ด้านที่ 5
ด้านพัฒนาและบริหารจัดการองค์กร

แนวปฏิบัติที่ดีในการพัฒนา
ความมั่นคงปลอดภัยระบบสารสนเทศ

สังเคราะห์องค์ความรู้จากการจัดการความรู้

(Knowledge Management Synthesis)

ประเด็นการจัดการความรู้แนวปฏิบัติที่ดีการพัฒนา

ความมั่นคงปลอดภัยระบบสารสนเทศ วิทยาลัยพยาบาลบรมราชชนนี สงขลา

แนวปฏิบัติที่ดีด้านการพัฒนาความมั่นคงปลอดภัยของระบบสารสนเทศ ของวิทยาลัยพยาบาลบรม ราชชนนี สงขลา พัฒนาขึ้นจากการจัดการความรู้ตามกรอบแนวคิด "การขับเคลื่อนนวัตกรรมตามเกณฑ์ ประเมิน KM to IM" โดยการถอดบทเรียนความสำเร็จและสร้างโมเดลเชิงแนวคิดในการยกระดับองค์กรสู่ ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อนำสู่การประกาศนโยบายและเผยแพร่แนวปฏิบัติให้กับ หน่วยงานในสังกัดคณะพยาบาลศาสตร์ สถาบันพระบรมราชชนก หรือหน่วยงานอื่นที่สนใจ มีรายละเอียด ดังนี้

1. การกำหนดวัตถุประสงค์และผลลัพธ์ที่เกิดขึ้น (Objectives & Outcomes)

การดำเนินงานจัดการความรู้ในเรื่องนี้มีการกำหนดเป้าหมายและผลลัพธ์ที่เชื่อมโยงกันอย่างเป็นระบบ ตั้งแต่ระดับบุคคล ระดับหน่วยงาน จนถึงระดับองค์กร ดังนี้

- **ระดับบุคคล (Individual Level) :**
  - **วัตถุประสงค์:** เพื่อให้อาจารย์และบุคลากร (กลุ่มเป้าหมายจำนวน 20 คน) มีองค์ความรู้ ความเข้าใจ และมีแนวปฏิบัติที่ถูกต้องในการบริหารจัดการความมั่นคงปลอดภัยระบบ สารสนเทศ การจัดการความเสี่ยงและการควบคุมดูแลทรัพย์สินสารสนเทศ
  - **ผลลัพธ์ (Outcomes):** บุคลากรเกิดการพัฒนาทักษะและความตระหนักรู้ (Cybersecurity Awareness) มีแนวปฏิบัติที่เป็นไปในทิศทางเดียวกัน สามารถปฏิบัติงานตามคู่มือและ นโยบายความปลอดภัยไซเบอร์ระบบคลาวด์ได้อย่างถูกต้องและมีประสิทธิภาพ
- **ระดับหน่วยงาน/กลุ่มงาน (Departmental/CoP Level) :**
  - **วัตถุประสงค์:** เพื่อสร้างพื้นที่การแลกเปลี่ยนเรียนรู้ร่วมกันของชุมชนนักปฏิบัติ (CoP) พัฒนาโครงสร้างพื้นฐานระบบสารสนเทศให้มีพื้นที่เพียงพอ ลดงบประมาณในการดูแลระบบ และแก้ไขปัญหาทางเทคนิค เช่น ระบบไม่พร้อมใช้งาน หรือ Server ชำรุดเสียหาย

- **ผลลัพธ์ (Outcomes):** เกิดคลังความรู้และสินทรัพย์ความรู้ (Knowledge Assets) ที่ สำคัญ 4 รายการ ได้แก่ คู่มือการพัฒนาความมั่นคงปลอดภัยระบบสารสนเทศ, ทะเบียน ทรัพย์สินบริการสำคัญ, แผนการจัดการความเสี่ยง และนโยบายความมั่นคงปลอดภัยไซเบอร์ ระบบคลาวด์. มีการย้ายระบบไปสู่ระบบคลาวด์กลางภาครัฐ (GDCC) ทำให้ได้พื้นที่บริการ อย่างน้อย 1 TB และมีระบบเฝ้าระวังภัยคุกคามอย่างน้อย 3 ระบบ

• **ระดับองค์กร (Organizational Level) :**

- **วัตถุประสงค์ :** เพื่อให้ระบบสารสนเทศของวิทยาลัยฯ มีความพร้อมใช้งาน (Availability) มี ความถูกต้องครบถ้วนของข้อมูล (Integrity) สอดคล้องตามมาตรการทางกฎหมาย (PDPA พ.ศ. 2565) และมาตรฐานความปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567. รวมถึงการเตรียมความพร้อมด้านแผนความต่อเนื่องทางธุรกิจ (BCP)
- **ผลลัพธ์ (Outcomes):** อุบัติการณ์การหยุดชะงักของระบบสารสนเทศจากไฟฟ้าขัดข้อง ลดลงเหลือร้อยละ 0. องค์กรมีความสามารถในการกู้คืนระบบจากการโจมตีทางไซเบอร์ได้ ภายใน 24 ชั่วโมง. ระบบผ่านเกณฑ์มาตรฐานของ สกมช. และที่สำคัญที่สุดคือองค์กรได้รับ การยอมรับในระดับชาติ โดยได้รับรางวัล Prime Minister Award: Thailand Cybersecurity Excellence Award ติดต่อกัน 2 ปีซ้อน (ปี 2024 และ 2025)

2. การวิเคราะห์ระดับองค์ความรู้ตามขั้นตอนการพัฒนานวัตกรรม (KM to IM Matrix)

เมื่อนำกรอบแนวคิดการขับเคลื่อนนวัตกรรม 6 ขั้นตอน (KM to IM) มาวิเคราะห์กระบวนการ ยกระดับองค์ความรู้ของวิทยาลัยฯ จากความรู้เดิม (As-Is) ไปสู่ความรู้เป้าหมาย (To-Be) โดยพบว่าแนวปฏิบัติ ที่ดีด้านการพัฒนาความมั่นคงปลอดภัยของระบบสารสนเทศ ของวิทยาลัยพยาบาลบรมราชชนนี สงขลา อยู่ ในระดับ IB (Innovation Based) - ความรู้เพื่อพัฒนานวัตกรรม: (ระดับเป้าหมายสูงสุดที่องค์กรบรรลุ) องค์กรสามารถยกระดับกระบวนการจัดการความรู้ (KM) ไปสู่นวัตกรรมการ

บริหารจัดการองค์กร (IM) ที่มี ความมั่นคงปลอดภัยสูง เกิดเป็นนโยบายและโมเดลการทำงานที่สามารถเป็นต้นแบบ (Best Practice) ให้แก่ สถาบันการศึกษาอื่นๆ และส่งผลให้ได้รับรางวัลเกียรติยศระดับประเทศ (Prime Minister Award)

3. แนวทางการสร้างแนวปฏิบัติที่ดีตามกระบวนการจัดการความรู้ (KM Process)

วิทยาลัยฯ ได้ประยุกต์ใช้กระบวนการจัดการความรู้อย่างเป็นขั้นตอนจนเกิดเป็นแนวปฏิบัติที่ดี (Best Practice) ดังนี้

- **การสร้างและแสวงหาความรู้ (Knowledge Creation & Acquisition):** เริ่ม จากการศึกษา วิเคราะห์ปัญหาเชิงลึก แยกส่วนการทำงานของระบบสำรองข้อมูลเดิม และแสวงหาเทคโนโลยีใหม่ อย่างระบบคลาวด์ภาครัฐ (GDCC) เพื่อรองรับการเปลี่ยนผ่าน
- **การจัดการความรู้ให้เป็นระบบและการจัดเก็บ (Knowledge Organization & Storage):** นำ องค์ความรู้ทางเทคนิคและแนวปฏิบัติมารวบรวมจัดทำเป็น "คู่มือการพัฒนาความมั่นคงปลอดภัย ระบบสารสนเทศ" และนำไปจัดเก็บไว้บนระบบคลาวด์ เพื่อให้สมาชิกทุกคนสามารถเข้าถึงคลังความรู้ นี้ได้สะดวกตลอดเวลา
- **การประมวลและกลั่นกรองความรู้ (Knowledge Codification & Refinement):** คณะกรรมการการจัดการความรู้ทำหน้าที่ติดตาม ตรวจสอบและกลั่นกรองเนื้อหาให้มีความครบถ้วน ถูกต้อง แม่นยำ และเหมาะสมกับการนำไปปฏิบัติงานจริง
- **การดำเนินการแลกเปลี่ยนเรียนรู้ (Knowledge Sharing):** จัดตั้งกลุ่ม CoP จำนวน 20 คน ประกอบด้วยผู้บริหาร (ผู้นำนโยบาย) และผู้ปฏิบัติงาน โดยมีการเชิญภาคีเครือข่ายภายนอกที่มีความ เชี่ยวชาญเฉพาะทาง (เช่น สกมช., GDCC, NT) มาเป็นที่ปรึกษา มีการแลกเปลี่ยนเรียนรู้ผ่านรูปแบบ On-site, ออนไลน์ และการนำไปเสนอในเวทีวิทยาลัยเครือข่าย
- **การนำความรู้ไปปฏิบัติจริงและการปรับปรุง (Knowledge Application & Lesson Learned):** มีการนำคู่มือและนโยบายไปใช้จริงทั้งในระยะสั้น (คุมทรัพย์สิน บริหารความเสี่ยง ทำแผน BCP) และ ระยะยาว (ทดสอบแผน เจาะ

ระบบ อย่างน้อยปีละ 1 ครั้ง) พร้อมทั้งบันทึกข้อควรปรับปรุงเพื่อนำไป พัฒนาแผน BCP ประจำปีต่อไป

4. แก่นความรู้และกรอบแนวคิดที่ได้จากการสังเคราะห์ (Knowledge Statement & Model) แก่นความรู้ (Knowledge Statement) :

"กระบวนการยกระดับความมั่นคงปลอดภัยไซเบอร์สู่ระบบคลาวด์ที่ยั่งยืน (Cybersecurity Cloud Transformation)" คือการบูรณาการมาตรฐานกฎหมายความปลอดภัยข้อมูล (PDPA & Cloud Security Standards) เข้ากับวงจรการพัฒนาระบบ (SDLC) และแผนความต่อเนื่องทางธุรกิจ (BCP) โดย ขับเคลื่อนผ่านชุมชนนักปฏิบัติ (CoP) และเครือข่ายผู้เชี่ยวชาญ เพื่อเปลี่ยนผ่านจากการตั้งรับปัญหาไปสู่การเฝ้าระวังเชิงรุกและการฟื้นฟูระบบอย่างรวดเร็ว

โมเดลเชิงแนวคิดที่ได้จากการสังเคราะห์: "SECURE-Cloud Model"

จากการถอดบทเรียนและสังเคราะห์เอกสาร สามารถสรุปออกมาเป็นโมเดลการบริหารจัดการความรู้ สู่นวัตกรรมความปลอดภัยไซเบอร์ ดังภาพจำลองและคำอธิบายนี้

• **S - System & Standards Driven:** ขับเคลื่อนด้วยทฤษฎีระบบ วงจร SDLC, PDCA และยึดโยง เกณฑ์มาตรฐานกฎหมาย (PDPA 2565 / มาตรฐาน สกมช. 2567) เป็นตัวตั้ง

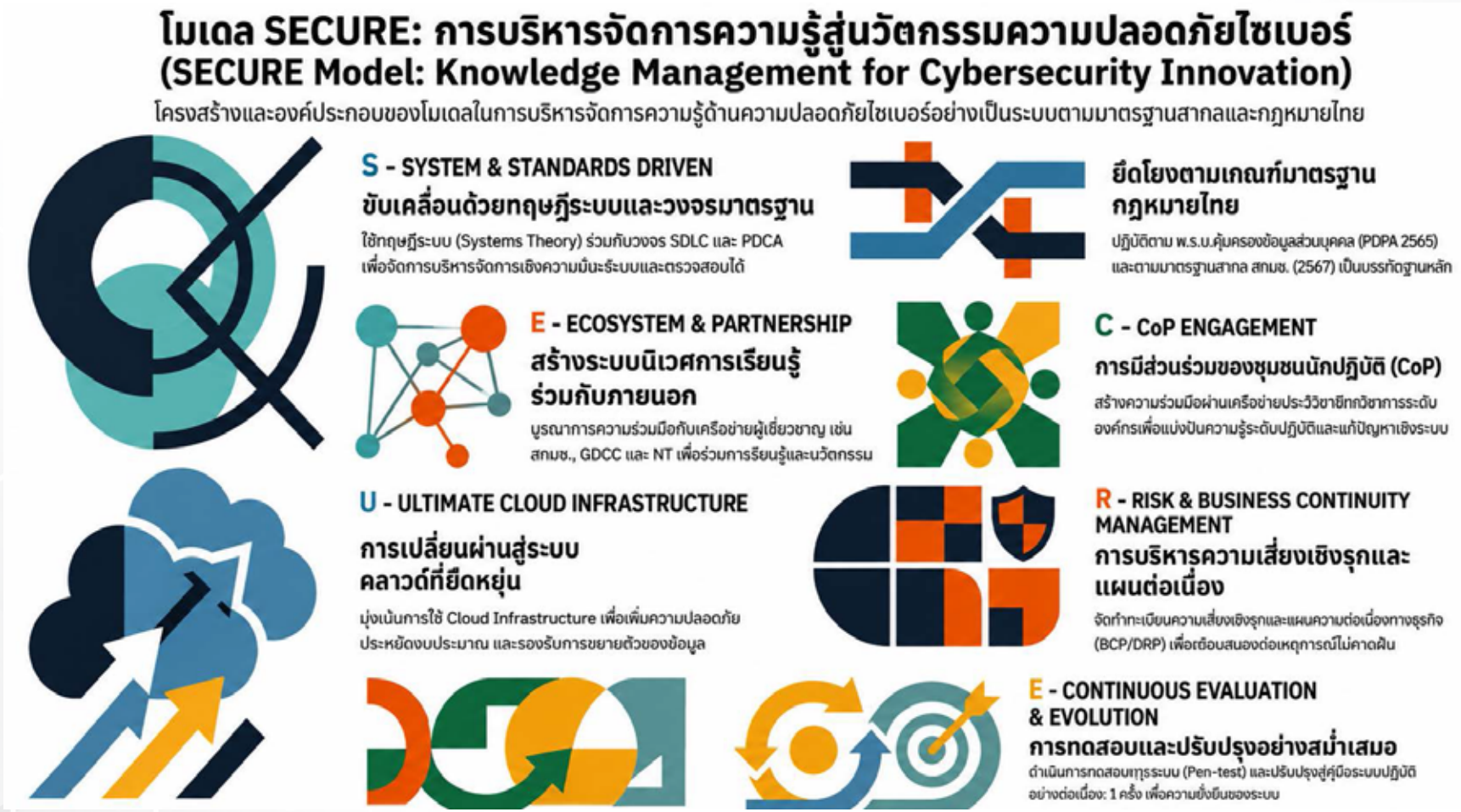
• **E - Ecosystem & Partnership:** การสร้างระบบนิเวศการเรียนรู้ที่มีเครือข่ายผู้เชี่ยวชาญภายนอก (สกมช., GDCC, NT) คอยสนับสนุนเชิงเทคนิค

• **C - CoP Engagement:** ชุมชนนักปฏิบัติที่เหนียวแน่น มีสมาชิกจากทุกระดับ (ผู้บริหารจนถึง ผู้ปฏิบัติงาน) ร่วมมือกัน

• **U - Ultimate Cloud Infrastructure:** การเปลี่ยนผ่านโครงสร้างพื้นฐานสู่ระบบคลาวด์ที่มีความ ยืดหยุ่น ปลอดภัย และประหยัดงบประมาณ

• **R - Risk & Business Continuity Management**: การบริหารความเสี่ยงเชิงรุกผ่านการทำ ทะเบียนทรัพย์สิน และการจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP/DRP)

• **E - Continuous Evaluation & Evolution:** การทดสอบเจาะระบบและปรับปรุงคู่มือแนวปฏิบัติ อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อความยั่งยืน



ประเด็นที่ 6 : โมเดล SECURE: การบริหารจัดการความรู้สู่นวัตกรรมความปลอดภัยไซเบอร์ (SECURE-Cloud Model)

5. ปัจจัยแห่งความสำเร็จ (Key Success Factors: KSFs)

ปัจจัยสำคัญที่ผลักดันให้การจัดการความรู้ฉบับนี้ประสบความสำเร็จอย่างโดดเด่นและได้รับรางวัล ระดับชาติ ประกอบด้วย 4 ปัจจัยหลัก

1. Tone from the Top (การสนับสนุนอย่างจริงจังจากผู้บริหาร) : ผู้บริหารระดับสูงของวิทยาลัยฯ (ผู้อำนวยการและรองผู้อำนวยการ) ไม่เพียงแต่อนุมัตินโยบาย แต่ยังเข้าร่วมเป็นสมาชิกในกลุ่ม CoP อย่างใกล้ชิด ช่วยผลักดัน ทุ่มเททรัพยากร และเชื่อมโยงงาน KM เข้ากับแผนยุทธศาสตร์องค์กร.

2. Strategic Alliance (การมีภาคีเครือข่ายเชี่ยวชาญเฉพาะทาง): งานเทคโนโลยีเชิงลึกต้องการ ผู้เชี่ยวชาญ การที่องค์กรดึงเอาหน่วยงานระดับประเทศ เช่น สกมช. (สำนักงานคณะกรรมการการ รักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ), ผู้ให้บริการ Cloud GDCC และ NT เข้ามาร่วมเป็นที่ ปรึกษา ทำให้องค์ความรู้ที่ได้รับมีความถูกต้อง ทันสมัย และเป็นไปตามมาตรฐานสากล

3. Cross-functional Collaboration (การทำงานร่วมกันแบบบูรณาการ): สมาชิก CoP จำนวน 20 คน มาจากหลากหลายกลุ่มงาน (บริหาร, ยุทธศาสตร์, ไอที, งานสารบรรณ, บรรณารักษ์) ทำให้ เกิดการมองปัญหาแบบรอบด้าน เกิดการสะท้อนคิด (Reflective Thinking) และสามารถนำคู่มือไป กระจายใช้ปฏิบัติงานได้จริงทั่วทั้งหน่วยงาน

4. Agile & Continuous Improvement Process (กระบวนการทำงานที่ยืดหยุ่นและต่อเนื่อง): มี การประยุกต์ใช้กรอบแนวคิด PDCA ร่วมกับ SDLC อย่างเหนียวแน่น มีกระบวนการตรวจสอบ (Check) และปรับปรุง (Act) เป็นระยะชัดเจน มีข้อกำหนดให้ต้องทดสอบกู้คืนระบบและเจาะระบบ (Penetration Test) ทุกปี ทำให้แนวปฏิบัติไม่ล้าสมัยและพร้อมรับมือภัยคุกคามรูปแบบใหม่ๆ เสมอ