
การปรับปรุงระบบ	มีการบันทึกการแก้ไขและปรับปรุง	เอกสารการดำเนินงาน

4.6 การถ่ายทอดและแลกเปลี่ยนองค์ความรู้ด้าน Cybersecurity

การจัดการความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นกระบวนการรวบรวม ประมวลผล จัดระบบ ถ่ายทอด และนำองค์ความรู้ไปประยุกต์ใช้ในการปฏิบัติงาน เพื่อให้บุคลากรมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ สามารถใช้งานระบบสารสนเทศได้อย่างปลอดภัย และมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยขององค์กร

การถ่ายทอดและแลกเปลี่ยนองค์ความรู้มีความสำคัญต่อการพัฒนาความสามารถของบุคลากร เนื่องจากการรักษาความปลอดภัยทางไซเบอร์ไม่ได้ขึ้นอยู่กับเทคโนโลยีเพียงอย่างเดียว แต่ยังเกี่ยวข้องกับความรู้ ทักษะ และพฤติกรรมของผู้ใช้งานระบบสารสนเทศ

4.6.1 การดำเนินงานด้านการจัดการความรู้ของวิทยาลัยชุมชนสตูล

ในปีงบประมาณ พ.ศ. 2569 วิทยาลัยชุมชนสตูลมีการเชื่อมโยงการทบทวนองค์ความรู้และแนวปฏิบัติด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ขององค์กร เพื่อส่งเสริมให้เกิดการรวบรวมและถ่ายทอดความรู้จากการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

การดำเนินงานดังกล่าวครอบคลุมประเด็นสำคัญ ได้แก่

1) การรวบรวมองค์ความรู้เกี่ยวกับการดูแลระบบสารสนเทศ
2) การทบทวนแนวทางการรักษาความปลอดภัยเว็บไซต์
3) การรวบรวมความรู้เกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์
4) การจัดระบบองค์ความรู้เพื่อให้สามารถนำไปใช้ประโยชน์ได้
5) การส่งเสริมการถ่ายทอดความรู้และประสบการณ์ระหว่างบุคลากร
6) การนำองค์ความรู้ไปใช้ประกอบการพัฒนาแนวปฏิบัติด้านความปลอดภัยขององค์กร

4.6.2 การรวบรวมองค์ความรู้จากการปฏิบัติงาน

การรวบรวมองค์ความรู้เป็นกระบวนการสำคัญที่ช่วยนำประสบการณ์จากผู้ดูแลระบบและผู้ปฏิบัติงานมาจัดทำเป็นองค์ความรู้ที่สามารถถ่ายทอดและนำกลับมาใช้ได้
องค์ความรู้ที่เกี่ยวข้องกับการดำเนินงานของวิทยาลัยประกอบด้วย

1. องค์ความรู้ด้านการดูแลระบบเครือข่าย

ครอบคลุมหลักการใช้ Firewall การควบคุมการรับส่งข้อมูล การตรวจสอบการเชื่อมต่อ และการดูแลอุปกรณ์เครือข่าย

2. องค์ความรู้ด้านการรักษาความปลอดภัยเว็บไซต์

ครอบคลุมการใช้ใบรับรองดิจิทัล การเข้ารหัสข้อมูลผ่าน HTTPS/TLS การดูแลบัญชีผู้ดูแลเว็บไซต์ และการตรวจสอบความผิดปกติของเว็บไซต์

3. องค์ความรู้ด้านการดูแล Server

ครอบคลุมการปรับปรุงรหัสโปรแกรม การบำรุงรักษาระบบ การตรวจสอบการทำงาน และการจัดการปัญหาทางเทคนิค

4. องค์ความรู้ด้านการบริหารจัดการข้อมูล

ครอบคลุมการควบคุมสิทธิ์ การรักษาความลับของข้อมูล การจัดเก็บข้อมูล และการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

5. องค์ความรู้ด้านการป้องกันภัยคุกคามทางไซเบอร์

ครอบคลุมการป้องกันมัลแวร์ การหลอกลวงทางอิเล็กทรอนิกส์ การโจมตีเว็บไซต์ และการรายงานเหตุการณ์ผิดปกติ

4.6.3 การเปลี่ยนความรู้จากประสบการณ์สู่แนวปฏิบัติที่เป็นเอกสาร

การจัดการความรู้ด้าน Cybersecurity สามารถประยุกต์ใช้แนวคิดการเปลี่ยนผ่านความรู้จากความรู้ที่ฝังอยู่ในตัวบุคคล (Tacit Knowledge) ไปสู่ความรู้ที่ชัดแจ้ง (Explicit Knowledge) โดยรวบรวมประสบการณ์จากการปฏิบัติงานและจัดทำเป็นเอกสารที่สามารถนำไปใช้ได้

กระบวนการดังกล่าวประกอบด้วย

1) **การรวบรวมประสบการณ์:** สัมภาษณ์หรือแลกเปลี่ยนความรู้กับผู้ดูแลระบบและผู้ปฏิบัติงานที่เกี่ยวข้อง
2) **การวิเคราะห์องค์ความรู้:** จำแนกประเด็นความรู้และตรวจสอบความถูกต้องของข้อมูล
3) **การเรียบเรียงความรู้:** จัดทำเอกสาร คู่มือ และขั้นตอนการปฏิบัติงาน
4) **การตรวจสอบความถูกต้อง:** ทบทวนเนื้อหาโดยผู้มีความรู้หรือผู้รับผิดชอบระบบ
5) **การเผยแพร่ความรู้:** จัดให้มีช่องทางเผยแพร่เอกสารและคู่มือแก่บุคลากร
6) **การนำไปใช้:** นำองค์ความรู้ไปประกอบการดูแลระบบและการปฏิบัติงาน
7) **การปรับปรุงองค์ความรู้:** ทบทวนเนื้อหาให้สอดคล้องกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลง

กระบวนการดังกล่าวสอดคล้องกับแนวคิดการสร้างองค์ความรู้ของ Nonaka และ Takeuchi (1995) ซึ่งอธิบายการเปลี่ยนผ่านระหว่างความรู้ที่ฝังอยู่ในตัวบุคคลและความรู้ที่ชัดแจ้งผ่านกระบวนการทางสังคมและการเรียนรู้ขององค์กร

4.6.4 การถ่ายทอดและแลกเปลี่ยนองค์ความรู้แก่บุคลากร

การถ่ายทอดองค์ความรู้เป็นกระบวนการส่งเสริมให้บุคลากรสามารถนำความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ไปใช้ในการปฏิบัติงาน โดยสามารถดำเนินการผ่านรูปแบบต่าง ๆ ดังนี้

1. การประชุมแลกเปลี่ยนเรียนรู้

เป็นการเปิดโอกาสให้ผู้ดูแลระบบและบุคลากรที่เกี่ยวข้องแลกเปลี่ยนประสบการณ์ ปัญหาที่พบ และแนวทางการแก้ไขปัญหาด้านความปลอดภัย

2. การจัดอบรมให้ความรู้

เป็นการพัฒนาความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การใช้งานระบบอย่างปลอดภัย และการป้องกันความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ

3. การจัดทำคู่มือและเอกสารแนวปฏิบัติ

เป็นการรวบรวมองค์ความรู้ให้เป็นเอกสารที่บุคลากรสามารถศึกษาและใช้เป็นแนวทางในการปฏิบัติงานได้

4. การสาธิตขั้นตอนการปฏิบัติงาน

เป็นการถ่ายทอดความรู้ผ่านการสาธิตการดูแลระบบ การตรวจสอบเว็บไซต์ การใช้ระบบเครือข่าย และการดำเนินการเมื่อพบเหตุการณ์ผิดปกติ

5. การเผยแพร่ความรู้ผ่านช่องทางดิจิทัล

เป็นการจัดเก็บและเผยแพร่เอกสารหรือสื่อความรู้ผ่านระบบออนไลน์ขององค์กร เพื่อให้บุคลากรสามารถเข้าถึงได้ตามความจำเป็น

4.6.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การสร้างความตระหนักรู้เป็นส่วนหนึ่งของการพัฒนาศักยภาพบุคลากร โดยมุ่งให้บุคลากรสามารถรับรู้ความเสี่ยงและเลือกปฏิบัติได้อย่างเหมาะสมเมื่อใช้งานระบบสารสนเทศ

ประเด็นที่ควรส่งเสริมความรู้ ได้แก่

ประเด็นความรู้	เนื้อหาที่ต้องถ่ายทอด
การรักษาความปลอดภัยรหัสผ่าน	การตั้งรหัสผ่านที่ปลอดภัยและไม่เปิดเผยข้อมูลยืนยันตัวตน
การป้องกัน Phishing	การตรวจสอบอีเมล ลิงก์ และข้อความหลอกลวง
การคุ้มครองข้อมูลส่วนบุคคล	การเก็บ ใช้ และเปิดเผยข้อมูลตามวัตถุประสงค์และกฎหมาย
การใช้งานเว็บไซต์	การตรวจสอบความน่าเชื่อถือของเว็บไซต์และการเชื่อมต่อ
การใช้งานอุปกรณ์	การป้องกันมัลแวร์และการใช้ซอฟต์แวร์อย่างปลอดภัย
การรายงานเหตุการณ์	การแจ้งผู้รับผิดชอบเมื่อพบความผิดปกติของระบบ

4.6.6 การจัดเก็บและเผยแพร่องค์ความรู้ขององค์กร

การจัดเก็บองค์ความรู้ด้าน Cybersecurity ควรดำเนินการอย่างเป็นระบบ เพื่อให้สามารถค้นหา ตรวจสอบ และนำกลับมาใช้ประโยชน์ได้ โดยองค์ความรู้ที่ควรจัดเก็บประกอบด้วย

1) คู่มือการดูแลระบบเครือข่ายและ Firewall
2) คู่มือการดูแลเว็บไซต์และใบรับรองดิจิทัล
3) แนวทางการปรับปรุงรหัสโปรแกรมและ Server
4) แนวปฏิบัติการใช้งานระบบสารสนเทศอย่างปลอดภัย
5) คู่มือการสำรองและกู้คืนข้อมูล
6) แนวทางการป้องกันภัยคุกคามทางไซเบอร์
7) รายงานการแลกเปลี่ยนเรียนรู้
8) เอกสารการถอดบทเรียนจากการปฏิบัติงาน

การเผยแพร่องค์ความรู้ต้องคำนึงถึงระดับความลับของข้อมูล โดยเอกสารที่มีรายละเอียดการตั้งค่าระบบ รหัสผ่าน หมายเลขเครือข่าย หรือข้อมูลที่อาจกระทบต่อความปลอดภัยขององค์กร ต้องจำกัดสิทธิ์การเข้าถึงเฉพาะผู้เกี่ยวข้อง

4.6.7 การติดตามและประเมินผลการจัดการความรู้

การติดตามและประเมินผลการจัดการความรู้เป็นกระบวนการตรวจสอบการดำเนินงานและผลที่เกิดจากการถ่ายทอดองค์ความรู้ โดยพิจารณาทั้งผลผลิตและผลลัพธ์ ดังนี้

ตารางที่ 4.2 ตัวชี้วัดการถ่ายทอดและแลกเปลี่ยนองค์ความรู้ด้าน Cybersecurity

ด้านการประเมิน	ตัวชี้วัด	วิธีการประเมิน
การรวบรวมองค์ความรู้	จำนวนองค์ความรู้ที่รวบรวม	ตรวจสอบเอกสาร
การจัดทำคู่มือ	จำนวนคู่มือหรือแนวปฏิบัติ	ตรวจสอบผลงาน

ด้านการประเมิน	ตัวชี้วัด	วิธีการประเมิน
การแลกเปลี่ยนเรียนรู้	จำนวนกิจกรรมที่จัดขึ้น	ตรวจสอบรายงานกิจกรรม
การมีส่วนร่วม	จำนวนบุคลากรที่เข้าร่วม	ตรวจสอบรายชื่อ
ความรู้ความเข้าใจ	คะแนนความรู้ก่อนและหลังการเรียนรู้	แบบทดสอบ
ความตระหนักรู้	ระดับความตระหนักด้านความปลอดภัย	แบบประเมิน
การนำความรู้ไปใช้	จำนวนบุคลากรที่นำความรู้ไปประยุกต์ใช้	แบบติดตามผล
การพัฒนาต่อยอด	จำนวนองค์ความรู้ที่ได้รับการปรับปรุง	ตรวจสอบเอกสาร KM

4.6.8 การพัฒนาต่อยอดองค์ความรู้ด้าน Cybersecurity

การพัฒนาต่อยอดองค์ความรู้เป็นกระบวนการนำผลจากการแลกเปลี่ยนเรียนรู้และประสบการณ์การปฏิบัติงานมาใช้ปรับปรุงแนวทางการดูแลระบบสารสนเทศให้มีความเหมาะสมกับบริบทขององค์กร โดยสามารถดำเนินการได้ดังนี้

1) ทบทวนองค์ความรู้และแนวปฏิบัติให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลง
2) ปรับปรุงคู่มือและเอกสารการปฏิบัติงานให้เป็นปัจจุบัน
3) พัฒนาฐานข้อมูลองค์ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์
4) ส่งเสริมการแลกเปลี่ยนความรู้ระหว่างผู้ดูแลระบบและบุคลากร
5) นำผลการประเมินความรู้ไปใช้วางแผนพัฒนาบุคลากร
6) เชื่อมโยงองค์ความรู้กับการดูแลระบบสารสนเทศของวิทยาลัย
7) ติดตามผลการนำความรู้ไปใช้และนำผลมาปรับปรุงการดำเนินงาน

ผลที่เกิดจากการดำเนินงาน: วิทยาลัยชุมชนสตูลได้นำประเด็นการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์มาเชื่อมโยงกับกระบวนการจัดการความรู้ในปีงบประมาณ พ.ศ. 2569 เพื่อเป็นแนวทางในการรวบรวม ทบทวน และถ่ายทอดองค์ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

สรุปแนวปฏิบัติที่ดีของวิทยาลัยชุมชนสตูล

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูลสามารถสรุปแนวปฏิบัติที่สำคัญได้ 6 ด้าน ดังนี้

ตารางที่ 4.3 สรุปแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยทางไซเบอร์

แนวปฏิบัติ	การดำเนินงาน	ปีงบประมาณ
1. การรักษาความปลอดภัยระบบเครือข่าย	ใช้ Firewall ป้องกันภัยคุกคามจากภายนอก	2568
2. การรักษาความปลอดภัยเว็บไซต์	ใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสาร	2568
3. การปรับปรุงระบบ Server	ปรับปรุงรหัสโปรแกรมของ Server	2568
4. การพัฒนาเว็บไซต์	รองรับอุปกรณ์หลากหลายและปรับโครงสร้างเมนู	2568

แนวปฏิบัติ	การดำเนินงาน	ปีงบประมาณ
5. การดูแลระบบสารสนเทศ	ดูแลระบบ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server	ต่อเนื่อง
6. การจัดการความรู้	ทบทวนและเชื่อมโยงองค์ความรู้ด้าน Cybersecurity กับกระบวนการ KM	2569

การดำเนินงานทั้ง 6 ด้านสะท้อนให้เห็นถึงการเชื่อมโยงมาตรการด้านเทคนิคเข้ากับการบริหารจัดการระบบสารสนเทศและการพัฒนาความรู้ของบุคลากร โดยมาตรการด้าน Firewall, SSL การปรับปรุง Server และการพัฒนาเว็บไซต์ เป็นการดำเนินงานที่มีข้อมูลรองรับในปีงบประมาณ พ.ศ. 2568 ขณะที่การจัดการความรู้ในปีงบประมาณ พ.ศ. 2569 เป็นการนำองค์ความรู้ด้านการดูแลระบบและการป้องกันภัยคุกคามมาเชื่อมโยงกับการเรียนรู้ขององค์กร

แนวปฏิบัติดังกล่าวสามารถใช้เป็นพื้นฐานในการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยให้มีความเป็นระบบและต่อเนื่อง โดยเชื่อมโยงกับกรอบ NIST Cybersecurity Framework 2.0 ซึ่งประกอบด้วยการกำกับดูแล การระบุความเสี่ยง การป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟูระบบ ตลอดจนการปรับปรุงแนวทางดำเนินงานให้สอดคล้องกับบริบทขององค์กร

บทที่ 5 ผลการดำเนินงานและผลลัพธ์

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ของวิทยาลัยชุมชนสตูลเป็นการพัฒนาระบบสารสนเทศและโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลให้มีความมั่นคงปลอดภัย รองรับการบริหารจัดการ การปฏิบัติงาน และการให้บริการทางการศึกษา โดยให้ความสำคัญกับการป้องกันภัยคุกคามจากภายนอก การรักษาความปลอดภัยของเว็บไซต์ การปรับปรุงระบบ Server และการพัฒนาช่องทางการเผยแพร่ข้อมูลขององค์กร

การดำเนินงานครอบคลุมปีงบประมาณ พ.ศ. 2568–2569 โดยในปีงบประมาณ พ.ศ. 2568 วิทยาลัยมีการดำเนินมาตรการด้านเทคนิค ได้แก่ การใช้ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก การใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย พร้อมปรับโครงสร้างเมนูให้เข้าถึงข้อมูลได้สะดวก

สำหรับปีงบประมาณ พ.ศ. 2569 วิทยาลัยได้เชื่อมโยงการทบทวนองค์ความรู้และแนวปฏิบัติด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ขององค์กร เพื่อส่งเสริมการรวบรวม ถ่ายทอด และประยุกต์ใช้ความรู้ในการดูแลระบบสารสนเทศอย่างปลอดภัย

การนำเสนอผลการดำเนินงานในบทนี้แบ่งออกเป็นผลการดำเนินงานตามปีงบประมาณ ผลลัพธ์ด้านความปลอดภัยของระบบสารสนเทศ ผลลัพธ์ด้านการบริหารจัดการและการให้บริการ และผลลัพธ์ด้านความรู้และความตระหนักของบุคลากร โดยแยกข้อมูลการดำเนินงานที่มีหลักฐานรองรับออกจากผลลัพธ์ที่ต้องอาศัยการตรวจวัดเพิ่มเติม เพื่อให้การรายงานมีความถูกต้องและสามารถตรวจสอบได้

5.1 ผลการดำเนินงานในปีงบประมาณ พ.ศ. 2568

ในปีงบประมาณ พ.ศ. 2568 วิทยาลัยชุมชนสตูลดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมุ่งเน้นการพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศที่ใช้สนับสนุนการบริหารจัดการและการให้บริการขององค์กร ครอบคลุมการรักษาความปลอดภัยระบบเครือข่าย เว็บไซต์ และ Server รวมถึงการพัฒนารูปแบบเว็บไซต์ให้เหมาะสมกับการใช้งานผ่านอุปกรณ์ที่หลากหลาย

การดำเนินงานดังกล่าวเป็นการนำมาตรการด้านเทคนิคมาใช้ในการดูแลระบบสารสนเทศ โดยมีรายละเอียดดังนี้

5.1.1 การใช้ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก

วิทยาลัยดำเนินการใช้ Firewall เป็นเครื่องมือในการรักษาความปลอดภัยระบบเครือข่าย เพื่อควบคุมการรับส่งข้อมูลและป้องกันภัยคุกคามจากเครือข่ายภายนอก โดย Firewall ทำหน้าที่ตรวจสอบและควบคุมการเชื่อมต่อตามกฎที่กำหนด ช่วยจำกัดการเข้าถึงระบบจากแหล่งที่ไม่ได้รับอนุญาตตามนโยบายความปลอดภัย

การดำเนินงานดังกล่าวเป็นมาตรการป้องกันในระดับโครงสร้างพื้นฐานเครือข่าย ซึ่งมีความสำคัญต่อการรักษาความปลอดภัยของระบบสารสนเทศที่เชื่อมต่อกับเครือข่ายภายในและอินเทอร์เน็ต ผลการดำเนินงานที่สามารถระบุได้ ได้แก่

- มีการนำ Firewall มาใช้เป็นมาตรการป้องกันภัยคุกคามจากภายนอก
- มีเครื่องมือควบคุมการเชื่อมต่อเครือข่ายตามหลักการรักษาความปลอดภัยสารสนเทศ
- สนับสนุนการดูแลระบบเครือข่ายที่รองรับการทำงานของระบบสารสนเทศของวิทยาลัย

5.1.2 การใช้ใบรับรอง SSL เพื่อรักษาความปลอดภัยเว็บไซต์

วิทยาลัยดำเนินการใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ เป็นมาตรการที่ช่วยรักษาความปลอดภัยในการรับส่งข้อมูลระหว่างผู้ใช้งานกับเว็บเซิร์ฟเวอร์ โดยใช้การเชื่อมต่อผ่าน HTTPS ซึ่งอาศัยโปรโตคอล TLS ในการเข้ารหัสข้อมูล

การดำเนินงานดังกล่าวมีส่วนสนับสนุนการรักษาความลับและความถูกต้องของข้อมูลระหว่างการสื่อสาร รวมถึงช่วยเพิ่มความน่าเชื่อถือในการเข้าถึงเว็บไซต์ของวิทยาลัย

ผลการดำเนินงานที่สามารถระบุได้ ได้แก่

- มีการใช้ใบรับรอง SSL สำหรับการสื่อสารผ่านเว็บไซต์
- สนับสนุนการเข้ารหัสข้อมูลระหว่างผู้ใช้งานกับเว็บไซต์
- เพิ่มความปลอดภัยของช่องทางการเข้าถึงข้อมูลผ่านเว็บไซต์

5.1.3 การปรับปรุงรหัสโปรแกรมของ Serverวิทยาลัยดำเนินการปรับปรุงรหัสโปรแกรมของ Server เพื่อพัฒนาระบบและดูแลโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้เหมาะสมต่อการใช้งาน โดยการปรับปรุงรหัสโปรแกรมเป็นส่วนหนึ่งของการบำรุงรักษาระบบและการพัฒนาความสามารถในการให้บริการของ Server

การดำเนินงานดังกล่าวเกี่ยวข้องกับการดูแลส่วนประกอบทางเทคนิคที่รองรับระบบสารสนเทศขององค์กร และเป็นพื้นฐานสำหรับการปรับปรุงระบบให้สามารถรองรับความต้องการในการใช้งานได้อย่างเหมาะสม

ผลการดำเนินงานที่สามารถระบุได้ ได้แก่

- มีการปรับปรุงรหัสโปรแกรมของ Server
- มีการดำเนินงานด้านการพัฒนาระบบสารสนเทศในระดับโครงสร้างพื้นฐาน
- สนับสนุนการดูแลและปรับปรุงระบบที่ใช้รองรับภารกิจของวิทยาลัย

5.1.4 การพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลายและปรับโครงสร้างเมนู

วิทยาลัยดำเนินการพัฒนาเว็บไซต์ให้รองรับการใช้งานผ่านอุปกรณ์หลากหลายประเภท พร้อมปรับปรุงโครงสร้างเมนูเพื่อให้ผู้ใช้งานสามารถเข้าถึงข้อมูลได้สะดวกยิ่งขึ้น

การพัฒนาเว็บไซต์ในลักษณะดังกล่าวเกี่ยวข้องกับการปรับปรุงการแสดงผลและการจัดโครงสร้างข้อมูล โดยคำนึงถึงความสะดวกในการใช้งานผ่านคอมพิวเตอร์ แท็บเล็ต และโทรศัพท์เคลื่อนที่ ซึ่งเป็นอุปกรณ์ที่มีบทบาทสำคัญต่อการเข้าถึงข้อมูลข่าวสารในปัจจุบัน

ผลการดำเนินงานที่สามารถระบุได้ ได้แก่

- มีการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย
- มีการปรับโครงสร้างเมนูเพื่อเพิ่มความสะดวกในการเข้าถึงข้อมูล
- สนับสนุนการเผยแพร่ข้อมูลข่าวสารและการประชาสัมพันธ์ของวิทยาลัยผ่านช่องทางดิจิทัล

5.1.5 สรุปผลการดำเนินงานในปีงบประมาณ พ.ศ. 2568

ตารางที่ 5.1 สรุปผลการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ ปีงบประมาณ พ.ศ. 2568

ลำดับ	ด้านการดำเนินงาน	ผลการดำเนินงาน	ประเด็นที่สนับสนุน
1	ระบบเครือข่าย	ใช้ Firewall	การป้องกันภัยคุกคามจากภายนอก
2	เว็บไซต์	ใช้ใบรับรอง SSL	การเข้ารหัสการสื่อสาร

ลำดับ	ด้านการดำเนินงาน	ผลการดำเนินงาน	ประเด็นที่สนับสนุน
3	Server	ปรับปรุงรหัสโปรแกรม	การพัฒนาและดูแลระบบ
4	เว็บไซต์	พัฒนาให้รองรับอุปกรณ์หลากหลาย	การเพิ่มความสะดวกในการเข้าถึงข้อมูล
5	โครงสร้างเว็บไซต์	ปรับปรุงเมนูและการจัดหมวดหมู่	การพัฒนาการให้บริการข้อมูล

จากผลการดำเนินงานพบว่า วิทยาลัยมีการดำเนินมาตรการด้านเทคนิคที่ครอบคลุมทั้งการป้องกันระบบเครือข่าย การเข้ารหัสการสื่อสาร การปรับปรุง Server และการพัฒนาเว็บไซต์ ซึ่งเป็นองค์ประกอบสำคัญในการดูแลระบบสารสนเทศขององค์กร ทั้งนี้ การประเมินประสิทธิผลของมาตรการดังกล่าวในเชิงปริมาณจำเป็นต้องใช้หลักฐานเพิ่มเติม เช่น รายงานการตรวจสอบระบบ บันทึกเหตุการณ์ และผลการทดสอบหลังการปรับปรุง

5.2 ผลการพัฒนาและปรับปรุงในปีงบประมาณ พ.ศ. 2569

ในปีงบประมาณ พ.ศ. 2569 วิทยาลัยชุมชนสตูลให้ความสำคัญกับการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ผ่านกระบวนการจัดการความรู้ (Knowledge Management: KM) โดยเชื่อมโยงองค์ความรู้จากการดูแลระบบสารสนเทศ การพัฒนาเว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับการพัฒนาความรู้ของบุคลากร เพื่อให้เกิดการรวบรวมและถ่ายทอดองค์ความรู้ที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

การดำเนินงานในปีงบประมาณนี้มีลักษณะเป็นการทบทวนและพัฒนาองค์ความรู้จากประสบการณ์การดำเนินงานที่ผ่านมา โดยมุ่งเน้นให้ความรู้ด้านความปลอดภัยสามารถนำไปใช้ในการดูแลระบบสารสนเทศของวิทยาลัยได้อย่างเหมาะสม และเป็นพื้นฐานสำหรับการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ในระยะต่อไป

5.2.1 การทบทวนองค์ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

วิทยาลัยดำเนินการเชื่อมโยงการทบทวนองค์ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ขององค์กร โดยให้ความสำคัญกับความรู้ที่เกี่ยวข้องกับการดูแลข้อมูล การรักษาความปลอดภัยเว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์

ประเด็นองค์ความรู้ที่นำมาทบทวนประกอบด้วย

1) ความรู้เกี่ยวกับการดูแลระบบเครือข่ายและการป้องกันภัยคุกคามจากภายนอก
2) ความรู้เกี่ยวกับการใช้ใบรับรอง SSL และการรักษาความปลอดภัยเว็บไซต์
3) ความรู้เกี่ยวกับการปรับปรุงและดูแลระบบ Server
4) ความรู้เกี่ยวกับการควบคุมการเข้าถึงระบบสารสนเทศ
5) ความรู้เกี่ยวกับการรักษาความปลอดภัยของข้อมูลและการป้องกันการเปิดเผยข้อมูล
6) ความรู้เกี่ยวกับการใช้งานระบบสารสนเทศอย่างปลอดภัย

การทบทวนองค์ความรู้ดังกล่าวเป็นกระบวนการนำความรู้ที่เกี่ยวข้องกับการปฏิบัติงานมาจัดระบบ เพื่อให้สามารถถ่ายทอดและนำไปใช้ในการดูแลระบบสารสนเทศของวิทยาลัยได้

5.2.2 การเชื่อมโยงองค์ความรู้กับระบบสารสนเทศของวิทยาลัย

การพัฒนาองค์ความรู้ด้าน Cybersecurity มีความเชื่อมโยงกับระบบสารสนเทศที่วิทยาลัยใช้ในการบริหารจัดการและปฏิบัติงาน ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server โดยแต่ละระบบมีลักษณะการใช้งานและประเภทข้อมูลที่แตกต่างกัน

การเชื่อมโยงองค์ความรู้กับระบบสารสนเทศมีสาระสำคัญดังนี้

ตารางที่ 5.2 การเชื่อมโยงองค์ความรู้ด้าน Cybersecurity กับระบบสารสนเทศของวิทยาลัย

ระบบสารสนเทศ	ประเด็นองค์ความรู้ที่เกี่ยวข้อง	แนวทางการประยุกต์ใช้
ICCS-PORTAL	การรักษาความถูกต้องและความปลอดภัยของข้อมูล	การกำหนดสิทธิ์และตรวจสอบข้อมูล
E-Office	การรักษาความปลอดภัยเอกสารอิเล็กทรอนิกส์	การควบคุมการเข้าถึงและการเผยแพร่เอกสาร
E-HR.ICCS	การคุ้มครองข้อมูลบุคลากร	การจำกัดสิทธิ์และรักษาความลับของข้อมูล
SMART ERPG	การควบคุมการเข้าถึงระบบงาน	การกำหนดบทบาทผู้ใช้งาน
เว็บไซต์วิทยาลัย	การรักษาความปลอดภัยเว็บไซต์	การใช้ HTTPS และการควบคุมสิทธิ์ผู้ดูแล
Server	การดูแลระบบและโครงสร้างพื้นฐาน	การปรับปรุงระบบและการบำรุงรักษา

5.2.3 การพัฒนาองค์ความรู้จากประสบการณ์การปฏิบัติงาน

การพัฒนาองค์ความรู้จากประสบการณ์เป็นกระบวนการนำความรู้ที่เกิดจากการปฏิบัติงานของผู้ดูแลระบบและบุคลากรที่เกี่ยวข้องมาจัดทำเป็นองค์ความรู้ที่สามารถถ่ายทอดได้ โดยเชื่อมโยงความรู้ที่ฝังอยู่ในตัวบุคคล (Tacit Knowledge) กับความรู้ที่ชัดแจ้ง (Explicit Knowledge)

กระบวนการพัฒนาประกอบด้วย

1) รวบรวมประสบการณ์และความรู้จากการดูแลระบบสารสนเทศ
2) จำแนกองค์ความรู้ตามประเภทของระบบและลักษณะการใช้งาน
3) วิเคราะห์และตรวจสอบความถูกต้องของข้อมูล
4) เรียบเรียงองค์ความรู้เป็นเอกสารหรือแนวปฏิบัติ
5) จัดหมวดหมู่และจัดเก็บองค์ความรู้
6) ถ่ายทอดความรู้แก่บุคลากรที่เกี่ยวข้อง
7) นำความรู้ไปใช้ประกอบการพัฒนาระบบสารสนเทศ

5.2.4 การพัฒนาแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์

การทบทวนองค์ความรู้สามารถนำมาใช้เป็นพื้นฐานในการจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยครอบคลุมประเด็นสำคัญ ดังนี้

- แนวปฏิบัติการใช้งานระบบสารสนเทศอย่างปลอดภัย
- แนวปฏิบัติการดูแลเว็บไซต์และการเข้าถึงระบบ
- แนวปฏิบัติการดูแลและปรับปรุง Server
- แนวปฏิบัติการรักษาความปลอดภัยของข้อมูล
- แนวปฏิบัติการป้องกันอีเมลและข้อความหลอกลวง
- แนวปฏิบัติการรายงานเหตุการณ์ผิดปกติทางไซเบอร์

การจัดทำแนวปฏิบัติดังกล่าวมีวัตถุประสงค์เพื่อให้บุคลากรสามารถใช้เป็นแนวทางในการปฏิบัติงาน และช่วยให้การดูแลระบบสารสนเทศมีมาตรฐานและทิศทางการดำเนินงานที่ชัดเจน

5.2.5 การสรุปผลการพัฒนาในปีงบประมาณ พ.ศ. 2569

ตารางที่ 5.3 สรุปประเด็นการพัฒนาและปรับปรุงด้าน Cybersecurity ปีงบประมาณ พ.ศ. 2569

ลำดับ	ประเด็นการพัฒนา	สาระสำคัญ
1	การทบทวนองค์ความรู้	รวบรวมความรู้ด้านการดูแลข้อมูล เว็บไซต์ และระบบสารสนเทศ
2	การจัดการความรู้	เชื่อมโยงองค์ความรู้ด้าน Cybersecurity กับกระบวนการ KM
3	การพัฒนาแนวปฏิบัติ	จัดระบบความรู้เพื่อใช้เป็นแนวทางการปฏิบัติงาน
4	การถ่ายทอดความรู้	ส่งเสริมการแลกเปลี่ยนความรู้ระหว่างผู้เกี่ยวข้อง
5	การนำความรู้ไปใช้	เชื่อมโยงความรู้กับการดูแลระบบสารสนเทศของวิทยาลัย

จากการดำเนินงานในปีงบประมาณ พ.ศ. 2569 วิทยาลัยได้นำประเด็นความมั่นคงปลอดภัยทางไซเบอร์มาเชื่อมโยงกับกระบวนการจัดการความรู้ เพื่อพัฒนาองค์ความรู้ด้านการดูแลระบบสารสนเทศและสนับสนุนการถ่ายทอดความรู้ภายในองค์กร ทั้งนี้ ผลผลิตที่เป็นรูปธรรม เช่น จำนวนคู่มือ จำนวนองค์ความรู้ จำนวนผู้เข้าร่วมกิจกรรม หรือผลการประเมินความรู้ ต้องอ้างอิงจากเอกสารและหลักฐานการดำเนินงานที่จัดเก็บจริง

5.3 ผลลัพธ์ด้านความปลอดภัยของระบบสารสนเทศ

ผลลัพธ์ด้านความปลอดภัยของระบบสารสนเทศเป็นการพิจารณาการเปลี่ยนแปลงที่เกิดขึ้นจากการนำมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาใช้ โดยครอบคลุมการป้องกันภัยคุกคาม การรักษาความลับของข้อมูล การรักษาความถูกต้องครบถ้วนของข้อมูล และการรักษาความพร้อมใช้งานของระบบสารสนเทศ

การประเมินผลลัพธ์ด้านความปลอดภัยสามารถเชื่อมโยงกับหลักการ CIA Triad ได้แก่ Confidentiality, Integrity และ Availability ซึ่งเป็นหลักการพื้นฐานในการรักษาความมั่นคงปลอดภัยของข้อมูล (NIST, 2020)

5.3.1 ผลลัพธ์ด้านการรักษาความลับของข้อมูล (Confidentiality)

การรักษาความลับของข้อมูลเป็นการป้องกันไม่ให้บุคคลที่ไม่มีสิทธิ์สามารถเข้าถึงหรือเปิดเผยข้อมูลขององค์กร โดยเฉพาะข้อมูลบุคลากร ข้อมูลนักศึกษา เอกสารอิเล็กทรอนิกส์ และข้อมูลการบริหารจัดการ

มาตรการที่เกี่ยวข้องกับการดำเนินงานของวิทยาลัย ได้แก่

1) การใช้ Firewall เพื่อควบคุมการเชื่อมต่อเครือข่าย
2) การใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์
3) การควบคุมสิทธิ์การเข้าถึงระบบสารสนเทศ
4) การส่งเสริมความรู้เกี่ยวกับการรักษาความปลอดภัยของข้อมูล

มาตรการดังกล่าวสนับสนุนการรักษาความลับของข้อมูล อย่างไรก็ตาม การยืนยันว่าข้อมูลไม่มีการรั่วไหลจำเป็นต้องมีรายงานเหตุการณ์ด้านความปลอดภัยและหลักฐานการตรวจสอบประกอบ

5.3.2 ผลลัพธ์ด้านความถูกต้องครบถ้วนของข้อมูล (Integrity)

ความถูกต้องครบถ้วนของข้อมูลเป็นการรักษาข้อมูลให้มีความถูกต้อง ไม่ถูกเปลี่ยนแปลงหรือทำลายโดยไม่ได้รับอนุญาต และสามารถตรวจสอบแหล่งที่มาหรือประวัติการเปลี่ยนแปลงได้

มาตรการที่เกี่ยวข้อง ได้แก่

- การปรับปรุงรหัสโปรแกรมของ Server
- การควบคุมสิทธิ์การเข้าถึงระบบ
- การตรวจสอบการเปลี่ยนแปลงข้อมูล
- การจัดเก็บบันทึกเหตุการณ์ของระบบ
- การกำหนดกระบวนการสำรองและกู้คืนข้อมูล

การดำเนินงานเหล่านี้เป็นแนวทางสนับสนุนความถูกต้องครบถ้วนของข้อมูล แต่การประเมินผลจริงต้องอาศัยหลักฐานการตรวจสอบข้อมูลและบันทึกการเปลี่ยนแปลงระบบ

5.3.3 ผลลัพธ์ด้านความพร้อมใช้งานของระบบ (Availability)

ความพร้อมใช้งานเป็นการทำให้ระบบสารสนเทศและข้อมูลสามารถเข้าถึงและใช้งานได้ตามความจำเป็น โดยลดโอกาสที่ระบบจะหยุดชะงักจากข้อผิดพลาดทางเทคนิคหรือภัยคุกคามทางไซเบอร์ มาตรการที่เกี่ยวข้อง ได้แก่

1) การดูแลและปรับปรุงระบบ Server
2) การพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย
3) การตรวจสอบสถานะการทำงานของระบบ
4) การบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี
5) การกำหนดแนวทางสำรองและกู้คืนข้อมูล

การดำเนินงานดังกล่าวสนับสนุนความพร้อมใช้งานของระบบสารสนเทศและช่องทางการให้บริการข้อมูลของวิทยาลัย ทั้งนี้ การยืนยันประสิทธิภาพต้องใช้ข้อมูลระยะเวลาการให้บริการ (Uptime) สถิติระบบขัดข้อง และผลการทดสอบกู้คืนระบบประกอบ

5.3.4 การเชื่อมโยงผลลัพธ์กับหลักการ CIA Triad

ตารางที่ 5.4 การวิเคราะห์ผลลัพธ์ด้านความปลอดภัยของระบบสารสนเทศตามหลัก CIA Triad

หลักการ	ความหมาย	มาตรการของวิทยาลัยที่เกี่ยวข้อง	หลักฐานที่ใช้ยืนยันผล
Confidentiality	การรักษาความลับ	Firewall และ SSL	การตั้งค่า Firewall และใบรับรอง SSL
Integrity	การรักษาความถูกต้องครบถ้วน	การปรับปรุงรหัสโปรแกรมและการควบคุมสิทธิ์	บันทึกการปรับปรุงและประวัติการเปลี่ยนแปลง
Availability	การรักษาความพร้อมใช้งาน	การดูแล Server และการพัฒนาเว็บไซต์	รายงานสถานะระบบและสถิติการให้บริการ

5.3.5 ตัวชี้วัดผลลัพธ์ด้านความปลอดภัยของระบบสารสนเทศ

การประเมินผลลัพธ์ด้านความปลอดภัยควรกำหนดตัวชี้วัดที่สามารถตรวจสอบได้ ดังนี้

ประเด็น	ตัวชี้วัด	วิธีการประเมิน
ความปลอดภัยเครือข่าย	จำนวนเหตุการณ์ผิดปกติที่ตรวจพบและจัดการ	ตรวจสอบ Firewall Log

ประเด็น	ตัวชี้วัด	วิธีการประเมิน
ความปลอดภัยเว็บไซต์	สถานะใบรับรองและการเชื่อมต่อ HTTPS	ตรวจสอบใบรับรองและการตั้งค่า TLS
ความปลอดภัย Server	จำนวนรายการปรับปรุงและแก้ไขช่องโหว่	ตรวจสอบบันทึกการปรับปรุง
ความถูกต้องของข้อมูล	จำนวนเหตุการณ์การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต	ตรวจสอบ Audit Log
ความพร้อมใช้งาน	ร้อยละระยะเวลาที่ระบบให้บริการได้	ตรวจสอบ Uptime
การกู้คืนข้อมูล	ผลการทดสอบกู้คืนข้อมูล	ตรวจสอบรายงานการทดสอบ

ตัวชี้วัดดังกล่าวเป็นกรอบการประเมินผลลัพธ์ โดยต้องใช้ข้อมูลจากระบบและรายงานการตรวจสอบจริงในการคำนวณผลการดำเนินงาน

5.4 ผลลัพธ์ด้านการบริหารจัดการและการให้บริการ

การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ส่งผลเชื่อมโยงกับการบริหารจัดการและการให้บริการขององค์กร เนื่องจากระบบสารสนเทศเป็นเครื่องมือสนับสนุนการปฏิบัติงานของบุคลากร การจัดเก็บข้อมูล การติดต่อสื่อสาร และการเผยแพร่ข้อมูลข่าวสาร การพัฒนาระบบให้มีความปลอดภัยและสามารถรองรับการใช้งานได้อย่างเหมาะสมจึงเป็นปัจจัยสำคัญต่อการดำเนินงานของวิทยาลัย

สำหรับวิทยาลัยชุมชนสตูล การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์มีความเชื่อมโยงกับระบบสารสนเทศสำคัญ ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server ซึ่งเป็นระบบที่สนับสนุนการบริหารจัดการและการปฏิบัติงานตามภารกิจขององค์กร

5.4.1 การสนับสนุนประสิทธิภาพการบริหารจัดการองค์กร

การดูแลระบบสารสนเทศและการพัฒนามาตรการรักษาความปลอดภัยช่วยสนับสนุนการบริหารจัดการข้อมูลและการปฏิบัติงานขององค์กร โดยระบบสารสนเทศสามารถใช้เป็นเครื่องมือในการรวบรวม จัดเก็บ ประมวลผล และเรียกใช้ข้อมูลเพื่อประกอบการบริหารงาน

ผลลัพธ์ที่เกี่ยวข้องกับการดำเนินงาน ได้แก่

1) มีมาตรการด้านเทคนิคสำหรับดูแลความปลอดภัยของระบบเครือข่าย
2) มีการใช้การเข้ารหัสการสื่อสารผ่านเว็บไซต์
3) มีการปรับปรุงรหัสโปรแกรมของ Server
4) มีการพัฒนาเว็บไซต์เพื่อสนับสนุนการเข้าถึงข้อมูล
5) มีการเชื่อมโยงองค์ความรู้ด้านความปลอดภัยเข้ากับกระบวนการจัดการความรู้ขององค์กร

มาตรการเหล่านี้เป็นองค์ประกอบที่สนับสนุนการบริหารจัดการระบบสารสนเทศให้มีความเป็นระบบ และช่วยสร้างพื้นฐานสำหรับการพัฒนาการบริหารงานดิจิทัลของวิทยาลัย

5.4.2 การเพิ่มประสิทธิภาพช่องทางการให้บริการข้อมูล

เว็บไซต์เป็นช่องทางสำคัญในการเผยแพร่ข้อมูลข่าวสารและประชาสัมพันธ์กิจกรรมของวิทยาลัย การพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลายและปรับโครงสร้างเมนูให้เหมาะสม ช่วยสนับสนุนการเข้าถึงข้อมูลของผู้เรียน บุคลากร และประชาชน

ผลลัพธ์ที่เกี่ยวข้อง ได้แก่

- การพัฒนาเว็บไซต์ให้รองรับการใช้งานผ่านอุปกรณ์หลากหลาย
- การปรับโครงสร้างเมนูให้เข้าถึงข้อมูลได้สะดวก
- การใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสาร
- การสนับสนุนการเผยแพร่ข้อมูลข่าวสารผ่านช่องทางดิจิทัล

การดำเนินงานดังกล่าวเชื่อมโยงกับการพัฒนาคุณภาพการให้บริการขององค์กร โดยเน้นความสะดวกในการเข้าถึงข้อมูลและความปลอดภัยของช่องทางการสื่อสาร

5.4.3 การสนับสนุนการปฏิบัติงานของบุคลากร

ระบบสารสนเทศที่มีการดูแลและกำหนดมาตรการรักษาความปลอดภัยอย่างเหมาะสมเป็นเครื่องมือสนับสนุนการปฏิบัติงานของบุคลากร โดยช่วยให้การเข้าถึงข้อมูลและการใช้ระบบเป็นไปตามบทบาทหน้าที่

ระบบที่เกี่ยวข้องประกอบด้วย

ระบบ	การสนับสนุนภารกิจ
ICCS-PORTAL	การบริหารจัดการและติดตามผลการดำเนินงาน
E-Office	การจัดการเอกสารและงานสารบรรณ
E-HR.ICCS	การบริหารจัดการข้อมูลบุคลากร
SMART ERPG	การสนับสนุนการบริหารจัดการองค์กร
เว็บไซต์วิทยาลัย	การประชาสัมพันธ์และเผยแพร่ข้อมูล
Server	การรองรับการจัดเก็บและประมวลผลข้อมูล

การดูแลระบบดังกล่าวมีส่วนสนับสนุนการดำเนินงานของหน่วยงานต่าง ๆ โดยการประเมินผลด้านประสิทธิภาพการปฏิบัติงานควรพิจารณาร่วมกับข้อมูลระยะเวลาการให้บริการ จำนวนผู้ใช้งาน และความพึงพอใจของผู้รับบริการ

5.4.4 การสนับสนุนการบริหารจัดการองค์กรดิจิทัล

การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์เป็นองค์ประกอบสำคัญของการพัฒนาองค์กรดิจิทัล เนื่องจากการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการจำเป็นต้องมีมาตรการรองรับความปลอดภัยของข้อมูลและระบบ

การดำเนินงานของวิทยาลัยที่เกี่ยวข้อง ได้แก่

1) การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ
2) การรักษาความปลอดภัยของระบบเครือข่ายและเว็บไซต์
3) การดูแลระบบ Server
4) การพัฒนาช่องทางเผยแพร่ข้อมูลผ่านเว็บไซต์
5) การส่งเสริมการจัดการความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การดำเนินงานดังกล่าวเป็นพื้นฐานสำหรับการพัฒนาองค์กรให้สามารถใช้เทคโนโลยีดิจิทัลในการบริหารจัดการและให้บริการได้อย่างมีประสิทธิภาพ โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูลเป็นสำคัญ

5.4.5 ตัวชี้วัดผลลัพธ์ด้านการบริหารจัดการและการให้บริการ

ตารางที่ 5.5 ตัวชี้วัดผลลัพธ์ด้านการบริหารจัดการและการให้บริการ

ประเด็น	ตัวชี้วัด	วิธีการประเมิน
การบริหารจัดการระบบ	จำนวนระบบที่มีการกำหนดผู้รับผิดชอบ	ตรวจสอบทะเบียนระบบ
การให้บริการเว็บไซต์	ระยะเวลาที่เว็บไซต์สามารถให้บริการได้	ตรวจสอบ Uptime
การเข้าถึงข้อมูล	จำนวนผู้เข้าชมเว็บไซต์	สถิติการใช้งานเว็บไซต์
ความสะดวกในการใช้งาน	ระดับความพึงพอใจของผู้ใช้งาน	แบบสอบถาม
ความต่อเนื่องในการให้บริการ	จำนวนครั้งและระยะเวลาที่ระบบหยุดชะงัก	รายงานเหตุการณ์ระบบ
การพัฒนาระบบ	จำนวนรายการปรับปรุงระบบสารสนเทศ	รายงานการดำเนินงาน

5.5 ผลลัพธ์ด้านความรู้และความตระหนักของบุคลากร

บุคลากรเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากการใช้งานระบบสารสนเทศในองค์กรเกี่ยวข้องกับการเข้าถึง การจัดเก็บ การประมวลผล และการเผยแพร่ข้อมูล หากบุคลากรขาดความรู้ความเข้าใจเกี่ยวกับภัยคุกคามและแนวทางป้องกัน อาจก่อให้เกิดความเสี่ยงต่อข้อมูลและระบบสารสนเทศขององค์กรได้

การจัดการความรู้ด้าน Cybersecurity จึงมีความสำคัญต่อการพัฒนาความสามารถของบุคลากร โดยมุ่งเน้นการรวบรวมและถ่ายทอดองค์ความรู้จากประสบการณ์การปฏิบัติงาน การจัดทำแนวปฏิบัติ และการส่งเสริมความตระหนักรู้เกี่ยวกับการใช้งานระบบสารสนเทศอย่างปลอดภัย

สำหรับวิทยาลัยชุมชนสตูล ในปีงบประมาณ พ.ศ. 2569 มีการเชื่อมโยงการทบทวนองค์ความรู้ด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ขององค์กร เพื่อสนับสนุนการพัฒนาความรู้และการนำองค์ความรู้ไปประยุกต์ใช้ในการปฏิบัติงาน

5.5.1 การพัฒนาความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การพัฒนาความรู้ของบุคลากรเป็นกระบวนการสร้างความเข้าใจเกี่ยวกับหลักการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ โดยครอบคลุมความรู้พื้นฐานและความรู้เฉพาะด้านที่เกี่ยวข้องกับหน้าที่ของผู้ใช้งาน

องค์ความรู้ที่เกี่ยวข้องประกอบด้วย

1) ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และรูปแบบการโจมตี
2) ความรู้เกี่ยวกับการรักษาความปลอดภัยของข้อมูล
3) ความรู้เกี่ยวกับการใช้ระบบสารสนเทศอย่างปลอดภัย
4) ความรู้เกี่ยวกับการตั้งรหัสผ่านและการควบคุมบัญชีผู้ใช้งาน
5) ความรู้เกี่ยวกับการป้องกันอีเมลและข้อความหลอกลวง
6) ความรู้เกี่ยวกับการรักษาความปลอดภัยเว็บไซต์
7) ความรู้เกี่ยวกับการดูแลและบำรุงรักษาระบบ Server
8) ความรู้เกี่ยวกับการรายงานเหตุการณ์ผิดปกติทางไซเบอร์

5.5.2 การพัฒนาความตระหนักรู้ในการใช้งานระบบสารสนเทศ

การสร้างความตระหนักรู้เป็นการพัฒนาความสามารถของบุคลากรในการรับรู้ความเสี่ยงและเลือกปฏิบัติอย่างเหมาะสมเมื่อใช้งานเทคโนโลยีสารสนเทศ โดยเน้นการสร้างพฤติกรรมการใช้งานที่ปลอดภัยและการมีส่วนร่วมในการป้องกันภัยคุกคามขององค์กร

พฤติกรรมที่ควรส่งเสริม ได้แก่

- ไม่เปิดเผยรหัสผ่านหรือข้อมูลยืนยันตัวตนแก่ผู้อื่น
- ตรวจสอบความน่าเชื่อถือของอีเมลและลิงก์ก่อนเปิดใช้งาน
- ไม่ติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต
- ระมัดระวังการส่งต่อข้อมูลส่วนบุคคล
- ใช้งานระบบสารสนเทศตามสิทธิ์ที่ได้รับ
- ออกจากระบบเมื่อสิ้นสุดการใช้งาน
- แจ้งผู้รับผิดชอบเมื่อพบความผิดปกติของระบบ

5.5.3 การถ่ายทอดและแลกเปลี่ยนองค์ความรู้ภายในองค์กร

การถ่ายทอดและแลกเปลี่ยนความรู้เป็นกระบวนการที่ช่วยให้บุคลากรสามารถเรียนรู้จากประสบการณ์ของผู้ปฏิบัติงานและนำความรู้ไปใช้ในการทำงานได้อย่างเหมาะสม

รูปแบบการถ่ายทอดความรู้ที่เกี่ยวข้อง ได้แก่

1. การแลกเปลี่ยนเรียนรู้จากผู้มีประสบการณ์

รวบรวมความรู้จากบุคลากรที่มีประสบการณ์ในการดูแลระบบเครือข่าย เว็บไซต์ และ Server เพื่อถ่ายทอดแนวทางการปฏิบัติงานและการแก้ไขปัญหา

2. การจัดทำเอกสารองค์ความรู้

รวบรวมความรู้และจัดทำเป็นเอกสาร คู่มือ หรือแนวปฏิบัติ เพื่อให้บุคลากรสามารถศึกษาและนำไปใช้ได้

3. การเผยแพร่ความรู้

จัดให้มีช่องทางเผยแพร่องค์ความรู้ด้านความปลอดภัยทางไซเบอร์ เพื่อให้บุคลากรสามารถเข้าถึงข้อมูลได้สะดวก

4. การนำความรู้ไปประยุกต์ใช้

ส่งเสริมให้บุคลากรนำความรู้ไปใช้ในการดูแลข้อมูลและระบบสารสนเทศตามหน้าที่รับผิดชอบ

5.5.4 การประเมินผลด้านความรู้และความตระหนักของบุคลากร

การประเมินผลด้านความรู้และความตระหนักรู้ควรพิจารณาทั้งระดับความรู้ ความเข้าใจ และพฤติกรรมการใช้งานระบบสารสนเทศ โดยสามารถใช้วิธีการประเมินที่หลากหลาย ดังนี้

ตารางที่ 5.6 ตัวชี้วัดผลลัพธ์ด้านความรู้และความตระหนักของบุคลากร

ประเด็นการประเมิน	ตัวชี้วัด	วิธีการประเมิน	หลักฐาน
ความรู้ด้าน Cybersecurity	คะแนนความรู้เกี่ยวกับภัยคุกคาม	แบบทดสอบ	ผ ล Pre-test/Post-test
ค ว า ม เ ข้ า ใ จ ด้ า น ค ว า ม ปลอดภัย	ร้อยละของบุคลากรที่ผ่านเกณฑ์	แบบทดสอบ	สรุปผลการประเมิน

ประเด็นการประเมิน	ตัวชี้วัด	วิธีการประเมิน	หลักฐาน
ความตระหนักรู้	ระดับความตระหนักในการใช้งานระบบ	แบบสอบถาม	ผลการประเมิน
การมีส่วนร่วม	จำนวนบุคลากรที่เข้าร่วมกิจกรรม	ตรวจสอบรายชื่อ	ใบลงทะเบียน
การนำความรู้ไปใช้	จำนวนบุคลากรที่นำความรู้ไปประยุกต์ใช้	แบบติดตามผล	รายงานการติดตาม
การพัฒนาองค์ความรู้	จำนวนเอกสารหรือคู่มือที่จัดทำ	ตรวจสอบเอกสาร	คู่มือและเอกสาร KM

5.5.5 แนวทางการติดตามผลการนำความรู้ไปใช้

การติดตามผลการนำความรู้ไปใช้เป็นกระบวนการตรวจสอบว่าบุคลากรสามารถนำองค์ความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานจริงได้หรือไม่ โดยสามารถดำเนินการดังนี้

1) ตรวจสอบการนำคู่มือและแนวปฏิบัติไปใช้
2) สัมภาษณ์บุคลากรเกี่ยวกับการประยุกต์ใช้ความรู้
3) ประเมินความรู้หลังการถ่ายทอดองค์ความรู้
4) ตรวจสอบการปฏิบัติตามแนวทางการใช้งานระบบอย่างปลอดภัย
5) รวบรวมปัญหาและข้อเสนอแนะจากการใช้งาน
6) นำผลการติดตามมาปรับปรุงองค์ความรู้และแนวปฏิบัติ

5.5.6 ผลลัพธ์ที่คาดหวังจากการพัฒนาความรู้และความตระหนักรู้

การดำเนินงานด้านการจัดการความรู้และการสร้างความตระหนักรู้มีเป้าหมายเพื่อให้เกิดผลลัพธ์ในระดับบุคลากรและองค์กร ดังนี้

ระดับบุคลากร

- มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์
- เข้าใจหลักการรักษาความปลอดภัยของข้อมูล
- สามารถใช้งานระบบสารสนเทศอย่างปลอดภัย
- มีความระมัดระวังในการเข้าถึงและเผยแพร่ข้อมูล
- สามารถรายงานเหตุการณ์ผิดปกติได้อย่างเหมาะสม

ระดับองค์กร

- มีการรวบรวมและจัดระบบองค์ความรู้ด้าน Cybersecurity
- มีแนวปฏิบัติสำหรับใช้ในการดูแลระบบสารสนเทศ
- มีช่องทางถ่ายทอดและแลกเปลี่ยนความรู้
- สามารถนำประสบการณ์จากการปฏิบัติงานมาพัฒนาองค์ความรู้
- มีพื้นฐานสำหรับการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง

ผลลัพธ์ข้างต้นเป็นผลลัพธ์ที่มุ่งหวังจากกระบวนการพัฒนาความรู้และความตระหนักรู้ การรายงานผลที่เกิดขึ้นจริงจำเป็นต้องมีข้อมูลจากการประเมินความรู้ การติดตามพฤติกรรม และหลักฐานการนำองค์ความรู้ไปใช้ประกอบ

สรุป

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูลในปีงบประมาณ พ.ศ. 2568–2569 แสดงให้เห็นถึงการพัฒนาระบบสารสนเทศควบคู่กับการส่งเสริมการจัดการความรู้ โดยในปีงบประมาณ พ.ศ. 2568 วิทยาลัยดำเนินมาตรการด้านเทคนิคที่สำคัญ ได้แก่ การใช้ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก การใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย พร้อมปรับโครงสร้างเมนูเพื่อเพิ่มความสะดวกในการเข้าถึงข้อมูล

ส่วนปีงบประมาณ พ.ศ. 2569 วิทยาลัยเชื่อมโยงการทบทวนองค์ความรู้ด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ เพื่อส่งเสริมการรวบรวมและถ่ายทอดความรู้ที่เกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

เมื่อพิจารณาตามหลักการรักษาความมั่นคงปลอดภัยของข้อมูล CIA Triad พบว่ามาตรการที่ดำเนินการมีความเกี่ยวข้องกับการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของระบบสารสนเทศ นอกจากนี้ การดูแลระบบสารสนเทศที่สำคัญของวิทยาลัยยังสนับสนุนการบริหารจัดการและการให้บริการผ่านระบบดิจิทัล

การดำเนินงานดังกล่าวจึงเป็นพื้นฐานสำหรับการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูลให้มีความเป็นระบบ โดยการประเมินผลสัมฤทธิ์ในระยะต่อไปควรให้ความสำคัญกับการจัดเก็บหลักฐานเชิงประจักษ์ การกำหนดตัวชี้วัด และการติดตามผลอย่างต่อเนื่อง เพื่อให้สามารถประเมินประสิทธิผลของมาตรการและนำผลการประเมินไปใช้ในการพัฒนาองค์กรได้อย่างเป็นรูปธรรม

บทที่ 6 ปัจจัยความสำเร็จและการพัฒนาต่อยอด

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) เป็นกระบวนการที่ต้องอาศัยการบริหารจัดการอย่างเป็นระบบ การสนับสนุนจากผู้บริหาร ความพร้อมของบุคลากร เทคโนโลยี และการมีส่วนร่วมของผู้เกี่ยวข้องทุกระดับ เพื่อให้ระบบสารสนเทศสามารถรองรับภารกิจขององค์กรได้อย่างมั่นคงปลอดภัยและต่อเนื่อง

สำหรับวิทยาลัยชุมชนสตูล การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ในปีงบประมาณ พ.ศ. 2568–2569 ครอบคลุมการใช้ Firewall เพื่อป้องกันภัยคุกคามจากภายนอก การใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์ การปรับปรุงรหัสโปรแกรมของ Server การพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย และการเชื่อมโยงองค์ความรู้ด้านการดูแลข้อมูลและการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ขององค์กร

การพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ให้เกิดประสิทธิผลจำเป็นต้องอาศัยการทบทวนปัจจัยที่สนับสนุนการดำเนินงาน การวิเคราะห์ปัญหาและอุปสรรค การสรุปบทเรียนจากประสบการณ์ตลอดจนการกำหนดแนวทางพัฒนาและขยายผลให้ครอบคลุมภารกิจขององค์กร โดยเชื่อมโยงกับกรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานสากล เพื่อให้การพัฒนาระบบสารสนเทศของวิทยาลัยมีความต่อเนื่องและสามารถปรับตัวต่อภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอยู่เสมอ

6.1 ปัจจัยแห่งความสำเร็จ

ปัจจัยแห่งความสำเร็จของการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ หมายถึงองค์ประกอบที่สนับสนุนให้องค์กรสามารถดำเนินมาตรการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศได้ตามวัตถุประสงค์ โดยครอบคลุมด้านการบริหารจัดการ เทคโนโลยี บุคลากร กระบวนการปฏิบัติงาน และการจัดการความรู้

จากการดำเนินงานของวิทยาลัยชุมชนสตูล สามารถจำแนกปัจจัยที่เกี่ยวข้องกับการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ได้ดังนี้

6.1.1 การสนับสนุนและกำกับดูแลจากผู้บริหาร

การสนับสนุนจากผู้บริหารเป็นปัจจัยสำคัญในการขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากการพัฒนาระบบสารสนเทศจำเป็นต้องอาศัยการกำหนดทิศทาง นโยบาย การจัดสรรทรัพยากร และการกำกับติดตามให้การดำเนินงานเป็นไปตามเป้าหมายขององค์กร

การกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ควรครอบคลุมประเด็นสำคัญ ได้แก่

1) การกำหนดนโยบายและแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ
2) การกำหนดผู้รับผิดชอบในการดูแลระบบสารสนเทศและโครงสร้างพื้นฐานด้านเทคโนโลยี
3) การสนับสนุนงบประมาณ อุปกรณ์ และทรัพยากรที่จำเป็น
4) การกำกับติดตามผลการดำเนินงานและการประเมินความเสี่ยง
5) การส่งเสริมให้บุคลากรมีส่วนร่วมในการรักษาความปลอดภัยขององค์กร

สำหรับวิทยาลัยชุมชนสตูล การดำเนินงานด้าน Firewall, SSL การปรับปรุง Server และการพัฒนาเว็บไซต์ เป็นตัวอย่างของการนำมาตรการด้านเทคโนโลยีมาใช้สนับสนุนความมั่นคงปลอดภัยขององค์กร ซึ่งการดำเนินงานในระยะต่อไปจำเป็นต้องเชื่อมโยงกับการกำกับดูแลและการติดตามผลอย่างเป็นระบบ

6.1.2 ความพร้อมด้านเทคโนโลยีและโครงสร้างพื้นฐาน

เทคโนโลยีและโครงสร้างพื้นฐานเป็นองค์ประกอบสำคัญที่รองรับการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะระบบเครือข่าย Server เว็บไซต์ และระบบสารสนเทศที่ใช้สนับสนุนภารกิจขององค์กร

ปัจจัยด้านเทคโนโลยีที่เกี่ยวข้อง ได้แก่

- การมีเครื่องมือควบคุมและป้องกันภัยคุกคามทางเครือข่าย เช่น Firewall
- การใช้ใบรับรองดิจิทัลเพื่อเข้ารหัสการสื่อสารผ่านเว็บไซต์
- การปรับปรุงรหัสโปรแกรมและองค์ประกอบของระบบ Server
- การพัฒนาเว็บไซต์ให้รองรับอุปกรณ์และรูปแบบการใช้งานที่หลากหลาย
- การตรวจสอบและบำรุงรักษาระบบสารสนเทศอย่างเหมาะสม
- การจัดให้มีมาตรการสำรองและกู้คืนข้อมูล

การพัฒนาเทคโนโลยีดังกล่าวต้องคำนึงถึงความเหมาะสมกับภารกิจของวิทยาลัย ความสามารถในการดูแลรักษา และความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงของเทคโนโลยี

6.1.3 ความรู้และความสามารถของบุคลากร

บุคลากรเป็นองค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากการใช้งานระบบสารสนเทศเกี่ยวข้องกับการเข้าถึง การจัดเก็บ การประมวลผล และการเผยแพร่ข้อมูล หากบุคลากรขาดความรู้ความเข้าใจเกี่ยวกับภัยคุกคาม อาจก่อให้เกิดความเสี่ยงต่อระบบสารสนเทศขององค์กรได้

การพัฒนาศักยภาพบุคลากรควรครอบคลุมความรู้และทักษะ ดังนี้

1) ความรู้พื้นฐานเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
2) ความเข้าใจเกี่ยวกับภัยคุกคามและรูปแบบการโจมตีทางไซเบอร์
3) ทักษะการใช้งานระบบสารสนเทศอย่างปลอดภัย
4) ความรู้เกี่ยวกับการรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล
5) ความสามารถในการสังเกตและรายงานเหตุการณ์ผิดปกติ
6) ความรู้เกี่ยวกับการสำรองข้อมูลและการป้องกันการสูญหายของข้อมูล

การพัฒนาบุคลากรต้องดำเนินการอย่างต่อเนื่อง โดยเชื่อมโยงกับการอบรม การแลกเปลี่ยนเรียนรู้ และการนำความรู้ไปประยุกต์ใช้ในการปฏิบัติงาน

6.1.4 การมีระบบและกระบวนการดำเนินงานที่ชัดเจน

การกำหนดกระบวนการดำเนินงานที่ชัดเจนช่วยให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์สามารถดำเนินการได้อย่างเป็นระบบ มีผู้รับผิดชอบ และสามารถตรวจสอบย้อนหลังได้

กระบวนการที่เกี่ยวข้องประกอบด้วย

- การสำรวจและจัดทำทะเบียนระบบสารสนเทศ
- การประเมินความเสี่ยงของระบบและข้อมูล
- การกำหนดมาตรการป้องกันตามระดับความเสี่ยง
- การตรวจสอบและบำรุงรักษาระบบ
- การจัดการเหตุการณ์ด้านความปลอดภัย
- การสำรองและกู้คืนข้อมูล
- การติดตามและประเมินผลการดำเนินงาน

กระบวนการดังกล่าวสอดคล้องกับแนวทาง NIST Cybersecurity Framework 2.0 ซึ่งกำหนดหน้าที่หลักในการบริหารความเสี่ยงทางไซเบอร์ 6 ด้าน ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover (NIST, 2024)

6.1.5 การจัดการความรู้และการแลกเปลี่ยนประสบการณ์

การจัดการความรู้เป็นปัจจัยสำคัญในการพัฒนาความสามารถขององค์กร เนื่องจากช่วยรวบรวมประสบการณ์จากผู้ปฏิบัติงานและเปลี่ยนความรู้ที่อยู่ในตัวบุคคลให้เป็นองค์ความรู้ที่สามารถถ่ายทอดและนำกลับมาใช้ได้

สำหรับวิทยาลัยชุมชนสตูล การเชื่อมโยงองค์ความรู้ด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการ KM ในปีงบประมาณ พ.ศ. 2569 เป็นแนวทางในการรวบรวมและพัฒนาความรู้จากการปฏิบัติงาน โดยมีประเด็นสำคัญ ได้แก่

1) การรวบรวมความรู้จากผู้ดูแลระบบและผู้เกี่ยวข้อง
2) การถอดบทเรียนจากการปฏิบัติงาน
3) การจัดทำคู่มือและแนวปฏิบัติด้านความปลอดภัย
4) การแลกเปลี่ยนความรู้ระหว่างบุคลากร
5) การจัดเก็บองค์ความรู้ในรูปแบบเอกสารหรือฐานข้อมูล
6) การนำความรู้ไปประยุกต์ใช้ในการดูแลระบบสารสนเทศ

6.1.6 การติดตามประเมินผลและปรับปรุงอย่างต่อเนื่อง

การติดตามและประเมินผลเป็นปัจจัยที่ช่วยให้องค์กรสามารถตรวจสอบประสิทธิผลของมาตรการรักษาความปลอดภัย และนำผลการประเมินไปใช้ปรับปรุงระบบให้เหมาะสมกับความเสี่ยงที่เปลี่ยนแปลง

การติดตามประเมินผลควรครอบคลุมการตรวจสอบสถานะระบบเครือข่าย การตรวจสอบใบรับรองเว็บไซต์ การบำรุงรักษา Server การตรวจสอบสิทธิ์ผู้ใช้งาน การประเมินความรู้ของบุคลากร และการติดตามผลการนำองค์ความรู้ไปใช้

ตารางที่ 6.1 ปัจจัยแห่งความสำเร็จในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์

ปัจจัย	สาระสำคัญ	แนวทางสนับสนุน
การบริหารจัดการ	การกำหนดนโยบายและทิศทาง	การกำกับติดตามจากผู้บริหาร
เทคโนโลยี	ความพร้อมของระบบและอุปกรณ์	การพัฒนาและบำรุงรักษาระบบ
บุคลากร	ความรู้และทักษะด้าน Cybersecurity	การอบรมและแลกเปลี่ยนเรียนรู้
กระบวนการ	การดำเนินงานอย่างเป็นระบบ	การกำหนดขั้นตอนและผู้รับผิดชอบ
การจัดการความรู้	การรวบรวมและถ่ายทอดประสบการณ์	การจัดทำคู่มือและฐานความรู้
การประเมินผล	การตรวจสอบประสิทธิผล	การติดตามตัวชี้วัดและปรับปรุง

จากองค์ประกอบดังกล่าว การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรจำเป็นต้องดำเนินการควบคู่กันทั้งด้านการบริหารจัดการ เทคโนโลยี บุคลากร และกระบวนการ โดยการจัดการความรู้เป็นกลไกสนับสนุนให้ประสบการณ์และแนวปฏิบัติสามารถนำไปใช้ประโยชน์ได้อย่างต่อเนื่อง

6.2 ปัญหา อุปสรรค และแนวทางแก้ไข

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์มีความเกี่ยวข้องกับเทคโนโลยี บุคลากร กระบวนการบริหารจัดการ และการเปลี่ยนแปลงของภัยคุกคาม ซึ่งอาจส่งผลต่อประสิทธิภาพของการรักษาความปลอดภัยระบบสารสนเทศ การวิเคราะห์ปัญหาและอุปสรรคจึงเป็นส่วนสำคัญในการกำหนดมาตรการป้องกันและพัฒนาระบบให้มีความเหมาะสม

สำหรับการดำเนินงานของวิทยาลัยชุมชนสตูล ข้อมูลที่มีอยู่แสดงให้เห็นถึงการใช้มาตรการทางเทคนิคและการเชื่อมโยงองค์ความรู้เข้ากับกระบวนการ KM แต่ยังไม่มีข้อมูลผลการประเมินปัญหาและอุปสรรคที่ยืนยันว่าเกิดขึ้นจริงในทุกประเด็น ดังนั้น การนำเสนอในหัวข้อนี้จึงจำแนกประเด็นความเสี่ยงที่ควรตรวจสอบและแนวทางจัดการ เพื่อใช้เป็นกรอบสำหรับการพัฒนาระบบของวิทยาลัย

6.2.1 ปัญหาด้านเทคโนโลยีและระบบสารสนเทศ

ระบบสารสนเทศประกอบด้วยองค์ประกอบหลายส่วน ได้แก่ ระบบเครือข่าย Server เว็บไซต์ โปรแกรมประยุกต์ และฐานข้อมูล ซึ่งต้องได้รับการดูแลให้มีความปลอดภัยและสามารถทำงานร่วมกันได้อย่างเหมาะสม

ประเด็นที่ควรตรวจสอบ ได้แก่

1) ความทันสมัยของระบบปฏิบัติการและซอฟต์แวร์
2) ช่องโหว่ที่อาจเกิดขึ้นจากโปรแกรมหรือระบบที่ไม่ได้รับการปรับปรุง
3) การกำหนดค่าความปลอดภัยของ Server และอุปกรณ์เครือข่าย
4) การควบคุมสิทธิ์การเข้าถึงระบบสารสนเทศ
5) ความพร้อมของระบบสำรองและกู้คืนข้อมูล
6) ความสามารถในการตรวจสอบและติดตามเหตุการณ์ผิดปกติ

แนวทางแก้ไข

- จัดทำทะเบียนระบบสารสนเทศและอุปกรณ์เทคโนโลยี
- กำหนดแผนตรวจสอบและปรับปรุงซอฟต์แวร์
- ตรวจสอบช่องโหว่ของระบบตามระดับความเสี่ยง
- ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน
- จัดทำแผนสำรองและกู้คืนข้อมูล
- จัดเก็บบันทึกเหตุการณ์เพื่อสนับสนุนการตรวจสอบย้อนหลัง

6.2.2 ปัญหาด้านบุคลากรและความตระหนักรู้

บุคลากรเป็นผู้ใช้งานระบบสารสนเทศโดยตรง การขาดความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์หรือการใช้งานระบบอย่างไม่ระมัดระวังอาจเพิ่มความเสี่ยงต่อองค์กร เช่น การเปิดไฟล์แนบที่เป็นอันตราย การคลิกลิงก์หลอกลวง การเปิดเผยรหัสผ่าน และการส่งข้อมูลส่วนบุคคลให้บุคคลที่ไม่มีสิทธิ์

แนวทางแก้ไข

1) จัดกิจกรรมอบรมความรู้ด้าน Cybersecurity
2) เผยแพร่แนวทางการตั้งรหัสผ่านที่ปลอดภัย
3) สร้างความเข้าใจเกี่ยวกับการป้องกัน Phishing
4) ส่งเสริมการรายงานเหตุการณ์ผิดปกติ
5) จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย
6) ประเมินความรู้ก่อนและหลังการพัฒนาบุคลากร

6.2.3 ปัญหาด้านการบริหารจัดการและการกำหนดผู้รับผิดชอบ

การดูแลระบบสารสนเทศหลายระบบจำเป็นต้องมีการกำหนดบทบาทและความรับผิดชอบที่ชัดเจน หากไม่มีการจัดทำทะเบียนระบบหรือกำหนดผู้รับผิดชอบ อาจส่งผลต่อความต่อเนื่องในการดูแลและการแก้ไขปัญหา

แนวทางแก้ไข

- จัดทำทะเบียนระบบสารสนเทศที่สำคัญ
- กำหนดผู้รับผิดชอบหลักและผู้ประสานงานของแต่ละระบบ
- จัดทำคู่มือและขั้นตอนการปฏิบัติงาน
- กำหนดช่องทางแจ้งปัญหาและรายงานเหตุการณ์
- จัดทำประวัติการบำรุงรักษาและการเปลี่ยนแปลงระบบ
- ทบทวนบทบาทหน้าที่เมื่อมีการเปลี่ยนแปลงบุคลากร

6.2.4 ปัญหาด้านการจัดเก็บและถ่ายทอดองค์ความรู้

ความรู้ด้านเทคโนโลยีสารสนเทศบางส่วนอาจอยู่ในรูปแบบประสบการณ์ของผู้ปฏิบัติงาน หากไม่มีการรวบรวมและจัดทำเป็นเอกสาร อาจทำให้ความรู้ดังกล่าวไม่สามารถถ่ายทอดไปยังบุคลากรคนอื่นได้อย่างครบถ้วน

แนวทางแก้ไข

1) จัดกิจกรรมถอดบทเรียนจากผู้ดูแลระบบ
2) จัดทำเอกสารองค์ความรู้ด้าน Cybersecurity
3) พัฒนาคู่มือการดูแลระบบและการแก้ไขปัญหา
4) จัดเก็บองค์ความรู้ในพื้นที่กลางที่กำหนดสิทธิ์เข้าถึง
5) กำหนดผู้รับผิดชอบในการทบทวนและปรับปรุงเอกสาร
6) ส่งเสริมการแลกเปลี่ยนเรียนรู้ระหว่างบุคลากร

6.2.5 ปัญหาด้านงบประมาณและทรัพยากรสนับสนุน

การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์จำเป็นต้องใช้ทรัพยากรด้านเทคโนโลยี บุคลากร และงบประมาณในการจัดหาอุปกรณ์ การบำรุงรักษาระบบ การพัฒนาซอฟต์แวร์ และการฝึกอบรมบุคลากร

แนวทางแก้ไข

- จัดลำดับความสำคัญของระบบตามระดับความเสี่ยง
- จัดทำแผนงบประมาณด้านความมั่นคงปลอดภัยทางไซเบอร์
- ใช้ทรัพยากรเทคโนโลยีที่มีอยู่ให้เกิดประโยชน์สูงสุด
- วางแผนบำรุงรักษาระบบตามรอบระยะเวลา
- พิจารณาความคุ้มค่าของการลงทุนด้านความปลอดภัย
- ส่งเสริมความร่วมมือกับหน่วยงานที่มีความเชี่ยวชาญ

6.2.6 ตารางสรุปปัญหา อุปสรรค และแนวทางแก้ไข

ตารางที่ 6.2 การวิเคราะห์ปัญหา อุปสรรค และแนวทางแก้ไขด้านความมั่นคงปลอดภัยทางไซเบอร์

ประเด็น	ความเสี่ยงหรืออุปสรรคที่ควรตรวจสอบ	แนวทางแก้ไข
เทคโนโลยี	ช่องโหว่และระบบที่ไม่ได้รับการปรับปรุง	ตรวจสอบและบำรุงรักษาระบบ
บุคลากร	ขาดความรู้และความตระหนักรู้	อบรมและสร้างความตระหนัก
การบริหารจัดการ	บทบาทและผู้รับผิดชอบไม่ชัดเจน	จัดทำทะเบียนและกำหนดผู้รับผิดชอบ
การจัดการความรู้	ความรู้กระจุกตัวอยู่กับผู้ปฏิบัติงาน	ถอดบทเรียนและจัดทำคู่มือ
งบประมาณ	ทรัพยากรสนับสนุนมีข้อจำกัด	จัดลำดับความสำคัญตามความเสี่ยง
การติดตามผล	ขาดข้อมูลเชิงประจักษ์สำหรับประเมินผล	กำหนดตัวชี้วัดและจัดเก็บหลักฐาน

6.3 บทเรียนที่ได้รับ

บทเรียนที่ได้รับจากการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นองค์ความรู้ที่เกิดจากการปฏิบัติงาน การแก้ไขปัญหา การพัฒนาระบบ และการแลกเปลี่ยนประสบการณ์ระหว่างบุคลากร ซึ่งสามารถนำมาใช้ปรับปรุงกระบวนการดำเนินงานและพัฒนาระบบสารสนเทศขององค์กรให้มีประสิทธิภาพมากยิ่งขึ้น

จากการดำเนินงานของวิทยาลัยชุมชนสตูลในปีงบประมาณ พ.ศ. 2568–2569 สามารถสังเคราะห์บทเรียนจากมาตรการทางเทคนิคและการจัดการความรู้ได้ดังนี้

6.3.1 การรักษาความปลอดภัยต้องดำเนินการหลายระดับ

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ไม่สามารถพึ่งพาเครื่องมือหรือมาตรการใดมาตรการหนึ่งเพียงอย่างเดียว เนื่องจากภัยคุกคามสามารถเกิดขึ้นได้จากหลายช่องทาง ทั้งระบบเครือข่าย เว็บไซต์ โปรแกรมประยุกต์ Server และพฤติกรรมการใช้งานของบุคลากร

การใช้ Firewall เป็นมาตรการควบคุมการเชื่อมต่อเครือข่าย การใช้ใบรับรอง SSL เป็นมาตรการเข้ารหัสการสื่อสาร และการปรับปรุงรหัสโปรแกรมของ Server เป็นการดูแลระบบในระดับโปรแกรมและโครงสร้างพื้นฐาน ซึ่งแต่ละมาตรการมีหน้าที่แตกต่างกันและต้องดำเนินการร่วมกับมาตรการอื่น

บทเรียนสำคัญคือ การรักษาความปลอดภัยจำเป็นต้องครอบคลุมทั้งเทคโนโลยี กระบวนการบริหารจัดการ และบุคลากร เพื่อให้สามารถป้องกัน ตรวจจับ และจัดการความเสี่ยงได้อย่างเหมาะสม

6.3.2 การดูแลระบบสารสนเทศต้องดำเนินการอย่างต่อเนื่อง

ระบบสารสนเทศมีการเปลี่ยนแปลงตามเทคโนโลยีและความต้องการของผู้ใช้งาน การพัฒนาระบบในช่วงเวลาใดเวลาหนึ่งจึงไม่เพียงพอต่อการรักษาความปลอดภัยในระยะยาว

การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ของวิทยาลัยในปีงบประมาณ พ.ศ. 2568 แสดงให้เห็นถึงการดำเนินงานด้านการพัฒนาและดูแลระบบสารสนเทศ ซึ่งจำเป็นต้องมีการตรวจสอบ บำรุงรักษา และปรับปรุงให้เหมาะสมกับสภาพแวดล้อมทางเทคโนโลยีที่เปลี่ยนแปลง

บทเรียนที่ได้รับคือ การดูแลระบบสารสนเทศควรมีแผนการบำรุงรักษา การตรวจสอบสถานะระบบ และการติดตามการเปลี่ยนแปลงอย่างสม่ำเสมอ

6.3.3 การรักษาความปลอดภัยต้องเชื่อมโยงกับการบริหารจัดการข้อมูล

ระบบสารสนเทศของวิทยาลัยประกอบด้วยระบบที่สนับสนุนภารกิจหลายด้าน ได้แก่ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server ซึ่งมีลักษณะการใช้งานและประเภทข้อมูลที่แตกต่างกัน

การดูแลระบบแต่ละประเภทจึงจำเป็นต้องคำนึงถึงความสำคัญของข้อมูล การกำหนดสิทธิ์การเข้าถึง และความพร้อมใช้งานของระบบ โดยเฉพาะข้อมูลที่เกี่ยวข้องกับบุคลากรและผู้เรียน ซึ่งต้องให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล

บทเรียนที่ได้รับคือ การรักษาความปลอดภัยทางไซเบอร์ต้องเชื่อมโยงกับการบริหารจัดการข้อมูลขององค์กร ไม่ใช่จำกัดอยู่เฉพาะการดูแลอุปกรณ์หรือระบบเครือข่ายเท่านั้น

6.3.4 การจัดการความรู้ช่วยสร้างความต่อเนื่องในการปฏิบัติงาน

ความรู้ด้านเทคโนโลยีสารสนเทศจำนวนหนึ่งเกิดจากประสบการณ์ของผู้ปฏิบัติงาน เช่น การดูแล Firewall การติดตั้งใบรับรองดิจิทัล การปรับปรุง Server และการแก้ไขปัญหาเว็บไซต์ หากไม่มีการจัดเก็บและถ่ายทอดองค์ความรู้ อาจทำให้การปฏิบัติงานขาดความต่อเนื่องเมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบ

การเชื่อมโยงการทบทวนองค์ความรู้ด้าน Cybersecurity เข้ากับกระบวนการ KM ในปีงบประมาณ พ.ศ. 2569 จึงเป็นแนวทางในการรวบรวมและพัฒนาความรู้จากประสบการณ์การทำงานให้สามารถนำไปใช้ประโยชน์ได้

บทเรียนที่ได้รับคือ การจัดการความรู้ควรดำเนินการควบคู่กับการปฏิบัติงานจริง โดยจัดทำเอกสาร คู่มือ และแนวปฏิบัติที่สามารถนำไปใช้ได้ รวมถึงมีการทบทวนเนื้อหาให้เป็นปัจจุบัน

6.3.5 บุคลากรทุกระดับมีส่วนร่วมในการรักษาความปลอดภัย

การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นความรับผิดชอบร่วมกันของบุคลากรทุกระดับ แม้การดูแลระบบในเชิงเทคนิคจะเป็นหน้าที่ของผู้ดูแลระบบ แต่การใช้งานข้อมูลและเทคโนโลยีในชีวิตประจำวันของบุคลากรมีผลต่อความปลอดภัยขององค์กรเช่นกัน

การสร้างความตระหนักรู้เกี่ยวกับการใช้งานรหัสผ่าน การตรวจสอบอีเมลและลิงก์ การรักษาความลับของข้อมูล และการแจ้งเหตุการณ์ผิดปกติ จึงเป็นองค์ประกอบสำคัญของการป้องกันภัยคุกคามทางไซเบอร์

บทเรียนที่ได้รับคือ การพัฒนาความมั่นคงปลอดภัยต้องให้ความสำคัญกับการพัฒนาความรู้และพฤติกรรมของผู้ใช้งานควบคู่กับการพัฒนาเทคโนโลยี

6.3.6 การจัดเก็บหลักฐานเป็นส่วนสำคัญของการประเมินผล

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์จำเป็นต้องมีหลักฐานประกอบ เพื่อให้สามารถตรวจสอบกระบวนการดำเนินงานและประเมินผลลัพธ์ได้อย่างถูกต้อง

หลักฐานที่เกี่ยวข้องประกอบด้วยภาพการดำเนินงาน เอกสารการปรับปรุงระบบ รายงานการตรวจสอบ บันทึกเหตุการณ์ รายงานการบำรุงรักษา และเอกสารการจัดการความรู้

บทเรียนที่ได้รับคือ การจัดเก็บหลักฐานควรดำเนินการตั้งแต่เริ่มต้นจนสิ้นสุดกระบวนการ โดยกำหนดผู้รับผิดชอบ รูปแบบเอกสาร และวิธีการจัดเก็บให้เป็นระบบ

ตารางที่ 6.3 สรุปบทเรียนที่ได้รับจากการดำเนินงาน

ลำดับ	บทเรียนที่ได้รับ	แนวทางนำไปใช้
1	การรักษาความปลอดภัยต้องครอบคลุมหลายระดับ	พัฒนามาตรการด้านเทคโนโลยีและบุคลากรร่วมกัน
2	ระบบสารสนเทศต้องได้รับการดูแลต่อเนื่อง	จัดทำแผนตรวจสอบและบำรุงรักษา
3	การรักษาความปลอดภัยต้องเชื่อมโยงกับข้อมูล	จัดประเภทข้อมูลและควบคุมสิทธิ์
4	การจัดการความรู้ช่วยสร้างความต่อเนื่อง	จัดทำคู่มือและถอดบทเรียน
5	บุคลากรมีส่วนร่วมในการรักษาความปลอดภัย	ส่งเสริมความรู้และความตระหนัก
6	หลักฐานมีความสำคัญต่อการประเมินผล	จัดเก็บเอกสารและผลการดำเนินงานอย่างเป็นระบบ

6.4 แนวทางการพัฒนาอย่างต่อเนื่อง

การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่องเป็นกระบวนการปรับปรุงระบบสารสนเทศและมาตรการบริหารความเสี่ยงให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี ภัยคุกคาม และภารกิจขององค์กร โดยมุ่งเน้นการพัฒนาระบบให้มีความปลอดภัย สามารถตรวจสอบได้ และรองรับการให้บริการอย่างต่อเนื่อง

การพัฒนาของวิทยาลัยชุมชนสตูลสามารถเชื่อมโยงกับกรอบ NIST Cybersecurity Framework 2.0 ซึ่งกำหนดหน้าที่หลัก 6 ด้าน ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover เพื่อใช้เป็นกรอบในการกำกับดูแลและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ (NIST, 2024)

6.4.1 การพัฒนาด้านการกำกับดูแลและนโยบายความปลอดภัย (Govern)

การกำกับดูแลเป็นพื้นฐานของการบริหารความมั่นคงปลอดภัยทางไซเบอร์ โดยมุ่งกำหนดนโยบาย บทบาทหน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องให้ชัดเจน

แนวทางการพัฒนาประกอบด้วย

1) จัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
2) กำหนดผู้รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์
3) จัดทำทะเบียนระบบสารสนเทศและทรัพย์สินดิจิทัล
4) กำหนดแนวทางการจัดการความเสี่ยงทางไซเบอร์
5) กำหนดแนวทางการรายงานเหตุการณ์ด้านความปลอดภัย
6) ติดตามและรายงานผลต่อผู้บริหารตามรอบระยะเวลา

6.4.2 การพัฒนาด้านการระบุและประเมินความเสี่ยง (Identify)

การระบุความเสี่ยงเป็นกระบวนการสำรวจทรัพย์สินสารสนเทศ ระบบงาน และข้อมูลที่มีความสำคัญ เพื่อให้สามารถกำหนดมาตรการป้องกันได้อย่างเหมาะสม

แนวทางการพัฒนาประกอบด้วย

- จัดทำทะเบียนระบบ ICCS-PORTAL, E-Office, E-HR.ICCS, SMART ERPG เว็บไซต์ และ Server

- จำแนกประเภทข้อมูลตามระดับความสำคัญและความอ่อนไหว
- วิเคราะห์ภัยคุกคามและช่องโหว่ของแต่ละระบบ
- ประเมินโอกาสเกิดเหตุการณ์และผลกระทบ
- จัดลำดับความสำคัญของความเสี่ยง
- จัดทำแผนบริหารจัดการความเสี่ยงและทบทวนตามรอบเวลา

6.4.3 การพัฒนาด้านการป้องกัน (Protect)

การป้องกันเป็นกระบวนการกำหนดมาตรการเพื่อลดโอกาสการเกิดเหตุการณ์ด้านความปลอดภัยและจำกัดผลกระทบที่อาจเกิดขึ้นกับระบบสารสนเทศ

แนวทางการพัฒนาประกอบด้วย

1) ปรับปรุงกฎและการตั้งค่า Firewall ให้เหมาะสมกับความเสี่ยง
2) ดูแลใบรับรองดิจิทัลและการเชื่อมต่อ HTTPS/TLS
3) ปรับปรุงระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบัน
4) ควบคุมสิทธิ์การเข้าถึงระบบตามบทบาทหน้าที่
5) จัดทำระบบสำรองข้อมูลและทดสอบการกู้คืน
6) ส่งเสริมการใช้รหัสผ่านที่ปลอดภัยและการยืนยันตัวตนหลายปัจจัยตามความเหมาะสม
7) สร้างความตระหนักรู้ให้แก่บุคลากรเกี่ยวกับการป้องกันภัยคุกคาม

6.4.4 การพัฒนาด้านการตรวจจับภัยคุกคาม (Detect)

การตรวจจับเป็นกระบวนการติดตามและวิเคราะห์เหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้สามารถค้นพบความผิดปกติได้อย่างรวดเร็ว

แนวทางการพัฒนาประกอบด้วย

- ตรวจสอบบันทึกเหตุการณ์จาก Firewall และ Server
- ติดตามสถานะการทำงานของเว็บไซต์และระบบสารสนเทศ
- ตรวจสอบการเข้าสู่ระบบที่ผิดปกติ
- เฝ้าระวังการเปลี่ยนแปลงข้อมูลและการตั้งค่าระบบ
- ตรวจสอบการแจ้งเตือนจากระบบรักษาความปลอดภัย
- จัดทำรายงานเหตุการณ์ที่ตรวจพบและผลการดำเนินการ

6.4.5 การพัฒนาด้านการตอบสนองต่อเหตุการณ์ (Respond)

การตอบสนองเป็นกระบวนการจัดการเมื่อเกิดเหตุการณ์ด้านความปลอดภัย โดยมีวัตถุประสงค์เพื่อควบคุมสถานการณ์ ลดผลกระทบ และป้องกันไม่ให้เหตุการณ์ขยายวงกว้าง

แนวทางการพัฒนาประกอบด้วย

1. กำหนดช่องทางการแจ้งเหตุการณ์ด้านความปลอดภัย
2. กำหนดผู้รับผิดชอบในการรับแจ้งและตรวจสอบเหตุการณ์
3. จำแนกระดับความรุนแรงของเหตุการณ์
4. ดำเนินการควบคุมหรือแยกส่วนระบบที่ได้รับผลกระทบตามความเหมาะสม
5. ตรวจสอบสาเหตุและขอบเขตความเสียหาย
6. บันทึกการดำเนินงานและจัดทำรายงานเหตุการณ์
7. ทบทวนมาตรการเพื่อป้องกันการเกิดเหตุซ้ำ

6.4.6 การพัฒนาด้านการฟื้นฟูระบบ (Recover)

การฟื้นฟูเป็นกระบวนการนำระบบสารสนเทศกลับมาให้บริการภายหลังเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบ โดยต้องมีการวางแผนและเตรียมความพร้อมด้านข้อมูล ระบบสำรอง และผู้รับผิดชอบ

แนวทางการพัฒนาประกอบด้วย

- จัดทำแผนสำรองและกู้คืนข้อมูล
- กำหนดระบบและข้อมูลที่ต้องได้รับการฟื้นฟูเป็นลำดับแรก
- จัดทำข้อมูลสำรองแยกจากระบบหลักตามระดับความเสี่ยง
- ทดสอบการกู้คืนข้อมูลตามรอบระยะเวลา
- ตรวจสอบความถูกต้องของข้อมูลหลังการกู้คืน
- จัดทำรายงานผลการฟื้นฟูและบทเรียนที่ได้รับ

6.4.7 การพัฒนาระบบจัดการความรู้ด้าน Cybersecurity

การจัดการความรู้เป็นกลไกสนับสนุนการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ โดยช่วยรวบรวมและถ่ายทอดความรู้จากผู้ปฏิบัติงานให้เป็นองค์ความรู้ที่สามารถนำไปใช้ได้อย่างต่อเนื่อง
แนวทางการพัฒนาประกอบด้วย

1) จัดทำฐานข้อมูลองค์ความรู้ด้าน Cybersecurity
2) รวบรวมคู่มือและขั้นตอนการดูแลระบบสารสนเทศ
3) ถอดบทเรียนจากการแก้ไขปัญหาและการบำรุงรักษาระบบ
4) จัดกิจกรรมแลกเปลี่ยนเรียนรู้ระหว่างผู้ดูแลระบบและบุคลากร
5) จัดทำแนวปฏิบัติด้านความปลอดภัยสำหรับผู้ใช้งาน
6) ทบทวนและปรับปรุงองค์ความรู้ให้เป็นปัจจุบัน
7) ประเมินผลการนำความรู้ไปใช้ในการปฏิบัติงาน

6.4.8 การกำหนดตัวชี้วัดเพื่อการพัฒนาอย่างต่อเนื่อง

การพัฒนาอย่างต่อเนื่องจำเป็นต้องกำหนดตัวชี้วัดที่สามารถติดตามและประเมินผลได้ โดยตัวชี้วัดต้องเชื่อมโยงกับเป้าหมายการดำเนินงานและมีหลักฐานประกอบ

ตารางที่ 6.4 ตัวชี้วัดการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง

ด้านการพัฒนา	ตัวชี้วัด	หลักฐาน
Govern	มีนโยบายและผู้รับผิดชอบด้าน Cybersecurity	นโยบายและคำสั่งแต่งตั้ง
Identify	ร้อยละของระบบสำคัญที่ได้รับการประเมินความเสี่ยง	ทะเบียนและรายงานความเสี่ยง
Protect	ร้อยละของระบบที่ได้รับการตรวจสอบมาตรการป้องกัน	รายงานการตรวจสอบ
Detect	จำนวนเหตุการณ์ที่ได้รับการตรวจสอบและบันทึก	รายงาน Incident
Respond	ร้อยละของเหตุการณ์ที่ได้รับการจัดการตามขั้นตอน	รายงานการตอบสนอง
Recover	ผลการทดสอบการสำรองและกู้คืนข้อมูล	รายงานการทดสอบ

ด้านการพัฒนา	ตัวชี้วัด	หลักฐาน
Knowledge Management	จำนวนองค์ความรู้หรือคู่มือที่ได้รับการพัฒนา	เอกสาร KM
Awareness	ร้อยละของบุคลากรที่ผ่านเกณฑ์การประเมินความรู้	ผล Pre-test/Post-test

6.5 การขยายผลสู่การเป็นองค์กรดิจิทัลที่มั่นคงปลอดภัย

การพัฒนาองค์กรดิจิทัลที่มีความมั่นคงปลอดภัยเป็นกระบวนการนำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการบริหารจัดการ การจัดการเรียนการสอน การให้บริการ และการดำเนินงานตามภารกิจขององค์กร โดยให้ความสำคัญกับการรักษาความปลอดภัยของข้อมูล การบริหารความเสี่ยง การพัฒนาศักยภาพบุคลากร และการสร้างระบบบริหารจัดการที่สามารถปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยีได้

สำหรับวิทยาลัยชุมชนสตูล การขยายผลการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์สามารถเชื่อมโยงกับการพัฒนาระบบสารสนเทศที่มีอยู่ การจัดการความรู้ และการสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้อง เพื่อพัฒนาองค์กรให้สามารถใช้เทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพและปลอดภัย

6.5.1 การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ระดับองค์กร

การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ระดับองค์กรเป็นการกำหนดกรอบการดำเนินงานที่ครอบคลุมระบบสารสนเทศทุกประเภท โดยเชื่อมโยงการกำกับดูแล การประเมินความเสี่ยง การป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟูระบบเข้าด้วยกัน

แนวทางการดำเนินงานประกอบด้วย

1) จัดทำนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัย
2) จัดทำทะเบียนทรัพย์สินและระบบสารสนเทศที่สำคัญ
3) จัดประเภทข้อมูลตามระดับความสำคัญและความอ่อนไหว
4) กำหนดผู้รับผิดชอบในการดูแลระบบและข้อมูล
5) จัดทำแผนบริหารความเสี่ยงทางไซเบอร์
6) กำหนดแนวทางการจัดการเหตุการณ์และการฟื้นฟูระบบ
7) ติดตามและประเมินผลการดำเนินงานตามรอบระยะเวลา

6.5.2 การพัฒนาระบบสารสนเทศให้มีความปลอดภัยครอบคลุมทุกภารกิจ

การขยายผลด้านความมั่นคงปลอดภัยทางไซเบอร์ต้องครอบคลุมระบบสารสนเทศที่สนับสนุนภารกิจของวิทยาลัย เพื่อให้การดูแลระบบมีมาตรฐานและสามารถบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

ระบบที่ควรได้รับการพัฒนา ได้แก่

- **ICCS-PORTAL:** เน้นการรักษาความถูกต้องของข้อมูลการบริหารจัดการและการติดตามผลการดำเนินงาน
- **E-Office:** เน้นการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์และการควบคุมสิทธิ์การเข้าถึง
- **E-HR.ICCS:** เน้นการคุ้มครองข้อมูลบุคลากรและข้อมูลส่วนบุคคล

- **SMART ERPG:** เน้นการควบคุมสิทธิ์และความปลอดภัยของข้อมูลการบริหารจัดการ
- **เว็บไซต์วิทยาลัย:** เน้นการรักษาความปลอดภัยของเว็บไซต์และการเผยแพร่ข้อมูลที่ถูกต้อง
- **Server:** เน้นการดูแลระบบปฏิบัติการ ซอฟต์แวร์ การสำรองข้อมูล และการตรวจสอบเหตุการณ์

การดำเนินงานควรคำนึงถึงระดับความสำคัญของระบบและข้อมูล เพื่อจัดลำดับความสำคัญในการพัฒนาและใช้ทรัพยากรให้เหมาะสม

6.5.3 การพัฒนาบุคลากรสู่การเป็นผู้ใช้งานดิจิทัลอย่างปลอดภัย

บุคลากรเป็นองค์ประกอบสำคัญขององค์กรดิจิทัล การพัฒนาความรู้และทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์จึงต้องดำเนินการอย่างต่อเนื่อง เพื่อให้สามารถใช้งานระบบสารสนเทศและจัดการข้อมูลได้อย่างถูกต้องและปลอดภัย

แนวทางการพัฒนาประกอบด้วย

1) จัดอบรมความรู้พื้นฐานด้าน Cybersecurity ให้แก่บุคลากร
2) พัฒนาทักษะการป้องกันภัยคุกคามจากอีเมลและเว็บไซต์หลอกลวง
3) ส่งเสริมการใช้งานรหัสผ่านที่ปลอดภัยและการยืนยันตัวตนหลายปัจจัย
4) พัฒนาความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
5) ส่งเสริมการใช้งานระบบสารสนเทศตามสิทธิ์ที่ได้รับ
6) จัดกิจกรรมแลกเปลี่ยนเรียนรู้และถอดบทเรียน
7) ประเมินความรู้และติดตามพฤติกรรมการใช้งานอย่างต่อเนื่อง

6.5.4 การพัฒนาฐานข้อมูลองค์ความรู้และเครือข่ายการเรียนรู้

การพัฒนาฐานข้อมูลองค์ความรู้เป็นแนวทางในการรวบรวมและจัดเก็บความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้บุคลากรสามารถเข้าถึงและนำความรู้ไปประยุกต์ใช้ในการปฏิบัติงานได้

องค์ความรู้ที่ควรจัดเก็บประกอบด้วย

- คู่มือการดูแลระบบเครือข่ายและ Firewall
- คู่มือการดูแลเว็บไซต์และใบรับรองดิจิทัล
- คู่มือการปรับปรุงและบำรุงรักษา Server
- แนวปฏิบัติการใช้งานระบบสารสนเทศอย่างปลอดภัย
- แนวทางการป้องกันภัยคุกคามทางไซเบอร์
- ขั้นตอนการรายงานและจัดการเหตุการณ์ผิดปกติ
- แนวทางการสำรองและกู้คืนข้อมูล
- กรณีศึกษาและบทเรียนจากการปฏิบัติงาน

นอกจากนี้ การสร้างเครือข่ายการเรียนรู้กับหน่วยงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ สามารถสนับสนุนการแลกเปลี่ยนความรู้ การเข้าถึงข้อมูลข่าวสารภัยคุกคาม และการพัฒนาศักยภาพบุคลากรให้ทันต่อสถานการณ์

6.5.5 การเชื่อมโยงการพัฒนาองค์กรดิจิทัลกับกฎหมายและมาตรฐาน

การพัฒนาองค์กรดิจิทัลที่มั่นคงปลอดภัยจำเป็นต้องดำเนินงานภายใต้กฎหมายและมาตรฐานที่เกี่ยวข้อง เพื่อให้การบริหารจัดการข้อมูลและระบบสารสนเทศมีความเหมาะสมและสามารถตรวจสอบได้

กรอบกฎหมายและมาตรฐานที่เกี่ยวข้อง ได้แก่

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เป็นกฎหมายที่กำหนดหลักเกณฑ์และมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เป็นกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

3. ISO/IEC 27001:2022

เป็นมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ซึ่งกำหนดข้อกำหนดในการจัดตั้ง ดำเนินการ รักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4. NIST Cybersecurity Framework 2.0

เป็นกรอบแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งประกอบด้วย 6 หน้าที่หลัก ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover สามารถนำมาประยุกต์ใช้ในการกำหนดทิศทางและติดตามการดำเนินงานขององค์กร

การเชื่อมโยงกับกฎหมายและมาตรฐานดังกล่าวช่วยให้การพัฒนาระบบสารสนเทศของวิทยาลัยมีกรอบการดำเนินงานที่ชัดเจน และสนับสนุนการบริหารความเสี่ยงด้านข้อมูลและเทคโนโลยีอย่างเป็นระบบ

6.5.6 แผนการขยายผลสู่การเป็นองค์กรดิจิทัลที่มั่นคงปลอดภัย

การขยายผลการดำเนินงานควรกำหนดเป็นระยะ เพื่อให้สอดคล้องกับทรัพยากรและความพร้อมขององค์กร โดยแบ่งแนวทางการดำเนินงานออกเป็น 3 ระยะ ดังนี้

ตารางที่ 6.5 แผนการขยายผลการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูล

ระยะการพัฒนา	แนวทางดำเนินงาน	ผลผลิตที่มุ่งหวัง
ระยะที่ 1 วางรากฐาน	จัดทำนโยบาย ทะเบียนระบบ และประเมินความเสี่ยง	มีกรอบบริหารจัดการและข้อมูลระบบสารสนเทศ
ระยะที่ 2 พัฒนาระบบ	ปรับปรุงมาตรการป้องกัน ตรวจสอบระบบ และพัฒนาบุคลากร	ระบบมีมาตรการรักษาความปลอดภัยและบุคลากรมีความรู้
ระยะที่ 3 ขยายผลและยกระดับ	พัฒนาฐานความรู้ ประเมินผล และสร้างเครือข่ายความร่วมมือ	มีระบบจัดการความรู้และกระบวนการพัฒนาอย่างต่อเนื่อง

6.5.7 ผลลัพธ์ที่มุ่งหวังจากการพัฒนาสู่องค์กรดิจิทัลที่มั่นคงปลอดภัย

การขยายผลการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์มีเป้าหมายเพื่อพัฒนาศักยภาพของวิทยาลัยใน 4 ด้าน ได้แก่

ด้านที่ 1 ด้านเทคโนโลยี

- ระบบสารสนเทศได้รับการดูแลและปรับปรุงตามความเสี่ยง
- มีมาตรการป้องกันและตรวจสอบภัยคุกคาม
- มีระบบสำรองและกู้คืนข้อมูลที่ได้รับการทดสอบ
- ระบบสามารถรองรับการปฏิบัติงานและการให้บริการได้อย่างต่อเนื่อง

ด้านที่ 2 ด้านการบริหารจัดการ

- มีนโยบายและแนวปฏิบัติด้านความปลอดภัยที่ชัดเจน
- มีการกำหนดผู้รับผิดชอบระบบสารสนเทศ
- มีการประเมินและติดตามความเสี่ยง
- มีหลักฐานประกอบการตรวจสอบและประเมินผล

ด้านที่ 3 ด้านบุคลากร

- บุคลากรมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์
- สามารถใช้งานระบบสารสนเทศอย่างปลอดภัย
- มีความตระหนักในการคุ้มครองข้อมูล
- สามารถถ่ายทอดและแลกเปลี่ยนองค์ความรู้ได้

ด้านที่ 4 ด้านการจัดการความรู้

- มีฐานข้อมูลองค์ความรู้ด้าน Cybersecurity
- มีคู่มือและแนวปฏิบัติที่เป็นเอกสาร
- มีการถอดบทเรียนจากการปฏิบัติงาน
- มีการนำองค์ความรู้ไปพัฒนาระบบสารสนเทศอย่างต่อเนื่อง

ผลลัพธ์ดังกล่าวเป็นเป้าหมายการพัฒนาขององค์กร ซึ่งต้องมีการกำหนดตัวชี้วัดและติดตามผลการดำเนินงานเพื่อยืนยันความสำเร็จในแต่ละระยะ

สรุป

การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูลเป็นกระบวนการที่ต้องอาศัยการบูรณาการด้านเทคโนโลยี การบริหารจัดการ และการพัฒนาศักยภาพบุคลากร โดยปัจจัยแห่งความสำเร็จประกอบด้วยการสนับสนุนจากผู้บริหาร ความพร้อมของโครงสร้างพื้นฐานด้านเทคโนโลยี ความรู้ความสามารถของบุคลากร การกำหนดกระบวนการดำเนินงานที่ชัดเจน การจัดการความรู้ และการติดตามประเมินผลอย่างต่อเนื่อง

จากการดำเนินงานในปีงบประมาณ พ.ศ. 2568 วิทยาลัยมีการใช้ Firewall การใช้ใบรับรอง SSL การปรับปรุงรหัสโปรแกรมของ Server และการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์หลากหลาย ซึ่งเป็นมาตรการด้านเทคนิคที่สนับสนุนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ส่วนในปีงบประมาณ พ.ศ. 2569 วิทยาลัยได้เชื่อมโยงการทบทวนองค์ความรู้ด้านการดูแลข้อมูล เว็บไซต์ และการป้องกันภัยคุกคามทางไซเบอร์เข้ากับกระบวนการจัดการความรู้ขององค์กร

บทเรียนจากการดำเนินงานสะท้อนให้เห็นถึงความสำคัญของการรักษาความปลอดภัยหลายระดับ การดูแลระบบอย่างต่อเนื่อง การควบคุมการเข้าถึงข้อมูล การถ่ายทอดองค์ความรู้ และการจัดเก็บหลักฐานเพื่อใช้ในการตรวจสอบและประเมินผล

แนวทางการพัฒนาต่อยอดจึงมุ่งเน้นการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุมการกำกับดูแล การประเมินความเสี่ยง การป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟู

ระบบ โดยประยุกต์ใช้กรอบ NIST Cybersecurity Framework 2.0 และมาตรฐาน ISO/IEC 27001:2022 ควบคู่กับการพัฒนาระบบจัดการความรู้และการสร้างความตระหนักรู้แก่บุคลากร

การดำเนินงานดังกล่าวเป็นพื้นฐานสำหรับการยกระดับวิทยาลัยชุมชนสตูลสู่การเป็นองค์กรดิจิทัลที่มีความมั่นคงปลอดภัย สามารถบริหารจัดการข้อมูลและระบบสารสนเทศได้อย่างเป็นระบบ รองรับการเปลี่ยนแปลงของเทคโนโลยี และสนับสนุนการดำเนินภารกิจด้านการศึกษาและการพัฒนาชุมชนได้อย่างต่อเนื่องและยั่งยืน

เอกสารอ้างอิง

เอกสารภาษาไทย

ราชกิจจานุเบกษา. (2550). *พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม*.

ราชกิจจานุเบกษา. (2562). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562*. เล่ม 136 ตอนที่ 69 ก.

ราชกิจจานุเบกษา. (2562). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*. เล่ม 136 ตอนที่ 69 ก.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2564). *ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564*.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (ม.ป.ป.). *กฎหมาย ข้อบังคับ ประกาศ และแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์*.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT). (ม.ป.ป.). *พื้นฐานความมั่นคงปลอดภัยไซเบอร์*.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT). (ม.ป.ป.). *แนวปฏิบัติและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์*.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT). (ม.ป.ป.). *แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline)*.

เอกสารภาษาต่างประเทศ

International Organization for Standardization. (2022a). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022)*.

International Organization for Standardization. (2022b). *Information security, cybersecurity and privacy protection—Information security controls (ISO/IEC 27002:2022)*.

McKay, K., & Cooper, D. (2019). *Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations* (NIST Special Publication 800-52 Revision 2). National Institute of Standards and Technology.

National Institute of Standards and Technology. (n.d.-a). *Cybersecurity*. Computer Security Resource Center Glossary.

National Institute of Standards and Technology. (n.d.-b). *Information security*. Computer Security Resource Center Glossary.

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Revision 1).

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Revision 5).

Nelson, A., Rekhi, S., Scarfone, K., & Souppaya, M. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61 Revision 3). National Institute of Standards and Technology.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

OWASP Foundation. (n.d.-b). *Secure coding practices—Quick reference guide*.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology.

ภาคผนวก

ภาคผนวก ก.

การถอดความรู้จากผู้รู้ในหน่วยงาน
(Tacit Knowledge to Explicit Knowledge)

การถอดความรู้จากผู้รู้ในหน่วยงาน (Tacit Knowledge to Explicit Knowledge)

1. ผู้รู้ (ข้อมูลผู้รู้)



ชื่อผู้รู้ นางสาวสุชฎา พรหมแก้ว
ตำแหน่ง ครู วิทยฐานะ ครูชำนาญการ
ภูมิลำเนา จังหวัดสตูล
มือถือ 0855867353

2. ผู้ถอดความรู้

2.1 นางสาวสุนิสา สะแหละ
2.2 นายอุใบ หมัดหมุด
2.3 นางสาวนวรัตน์ ลิ่มสกุล

3. ชื่อหัวข้อความรู้

การดูแลข้อมูลและการใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร

4. ประโยชน์ของความรู้

1) ทำให้บุคลากรมีความรู้ความเข้าใจเกี่ยวกับการดูแลข้อมูลและการใช้งานระบบสารสนเทศของวิทยาลัยอย่างปลอดภัย

2) ช่วยลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่เหมาะสม และการใช้งานระบบที่อาจก่อให้เกิดภัยคุกคามทางไซเบอร์

3) ส่งเสริมให้บุคลากรตระหนักถึงความสำคัญของการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล

4) ช่วยให้การปฏิบัติงานผ่านระบบสารสนเทศ เช่น ระบบงานสำนักงานอิเล็กทรอนิกส์ ระบบบริหารงานบุคคล และระบบสารสนเทศของวิทยาลัย เป็นไปอย่างระมัดระวังและมีความรับผิดชอบ

5) สนับสนุนการสร้างวัฒนธรรมการใช้เทคโนโลยีดิจิทัลอย่างปลอดภัยภายในวิทยาลัยชุมชนสตูล

5. เนื้อหาและสาระสำคัญขององค์ความรู้

5.1 หัวข้อความรู้ ประกอบด้วย

1) ความสำคัญของการดูแลข้อมูลในองค์กร

ข้อมูลเป็นทรัพยากรสำคัญที่ใช้สนับสนุนการบริหารจัดการและการปฏิบัติงานของวิทยาลัย ทั้งข้อมูลบุคลากร ข้อมูลนักศึกษา ข้อมูลการเงินและพัสดุ ตลอดจนข้อมูลการดำเนินงานของหน่วยงาน การดูแลข้อมูลจึงต้องคำนึงถึงความถูกต้อง ความครบถ้วน ความเป็นปัจจุบัน และการกำหนดสิทธิ์ในการเข้าถึงให้เหมาะสมกับหน้าที่ของผู้ใช้งาน

2) การใช้งานระบบสารสนเทศอย่างปลอดภัย

บุคลากรควรใช้งานระบบสารสนเทศของวิทยาลัยตามสิทธิ์ที่ได้รับมอบหมาย ไม่เปิดเผยบัญชีผู้ใช้และรหัสผ่านแก่บุคคลอื่น ไม่ใช้รหัสผ่านร่วมกัน และออกจากระบบทุกครั้งเมื่อใช้งานเสร็จ โดยเฉพาะเมื่อใช้งานผ่านคอมพิวเตอร์หรืออุปกรณ์ที่มีผู้ใช้งานร่วมกัน

3) การป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์อาจเกิดจากอีเมลหรือข้อความหลอกลวง เว็บไซต์ที่ไม่น่าเชื่อถือ ไฟล์แนบที่มีโปรแกรมไม่พึงประสงค์ หรือการเปิดเผยข้อมูลโดยไม่ระมัดระวัง ผู้ใช้งานจึงควรตรวจสอบแหล่งที่มาก่อนคลิกลิงก์ ดาวน์โหลดไฟล์ หรือเปิดเผยข้อมูลสำคัญ หากพบความผิดปกติควรแจ้งผู้รับผิดชอบระบบเพื่อดำเนินการตรวจสอบ

4) การรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล

การนำข้อมูลของนักศึกษา บุคลากร และบุคคลภายนอกไปใช้หรือเผยแพร่ต้องคำนึงถึงวัตถุประสงค์และสิทธิของเจ้าของข้อมูล ไม่เปิดเผยข้อมูลส่วนบุคคลเกินความจำเป็น และปฏิบัติตามกฎหมายที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5) ความรับผิดชอบร่วมกันในการรักษาความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์ไม่ใช่หน้าที่ของผู้ดูแลระบบเท่านั้น แต่เป็นความรับผิดชอบของบุคลากรทุกคน ผู้ใช้งานต้องปฏิบัติตามแนวทางที่หน่วยงานกำหนด รักษาข้อมูลที่ได้รับมอบหมาย และแจ้งเหตุผิดปกติที่อาจส่งผลกระทบต่อระบบหรือข้อมูลขององค์กรอย่างเหมาะสม

5.2 ปัญหาอุปสรรคที่พบ

1) บุคลากรมีระดับความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์แตกต่างกัน ทำให้การตระหนักรู้และการปฏิบัติตามแนวทางความปลอดภัยอาจไม่สม่ำเสมอ

2) การใช้งานระบบสารสนเทศหลายระบบจำเป็นต้องอาศัยความระมัดระวังในการจัดเก็บและส่งต่อข้อมูล รวมถึงการควบคุมสิทธิ์การเข้าถึง

3) ภัยคุกคามทางไซเบอร์มีรูปแบบเปลี่ยนแปลงอยู่เสมอ ผู้ใช้งานจึงจำเป็นต้องเรียนรู้และปรับพฤติกรรมการใช้งานให้เท่าทันสถานการณ์

4) การสร้างความเข้าใจให้บุคลากรทุกกลุ่มปฏิบัติตามแนวทางการรักษาความปลอดภัยอย่างต่อเนื่อง จำเป็นต้องอาศัยการสื่อสารและการแลกเปลี่ยนเรียนรู้ภายในองค์กร

6. วิธีการนำความรู้ไปใช้

1) นำองค์ความรู้ไปใช้เป็นแนวทางในการปฏิบัติงานของบุคลากรที่ต้องใช้ระบบสารสนเทศและข้อมูลของวิทยาลัย

2) จัดทำคู่มือการดูแลข้อมูลและการใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อเผยแพร่ให้บุคลากรภายในวิทยาลัยชุมชนสตูล

3) เผยแพร่คู่มือและองค์ความรู้ผ่านเว็บไซต์ของวิทยาลัยชุมชนสตูล เพื่อให้บุคลากรและผู้สนใจสามารถศึกษาและนำไปประยุกต์ใช้ได้

4) ใช้เป็นเนื้อหาประกอบการแลกเปลี่ยนเรียนรู้และสร้างความตระหนักรู้เกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์

5) นำข้อเสนอแนะและประเด็นที่พบจากการใช้งานจริงมาปรับปรุงแนวทางการดูแลข้อมูลให้เหมาะสมกับบริบทของวิทยาลัย

7. ผู้เรียนรู้

1) บุคลากรสายวิชาการและสายสนับสนุนของวิทยาลัยชุมชนสตูล
2) ผู้รับผิดชอบงานสารสนเทศและผู้ปฏิบัติงานที่เกี่ยวข้องกับการจัดเก็บและใช้ข้อมูล
3) ผู้บริหารและผู้รับผิดชอบงานบริหารจัดการข้อมูลของหน่วยงาน
4) บุคลากรที่ต้องใช้ระบบสารสนเทศในการปฏิบัติงานประจำวัน

8. ประสบการณ์ที่ประทับใจ

การได้มีส่วนร่วมในการแลกเปลี่ยนเรียนรู้เกี่ยวกับการดูแลข้อมูลและการใช้งานระบบสารสนเทศ ทำให้เห็นความสำคัญของการสร้างความเข้าใจให้บุคลากรทุกคนตระหนักถึงความปลอดภัยของข้อมูล เพราะแม้จะเป็นการใช้งานระบบในกิจวัตรประจำวัน แต่หากขาดความระมัดระวังอาจส่งผลกระทบต่อข้อมูลและการดำเนินงานขององค์กรได้ การถ่ายทอดความรู้จึงเป็นส่วนสำคัญที่ช่วยให้เกิดความเข้าใจร่วมกันและส่งเสริมการใช้เทคโนโลยีอย่างรับผิดชอบ

9. ข้อคิด

“ความมั่นคงปลอดภัยของข้อมูลเริ่มต้นจากความรับผิดชอบของผู้ใช้งานทุกคน การรู้เท่าทันภัยคุกคามและการปฏิบัติตามแนวทางความปลอดภัยอย่างสม่ำเสมอ จะช่วยลดความเสี่ยงและสร้างความเชื่อมั่นในการทำงานด้วยเทคโนโลยีดิจิทัล”

****

การถอดความรู้จากผู้รู้ในหน่วยงาน (Tacit Knowledge to Explicit Knowledge)

1. ผู้รู้ (ข้อมูลผู้รู้)



ชื่อผู้รู้ นายมนตรี กุมวาปี
ตำแหน่ง นักวิชาการคอมพิวเตอร์
ภูมิลำเนา จังหวัดสตูล
มือถือ 0835511837

2. ผู้ถอดความรู้

2.1 นางสาวสุนิสา สะแหละ

2.2 นายอุใบ หมัดหมุด

2.3 นางสาวนวรัตน์ ลิ่มสกุล

3. ชื่อหัวข้อความรู้

การดูแลและพัฒนาเว็บไซต์และระบบสารสนเทศ เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของวิทยาลัยชุมชนสตูล

4. ประโยชน์ของความรู้

1) ทำให้เกิดแนวทางในการดูแลและพัฒนาเว็บไซต์และระบบสารสนเทศของวิทยาลัยให้มีความเหมาะสมกับการใช้งาน

2) ช่วยให้ผู้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศเข้าใจความสำคัญของการดูแลระบบ การปรับปรุงซอฟต์แวร์ และการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์

3) สนับสนุนให้เว็บไซต์ของวิทยาลัยสามารถเผยแพร่ข้อมูลข่าวสารและให้บริการแก่ผู้ใช้งานได้อย่างมีประสิทธิภาพ

4) ส่งเสริมการรักษาความปลอดภัยในการรับส่งข้อมูลผ่านเว็บไซต์ด้วยการใช้ใบรับรอง SSL เพื่อเข้ารหัสการสื่อสาร

5) เป็นแนวทางในการพัฒนาระบบสารสนเทศให้มีความพร้อมใช้งานและรองรับการเปลี่ยนแปลงของเทคโนโลยี

6) ช่วยสนับสนุนการบริหารจัดการองค์กรด้วยระบบดิจิทัลอย่างเป็นระบบและต่อเนื่อง

5. เนื้อหาและสาระสำคัญขององค์ความรู้

5.1 หัวข้อความรู้ ประกอบด้วย

1) การดูแลและพัฒนาเว็บไซต์ของวิทยาลัย

เว็บไซต์เป็นช่องทางสำคัญในการประชาสัมพันธ์ข้อมูลข่าวสาร เผยแพร่ผลงาน และให้บริการข้อมูลแก่บุคลากร นักศึกษา และประชาชน การพัฒนาเว็บไซต์จึงต้องคำนึงถึงความถูกต้องของข้อมูล ความสะดวกในการเข้าถึง และความเหมาะสมกับอุปกรณ์ที่หลากหลาย ทั้งคอมพิวเตอร์ โทรศัพท์มือถือ และแท็บเล็ต

2) การปรับปรุงโครงสร้างและประสิทธิภาพเว็บไซต์

การปรับปรุงเว็บไซต์ควรให้ความสำคัญกับโครงสร้างเมนู การจัดหมวดหมู่เนื้อหา และความสะดวกในการค้นหาข้อมูล รวมถึงการปรับรูปแบบการแสดงผลให้เหมาะสมกับขนาดหน้าจอที่แตกต่างกัน เพื่อให้ผู้ใช้งานสามารถเข้าถึงข้อมูลได้อย่างสะดวกและรวดเร็ว

3) การใช้เทคโนโลยีเพื่อรักษาความปลอดภัยของเว็บไซต์

การใช้ใบรับรอง SSL เป็นแนวทางหนึ่งในการเข้ารหัสการสื่อสารระหว่างเว็บไซต์กับผู้ใช้งาน ช่วยลดความเสี่ยงจากการถูกดักอ่านข้อมูลระหว่างการรับส่งข้อมูล นอกจากนี้ยังควรตรวจสอบสถานะใบรับรองและการตั้งค่าที่เกี่ยวข้องให้เหมาะสมกับการใช้งาน

4) การป้องกันภัยคุกคามด้วยระบบ Firewall

Firewall เป็นกลไกสำคัญในการควบคุมและตรวจสอบการรับส่งข้อมูลเครือข่ายตามกฎที่กำหนด เพื่อช่วยป้องกันการเชื่อมต่อที่ไม่พึงประสงค์จากภายนอก การใช้งาน Firewall จึงควรควบคู่กับการกำหนดค่าที่เหมาะสมและการตรวจสอบการทำงานอย่างต่อเนื่อง

5) การปรับปรุงโปรแกรมและระบบ Server

การดูแลระบบ Server ต้องให้ความสำคัญกับการปรับปรุงโปรแกรมและรหัสคำสั่งให้มีความทันสมัย แก้ไขข้อบกพร่อง และลดช่องโหว่ที่อาจถูกใช้เป็นช่องทางโจมตีระบบ รวมถึงการตรวจสอบความพร้อมใช้งานของระบบและองค์ประกอบที่เกี่ยวข้อง

6) การดูแลระบบสารสนเทศที่สนับสนุนการปฏิบัติงาน

วิทยาลัยมีระบบสารสนเทศที่สนับสนุนภารกิจหลายด้าน เช่น ICCS-PORTAL, E-Office, E-HR.ICCS และ SMART ERPG การดูแลระบบเหล่านี้จำเป็นต้องคำนึงถึงความต่อเนื่องในการให้บริการ ความถูกต้องของข้อมูล และความปลอดภัยในการเข้าถึง โดยประสานงานกับผู้รับผิดชอบระบบตามขอบเขตหน้าที่

7) การติดตามและปรับปรุงระบบอย่างต่อเนื่อง

การดูแลระบบสารสนเทศไม่ใช่การดำเนินการเพียงครั้งเดียว แต่ต้องมีการตรวจสอบ ปรับปรุง และพัฒนาตามสภาพการใช้งานและความเปลี่ยนแปลงของภัยคุกคาม เพื่อให้ระบบมีความพร้อมและลดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานของวิทยาลัย

5.2 ปัญหาอุปสรรคที่พบ

1) เทคโนโลยีและภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงอย่างต่อเนื่อง ทำให้ต้องติดตามความรู้และปรับปรุงระบบให้ทันต่อสถานการณ์

2) การดูแลเว็บไซต์และระบบสารสนเทศต้องอาศัยความรู้เฉพาะด้าน ทั้งการจัดการเว็บไซต์ ระบบเครือข่าย Server และการรักษาความปลอดภัย

3) ระบบสารสนเทศมีองค์ประกอบและผู้เกี่ยวข้องหลายส่วน การแก้ไขหรือปรับปรุงระบบจึงต้องคำนึงถึงผลกระทบต่อการให้บริการและการปฏิบัติงาน

4) การพัฒนาเว็บไซต์ให้มีความสะดวกต่อผู้ใช้งานควบคู่กับการรักษาความปลอดภัย จำเป็นต้องพิจารณาทั้งด้านเทคนิคและประสบการณ์ของผู้ใช้งาน

5) การดูแลระบบให้มีความพร้อมใช้งานอย่างต่อเนื่องจำเป็นต้องมีการตรวจสอบและบำรุงรักษาอย่างเป็นระบบ

6. วิธีการนำความรู้ไปใช้

1) นำองค์ความรู้ไปใช้เป็นแนวทางในการดูแล ปรับปรุง และพัฒนาเว็บไซต์ของวิทยาลัยชุมชนสตูล

2) ใช้เป็นแนวทางในการตรวจสอบและบำรุงรักษาระบบ Server รวมถึงการปรับปรุงโปรแกรมและรหัสคำสั่งที่เกี่ยวข้อง

3) นำความรู้เกี่ยวกับ Firewall และ SSL ไปใช้ประกอบการดูแลความปลอดภัยของเว็บไซต์และระบบเครือข่ายตามขอบเขตความรับผิดชอบ

4) จัดทำคู่มือการดูแลเว็บไซต์และระบบสารสนเทศอย่างปลอดภัย เพื่อเผยแพร่ภายในวิทยาลัยชุมชนสตูล

5) เผยแพร่คู่มือและองค์ความรู้ผ่านเว็บไซต์ของวิทยาลัยชุมชนสตูล เพื่อให้บุคลากรและผู้เกี่ยวข้องสามารถศึกษาและใช้เป็นแนวทางในการปฏิบัติงาน

6) ใช้เป็นฐานความรู้สำหรับการแลกเปลี่ยนเรียนรู้และพัฒนากระบวนการดูแลระบบสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น

7. ผู้เรียนรู้

1) บุคลากรผู้รับผิดชอบงานเทคโนโลยีสารสนเทศและระบบเครือข่าย
2) ผู้ดูแลเว็บไซต์และระบบสารสนเทศของวิทยาลัย
3) บุคลากรที่เกี่ยวข้องกับการบริหารจัดการและให้บริการผ่านระบบดิจิทัล
4) บุคลากรสายสนับสนุนที่ต้องประสานงานด้านระบบสารสนเทศ
5) ผู้สนใจด้านการพัฒนาเว็บไซต์และความมั่นคงปลอดภัยทางไซเบอร์

8. ประสบการณ์ที่ประทับใจ

การพัฒนาและปรับปรุงเว็บไซต์และระบบสารสนเทศของวิทยาลัยเป็นงานที่ต้องคำนึงถึงทั้งประสิทธิภาพ ความสะดวกของผู้ใช้งาน และความปลอดภัยของข้อมูล การดำเนินงานที่เกี่ยวข้องกับการใช้ Firewall การติดตั้งใบรับรอง SSL การปรับปรุงโปรแกรมบน Server และการพัฒนาเว็บไซต์ให้รองรับอุปกรณ์ที่หลากหลาย สะท้อนให้เห็นว่าการพัฒนาระบบดิจิทัลต้องดำเนินควบคู่ไปกับการดูแลความมั่นคงปลอดภัย และต้องมีการเรียนรู้ปรับปรุงอย่างต่อเนื่อง

9. ข้อคิด

“ระบบสารสนเทศที่ดีไม่ใช่เพียงระบบที่ใช้งานได้สะดวก แต่ต้องมีความปลอดภัย เชื่อถือได้ และได้รับการดูแลอย่างต่อเนื่อง การพัฒนาเทคโนโลยีจึงต้องดำเนินควบคู่กับการบริหารความเสี่ยงและการเรียนรู้อย่างไม่หยุดนิ่ง”

****

สถาบันวิทยาลัยชุมชน
INSTITUTE OF COMMUNITY COLLEGES

วิทยาลัยชุมชนสตูล
SATUN COMMUNITY COLLEGE



กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

วิทยาลัยชุมชนสตูล
271 หมู่ 4 ตำบลเกตรี อำเภอเมืองสตูล
จังหวัดสตูล 91140

เว็บไซต์
www.stcc.ac.th