IS PRACTICE

ขีดความสามารถด้านความมั่นคงปลอดภัยสารสนเทศ

Photo by Akira Hojo on Unsplash
“ความมั่นคงปลอดภัยสารสนเทศ คือ การคงไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ ของสารสนเทศ”

ที่มาและความสำคัญ

เอกสารฉบับนี้อธิบายถึงแนวปฏิบัติการทำงานของเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศและผู้ที่เกี่ยวข้อง ในการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ รวมถึงการใช้มาตรการในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ที่เกี่ยวข้องกับคณะแพทยศาสตร์มหาวิทยาลัยสงขลานครินทร์

Informative Reference: ISO/IEC 27001:2022 Security Controls
Document Unique Identification: IS-PR
Document Version: 2569-17June
Language: TH

Reviewed By: นายจรูญ แก้วมี และ นายโกเมน เรืองฤทธิ์
Approved By: ผศ.นพ.บุญชัย หวังศุภดิลก

อนุมัติตามหนังสือเลขที่ มอ 104.0135210/69-00410

2569-June 17, 2026

คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

ข้อมูลข่าวสารราชการ ประเภท แนวปฏิบัติภายใน

สารบัญ

ศัพท์และคำนิยามที่ใช้ในเอกสาร

นอกเหนือจากที่ระบุไว้ในเอกสารฉบับนี้ให้ยึดตามมาตรฐานสากล ISO/IEC27000 เป็นสำคัญ

คำนิยามที่ใช้ในแนวปฏิบัตินี้ประกอบด้วย

“คณะแพทยศาสตร์” หมายถึง คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของคณะแพทยศาสตร์

“ฝ่ายเทคโนโลยีสารสนเทศ” หมายถึง ฝ่ายเทคโนโลยีสารสนเทศเป็นหน่วยงานที่ให้บริการด้าน เทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายของคณะแพทยศาสตร์

“รองคณบดีฝ่ายเวชสารสนเทศ” หมายถึง ผู้มีอำนาจในด้านเทคโนโลยี สารสนเทศและการสื่อสารของคณะแพทยศาสตร์ ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนด นโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศและการสื่อสารของคณะแพทยศาสตร์

“มาตรฐาน” (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย

“วิธีการปฏิบัติ” (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มา ซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้ สามารถบรรลุเป้าหมายได้ง่ายขึ้น

“ผู้ใช้” หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่ง คณะแพทยศาสตร์กำหนดไว้ดังนี้

“ผู้บริหาร” หมายถึง ผู้มีอำนาจบริหารในระดับสูงของคณะแพทยศาสตร์ เช่น หัวหน้าหน่วยงาน เป็นต้น

“ผู้ดูแลระบบ” (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจาก ผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถ เข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานเงินรายได้คณะแพทยศาสตร์ ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการของคณะแพทยศาสตร์

“นักศึกษา” หมายถึง นักศึกษาของคณะแพทยศาสตร์

“หน่วยงานภายนอก” หมายถึง บุคคลหรือนิติบุคคลภายนอกที่คณะแพทยศาสตร์อนุญาตให้มีสิทธิ์ในการ เข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของคณะแพทยศาสตร์ โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจ หน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“ข้อมูลคอมพิวเตอร์” หมายถึงข้อมูลข้อความ คำสั่งชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ใน สภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมาย ว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“สารสนเทศ” (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัด ระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจ ได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดย ได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำ หน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและ สารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆของคณะแพทยศาสตร์ได้เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น

“ระบบ LAN และระบบอินทราเน็ต” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบ คอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการ ติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่ นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและ ควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ระบบเครือข่าย โปรแกรม ข้อมูล และ สารสนเทศ เป็นต้น

“ระบบสารสนเทศโรงพยาบาล” (Hospital Information System: HIS) หมายถึง ระบบงานสารสนเทศส่วนการบริหารและการบริการข้อมูลผู้ป่วย และข้อมูลสุขภาพ ภายใต้การดูแลของโรงพยาบาลสงขลานครินทร์

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

“พื้นที่ทำงานทั่วไป” (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา (Notebook)ที่ประจำโต๊ะทำงาน

“พื้นที่ทำงาน งานบริการโรงพยาบาล” (HIS service area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย ทั้งชนิดส่วนบุคคล (PC) และชนิดพกพา (Notebook) ของระบบงานสารสนเทศโรงพยาบาลสงขลานครินทร์ เช่น หอผู้ป่วย คลินิกผู้ป่วยนอก ห้องจ่ายยา เป็นต้น

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“ทรัพย์สิน” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของ หน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์เป็นต้น

“จดหมายอิเล็กทรอนิกส์” (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน เครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้มาตรฐานที่ใช้ใน การรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

“รหัสผ่าน” (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

“ชุดคำสั่งไม่พึงประสงค์” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่ง อื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ” (Information Security Management System: ISMS) หมายถึง กรอบแนวทางอันเป็นองค์ประกอบของ นโยบาย กระบวนการ

เทคโนโลยี และบุคลากร ที่ทำให้หน่วยงานบรรลุวัตถุประสงค์ของการสร้างความมั่นคงปลอดภัยสารสนเทศ

“ความมั่นคงปลอดภัยสารสนเทศ” (Information Security) หมายถึง การรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของสารสนเทศ

“การทดสอบเจาะระบบ” (Penetration Testing) หมายถึง การทดสอบความปลอดภัยเชิงรุกโดยจำลองการโจมตีจากผู้ไม่ประสงค์ดีเพื่อค้นหาและพิสูจน์ช่องโหว่ของระบบก่อนถูกโจมตีจริง

“การทดสอบความปลอดภัยแบบวิเคราะห์โค้ด” (Static Application Security Testing: SAST) หมายถึง การตรวจสอบความปลอดภัยด้วยการวิเคราะห์ซอร์สโค้ดขณะที่ระบบยังไม่ทำงาน เพื่อค้นหาจุดอ่อนในการเขียนโปรแกรมก่อนนำระบบขึ้นใช้งาน

“การทดสอบความปลอดภัยขณะทำงาน” (Dynamic Application Security Testing: DAST) หมายถึง การตรวจสอบความปลอดภัยของแอปพลิเคชันขณะทำงานจริงจากภายนอกเสมือนเป็นผู้โจมตี โดยไม่ต้องเข้าถึงซอร์สโค้ด

ระบบการใช้คำใกล้เคียง

การใช้ระบบคำใกล้เคียงที่ให้ความหมายหรือนัยสำคัญในทำนองเดียวกัน แม้ว่าจะไม่ใช่คำเดียวกัน ให้ถือว่ามีความหมายเดียวกันภายใต้บริบทที่กำหนด โดยไม่คำนึงถึงภาษาที่ใช้ ได้แก่

- สูงมาก: Extreme, Critical, Very High, ฯลฯ
- ต่ำมาก: Very Low, Insignificant, ฯลฯ
- ระบบสารสนเทศ: แอพพลิเคชั่น

บทบาทหน้าที่สำคัญ

ผู้อนุมัติการเปลี่ยนแปลง: โดยปกติแล้วหัวหน้าฝ่ายเทคโนโลยีสารสนเทศเป็นผู้อนุมัติการเปลี่ยนแปลง ยกเว้น กรณี การเปลี่ยนแปลงต้องการทรัพยากรเพิ่มเติม จะต้องจัดส่งให้รองคณบดีฝ่ายเวชสารสนเทศ เป็นผู้พิจารณาอนุมัติการจัดสรรทรัพยากร

ผู้ตรวจทานการเปลี่ยนแปลง: หัวหน้างานเครือข่ายและฐานข้อมูล

ผู้ร้องขอการเปลี่ยนแปลง: เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

ผู้บันทึกรายการอุบัติการณ์: เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ ที่พบเหตุผิดปกติ (แม้ว่าจะยังไม่ได้รับการยืนยันว่าเป็นอุบัติการณ์ก็ตาม)

ผู้ดำเนินการแก้ไขอุบัติการณ์: เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

บุคคลภายนอก หรือ หน่วยงานภายนอก: บุคคลภายนอกทั้งบุคคลธรรมดา หรือนิติบุคคล หรือตัวแทนจากนิติบุคคล ที่ให้บริการหรือติดต่อองค์กร เช่น ผู้รับเหมา ผู้รับเหมาที่จ้างช่วง ที่ปรึกษา ผู้สอบบัญชี ลูกค้า และบุคคลอื่น ๆ

ผู้ดูแลบุคคลภายนอก: เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่มีความรับผิดชอบต่อบุคคลภายนอกหรือหน่วยงานภายนอก

แนวปฏิบัติการจัดการการเปลี่ยนแปลง

Change Management Procedure

แนวปฏิบัตินี้คือเพื่อให้แน่ใจว่าการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ องค์ประกอบของเทคโนโลยีสารสนเทศ และระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ มีการควบคุม กำกับ ติดตาม และวางแผน อย่างเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงกับบริการและการปฏิบัติงานของเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

๑. การเปลี่ยนแปลงจำแนกเป็น 4 ประเภท สำคัญ

๑.๑ Standard change: การเปลี่ยนแปลงที่ทำซ้ำได้ ที่มีโอกาสเกิดขึ้นอย่างเป็นประจำ ซึ่งได้รับอนุญาตล่วงหน้าจาก Change Manager ตัวอย่าง เช่น ปรับปรุงฐานข้อมูล Anti-Virus, ปรับปรุง Certificate SSL, Upgrade Firmware ของอุปกรณ์ต่างๆ.

๑.๒ Minor Change: การเปลี่ยนแปลงที่เป็นไปตามขั้นตอนที่กำหนดอาจมีผลกระทบ เช่น การเปลี่ยนเงื่อนไขบน Firewall การเปลี่ยนแปลงเอกสาร (Document Control) การติดตั้ง Patch

๑.๓ Major Change: การเปลี่ยนแปลงที่เป็นไปตามขั้นตอนที่กำหนด และมีการวางแผนอย่างละเอียดรัดกุม เพราะอาจมีผลกระทบสูง เช่น การเปลี่ยนแปลงที่อาจจะกระทบกับระบบสารสนเทศ การเปลี่ยนแปลงใน

องค์ประกอบของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ

๑.๔ Emergency Change: การเปลี่ยนแปลงที่จะนำมาใช้โดยเร็วที่สุด เนื่องจากผลกระทบด้านลบที่อาจเกิดขึ้นกับบริการ อย่างไรก็ตามการเปลี่ยนแปลงฉุกเฉินใดๆ จะยังคงได้รับอนุญาตจากผู้อนุมัติ ย้อนหลัง

๒. การพิจารณาประเภทของการเปลี่ยนให้อ้างอิงผลกระทบที่อาจเกิดขึ้นตามเกณฑ์ด้านความเสี่ยงของหน่วยงาน ยกเว้นการเปลี่ยนแปลงแบบเร่งด่วน ให้พิจารณาควบคู่กับความเร่งด่วนหรือความต้องการในการเปลี่ยนแปลงประกอบด้วย

๓. การดำเนินการเปลี่ยนแปลงจะต้องคำนึงในการทำงาน และคำนึงถึงช่วงเวลาที่จะส่งผลกระทบน้อยที่สุด อาทิ ช่วงเวลาที่ระบบสารสนเทศสำคัญมีการเข้าถึงน้อย

๔. ขั้นตอนการจัดการการเปลี่ยนแปลงต้องจัดทำโดยให้เป็นขั้นตอนที่สอดคล้องกันเป็นมาตรฐาน สอดรับกับบริบท และสามารถปฏิบัติได้จริง

๕. จัดให้มีการทบทวนขั้นตอนการจัดการการเปลี่ยนแปลงเป็นประจำทุกปี

๖. จัดให้มีรายการสรุปการเปลี่ยนแปลงรายเดือน

๗. การเปลี่ยนแปลงระบบและบริการที่มีการจัดหาให้กับองค์กรโดยผู้ให้บริการภายนอกจะต้องอยู่ภายใต้ขั้นตอนการจัดการการเปลี่ยนแปลง

๘. ทุกการเปลี่ยนแปลงที่เกิดขึ้นจะถูกจดบันทึกลงในระบบ Service Desk สำหรับการติดตาม และจัดการอย่างเป็นระบบ รหัส (Code) ที่ใช้สำหรับการบันทึกแต่ละประเภทของการเปลี่ยนแปลงจะถูกกำหนดไว้อย่างชัดเจน สามารถศึกษารายละเอียดเกี่ยวกับรหัสและขั้นตอนที่เกี่ยวข้องได้จากคู่มือการใช้งานที่มีในระบบ Service Desk

๙. การเปลี่ยนแปลงในกรณีฉุกเฉินจะถูกบันทึกย้อนหลังในระบบการจัดการการเปลี่ยนแปลงภายในวันทำการถัดไป

๑๐. การเปลี่ยนแปลงควรได้รับการบันทึกและวางแผนล่วงหน้าเสมอ การเกิดขึ้นของการเปลี่ยนแปลงฉุกเฉินเป็นพฤติการณ์ที่ไม่ควรเกิดขึ้น

๑๑. ในบางกรณี ควรจัดให้มีการทดสอบการเปลี่ยนแปลงเพื่อให้มั่นใจว่าสามารถเปลี่ยนแปลงได้

๑๒. ในบางกรณี ควรจัดทำแผนการกู้คืนหรือเผชิญเหตุเมื่อการเปลี่ยนแปลงล้มเหลว

๑๓. ขั้นตอนการเปลี่ยนแปลงมีดังนี้

๑๓.๑ ผู้ร้องขอการเปลี่ยนแปลงกรอกข้อมูลให้ครบถ้วนในระบบ Service Desk

๑๓.๒ เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ วิเคราะห์คำร้องและมอบหมายการเปลี่ยนแปลงให้บุคคลที่เกี่ยวข้อง โดยให้มอบหมายถึงผู้อนุมัติและผู้ตรวจทานการเปลี่ยนแปลงด้วย

๑๓.๓ กรณีผู้อนุมัติไม่มีการโต้แย้ง ในการมอบหมายให้ถือว่าการเปลี่ยนแปลงมีผลอนุมัติให้ดำเนินการ ยกเว้นการเปลี่ยนแปลงเร่งด่วน (emergency) ให้ดำเนินการทันที

๑๓.๔ เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่ได้รับมอบหมายดำเนินการเปลี่ยนแปลงกรอกข้อมูลการดำเนินการและผลการดำเนินการให้ครบถ้วน

๑๓.๕ ผู้ตรวจทานการเปลี่ยนแปลงต้องตรวจทานคำขอและแนวทางการดำเนินการการเปลี่ยนแปลง เพื่อให้แน่ใจว่ารายละเอียดการเปลี่ยนแปลงมีความถูกต้อง

แนวปฏิบัติการจัดการทรัพย์สินสารสนเทศ

Asset Management Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่า หน่วยงานมีการบริหารจัดการทรัพย์สินสารสนเทศ

๑๔. ทรัพย์สินสารสนเทศที่สำคัญแบ่งออกเป็น 6 ประเภท 1) Hardware, 2) Software, 3) Information, 4) Service 5) People และ 6) Facility (สิ่งอำนวยความสะดวก เช่น ศูนย์คอมพิวเตอร์ ระบบไฟฟ้า UPS ระบบปรับอากาศ Data Center)

๑๕. ทรัพย์สินสารสนเทศต้องประเมินความสำคัญ (Criticality) บนพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ 3 ประการ (CIA) ซึ่งหลักเกณฑ์เชิงคุณภาพมีดังนี้

๑๕.๑ ระดับ 1: การสูญเสียคุณลักษณะ CIA ไม่กระทบต่อความสามารถในการปฏิบัติงานของเจ้าหน้าที่ หรือมี

ผลกระทบน้อยมาก หรือเป็นบริการเสริมที่ไม่สำคัญทางการแพทย์

๑๕.๒ ระดับ 2: การสูญเสียคุณลักษณะ CIA กระทบต่อบริการทั่วไปของคณะแพทยศาสตร์ แต่ไม่กระทบต่อ HIS และการให้บริการทางการแพทย์

๑๕.๓ ระดับ 3: การสูญเสียคุณลักษณะ CIA กระทบต่อบริการ HIS และการให้บริการทางการแพทย์

๑๖. ให้นำค่าผลกระทบ CIA มาบวกกันเมื่อทรัพย์สินมีค่ามากกว่าหรือเท่ากับ 7 ถือเป็นทรัพย์สินสารสนเทศที่สำคัญต้องนำไปประเมินความเสี่ยง โดยการประเมินความเสี่ยงต้องครอบคลุมการตรวจทานช่องโหว่ของทรัพย์สินสารสนเทศนั้น

๑๗. สารสนเทศ (Information) ต้องถูกกำหนดระดับชั้นความลับตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ เมื่อไม่ปรากฏการระบุชั้นความลับ ให้ยึดถือเป็นข้อมูลภายใน (Internal Use) ที่ไม่สามารถเปิดเผยแก่สาธารณะได้เสมอ

๑๘. สารสนเทศ ที่มีระดับชั้นความลับตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ ให้ดำเนินการตามที่กำหนดไว้ใน ระเบียบว่าด้วยการรักษาความลับของทางราชการ

๑๙. กำหนดให้มีกลไกการระบุระดับชั้นสารสนเทศบนสื่อสิ่งพิมพ์ ข้อมูลทุกชนิด โดยอาจจะเป็นการประทับตราสัญลักษณ์หรือการสร้าง Header/Footer ที่บ่งชี้ระดับชั้นความลับ หรือกลไกใด ๆ ที่ให้ผลในทำนองเดียวกัน

แนวปฏิบัติการจัดการข้อมูลระดับชั้นความลับ

Information Classification, Labelling, and Handling Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่า หน่วยงานสามารถจัดการข้อมูลสารสนเทศตามระดับชั้นความลับได้อย่างเหมาะสม

๒๐. ข้อมูลอ่อนไหวภายใต้ขอบเขตของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ถือเป็นข้อมูลภายในทุกประเภท แต่มีความอ่อนไหวหรืออาจก่อให้เกิดความเสี่ยงเมื่อมีการเปิดเผยต่อผู้ที่ไม่มีสิทธิ ได้แก่ ข้อมูลหมายเลข IP Address ข้อมูลโครงสร้างแผนผังเครือข่าย

๒๑. ข้อมูลส่วนบุคคลให้ดำเนินการผ่านนโยบายคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย

๒๒. กรณีที่ข้อมูลสารสนเทศไม่ปรากฏชั้นความลับตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ อันหมายถึงเป็นข้อมูลภายใน ให้ดำเนินการตามแนวปฏิบัตินี้

๒๒.๑ การจัดทำ: พิจารณาการเข้ารหัสตามความเหมาะสม หากเป็นข้อมูลอ่อนไหว ให้พิจารณาทำ Data Masking

๒๒.๒ การทำสำเนาและการแปล: ต้องทำสำเนาเฉพาะเมื่อจำเป็นเท่านั้น ไม่อนุญาตให้ทำสำเนาลงบนสื่อบันทึกภายนอก

๒๒.๓ การโอน: การโอนย้ายต้องเป็นไปเพื่อการปฏิบัติงาน หากเป็นข้อมูลอ่อนไหว ให้พิจารณาทำ Data Masking

๒๒.๔ การส่งและรับ: รับส่งและรับตามปกติทุกช่องทาง หากเป็นข้อมูลอ่อนไหว ให้พิจารณาทำ Data Masking เว้นแต่จำเป็นต้องปฏิบัติเพื่อให้บรรลุหน้าที่

๒๒.๕ การเก็บรักษา: เก็บรักษาด้วยมาตรการพื้นฐานที่ปลอดภัย อาทิ ใส่ตู้จัดเก็บ ล็อค อย่างเหมาะสม

๒๒.๖ การยืม: ไม่อนุญาตให้มีการยืมข้อมูลอ่อนไหว

๒๒.๗ การทำลาย: ทำลายตามรูปแบบของสื่อบันทึก

๒๒.๘ การเปิดเผย: ไม่มีการเปิดเผยต่อสาธารณะ เว้นแต่จำเป็นต้องปฏิบัติเพื่อให้บรรลุหน้าที่

๒๓. แนวปฏิบัตินี้จะไม่ครอบคลุมข้อมูลสารสนเทศที่อยู่ภายในระบบสารสนเทศ อาทิ ข้อมูลเวชระเบียน

๒๔. ภายใต้ระบบการจัดการนี้ ไม่มีข้อมูลสาธารณะ กล่าวคือ ไม่มีข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ ยกเว้น นโยบาย แนวปฏิบัติ หรือข้อมูลที่กฎหมายกำหนดให้มีการเปิดเผยหรือเผยแพร่ต่อสาธารณะ

๒๕. การเข้ารหัสข้อมูล หมายถึง การใช้เทคโนโลยีที่แปรข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยมนุษย์หรือระบบสารสนเทศ โดยปราศจากกุญแจรหัส การป้องกันการเข้าถึงด้วยรหัสผ่าน (password protection) ไม่ถือว่าเป็นการเข้ารหัสข้อมูล และพิจารณาใช้ตามระดับความเสี่ยง

แนวปฏิบัติการจัดการบัญชีผู้ใช้งาน

User Management Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่า หน่วยงานมีการควบคุมการสร้าง แก้ไข และลบบัญชีผู้ใช้งานและสิทธิการใช้งานระบบสารสนเทศและระบบเครือข่ายอย่างเหมาะสม

๒๖. การจัดการบัญชีผู้ใช้งานต้องมุ่งหวังกลไกที่เป็นระบบอัตโนมัติมากกว่าการตรวจทานโดยเจ้าหน้าที่ เพราะบริบทของการควบคุมจำนวนผู้ใช้งานและการเปลี่ยนแปลงข้อมูลผู้ใช้งานที่ซับซ้อนและมีปริมาณมาก กลไกนี้ให้ครอบคลุมการตรวจทานด้วยเช่นกัน

๒๗. ระบบสารสนเทศที่ได้รับการพัฒนาหรือจัดหาต้องมีกลไกในการตรวจสอบและเชื่อมโยงฐานข้อมูลบุคลากร โดยอัตโนมัติและมีรอบของการปรับปรุงฐานข้อมูลผู้ใช้งานให้เป็นปัจจุบันอย่างเหมาะสมต่อความเสี่ยงและบริบทการใช้งานระบบสารสนเทศดังกล่าว

๒๘. การจัดการสิทธิการเข้าใช้งานระบบสารสนเทศ อาจไม่ได้ถูกกำกับและควบคุมโดยฝ่ายเทคโนโลยีสารสนเทศ เนื่องจากการเปลี่ยนแปลงบุคลากร ปริมาณผู้ใช้งาน และอำนาจหน้าที่ในการเป็นผู้ดูแลระบบสารสนเทศที่ต้องพิจารณาให้สอดคล้องต่อระเบียบทางการแพทย์ในการคุ้มครองข้อมูลผู้ป่วยและวิชาชีพทางการแพทย์ ดังนั้นบางระบบสารสนเทศจึงจำเป็นต้องถูกจัดการโดยหน่วยงานที่เป็นผู้ใช้งานเอง

การลงทะเบียนผู้ใช้งาน

๒๙. เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศตรวจสอบรายการผู้ใช้งานใหม่กับฝ่ายทรัพยากรบุคคล ก่อนที่จะส่งมอบบัญชีผู้ใช้งาน และส่งข้อความ (SMS) เพื่อแจ้ง username และ password

๓๐. ผู้ใช้งานดำเนินการเปลี่ยนแปลง password ด้วยตนเอง

๓๑. การเปลี่ยนแปลงข้อมูลส่วนบุคคลของผู้ใช้งานจะไม่กระทบต่อบัญชีที่ถูกสร้างไว้แล้ว

การยกเลิกบัญชีผู้ใช้งาน

๓๒. ระบบสารสนเทศจะเชื่อมโยงกับฐานข้อมูลบุคลากรของฝ่ายทรัพยากรบุคคล เพื่อกำหนดรายการบัญชีผู้ใช้งาน เมื่อผู้ใช้งานพ้นสภาพพนักงาน การปรับปรุงฐานข้อมูลบุคลากรของฝ่ายทรัพยากรบุคคลจะเป็นกลไกที่ทำให้เกิดการปรับปรุงฐานข้อมูลบัญชีผู้ใช้งานของระบบสารสนเทศอัตโนมัติ

การตรวจสอบการเข้าถึงระบบสารสนเทศ

๓๓. ระบบสารสนเทศถูกออกแบบให้มีกลไกในการขึ้นทะเบียนผู้ใช้งานและสิทธิการใช้งาน อย่างไรก็ตามหน่วยงานมีการควบคุมการติดตั้งเครื่องคอมพิวเตอร์ที่กำหนดระบบสารสนเทศที่สามารถถูกใช้งานได้ ซึ่งการขึ้นทะเบียนผู้ใช้งานอาจจะดำเนินการโดยหน่วยงานที่เกี่ยวข้องด้วยตนเองหรือจากฝ่ายเทคโนโลยีสารสนเทศ

๓๔. การกำหนดสิทธิของผู้มีสิทธิเข้าระบบสารสนเทศในกลุ่มระบบ HIS จะต้องดำเนินการทุกวัน

การตรวจสอบการเข้าถึงระบบเครือข่าย

๓๕. ในการจัดสิทธิการเข้าถึงระบบเครือข่าย เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินตรวจสอบรายการบุคลากรจากฐานข้อมูลฝ่ายบุคคล (การตรวจสอบผ่าน script) และปรับปรุงฐานข้อมูล Active Directory ทุกสัปดาห์

คุณภาพของรหัสผ่านและการเข้าถึง

๓๖. รหัสผ่านจะมีการเปลี่ยนแปลงเมื่อเข้าสู่ระบบครั้งแรก

๓๗. รหัสผ่านระดับระบบทั้งหมด (เช่น Root, เปิดใช้งาน, ผู้ดูแลระบบเครือข่าย, บัญชีการดูแลแอปพลิเคชัน ฯลฯ) จะต้องเปลี่ยนแปลงอย่างน้อย 1 ครั้ง ทุก 90 วัน

๓๘. รหัสผ่านระดับผู้ใช้ทั้งหมด (เช่น อีเมล เว็บ คอมพิวเตอร์เดสก์ท็อป ฯลฯ) จะต้องเปลี่ยนอย่างน้อยทุกๆ ช่วงเวลาการเปลี่ยนแปลงที่แนะนำ คือ ทุก 90 วัน

๓๙. รหัสผ่านเก่าไม่สามารถใช้ซ้ำได้เป็นระยะเวลา 12 เดือน

๔๐. ผู้ใช้จะได้รับแจ้งล่วงหน้า 2 สัปดาห์ก่อนวันหมดอายุของรหัสผ่านและผู้ใช้จะได้รับแจ้งให้เลือกรหัสผ่านใหม่

๔๑. รหัสผ่านทั้งหมดจะต้องเป็นไปตามหลักเกณฑ์ที่อธิบายไว้ด้านล่าง

๔๒. รหัสผ่านต้องมีอักขระอย่างน้อย 8 ตัวขึ้นไป

๔๓. รหัสผ่านจะต้องรวมอักขระอย่างน้อย 3 ตัว จาก 4 ประเภทต่อไปนี้:

- ๔๓.๑ ตัวอักษรพิมพ์ใหญ่ (เช่น A, B, C)
- ๔๓.๒ ตัวอักษรพิมพ์เล็ก (เช่น a, b, c)
- ๔๓.๓ อักขระตัวเลข (เช่น 1, 2, 3)

๔๓.๔ อักขระพิเศษ (เช่น! @ # $ % ^ &* * ( ) _ + | ~ - = \ ' { } [ ] : " ; ' < > ? , . /)

๔๔. รหัสผ่านจะต้องไม่ขึ้นอยู่กับข้อมูลส่วนบุคคลของผู้ใช้หรือของเพื่อนสมาชิกในครอบครัว ข้อมูลส่วนบุคคลรวมถึงการเข้าสู่ระบบ ID, ชื่อ, วันเกิด, ที่อยู่, หมายเลขโทรศัพท์, หมายเลขประกันสังคม หรือการเปลี่ยนแปลงใด ๆ

๔๕. รหัสผ่านจะต้องไม่อยู่ในรูปแบบหรือรูปแบบซ้ำๆ หรือตามลำดับ (เช่น aaabbb, qwerty, ABCabc)

๔๖. รหัสผ่านต้องไม่เป็นคำที่สามารถพบได้ในพจนานุกรมมาตรฐาน (ภาษาอังกฤษหรือภาษาต่างประเทศ) หรือเป็นคำสแลงหรือศัพท์ที่เป็นที่รู้จักในที่สาธารณะ

๔๗. รหัสผ่านจะต้องไม่ขึ้นอยู่กับตัวละครที่เป็นที่รู้จักในที่สาธารณะจากหนังสือภาพยนตร์และอื่น ๆ

๔๘. รหัสผ่านจะต้องไม่ขึ้นอยู่กับชื่อหรือที่ตั้งทางภูมิศาสตร์ขององค์กร

๔๙. รหัสผ่านควรถือเป็นข้อมูลที่เป็นความลับ ไม่ควรมีเจ้าหน้าที่คนใดบอกหรือบอกใบ้รหัสผ่านแก่บุคคลอื่นรวมถึงบอกกับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ ผู้บังคับบัญชา เพื่อนร่วมงาน เพื่อนและสมาชิกในครอบครัวอื่น ๆ ไม่ว่าในกรณีใด ๆ

๕๐. รหัสผ่านจะไม่ถูกส่งทางอิเล็กทรอนิกส์ผ่านช่องทางการสื่อสารที่ไม่มีการป้องกัน เช่น ผ่าน อีเมล หรือระบบ Chat ต่างๆ บนอินเทอร์เน็ต แต่รหัสผ่านอาจถูกใช้เพื่อเข้าถึงทรัพยากรขององค์กรจากระยะไกลผ่านเครือข่ายส่วนตัวเสมือนที่ปลอดภัยขององค์กร หรือเว็บไซต์ที่มีการป้องกัน SSL ได้

๕๑. เจ้าหน้าที่และบุคลากรต้องไม่จัดเก็บบันทึกรหัสผ่านของตนเป็นลายลักษณ์อักษรที่ไม่ปลอดภัยทั้งบนกระดาษหรือในไฟล์อิเล็กทรอนิกส์ หากพิสูจน์ได้ว่าจำเป็นต้องเก็บบันทึกรหัสผ่านไว้จะถูกเก็บไว้ในที่ปลอดภัยในการเข้าถึงที่มีการควบคุมหากอยู่ในรูปแบบเอกสารหรือในไฟล์ที่เข้ารหัสหากอยู่ในรูปแบบอิเล็กทรอนิกส์

๕๒. ไม่ควรใช้คุณสมบัติ "จำรหัสผ่าน" ของระบบสารสนเทศและเว็บไซต์ใด ๆ

๕๓. ไม่ควรใช้รหัสผ่านที่ใช้ในการเข้าถึงระบบองค์กรเป็นรหัสผ่านเพื่อเข้าถึงบัญชีหรือข้อมูลที่ไม่ใช่องค์กร

๕๔. หากเป็นไปได้อย่าใช้รหัสผ่านเดียวกันเพื่อเข้าถึงระบบหลายระบบขององค์กร

๕๕. หากพนักงานทราบหรือสงสัยว่ารหัสผ่านของตนเองถูกบุกรุกจะต้องรายงานไปยังฝ่ายเทคโนโลยีสารสนเทศและรหัสผ่านจะต้องถูกเปลี่ยนแปลงทันที

๕๖. ระบบสารสนเทศจะต้องไม่จัดเก็บรหัสผ่านในรูปแบบข้อความที่ชัดเจนหรือในรูปแบบที่ย้อนกลับได้ง่าย (ควรเก็บในรูปแบบ Hash Value)

๕๗. รหัสผ่านจะไม่รวมอยู่ในโปรแกรมซอร์สโค้ดหรือสคริปต์ (Hard Code)

๕๘. ระบบสารสนเทศควรให้การจัดการบทบาทเพื่อให้ผู้ใช้รายหนึ่งสามารถเข้าควบคุมฟังก์ชันของอีกคนหนึ่งได้โดยไม่ต้องรู้รหัสผ่านของอีกฝ่าย

๕๙. ระบบสารสนเทศและอุปกรณ์ควรรองรับ TACACS+, RADIUS และ/หรือ X.509 ที่มีการดึงข้อมูลความปลอดภัยของ LDAP มาใช้งาน

แนวปฏิบัติการจัดการช่องโหว่เชิงเทคนิค

Technical Vulnerability Management Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่าช่องโหว่เชิงเทคนิคในระบบสารสนเทศ เครื่องแม่ข่าย และระบบเครือข่าย ได้รับการบ่งชี้และวางแผนการแก้ไขอย่างเหมาะสม

การจัดการช่องโหว่เชิงเทคนิค

๖๐. ก่อนเริ่มการประเมินควรวางรายการต่อไปนี้ไว้

๖๐.๑ ขอบเขตการประเมินถูกกำหนดไว้อย่างสมบูรณ์

๖๐.๒ ผู้ประเมินได้รับการฝึกอบรมอย่างเพียงพอเกี่ยวกับเครื่องมือที่จะใช้และกระบวนการประเมินช่องโหว่

๖๐.๓ เจ้าของบริการที่เป็นเจ้าของระบบการประเมินได้รับแจ้งถึงวัตถุประสงค์และระยะเวลาของการดำเนินการ

๖๐.๔ เครื่องมือที่จะใช้ได้รับการติดตั้งและอัปเดตอย่างสมบูรณ์

๖๐.๕ หากใช้หน่วยงานภายนอกจะต้องได้รับการอนุมัติ

๖๐.๖ การประเมินครอบคลุมทั้งการสแกนช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Testing) สำหรับระบบที่เชื่อมต่ออินเทอร์เน็ตและระบบสำคัญ โดยดำเนินการอย่างน้อยปีละครั้งหรือเมื่อมีการเปลี่ยนแปลงสำคัญ

ทั้งนี้หากใช้หน่วยงานภายนอกต้องมีข้อตกลงรักษาความลับ (NDA) และขอบเขตการทดสอบที่ได้รับอนุมัติเป็นลายลักษณ์อักษรก่อนดำเนินการ

๖๑. การประเมินช่องโหว่ควรดำเนินการโดยใช้ชุดเครื่องมือที่น่าเชื่อถือหรือได้รับความนิยมในระดับสากล

๖๒. สแกนช่องโหว่ภายในเป็นระยะ ๆ หรืออย่างน้อยปีละ 1 ครั้ง

๖๓. ควรสแกนอุปกรณ์สำคัญทั้งหมดที่เชื่อมต่อเครือข่าย สำหรับการสแกนจะต้องใช้คอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายภายในและสามารถเข้าถึงโฮสต์และเครือข่ายที่จำเป็นต้องสแกนได้

๖๔. ในการรายงานผลให้จำแนกออกเป็น 2 ประเภท 1) ช่องโหว่ของทรัพย์สินด้านเทคโนโลยีสารสนเทศ 2) การติดตั้ง Patch

๖๕. เมื่อการสแกนช่องโหว่นำมาซึ่งความผิดพลาดให้พิจารณาเบื้องต้นดังนี้

ตัวอย่างข้อผิดพลาด	สาเหตุ (ที่มีความเป็นไปได้)	แนวทางที่แนะนำ	บุคคลที่ต้องได้รับรายงานปัญหา
ระหว่างการสแกนอาจทำให้ระบบสารสนเทศทำงานช้าลง	พยายามรับข้อมูลจากโฮสต์เป้าหมาย	ตรวจสอบบริการเป้าหมายว่าแฮงค์หรือไม่ตอบสนอง	หน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ
ไม่สามารถรับข้อมูลใดๆ จากการประเมินได้	Firewall อาจปิดกั้นการติดต่อสื่อสารของระบบ	แก้ไขการตั้งค่า Firewall หรือสแกนจากเครือข่ายภายใน	หัวหน้างานเครือข่ายและฐานข้อมูล
ไม่สามารถเข้าถึงโฮสต์ที่จะทดสอบได้	โฮสต์อยู่บน VLAN อื่นของคอมพิวเตอร์ทดสอบ	เชื่อมต่อเพื่อแก้ไข VLAN	หัวหน้างานเครือข่ายและฐานข้อมูล

๖๖. ควรเก็บบันทึกกิจกรรมทั้งหมดที่ดำเนินการเป็นส่วนหนึ่งของการประเมินช่องโหว่รวมถึงชื่อวันที่และเวลา

๖๗. เมื่อได้รับรายงานเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่เกี่ยวข้องพิจารณาดำเนินการ ดังต่อไปนี้:

- ๖๗.๑ การตรวจสอบผลลัพธ์
- ๖๗.๒ ให้การแก้ไขผ่านการกระบวนการเปลี่ยนแปลง
- ๖๗.๓ การใช้มาตรการบรรเทาผลกระทบอื่นๆ
- ๖๗.๔ การจัดทำเอกสารข้อยกเว้นอย่างถูกต้อง

๖๘. แผนการแก้ไขช่องโหว่จะต้องดำเนินการให้เสร็จสิ้น ขึ้นอยู่กับการรายงานระดับความรุนแรง ดังนี้

ระดับ CVSS	ระยะเวลาที่เหมาะสม (วัน)
Critical (สูงมาก)	30
High (สูง)	60
Medium (ปานกลาง)	90
Low (ต่ำ)	120
หมายเหตุ: ยกเว้นเป็นข้อจำกัดทางเทคโนโลยี ระบบสารสนเทศ ที่เกี่ยวข้อง หรือการแก้ไขจำเป็นต้องใช้ทรัพยากรอื่น ๆ เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศสามารถกำหนดระยะเวลาที่คาดหมายและรายละเอียดอื่น ๆนำเสนอเพื่ออนุมัติ	

๖๙. เมื่อดำเนินการแก้ไขช่องโหว่แล้วควรพิจารณาการตรวจสอบช่องโหว่อีกครั้งเพื่อยืนยันผลการแก้ไข

การจัดการแพตช์

๗๐. ใช้ข้อมูลของแพตช์จากแหล่งที่เชื่อถือได้ เช่น เว็บไซต์ของซัพพลายเออร์ เว็บไซต์ของผู้จำหน่าย (เช่น ส่งตรงจากไมโครซอฟท์, ซิสโก้, CVE, NIST, US-CERT)

๗๑. การแจ้งเตือนช่องโหว่แต่ละครั้งและการปล่อยแพตช์จะต้องได้รับการตรวจสอบกับองค์กรที่มีอยู่ก่อนที่จะดำเนินการใด ๆ เพื่อหลีกเลี่ยงการแพตช์ที่ไม่จำเป็น อ่านการแจ้งเตือนทั้งหมดอย่างระมัดระวัง

๗๒. การตัดสินใจใช้แพตช์กับเครื่องแม่ข่ายภายในกรอบเวลาใดจะต้องดำเนินการโดยแนวทางต่อไปนี้

- ๗๒.๑ แพตช์ทั้งหมดจะต้องดาวน์โหลดจากผู้จำหน่ายระบบที่เกี่ยวข้องหรือแหล่งที่เชื่อถือได้ แหล่งที่มาของแพตช์และการตรวจสอบความสมบูรณ์ของแพตช์
- ๗๒.๒ อุปกรณ์ใด ๆ จะต้องติดตั้งแพตช์พื้นฐานให้เป็นปัจจุบันก่อนที่จะเชื่อมต่อกับเครือข่าย
- ๗๒.๓ ซอฟต์แวร์จะต้องติดตั้งแพตช์ให้เป็นปัจจุบัน เมื่อติดตั้งบนทรัพย์สินขององค์กร
- ๗๒.๔ แพตช์สำคัญหรือที่คาดว่าจะส่งผลกระทบต่อการทำงานของระบบสารสนเทศ จะต้องได้รับการทดสอบก่อนการใช้งานเต็มรูปแบบเนื่องจากแพตช์อาจมีผลข้างเคียง

๗๓. การแพตช์ให้ดำเนินการผ่านกระบวนการเปลี่ยนแปลง

แนวปฏิบัติการจัดการอุบัติการณ์

Incident Management Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่าเหตุการณ์ผิดปกติและอุบัติการณ์ได้รับการรายงานและแก้ไขอย่างเป็นระบบ มีการเรียนรู้และจัดเก็บข้อมูลอุบัติการณ์เพื่อการพัฒนาปรับปรุงกระบวนการทำงานให้ดียิ่งขึ้น รวมถึงการเตรียมความพร้อมรับมือต่อเหตุวิกฤตที่อาจนำสู่การหยุดชะงักของบริการ

๗๔. อุบัติการณ์ต้องพิจารณาผลกระทบตามเกณฑ์ของการบริหารความเสี่ยง

การแจ้งเหตุการณ์

๗๕. ผู้แจ้งเหตุการณ์อาจจะยังไม่ทราบว่าเป็นอุบัติการณ์ในทันทีจนกว่าจะมีการวิเคราะห์จากเจ้าหน้าที่ที่เกี่ยวข้อง อย่างไรก็ตาม การแจ้งดังกล่าวต้องได้รับการบันทึกในระบบ Service Desk

๗๖. เมื่อพิจารณาแล้วว่าเป็นอุบัติการณ์ให้มีการมอบหมายเจ้าหน้าที่ที่เกี่ยวข้อง ซึ่งอาจจะเป็นเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศหรือจากฝ่ายงานอื่นก็ได้

การประเมินความรุนแรงของอุบัติการณ์

๗๗. การประเมินระดับความรุนแรงต้องดำเนินการและแจ้งผู้ที่เกี่ยวข้องภายใน 10 นาที

๗๘. การประเมินระดับความรุนแรงของอุบัติการณ์ให้ยึดตามผลกระทบตามเกณฑ์การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ประกอบด้วย 5 ระดับสำคัญ ดังนี้

ระดับอุบัติการณ์	ผลกระทบด้านเทคโนโลยีสารสนเทศ (ปรับแก้)	ผลกระทบด้านการดำเนินงานของเจ้าหน้าที่ (ปรับแก้)	ผลกระทบด้านภาพลักษณ์	ผลกระทบด้านการเงิน	ผลกระทบด้านบุคลากร
Critical (สูงมาก)	กระทบต่อการหยุดชะงักทั้งหมดของระบบ HIS	เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้ทั้งหมด (กระทบเป็นวงกว้าง)	การเผยแพร่ข่าวในวงกว้างทั้งในหนังสือพิมพ์ วิทยุ และโทรทัศน์ หรือสื่อสังคมออนไลน์ที่กว้าง กระทบต่อความมั่นคงและความเชื่อมั่นต่อมหาวิทยาลัย	> 10 ล้านบาท	อันตรายถึงชีวิต/สูญเสียอวัยวะ/ทุพพลภาพ
High (สูง)	กระทบต่อการหยุดชะงักทั้งหมดของระบบภายใต้ Colocation Service หรือระบบอื่น ๆ ของคณะแพทยศาสตร์ หรือ กระทบต่อการหยุดชะงักบางส่วนของระบบ HIS	เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้บางส่วน (กระทบ 3-4 แผนก)	การเผยแพร่ข่าวในวงกว้างทั้งในหนังสือพิมพ์ วิทยุ และโทรทัศน์ หรือสื่อสังคมออนไลน์ที่กว้าง ต้องมีการชี้แจงจากผู้บริหารระดับสูง	> 2.5 แสนบาท – 10 ล้านบาท	การบาดเจ็บสาหัสถึงขั้นพักงานไม่เกิน 1 เดือน
Medium (ปานกลาง)	กระทบต่อประสิทธิภาพและเสถียรภาพทั้งหมดระบบ HIS แต่ไม่	เจ้าหน้าที่ทั้งหมดปฏิบัติงานได้ไม่เต็มประสิทธิภาพ	การเผยแพร่ข่าวทั้งในหนังสือพิมพ์ วิทยุและโทรทัศน์ หรือสื่อสังคม	> 50,000 – 2.5 แสนบาท	การบาดเจ็บถึงขั้นพักงานไม่เกิน 7 วัน
	หยุดชะงัก เช่น ความหน่วงช้า	(กระทบ 1-2 แผนก)	ออนไลน์ในวงจำกัด		
Low (ต่ำ)	กระทบต่อประสิทธิภาพและเสถียรภาพของระบบทั้งหมดภายใต้ Colocation Service หรือระบบอื่น ๆ ของคณะแพทยศาสตร์ หรือ กระทบต่อประสิทธิภาพและเสถียรภาพบางส่วนของระบบ HIS	เจ้าหน้าที่บางส่วนปฏิบัติงานได้ไม่เต็มประสิทธิภาพ (กระทบบางจุด)	การเผยแพร่ข่าวในวงจำกัด ไม่ออกสื่อ	> 10,000 – 50,000 บาท	การบาดเจ็บพักงานไม่เกิน 2 วัน
Very Low (ต่ำมาก)	กระทบต่อประสิทธิภาพและเสถียรภาพของระบบบางส่วนภายใต้ Colocation Service หรือระบบอื่น ๆ ของคณะแพทยศาสตร์	เจ้าหน้าที่เป็นรายบุคคลไม่สามารถปฏิบัติงานได้หรือไม่เต็มประสิทธิภาพ (กระทบน้อยมาก)	ไม่มีการเผยแพร่ข่าว	ไม่เกิน 10,000 บาท	บาดเจ็บเล็กน้อยไม่พักงาน

กรอบระยะเวลาแก้ไขและการยกระดับความรุนแรง

๗๙. เมื่อเกิดเหตุการณ์ขึ้นผู้ใช้จำเป็นต้องแจ้งเหตุการณ์ให้บุคคลที่เกี่ยวข้องทราบ ลำดับความสำคัญของเหตุการณ์ระยะเวลาและการยกระดับความรุนแรง

ระดับอุบัติการณ์	ระยะเวลาก่อนการยกระดับความรุนแรง (ชั่วโมง)	ยกระดับถึง
Critical (สูงมาก)	0.5 (30 นาที)	รองคณบดีฝ่ายเวชสารสนเทศ
High (สูง)	4	หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
Medium (ปานกลาง)	8	
Low (ต่ำ)	24	
Very Low (ต่ำมาก)	48	

อุบัติการณ์และหลักนิติวิทยาศาสตร์

๘๐. การเก็บหลักฐานเพื่อดำเนินการทางนิติวิทยาศาสตร์ให้อยู่ภายใต้ความเห็นชอบของรองคณบดีฝ่ายเวชสารสนเทศ การเก็บหลักฐานทั่วไป อาทิ บันทึกคอมพิวเตอร์และเครือข่าย (log) สามารถดำเนินการได้

การแก้ไขและบันทึกอุบัติการณ์

๘๑. การแก้ไขต้องมุ่งเน้นผลลัพธ์ให้การให้บริการที่สำคัญหรือส่งผลกระทบน้อยและรวดเร็วที่สุด แม้ว่าสาเหตุที่แท้จริงของเหตุอุบัติการณ์จะพบหรือไม่ก็ตาม การแก้ไขในพฤติการณ์ดังกล่าวเรียกว่า “workaround”

๘๒. การแก้ไขต้องมีการบันทึกรายละเอียดของการแก้ไขในระบบ Service Desk โดยต้องบันทึกในลักษณะที่สร้างความเข้าใจแก่ผู้ที่เกี่ยวข้อง

การเรียนรู้จากเหตุอุบัติการณ์

๘๓. กำหนดให้มีการรายงานผลการดำเนินการในการแก้ไขเหตุอุบัติการณ์เป็นรายเดือน

๘๔. เมื่อมีการแก้ไขอุบัติการณ์แล้วเสร็จ เจ้าหน้าที่ที่ดำเนินการควรพิจารณาเพิ่มองค์ความรู้ที่ได้จากการแก้ไข เพื่อรองรับการแก้ไขในอนาคต กรณีที่อุบัติการณ์อาจเกิดซ้ำได้

การวิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis)

๘๕. เมื่อเกิดอุบัติการณ์ระดับ Medium ขึ้นไป หรือ Nonconformity ทุกกรณี ให้ดำเนินการวิเคราะห์สาเหตุที่แท้จริงภายใน 14 วัน โดยใช้วิธี 5 Whys

๘๖. ขั้นตอนการวิเคราะห์: 1) บันทึกเหตุการณ์พร้อม Timeline ใน Service Desk 2) ระบุสาเหตุโดยตรง (Direct Cause) 3) ถาม "ทำไม?" ซ้ำ 5 รอบจนพบ Root Cause ที่เป็น Process หรือ System 4) กำหนด Corrective Action พร้อมระบุผู้รับผิดชอบและวันแล้วเสร็จ 5) ตรวจสอบผลภายใน 30 วัน

๘๗. ผลการวิเคราะห์และแนวทางแก้ไขต้องบันทึกใน Service Desk และรายงานต่อคณะกรรมการ ISMS ในการประชุมครั้งถัดไป

แนวปฏิบัติการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (PDPA Breach)

๘๘. เมื่อตรวจพบหรือได้รับแจ้งว่าอาจเกิดการละเมิดข้อมูลส่วนบุคคล ให้บันทึกทันทีใน Service Desk และระบุเวลาที่ทราบเรื่อง (T_0) ซึ่งเป็นจุดเริ่มต้นนับกรอบเวลา 72 ชั่วโมงตาม PDPA มาตรา 37

๘๙. ภายใน 4 ชั่วโมงนับจาก T_0 ให้ประเมินความเสี่ยงและแจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เป็นลายลักษณ์อักษรทันที

๙๐. หากผลการประเมินพบว่ามีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล ให้แจ้ง PDPC ภายใน 72 ชั่วโมงนับจาก T_0 โดยระบุ: ลักษณะการละเมิด จำนวนเจ้าของข้อมูลที่ได้รับผลกระทบ ผลที่อาจเกิดขึ้น และมาตรการที่ดำเนินการแล้ว

๙๑. ต้องบันทึก Breach Log ทุกกรณีโดยระบุวันเวลาที่แจ้ง DPO และ PDPC เก็บรักษาไว้อย่างน้อย 3 ปี โดยใช้แบบฟอร์ม PDPA-Breach-Log-SD

๙๒. ให้จัดซ้อมรับมือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Tabletop Exercise) อย่างน้อยปีละ 1 ครั้ง บันทึก Attendance List และ After-Action Report เป็นหลักฐานสำหรับการตรวจสอบ

แนวปฏิบัติการกำกับหน่วยงานภายนอก

Supplier Management Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่าการใช้บริการจากหน่วยงานภายนอกมีความมั่นคงปลอดภัยสารสนเทศ หน่วยงานภายนอกได้ให้บริการตามข้อกำหนดด้านความมั่นคงปลอดภัย มีการติดตามและประเมินผลการดำเนินงานของหน่วยงานภายนอก และเพิ่มเติมจากกระบวนการทางพัสดุของภาครัฐอันเป็นประโยชน์แก่การดำเนินงานของหน่วยงาน

๙๓. การจัดการหน่วยงานภายนอกต้องไม่ขัดต่อระเบียบพัสดุของระบบราชการ และให้กระบวนการคัดเลือกและจัดจ้างต้องเป็นไปตามระเบียบราชการอย่างเคร่งครัด

๙๔. หากมิได้กำหนดไว้เป็นการเฉพาะ หน่วยงานภายนอกจะต้องรับผิดชอบทั้งหมดในการใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อให้แน่ใจว่ามีการปกป้องเครือข่ายและข้อมูลภายใต้การให้บริการตามสัญญา

๙๕. หน่วยงานภายนอกจะต้องสื่อสารกับบุคลากรผู้รับเหมาที่จ้างช่วงและตรวจสอบให้แน่ใจว่าบุคลากรของตนเข้าใจและปฏิบัติตาม

ข้อกำหนดที่กำหนดไว้ในสัญญารวมถึงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

๙๖. บุคลากรหน่วยงานภายนอกผู้รับเหมาที่จ้างช่วงที่มีสัญญาการพัฒนาระบบสารสนเทศจะต้องปฏิบัติตามนโยบายขั้นตอนและแนวทางขององค์กร ทั้งในมิติของมาตรฐานการพัฒนา การยืนยันตัวตน วิธีการจัดการสิทธิ และการทดสอบด้านความมั่นคงปลอดภัยสารสนเทศที่จำเป็น เมื่อเป็นไปได้ให้ดำเนินการตามมาตรฐานสากล ISO29110 เป็นขั้นต่ำ

๙๗. หน่วยงานภายนอกจะต้องแจ้งชื่อพนักงานก่อนเข้าถึงองค์กรและพนักงานที่เข้าพื้นที่ต้องปฏิบัติตามกฎระเบียบและข้อบังคับทั้งหมดสำหรับการเข้าสู่ห้องศูนย์คอมพิวเตอร์ การเปลี่ยนแปลงใด ๆ จะต้องได้รับแจ้งเป็นลายลักษณ์อักษรล่วงหน้า และเมื่อมีการเปลี่ยนแปลงตัวพนักงานจะต้องมีการแจ้งล่วงหน้าหรือทันที

๙๘. ข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement: NDA) ต้องจัดให้มีประกอบหรือเป็นส่วนหนึ่งของสัญญาบริการที่มีการเข้าถึงข้อมูลหรือระบบงานสำคัญของฝ่ายเทคโนโลยีสารสนเทศ เว้นแต่หน่วยงานภายนอกนั้นกำกับและดูแลโดยหน่วยงานอื่น ๆ

๙๙. NDA จะอยู่ในรูปแบบใด ๆ นั้นให้ยึดสาระสำคัญที่ข้อมูลและระบบงานสำคัญของฝ่ายเทคโนโลยีสารสนเทศได้รับการคุ้มครองที่ดีพอและเหมาะสมต่อบริบทของบริการภายใต้สัญญา

๑๐๐. หน่วยงานภายนอกจะต้องไม่ถ่ายภาพ บันทึกเสียงในระหว่างการปฏิบัติหน้าที่ของตนต่อองค์กร หากจำเป็น จะต้องได้รับการอนุญาตจากเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

๑๐๑. หากมีการละเมิดความปลอดภัยหรือพบปัญหาใดๆ หน่วยงานภายนอกจะต้องรายงานทันที

๑๐๒. การเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อผลิตภัณฑ์หรือบริการหน่วยงานภายนอกจะต้องแจ้งเป็นลายลักษณ์อักษรต่อองค์กรล่วงหน้าอย่างน้อย 30 วัน องค์กรจะวิเคราะห์ผลกระทบและระบุการควบคุมที่เหมาะสมเพื่อลดความเสี่ยง

๑๐๓. หน่วยงานภายนอกจะต้องส่งคืนทรัพย์สินทั้งหมดขององค์การ เช่น สื่อ เอกสารกระดาษ ฯลฯ ให้กับหน่วยงาน

๑๐๔. การขอเข้าถึงระบบสารสนเทศ ระบบเครือข่าย พื้นที่ศูนย์คอมพิวเตอร์ ตลอดจนการเปลี่ยนแปลงใด ๆ อันเป็นผลจากการให้บริการ ต้องดำเนินการผ่านแนวปฏิบัติการจัดการการเปลี่ยนแปลงและคำขอรับบริการในระบบ Service Desk

๑๐๕. หน่วยงานภายนอกจะใช้ทรัพย์สินของฝ่ายเทคโนโลยีสารสนเทศ รวมถึง ข้อมูล ซอฟต์แวร์ และฮาร์ดแวร์เพื่อวัตถุประสงค์ทางธุรกิจขององค์กรเท่านั้น และจะไม่ติดตั้งหรือแจกจ่ายเพื่อ "ละเมิดลิขสิทธิ์" หรือผลิตภัณฑ์ซอฟต์แวร์อื่นๆ ที่ไม่ได้รับอนุญาต

๑๐๖. ห้ามสแกนเครือข่าย ดักจับเครือข่าย พยายามเลี่ยงการควบคุมการเข้าถึงระบบ หรือการเข้าถึงระบบสารสนเทศของหน่วยงานโดยไม่ได้รับการอนุญาตจากเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

๑๐๗. ฝ่ายเทคโนโลยีสารสนเทศควรพิจารณาสิทธิในการเข้าตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศในบริการและบริการช่วง โดยกำหนดเป็นองค์ประกอบของสัญญา เพื่อให้สิทธิดังกล่าวชอบด้วยระเบียบทางสัญญาและเป็นประโยชน์ต่อหน่วยงาน

ข้อกำหนดสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

๑๐๘. หน่วยงานภายนอกที่ประมวลผลข้อมูลส่วนบุคคลในนามของคณะแพทยศาสตร์ (Data Processor) ต้องลงทะเบียนใน DP Register ก่อนเริ่มดำเนินการ และทบทวนรายชื่อทุกปี

๑๐๙. Data Processor ทุกรายต้องลงนามใน Data Processing Agreement (DPA) ที่ระบุขอบเขตการประมวลผล มาตรการความปลอดภัย ข้อกำหนด Sub-processor และสิทธิ์ตรวจสอบของคณะแพทยศาสตร์

๑๑๐. Data Processor ต้องแจ้งคณะแพทยศาสตร์ภายใน 24 ชั่วโมงเมื่อทราบว่าเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เพื่อให้สามารถแจ้ง PDPC ได้ทันภายใน 72 ชั่วโมง

๑๑๑. เมื่อสิ้นสุดสัญญา Data Processor ต้องคืนหรือลบข้อมูลส่วนบุคคลทั้งหมดและส่งหลักฐานยืนยันให้คณะแพทยศาสตร์

ลิขสิทธิ์และสิทธิทางปัญญา

๑๑๒. หากไม่ได้กำหนดไว้เป็นอื่น ลิขสิทธิ์ในผลงานสร้างสรรค์ให้เป็นไปตามข้อปริยายทางกฎหมาย

๑๑๓. สิทธิทางปัญญาและลิขสิทธิ์ที่เป็นของฝ่ายใด หากไม่ได้กำหนดไว้เป็นอื่น หรือมีการเปลี่ยนถ่ายย้ายโอนลิขสิทธิ์และสิทธิทางปัญญาให้คงไว้แก่ผู้ทรงสิทธิฝ่ายนั้น

แนวปฏิบัติการทำลายสื่อ

Media Disposal Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่ามีการกำหนดหลักเกณฑ์และวิธีการในการทำลายสื่อบันทึกสารสนเทศทุกประเภทไว้เพียงพอและเหมาะสมต่อความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๑๑๔. ไม่ว่าระดับสารสนเทศจะเป็นชั้นความลับใดที่ไม่ใช่ข้อมูลสาธารณะหรือข้อมูลเปิดตาม พ.ร.บ. ข้อมูลข่าวสารราชการ และประกาศที่เกี่ยวข้อง ให้ดำเนินการด้วยวิธีการทำลายสื่อหรือลบข้อมูลที่ปลอดภัยที่สุดเสมอ

๑๑๕. ไม่อนุญาตให้มีการนำกระดาษมาใช้ใหม่ (reuse) ยกเว้นกระดาษที่เป็นข้อมูลสาธารณะ

๑๑๖. การทำลายสื่อบันทึกประเภทกระดาษและแผ่นบันทึก (CD/DVD) ให้ใช้เครื่องทำลายเอกสาร

๑๑๗. การทำลายสื่อบันทึกประเภท Hard Disk ให้ดำเนินการทุบทำลายจนเป็นซาก จนมั่นใจว่าไม่สามารถนำกลับมาได้

๑๑๘. ในกรณีเป็นการลบข้อมูลสารสนเทศ (Information Deletion) บนเครื่องคอมพิวเตอร์ ให้ใช้วิธีการโคลน image file ต้นฉบับทับลงบนคอมพิวเตอร์เครื่องนั้น (มีผลเสมือนข้อมูลถูกเขียนทับทั้งหมด รวมถึงระบบปฏิบัติการด้วย)

๑๑๙. ในกรณีเป็นการลบข้อมูลสารสนเทศบนระบบฐานข้อมูล โดยใช้คำสั่ง Delete ของภาษาฐานข้อมูลประเภทนั้น ๆ (อาทิ SQL language) ให้ Commit ชุดคำสั่งทันทีที่การลบมีผล ยกเว้นเป็นการออกแบบระบบสารสนเทศให้ Flag สารสนเทศแทนการลบ

๑๒๐. ในกรณีเป็นการลบบนระบบปฏิบัติการที่ยังคงใช้งานอยู่ให้ลบข้อมูลดังกล่าวออกจาก Recycle Bin อีกครั้ง

๑๒๑. ในกรณีเป็นการลบจากสื่อบันทึกข้อมูลประเภทรอทำลายหรือเจตนานำส่งทำลาย ให้ทำลายที่สื่อบันทึกข้อมูลจนเป็นซาก

๑๒๒. ในกรณีเป็นการลบจากสื่อบันทึกข้อมูลเพื่อนำกลับมาใช้ใหม่ หากผู้ใช้งานเป็นบุคคลเดิมหรือกลุ่มงานเดิมที่มีสิทธิเข้าถึงข้อมูลที่ต้องการลบ สามารถลบด้วยวิธีการทั่วไปได้ แต่หากสื่อบันทึกจะมีการใช้งานโดยหน่วยงานอื่น บุคคลอื่น หรือกลุ่มบุคคลอื่น ที่ไม่มีสิทธิในการเข้าถึงข้อมูลที่ต้องการลบ ให้ใช้วิธีการลบแบบ Low Level Format ของระบบปฏิบัติการ (ห้ามใช้ Quick Format)

การนำสื่อบันทึกข้อมูลออกจากขอบเขตความรับผิดชอบ

๑๒๓. ไม่ว่าจะเป็นกรณีใด ๆเมื่อมีการส่งสื่อบันทึกข้อมูล (ที่ไม่ใช่กระดาษ) ออกภายนอกหน่วยงาน (เช่น ซ่อมบำรุง บริจาค ตัดจำหน่ายซาก) ต้องพิจารณา ดังนี้

๑๒๓.๑ กรณีเครื่องพิมพ์และเครื่องถ่ายเอกสารที่มีหน่วยความจำ ให้ทำการคืนค่า (clear cache) ก่อนการส่ง

๑๒๓.๒ กรณี Hard Disk ของเครื่องคอมพิวเตอร์และแม่ข่ายที่ไม่ใช่สถาปัตยกรรม RAID ให้ดำเนินการลบ (format) ข้อมูลและเขียนระบบปฏิบัติการทับ การลบโดยการเขียนทับเป็นวิธีที่ยอมรับได้ในการทำลายข้อมูล ควรมีการทำหลายครั้ง และควรดำเนินการด้วยรูปแบบการเขียนทับแบบสุ่ม ต้องมีการเขียนข้อมูลทับ (แนะนำให้ใช้การเขียนทับเพิ่มเติมขึ้นอยู่กับความไวของข้อมูลที่จะลบ) ผลิตภัณฑ์ที่แสดงด้านล่างสามารถเขียนทับระบบปฏิบัติการ Microsoft และ UNIX และเป็นที่ยอมรับได้ เช่น Disk Active@Kill, Secure Eraser for Windows

๑๒๔. กรณีใช้หน่วยงานภายนอกในการดำเนินการต้องมีการจัดส่งหลักฐานการทำลายที่เชื่อถือได้ว่ามีการดำเนินการเกิดขึ้นจริงตามข้อตกลงทางสัญญา ด้วยวิธีการที่มีความมั่นคงปลอดภัย

๑๒๕. ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องใช้ข้อมูลเดิม ผู้ใช้งานต้องสำรองข้อมูลสารสนเทศด้วยตนเอง ก่อนการส่งมอบอุปกรณ์หรือสื่อบันทึกเพื่อการส่งออกนอกหน่วยงาน

๑๒๖. การส่งออกเครื่องคอมพิวเตอร์คืนสู่ผู้ให้เช่า ต้องจัดให้มีหลักฐานในระบบ Service Desk เพื่อชี้แจงรายละเอียดของเครื่องคอมพิวเตอร์ที่มีการจัดส่ง โดยสามารถอ้างอิงและติดตามได้

แนวปฏิบัติการจัดการบันทึกของระบบ

Log Management Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่ามีการกำหนดแนวทางการบริหารจัดการบันทึก (log) ของระบบสารสนเทศและระบบเครือข่ายอย่างมั่นคงปลอดภัย และมีแนวทางการใช้ประโยชน์อย่างเหมาะสม

๑๒๗. กำหนดระบบที่ต้องเก็บบันทึกเพื่อตรวจสอบและติดตามรายการด้านล่างเป็นระบบที่ต้องเก็บบันทึก ดังนี้

๑๒๗.๑ เซิร์ฟเวอร์ AD

๑๒๗.๒ เซิร์ฟเวอร์เมลหรือบัญชีเมล

๑๒๗.๓ สวิตช์/เราเตอร์

๑๒๗.๔ ไฟร์วอลล์

๑๒๗.๕ Anti-Virus

๑๒๘. การจัดเก็บบันทึกอาจอยู่ในรูปแบบของระบบบูรณาการอาทิ SIEM หรือระบบวิเคราะห์ส่วนกลางก็ได้

๑๒๙. การจัดเก็บบันทึกต้องสอดรับต่อข้อกำหนดกฎหมายที่เกี่ยวข้อง

๑๒๙.๑ ระบบทางบัญชี: ขั้นต่ำ 5 ปี

๑๒๙.๒ บันทึกจราจรบนเครือข่าย: ขั้นต่ำ 90 วัน

๑๒๙.๓ เมื่อไม่ได้กำหนดไว้เป็นการเฉพาะ การพิจารณาการจัดเก็บบันทึกที่อาจเกี่ยวข้องกับหลักนิติวิทยาศาสตร์ให้ดำเนินการเก็บขั้นต่ำ 10 ปี หรือตามอายุความของเรื่องนั้น ๆ ตามที่กฎหมายกำหนด ยกเว้นแต่ไม่สามารถดำเนินการได้ด้วยข้อจำกัดทางเทคโนโลยีและงบประมาณ

๑๓๐. ผู้ที่เข้าถึงบันทึกต้องเป็นผู้ดูแลระบบเท่านั้น และกำหนดให้มีการเก็บบันทึกการแก้ไขของผู้ดูแลระบบด้วย (audit log)

๑๓๑. ความผิดปกติของการวิเคราะห์บันทึกของกลุ่มผู้ใช้งานให้พิจารณาดำเนินการแจ้งไปยังผู้ใช้งาน

๑๓๒. ความผิดปกติของการวิเคราะห์บันทึกของระบบเครือข่ายให้พิจารณาดำเนินการใช้กระบวนการอุบัติการณ์ (incident)

๑๓๓. บนระบบสารสนเทศใด ๆ ประเภทและข้อมูลที่บันทึกจำแนกได้ดังนี้

๑๓๓.๑ บันทึกระบบปฏิบัติการ (access log): ให้บันทึกการเข้าถึงและบัญชีผู้ใช้งานที่เข้าถึง

๑๓๓.๒ บันทึกกิจกรรมและธุรกรรม (activity and transaction log): ให้บันทึกบัญชีผู้ใช้งานที่กระทำกิจกรรมหรือธุรกรรมบนระบบ

๑๓๓.๓ บันทึกเพื่อการตรวจสอบ (audit log): ให้บันทึกการเปลี่ยนแปลงที่ดำเนินการโดยผู้ดูแลระบบ

๑๓๔. องค์ประกอบของบันทึกต้องประกอบด้วยสาระสำคัญ ดังนี้

๑๓๔.๑ การบ่งชี้ตัวตน เครื่องคอมพิวเตอร์ หรืออุปกรณ์

๑๓๔.๒ การบ่งชี้เวลาที่เกิดของบันทึก

๑๓๔.๓ การบ่งชี้กิจกรรม การเปลี่ยนแปลง หรือฟังก์ชั่นงาน

๑๓๔.๔ ในบางกรณี ให้พิจารณาบันทึกผลแห่งการกระทำ (สำเร็จ/ล้มเหลว)

การเฝ้าระวังทรัพยากรระบบ (Capacity & Resource Monitoring)

๑๓๕. กำหนดให้มีการตั้งค่าเตือนและค่าวิกฤติสำหรับทรัพยากรระบบตามตารางด้านล่าง โดยทบทวนค่าเหล่านี้อย่างน้อยปีละ 1 ครั้งในการประชุม Management Review

ทรัพยากร	Warning	Critical
CPU Utilization	≥ 80%	≥ 95%
RAM Utilization	≥ 75%	≥ 90%
Disk Utilization	≥ 85%	≥ 95%
Network Bandwidth	≥ 70%	≥ 90%
DC Temperature	≥ 25°C	≥ 28°C
DC Humidity	< 40% หรือ > 60%	< 35% หรือ > 65%
UPS Load	≥ 70%	≥ 85%

๑๓๖. เมื่อเกิด Warning ให้แจ้งผู้ดูแลระบบทันที เมื่อเกิด Critical ให้แจ้งหัวหน้าฝ่ายเทคโนโลยีสารสนเทศภายใน 15 นาที และเปิด Incident Ticket ระดับ High ขึ้นไป

การตรวจสอบการสำรองข้อมูล (Backup Monitoring)

๑๓๗. ผู้ดูแลระบบต้องตรวจสอบผล Backup Job ทุกวันทำการก่อนเวลา 09:00 น. ผ่าน Dashboard หรือ Log ของระบบ Backup และบันทึกผลในแบบฟอร์ม BKP-LOG-SD

๑๓๘. กรณี Automated Backup ล้มเหลว ให้ดำเนินการ Manual Backup ทันทีและเปิด Service Desk Ticket บันทึกสาเหตุและผลการแก้ไข

๑๓๙. ทดสอบการกู้คืนข้อมูล (Restore Test) สำหรับระบบ HIS อย่างน้อยเดือนละ 1 ครั้ง และรายงาน Backup Success Rate ต่อหัวหน้าฝ่ายเทคโนโลยีสารสนเทศรายเดือน

แนวปฏิบัติการพัฒนาระบบสารสนเทศ

Secure Software Development Procedure

แนวปฏิบัตินี้คือเพื่อให้มั่นใจว่ามีการกำหนดแนวทางการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย

๑๔๐. ระบบต้องถูกพัฒนาให้รองรับนโยบายความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

๑๔๑. เจ้าของโครงการจะได้รับการกำหนดข้อกำหนดด้านความปลอดภัยของข้อมูลของระบบโดยมีรายละเอียดดังนี้

๑๔๑.๑ การจัดการผู้ใช้

- ระบบจะสามารถสร้างบัญชีและสามารถกำหนดสิทธิ์การใช้งานบัญชีในกลุ่มหรือบัญชีบุคคลได้
- ระบบจะต้องสามารถกำหนดความยาวของบัญชีได้
- ระบบจะต้องสามารถเตรียมเมทริกซ์การเข้าถึง แสดงบนหน้าจอ และพิมพ์เป็นเอกสารได้ ซึ่งมีรายละเอียดดังนี้
  - ชื่อระบบ
  - ชื่อบัญชี
  - การเข้าถึงสิทธิ์
  - วันที่ที่ใช้งานอยู่ของบัญชี
  - สถานะบัญชี
- ระบบจะสามารถเพิกถอนการเข้าถึงระบบสำหรับบัญชีบุคคลและบัญชีกลุ่มได้
- ระบบจะระงับการเข้าถึงหรือระงับหรือหน่วงเวลาหน้าจอชั่วคราวหากผู้ใช้ป้อนข้อมูลไม่ถูกต้องเกิน 3 ครั้ง และสามารถระบุการเปลี่ยนแปลงระยะเวลาที่ไม่ถูกต้องได้
- ระบบจะไม่ใช้บัญชีปกติเพื่อเริ่มหรือหยุดบริการในระบบปฏิบัติการหรือซอร์สโค้ดของโปรแกรม
- ระบบจะต้องไม่ระบุบัญชีผู้ใช้หรือรหัสผ่านในซอร์สโค้ดของโปรแกรม (โปรแกรมฮาร์ดโค้ด)

การตรวจสอบค่าป้อนเข้า

๑๔๒. ระบบจะต้องตรวจสอบความถูกต้องของข้อมูลที่ป้อนเพื่อตรวจจับและป้องกันจากอักขระพิเศษเช่น <@@! ว่าไม่จำเป็นต้องป้อนหรือจัดเก็บเพื่อป้องกันการประมวลผลข้อผิดพลาด

๑๔๓. ระบบจะต้องกำหนดเงื่อนไขของการป้อนข้อมูลอย่างถูกต้องในกล่องป้อนข้อมูลเพื่อให้ตรงกับความต้องการของระบบด้านล่าง

๑๔๔. ตรวจสอบการป้อนข้อมูลให้ตรงกับชนิดข้อมูลของตัวแปรในโปรแกรม (input type)

๑๔๕. ตรวจสอบความถูกต้องของข้อมูลที่ป้อนภายในขอบเขตบนและล่างของตัวแปรในโปรแกรม (min-max)

๑๔๖. ตรวจสอบความถูกต้องของการป้อนข้อมูลเพื่อป้องกันการอยู่นอกช่วงของค่าที่กำหนด (range)

๑๔๗. ป้องกันการลืมป้อนข้อมูลในส่วนสำคัญ (required field)

การตรวจสอบการแสดงผล

๑๔๘. ระบบจะต้องตรวจสอบการแสดงผลหากมีข้อผิดพลาดเกิดขึ้น ระหว่างการประมวลผลและข้อความเตือนจะต้องแสดงเป็นข้อความทั่วไปเพื่อปกป้องการเปิดเผยข้อมูลที่อาจส่งผลกระทบต่อความปลอดภัยของข้อมูล

๑๔๙. ระบบจะต้องควบคุมการเข้าถึงระบบโดยตั้งค่าการล็อกหน้าจอโดยอัตโนมัติและตัดการเชื่อมต่อหากไม่ได้ใช้งานเกิน 15 นาที และจะต้องสามารถระบุ / เปลี่ยนระยะเวลาที่ไม่ได้ใช้งานของระบบได้

๑๕๐. พิจารณามาตรฐานการปิดบังข้อมูล (data masking) ให้สอดรับกับความจำเป็นในการเปิดเผยข้อมูลบนหน้าจอของระบบ ตัวอย่างเช่น

๑๕๐.๑ 087-XXX-7070 (สำหรับเบอร์โทรศัพท์)

๑๕๐.๒ 1-XXXX-XXXXX-8-00 (เลขบัตรประชาชน)

๑๕๑. ระบบจะต้องควบคุมการเข้าถึงระบบของผู้ใช้หรือกลุ่มบัญชีแต่ละกลุ่มตามระยะเวลาเพื่ออนุญาตการเข้าถึงหรือไม่ได้รับอนุญาตให้ใช้ระบบ

๑๕๒. เจ้าของโครงการจะต้องมอบหมายให้ผู้รับผิดชอบตรวจสอบความถูกต้องของข้อกำหนดด้านความปลอดภัยของระบบที่พัฒนาขึ้นซึ่งกำหนดไว้ก่อนเริ่มโครงการ

๑๕๓. การจัดพิมพ์รายงานจากระบบสารสนเทศต้องประกอบด้วยดังนี้

๑๕๓.๑ บัญชีผู้ใช้งานที่สั่งพิมพ์

๑๕๓.๒ วันและเวลาที่มีการสั่งพิมพ์ (timestamp)

การทดสอบด้านความปลอดภัย

๑๕๔. กำหนดให้มีผลการจัดทำ source code scan ในระบบที่พัฒนาขึ้นเอง

๑๕๕. การทดสอบจะได้รับการพิจารณาเพื่อให้ครอบคลุมข้อกำหนดด้านความปลอดภัยตามที่กำหนดไว้ ทั้งนี้ ให้รวมการทดสอบเจาะระบบ (Penetration Testing) และการทดสอบความปลอดภัยของแอปพลิเคชันขณะทำงาน (Dynamic Application Security Testing: DAST) สำหรับระบบที่เชื่อมต่ออินเทอร์เน็ตหรือระบบสำคัญ ก่อนเปิดใช้งานจริงและเมื่อมีการเปลี่ยนแปลงสำคัญ โดยช่องโหว่ที่พบต้องถูกบันทึกและแก้ไขตามกรอบระยะเวลาในแนวปฏิบัติการจัดการช่องโหว่เชิงเทคนิค

๑๕๖. การทดสอบการรวมระบบที่กำหนดไว้เพื่อทดสอบการรวมเข้ากับระบบอื่น ๆ เมื่อพัฒนาระบบใหม่หรือระบบเพิ่มประสิทธิภาพที่ทดสอบจะต้องมีการควบคุมสภาพแวดล้อมของระบบอย่างเหมาะสมเพื่อป้องกันผลกระทบที่อาจเกิดขึ้นกับระบบอื่น ๆ ที่เกี่ยวข้อง

๑๕๗. การทดสอบการยอมรับของผู้ใช้ – UAT ที่กำหนดให้กับผู้ใช้และผู้ที่เกี่ยวข้องร่วมกันทดสอบเพื่อยืนยันความถูกต้องของผลลัพธ์ของระบบ

๑๕๘. หลังจากระบบการทดสอบเสร็จสมบูรณ์ทีมโครงสร้างพื้นฐานจะต้องประสานงานกับทีมที่รับผิดชอบในการพัฒนาเพื่อให้เป็นไปตามการติดตั้งระบบ

๑๕๙. หน่วยงานที่รับผิดชอบในการพัฒนาจะถูกบันทึกการปรับปรุงหรือแก้ไขซอร์สโค้ดในระบบการพัฒนาและระบบทดสอบเพื่อตรวจสอบความถูกต้องของบันทึกการแก้ไขซอร์สโค้ด

หลักการวิศวกรรมระบบที่ปลอดภัย

๑๖๐. วิศวกรรมระบบรักษาความปลอดภัยได้รับการกำหนดเพื่อปรับปรุงความน่าเชื่อถือของระบบสารสนเทศด้านความปลอดภัยของข้อมูลที่เหมาะสมและตอบสนองต่อความต้องการทางธุรกิจขององค์กร หลักการนี้ควรใช้กับกระบวนการพัฒนาระบบสารสนเทศขององค์กรหรือวงจรชีวิตการพัฒนาซอฟต์แวร์ (SDLC) ที่ควรพิจารณาอย่างน้อยดังต่อไปนี้

๑๖๐.๑ ความปลอดภัยตามการออกแบบ: การควบคุมความปลอดภัยควรได้รับการพิจารณาและกำหนดในระยะแรกของการพัฒนา (การพัฒนาข้อกำหนด) ในกรณีที่มีการเปลี่ยนแปลงความต้องการของระบบผู้พัฒนา / เจ้าของระบบจะได้รับการพิจารณาให้อัปเดตหรือเพิ่มการควบคุมความปลอดภัยเพื่อให้เป็นไปตามข้อกำหนดใหม่

๑๖๐.๒ ปรับสมดุลความเสี่ยงและการควบคุม: การควบคุมความปลอดภัยควรเลือกตามระดับความเสี่ยงด้านต้นทุนความเสี่ยงต่อวัตถุประสงค์ทางธุรกิจและความเสี่ยงต่อประสิทธิภาพของระบบสารสนเทศเพื่อ

ป้องกันปัญหาจากการเลือกการควบคุมความปลอดภัยอย่างไม่เหมาะสมเช่นการควบคุมความปลอดภัยที่เข้มงวดเกินไปซึ่งก่อให้เกิดต้นทุนสูงกว่าที่จำเป็น

๑๖๐.๓ การใช้งานและความสามารถในการจัดการ: การควบคุมความปลอดภัยของข้อมูลควรได้รับการออกแบบมาเพื่อให้ใช้งานง่าย ระบบการจัดการความปลอดภัยของข้อมูลไม่ควรซับซ้อนเกินไปซึ่งอาจทำให้เกิดข้อผิดพลาดได้ การจัดการความปลอดภัย (เช่น การตั้งค่าการกำหนดค่า) ไม่ควรซับซ้อนโดยไม่จำเป็นซึ่งอาจทำให้เกิดข้อผิดพลาดได้ง่าย

๑๖๐.๔ การป้องกันในเชิงลึก: การควบคุมความปลอดภัยควรถูกกำหนดในหลายชั้นและเพื่อให้ครอบคลุมการควบคุมทางกายภาพและเชิงตรรกะในระบบปฏิบัติการ (OS), ฐานข้อมูล, แอปพลิเคชันและเครือข่ายเพื่อทดแทนที่เข้ากันได้เมื่อการควบคุมความปลอดภัยทำงานผิดปกติหรือถูกบุกรุก

๑๖๐.๕ ความเรียบง่าย: ระบบข้อมูลควรได้รับการออกแบบให้ซับซ้อนน้อยลงเพื่อลดองค์ประกอบที่ไม่จำเป็นข้อผิดพลาดที่อาจเกิดขึ้นและโอกาสในการโจมตีโดยบุคคลที่เป็นอันตราย

๑๖๐.๖ ความยืดหยุ่นและความสามารถในการกู้คืน: ระบบควรได้รับการออกแบบมาเพื่อป้องกันภัยคุกคาม เช่น ระบบจะกำจัดหรือปฏิเสธเมื่อเกิดข้อผิดพลาดในการควบคุมความปลอดภัยของข้อมูลหรือถูกบุกรุกและความสามารถในการกู้คืนในเวลาที่เหมาะสมที่ตรงตามข้อกำหนดทางธุรกิจ

๑๖๐.๗ การรักษาความลับและความซื่อสัตย์: ระบบควรสร้างการควบคุมความปลอดภัยเพื่อปกป้องความลับและความสมบูรณ์ของข้อมูลในขณะที่ประมวลผลถ่ายโอนและจัดเก็บ

๑๖๐.๘ การเคลื่อนที่: ระบบข้อมูลที่ให้บริการหรือทำงานกับอุปกรณ์มือถือควรได้รับการออกแบบหรือกำหนดค่าเพื่อพิจารณาความเสี่ยงของความปลอดภัยของข้อมูลเช่นการควบคุมความปลอดภัยทางกายภาพอุปกรณ์มือถือส่วนบุคคลการเชื่อมต่อเครือข่ายแอปพลิเคชันมือถือการแลกเปลี่ยนข้อมูลและฟังก์ชั่นเพื่อระบุที่อยู่

มาตรฐานการควบคุมซอร์สโค้ด

๑๖๑. จัดให้มีกลไกในการป้องกันการรั่วไหลของซอร์สโค้ดในระบบการผลิตการทดสอบและการพัฒนาไปยังบุคคลที่ไม่ได้รับอนุญาต เช่น จัดเก็บซอร์สโค้ดใน Library กลางเทคนิคระยะไกลและอื่นๆ

๑๖๒. การบันทึกบันทึกการเข้าถึงซอร์สโค้ดในระบบการผลิตการทดสอบและการพัฒนาจะต้องครอบคลุมหัวข้อต่อไปนี้เป็นอย่างน้อย

- ๑๖๒.๑ วันที่, เวลา, ID ผู้ใช้และที่อยู่ IP
- ๑๖๒.๒ การแก้ไขซอร์สโค้ด
- ๑๖๒.๓ ส่งออกซอร์สโค้ดออกจากไลบรารี
- ๑๖๒.๔ นำเข้าซอร์สโค้ดที่อัปเดตแล้วไปยังไลบรารี

๑๖๓. จัดให้มีกลไกในการตรวจสอบความถูกต้องของซอร์สโค้ด เช่น เทคโนโลยีการเข้ารหัส เทคนิคแฮช และอื่นๆ

๑๖๔. นำเข้าซอร์สโค้ดลงในระบบการผลิตที่กำหนดให้กับผู้ดูแลระบบเท่านั้นจะดำเนินการอัปโหลดซอร์สโค้ดไปยังระบบการผลิต

๑๖๕. ต้องจัดเก็บซอร์สโค้ดของระบบการผลิตตามมาตรฐานการสำรองและเรียกคืนขององค์กรเพื่อให้แน่ใจว่าซอร์สโค้ดถูกสำรองและกู้คืนเมื่อจำเป็น

การใช้งาน Open Source

๑๖๖. ตรวจสอบลักษณะสิทธิ์การใช้งานของระบบสารสนเทศหรือองค์ประกอบของระบบสารสนเทศ และปฏิบัติการเงื่อนไขอย่างเคร่งครัด อาทิ การให้เครดิต หรือข้อห้ามด้านการจำหน่าย จ่ายแจก

แนวปฏิบัติการตรวจสอบภายใน

Internal Audit Procedure

แนวปฏิบัตินี้คือเพื่อวางหลักเกณฑ์การตรวจสอบภายในในระบบการจัดการอย่างเหมาะสม

๑๖๗. กำหนดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ และอย่างน้อย 1 ครั้งต่อปี และทำเป็นแผนงานการตรวจสอบประจำปี (Audit Program)

๑๖๘. กำหนดให้เกณฑ์การตรวจสอบ (Audit Criteria) ระบบการจัดการต้องมีความสอดคล้องต่อเกณฑ์ตามมาตรฐานสากลที่หน่วยงานได้รับการรับรอง เพื่อมั่นใจว่าหน่วยงานมีการรักษามาตรฐานการทำงานให้เป็นสากลอยู่เสมอ ในการกำหนดเกณฑ์การตรวจสอบต้องสอดคล้องต่อวัตถุประสงค์การตรวจสอบ (Audit Objective)

๑๖๙. กำหนดให้เกณฑ์การตรวจสอบต้องประกอบด้วยการตรวจทานรายการข้อกฎหมายที่เกี่ยวข้องกับหน่วยงาน หรือที่ระบุไว้ในผลการวิเคราะห์บริบทของระบบการจัดการ

๑๗๐. กำหนดให้การตรวจสอบสามารถดำเนินการโดยบุคลากรภายในหรือภายนอกก็ได้ตามความเหมาะสมและทักษะความสามารถหรือความซับซ้อนในเรื่องที่ตรวจสอบ

๑๗๑. เกณฑ์ประกอบผลการตรวจสอบ (Finding) ประกอบด้วย

๑๗๑.๑ ความไม่สอดคล้อง (Nonconformity: NC): หมายถึงการทำงานปัจจุบันของหน่วยงานไม่สอดคล้องตามเกณฑ์การตรวจสอบ ซึ่งสามารถจำแนกตามระดับความรุนแรงได้ 2 ประเภท

- Major: ความไม่สอดคล้องที่นำมาซึ่งผลกระทบสูง อาทิ ผิดกฎหมาย เสื่อมเสียชื่อเสียง หรือทำให้เกิดความเสี่ยงในระดับสูงมาก
- Minor: ความไม่สอดคล้องที่ไม่จัดว่าเป็น Major

๑๗๑.๒ ข้อสังเกต (Observation): การตั้งข้อสังเกตเกี่ยวกับการดำเนินงานที่นำมาซึ่งความเสี่ยงแล้วเกิดเป็นความไม่สอดคล้องได้ในอนาคต

๑๗๑.๓ โอกาสในการพัฒนาปรับปรุง (Opportunity for Improvement) คือ ข้อเสนอแนะในการพัฒนาปรับปรุงซึ่งไม่ใช่ความไม่สอดคล้องและไม่ใช่ข้อสังเกต

๑๗๒. ผลการตรวจสอบต้องจัดทำเป็นลายลักษณ์อักษรและสื่อสารให้ผู้ที่มีส่วนได้ส่วนเสียรับทราบ

๑๗๓. ผลการดำเนินการแก้ไขต้องได้รับการบันทึกและติดตาม ทุกความไม่สอดคล้องต้องมีการออกใบดำเนินการแก้ไข (Corrective Action Report)

๑๗๔. ผลการตรวจสอบและการดำเนินการแก้ไขต้องรายงานถึงคณะกรรมการ

๑๗๕. กำหนดให้มีการตรวจสอบหน่วยงานภายนอกที่สำคัญ (Critical Service) โดยกำหนดแผนงานให้สอดคล้องกับความเสี่ยงและการเปลี่ยนแปลงของบริบทที่เกี่ยวข้องกับบริการอันเป็นสาระสำคัญของการว่าจ้างหน่วยงานดังกล่าว ในกรณีที่ไม่สามารถเข้าดำเนินการตรวจสอบได้ให้หน่วยงานดังกล่าวส่งผลการตรวจสอบที่เกี่ยวข้องหรือผลการตรวจรับรองมาตรฐานสากลจากหน่วยงานตรวจรับรอง

๑๗๖. การกำหนดระยะเวลาการแก้ไขความไม่สอดคล้องให้ขึ้นอยู่กับผู้ดำเนินการแก้ไขกำหนดแต่ต้องไม่มากกว่า 365 วัน ทั้งนี้หากการกำหนดระยะเวลาดังกล่าวไม่สมเหตุสมผลต่อความเสี่ยงหรือหลักการทางเทคโนโลยี ให้ผู้ตรวจสอบภายในนำเสนอต่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ เพื่อพิจารณา

การตรวจสอบระบบการจัดการ

๑๗๗. ผู้ตรวจสอบมีหน้าที่จัดการและควบคุมให้การตรวจสอบภายในเป็นไปอย่างมีประสิทธิภาพและสม่ำเสมอ รวมทั้งควบคุมดูแลให้การตรวจสอบภายในเป็นไปอย่างถูกต้องและเหมาะสม

๑๗๘. ผู้ตรวจสอบจัดทำแผนแล้วเสนอคณะกรรมการ

๑๗๙. คณะกรรมการพิจารณาอนุมัติ และสั่งการเพิ่มเติม (ถ้ามี)

๑๘๐. ผู้ตรวจสอบแจ้งแผนการตรวจสอบภายในให้ผู้ที่เกี่ยวข้องรับทราบ

๑๘๑. ในกรณีที่หน่วยงานไม่มีผู้ตรวจสอบ ให้ทำการคัดเลือกผู้ทำการตรวจสอบภายใน แล้วเสนอคณะกรรมการพิจารณาอนุมัติ โดยผู้ตรวจสอบต้องได้รับการฝึกอบรม และต้องไม่มีส่วนรับผิดชอบกับพื้นที่ หรือส่วนงานนั้นๆ

๑๘๒. การตรวจสอบภายในต้องจัดทำให้ครอบคลุมกระบวนการหรือพื้นที่ที่อยู่ภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เป็นประจำทุกปี อย่างน้อยปีละ 1 ครั้ง

๑๘๓. การตรวจสอบภายในต้องพิจารณาถึงความสำคัญของกระบวนการหรือพื้นที่ที่จะทำการตรวจสอบภายในและผลจากการตรวจสอบครั้งที่ผ่านมา

๑๘๔. การเปลี่ยนแปลงกำหนดการตรวจสอบภายในที่กระทำภายในพื้นที่ บริการหรือส่วนงานใด ให้ผู้ตรวจและผู้รับการตรวจสอบทำบันทึกข้อตกลงเพื่อเปลี่ยนแปลงวันตรวจ ก่อนถึงกำหนด

อย่างน้อย 5 วัน ทั้งนี้การเปลี่ยนแปลงดังกล่าวต้องกระทำเฉพาะกรณีที่มีความจำเป็นเหมาะสมเท่านั้น

๑๘๕. ผู้ตรวจสอบ ศึกษาขั้นตอนการปฏิบัติงาน และเอกสารระบบการจัดการที่เกี่ยวข้อง กับพื้นที่หรือบริการที่ตรวจสอบ และจัดทำแบบตรวจสอบ รายการ (Check Lists) หรือแผนตรวจสอบอื่น ๆ ตามความจำเป็น ทั้งนี้ รายการตรวจสอบจะมีหรือไม่ขึ้นอยู่กับความซับซ้อนของระบบการจัดการที่ดำเนินการตรวจสอบ

๑๘๖. ผู้ตรวจสอบนำแบบตรวจสอบรายการหรือแผนตรวจสอบไปดำเนินการตรวจสอบ ตามกำหนดวันและเวลาที่ตกลงกับผู้รับการตรวจสอบ โดยประกอบด้วยกิจกรรม ดังนี้

๑๘๖.๑ การประชุมเปิดการตรวจสอบ โดยมุ่งเน้นการชี้แจงรายละเอียดเกี่ยวกับการตรวจตามแผนงาน อาทิ ขอบเขตและเกณฑ์การตรวจสอบ

๑๘๖.๒ ดำเนินการตรวจสอบ โดยวิธีการสุ่มตรวจสอบด้วยสัดส่วนหรืออัตราส่วนที่เชื่อได้ว่าจะได้ผลการตรวจสอบที่มีประสิทธิภาพ สะท้อนถึงสมรรถนะและข้อเท็จจริง แนวทางการตรวจสอบอาจครอบคลุม การสัมภาษณ์ การสังเกต และการศึกษาเชิงเอกสารทั้งปฐมภูมิและทุติยภูมิ

๑๘๖.๓ ดำเนินการสรุปปิดการตรวจสอบ มุ่งเน้นการชี้แจงปัญหาหรือประเด็นที่ยังคงค้าง ผลการตรวจสอบเบื้องต้น และมติการยอมรับในผลการตรวจสอบเบื้องต้นจากผู้รับการตรวจสอบ

๑๘๗. ผู้ตรวจสอบสรุปผลการตรวจสอบและออกใบร้องขอให้มีการแก้ไข (ถ้ามี) ในระบบ Service Desk ชี้แจงผลการตรวจสอบและส่งมอบใบร้องขอให้มีการแก้ไข ให้ผู้รับการตรวจสอบหรือผู้มีส่วนได้ส่วนเสียนำไปดำเนินการแก้ไข ป้องกัน

๑๘๘. ผู้ตรวจสอบส่งรายงานผลการตรวจสอบภายในและแบบตรวจสอบรายการ ให้คณะกรรมการ

แนวปฏิบัติการแก้ไขความไม่สอดคล้อง

Corrective Action Procedure

แนวปฏิบัตินี้คือเพื่อวางหลักเกณฑ์การแก้ไขความไม่สอดคล้องที่ตรวจพบทั้งจากบุคลากรภายในหรือภายนอก โดยมุ่งเน้นการบันทึกเพื่อแสดงหลักฐานการแก้ไขอย่างเหมาะสม

๑๘๙. เมื่อตรวจพบความไม่สอดคล้อง เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการบันทึกการแก้ไข พร้อมกำหนดความไม่สอดคล้องที่ตรวจพบ โดยยึดแนวปฏิบัติการตรวจสอบภายใน แม้ว่าตนจะไม่ใช่ผู้ตรวจสอบภายในก็ตาม

๑๙๐. เจตนาของการบันทึกความไม่สอดคล้องเพื่อให้เกิดการแก้ไขตามแนวปฏิบัตินี้อย่างสมบูรณ์ หรือเพื่อสร้างหลักฐานเชิงประจักษ์ต่อปัญหาที่ตรวจพบ แม้ว่าวิธีการแก้ไขจะยังไม่มีก็ตาม บุคลากรที่ดำเนินการด้วยความบริสุทธิ์ใจย่อมถือว่าได้ดำเนินการแก้ไขปัญหาอย่างสุดความสามารถแล้ว

๑๙๑. ในการแก้ไขความไม่สอดคล้องต้องกำหนดถึงสาเหตุของปัญหาและความไม่สอดคล้องที่ชัดเจน

๑๙๒. ในการแก้ไขความไม่สอดคล้องต้องพิจารณาการแก้ไขความไม่สอดคล้องทั้งในระยะสั้น (correction) และการแก้ไขที่สาเหตุของปัญหาที่แท้จริง (corrective action) เพื่อให้ไม่มีการเกิดขึ้นซ้ำของความไม่สอดคล้อง

๑๙๓. การแก้ไขความไม่สอดคล้องต้องได้รับการติดตามผลการแก้ไขหรือตรวจทานให้มั่นใจว่าแนวทางการแก้ไขมีประสิทธิภาพ และจัดลำดับความสำคัญของการแก้ไขความไม่สอดคล้องตามเกณฑ์ด้านความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๑๙๔. การแก้ไขความไม่สอดคล้องให้บันทึกเป็นผลการดำเนินงานตามความไม่สอดคล้องที่กำหนดขึ้นในระบบ Service Desk

แนวปฏิบัติทางกฎหมายและระเบียบ

Legal and Compliance Procedure

แนวปฏิบัตินี้คือเพื่อวางหลักในการปฏิบัติงานของเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศให้สอดรับกับบทกฎหมาย ระเบียบปฏิบัติ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และกฎหมายดิจิทัลที่สำคัญยิ่ง

การได้มาซึ่งข้อกำหนดกฎหมาย

๑๙๕. หน่วยงานต้องปฏิบัติตามการสั่งการของนิติกรของคณะแพทยศาสตร์และมหาวิทยาลัยสงขลานครินทร์ ในประเด็นที่เกี่ยวข้องกับกฎหมาย

๑๙๖. ข้อกำหนดกฎหมายอาจจะถูกส่งมาถึงหน่วยงานตามสายบังคับบัญชาและเรียนแจ้งเพื่อทราบและปฏิบัติตาม

๑๙๗. หน่วยงานต้องพิจารณาข้อกฎหมายที่เกี่ยวข้องกับระบบการจัดการและจัดทำรายการหรือบันทึกที่จำเป็นเกี่ยวกับการ

ปฏิบัติตามกฎหมาย โดยให้พิจารณาเป็นข้อกำหนดตามบริบทของระบบการจัดการ

การตีความและกำหนดบทมาตรากฎหมายที่เกี่ยวข้อง

๑๙๘. หากพ้นวิสัยที่หน่วยงานพึงจะตีความบทกฎหมายที่เกี่ยวข้องกับระบบการจัดการ ให้ทำหนังสือถึงนิติกร องค์กร เพื่อการพิจารณากำหนดบทกฎหมายและการตีความให้กระจ่าง

๑๙๙. การตีความบทกฎหมายโดยปราศจากฐานความรู้ทางนิติศาสตร์อย่างชัดเจน อาจก่อให้เกิดความเสี่ยงหรือภาระงานเกินความจำเป็นในระบบการจัดการ

๒๐๐. ประมวลกฎหมายแพ่งพาณิชย์และอาญา (กฎหมายทั่วไป) ย่อมมีความสัมพันธ์กับระบบการจัดการเป็นปรกติ ในหลายมาตรากฎหมาย จึงควรพิจารณากฎหมายที่มีลักษณ์เป็นการเฉพาะเจาะจงเป็นสำคัญ หรือกฎหมายทั่วไปที่มีลักษณะเป็นการเฉพาะเรื่อง อาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

นิติวิทยาศาสตร์

๒๐๑. กรณีต้องใช้หลักฐานทางนิติวิทยาศาสตร์ให้ติดต่อหน่วยงานที่เกี่ยวข้อง หรือปรึกษากับนิติกรขององค์กรก่อนการดำเนินการ โดยมีหลักปฏิบัติ ดังนี้

๒๐๑.๑ จัดทำ Audit Trail เพื่อให้ได้หลักฐานที่สมบูรณ์และมีคุณภาพ จำเป็นต้องจัดทำ Audit Trail ที่มีความชัดเจน โดยต้องมีการจัดเก็บวัน เวลา ต้นทาง ปลายทาง การพิสูจน์ตัวตน และรายละเอียดกิจกรรมต่าง ๆ ดังนี้

- สำหรับเอกสารที่เป็นลายลักษณ์อักษร รายงานต้นฉบับจะต้องถูกเก็บไว้ให้ปลอดภัย โดยเอกสารดังกล่าวจะต้องบันทึกชื่อผู้จัดทำ สถานที่พบ เวลาที่พบ และผู้แจ้งปัญหา
- สำหรับข้อมูลสารสนเทศที่อยู่ในสื่อบันทึกคอมพิวเตอร์ ต้องมีการทำสำเนาของข้อมูลทั้งในฮาร์ดดิสก์ และในหน่วยความจำ (RAM/ROM) โดยจะต้องเก็บบันทึก และ/หรือมีพยานในระหว่างการทำสำเนาข้อมูล ทั้งนี้สื่อบันทึกจะต้องถูกเก็บให้ปลอดภัย

๒๐๑.๒ กรณีเป็นหลักฐานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ หากตรวจพบเครื่องคอมพิวเตอร์/เครื่องแม่ข่าย รวมถึงอุปกรณ์เครือข่าย รวมเรียกว่า “พยานวัตถุ” ถูกโจมตีหรือถูกบุกรุก ให้ดำเนินการปลดพยานวัตถุดังกล่าวออกจากระบบเครือข่ายเป็นอันดับแรก หรือดำเนินการย้ายไปไว้ในเครือข่ายเฉพาะ

๒๐๑.๓ ห้ามปิดหรือรีบูทหรือกระทำการใด ๆ ที่จะส่งผลต่อการเปลี่ยนแปลงกระแสไฟฟ้า แหล่งจ่ายไฟตลอดจนหน่วยความจำชั่วคราว ก่อนที่จะทำการจัดเก็บหลักฐานโดยเด็ดขาดเนื่องจากหลักฐานการกระทำผิดอาจสูญหายได้

๒๐๑.๔ กรณีพยานวัตถุเป็นเครื่องคอมพิวเตอร์ ห้ามเรียกใช้โปรแกรมใด ๆ โดยเด็ดขาด

๒๐๑.๕ กรณีพยานวัตถุเป็นเครื่องคอมพิวเตอร์ อาจถูกติดตั้งโปรแกรมประสงค์ร้าย เช่น โทรจัน (Trojan) ไว้ในระบบ การเรียกใช้โปรแกรมใด ๆ ในเครื่องนั้น อาจเป็นการเรียกให้โปรแกรมโทรจันทำงานและส่งผลให้มีการเปลี่ยนแปลงหรือทำลายหลักฐานที่ต้องการภายในเครื่องดังกล่าวได้ หากจำเป็นควรเรียกใช้โปรแกรมจากแหล่งที่มาภายนอกเครื่องคอมพิวเตอร์ เช่น USB เพื่อให้แน่ใจได้ว่าโปรแกรมนั้นไม่มีซอฟต์แวร์ประสงค์ร้ายอยู่

๒๐๑.๖ ลดการดำเนินการใด ๆ จากข้อมูลเดิม

๒๐๑.๗ เมื่อได้มีการทำสำเนาต้นฉบับ (Master Copy) แล้ว หากต้องการดำเนินการใดๆ ให้ดำเนินการจากสำเนาต้นฉบับ เนื่องจากการเปลี่ยนแปลงใดๆ จากข้อมูลเดิมจะมีผลกระทบต่อการวิเคราะห์ นอกจากนี้ไม่ควรกระทำการใด ๆ ที่ทำให้เกิดการเปลี่ยนแปลงข้อมูลเวลาในการเข้าถึง (Access Time)

๒๐๑.๘ ทำบันทึกสำหรับการเปลี่ยนแปลงใด ๆ และเก็บรายละเอียดบันทึกของกิจกรรมต่าง ๆ รวมถึงบันทึก

เหตุการณ์ไม่ปกติและอุบัติการณ์ และการแก้ไขที่เกิดขึ้น

๒๐๑.๙ ในกรณีที่การเปลี่ยนแปลงหลักฐานไม่สามารถหลีกเลี่ยงได้ ต้องจัดทำรายงานเพื่ออธิบายเหตุผลในการเปลี่ยนแปลง โดยการเปลี่ยนแปลงใดๆ ต้องได้รับการบันทึก รวมถึงข้อมูลและการเปลี่ยนแปลงทางกายภาพของสื่อที่ใช้ในการจัดเก็บหลักฐานดังกล่าว เช่น การเปลี่ยนอุปกรณ์ ฮาร์ดแวร์ การเขียนรายงานที่ไม่สามารถระบุช่วงเวลาได้ชัดเจน

๒๐๑.๑๐ กรณีเหตุการณ์ละเมิดความมั่นคงปลอดภัยเกิดขึ้น และพยานวัตถุที่โดนโจมตียังสามารถทำงานต่อไปได้ จะทำให้เจ้าหน้าที่สามารถเก็บหลักฐานได้มากยิ่งขึ้น แต่ทั้งนี้จะต้องมีการป้องกันทรัพยากรสารสนเทศที่ดีเพียงพอด้วย

ทรัพย์สินทางปัญญาและลิขสิทธิ์

๒๐๒. ระบบการจัดการต้องมีมาตรการในการตรวจสอบและควบคุมไม่ให้มีการละเมิดทรัพย์สินทางปัญญาและลิขสิทธิ์ รวมถึงการใช้สัญลักษณ์ทางการค้า (โลโก้) โดยให้ยึดระเบียบการจัดซื้อจัดจ้างเป็นสำคัญ เพื่อหลีกเลี่ยงประเด็นการละเมิด

๒๐๓. ทรัพยากรในระบบการจัดการต้องไม่ละเมิดลิขสิทธิ์

๒๐๔. ระบบการจัดการต้องสอดคล้องต่อข้อกำหนดที่เกี่ยวข้องกับทรัพย์สินทางปัญญา ที่องค์กรประกาศกำหนด

๒๐๕. ไม่นำผลงานของผู้อื่น หรือผลงานใดๆ ที่มีลิขสิทธิ์มาทำการคัดลอก หรือดัดแปลงก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์ หรือนำมาเป็นส่วนหนึ่งของระบบการจัดการ

๒๐๖. การจัดซื้อจัดหาเอกสาร ข้อมูล ซอฟต์แวร์ และทรัพย์สินทางปัญญา ต้องจัดซื้อกับผู้ผลิต หรือตัวแทนจำหน่ายที่เชื่อถือได้เท่านั้น

๒๐๗. เอกสาร ข้อมูล ซอฟต์แวร์ และทรัพย์สินทางปัญญา ที่จัดซื้อจัดหาเข้ามา ต้องถูกบันทึกลงในทะเบียนทรัพย์สิน และจัดเก็บเอกสารระบุสิทธิ์ในการใช้งาน หรือเอกสารในการซื้อขายที่สามารถใช้ยืนยันสิทธิ์ในการใช้งานเอาไว้อย่างครบถ้วน

๒๐๘. หน่วยงานต้องเฝ้าติดตามปริมาณการใช้งาน รูปแบบการใช้งาน และรายละเอียดที่เกี่ยวข้องกับการใช้งานทรัพย์สินทางปัญญา ให้เป็นไปตามที่เจ้าของลิขสิทธิ์กำหนด

๒๐๙. ทรัพย์สินทรัพย์สินทางปัญญาที่เจ้าหน้าที่สร้างขึ้นเพื่อใช้ประกอบการทำงานให้กับองค์กร ถือเป็นลิขสิทธิ์ขององค์กร ยกเว้นกรณีที่มีการจัดทำข้อตกลงอื่นที่ระบุเรื่องลิขสิทธิ์ของทรัพย์สินเหล่านี้

๒๑๐. ทรัพย์สินทรัพย์สินทางปัญญาที่หน่วยงานภายนอกสร้างขึ้นเพื่อใช้ประกอบการทำงานให้กับองค์กร ให้เป็นไปตามที่ระบุไว้ในสัญญาจ้างหรือสัญญาบริการ

แนวปฏิบัติการพัฒนาปรับปรุงอย่างต่อเนื่อง

Continuous Improvement Procedure

แนวปฏิบัตินี้เพื่อให้มีกระบวนการในการตรวจสอบ วิเคราะห์ และให้ข้อเสนอแนะในการปรับปรุงระบบการจัดการ รวมทั้งปรับปรุงกระบวนการของหน่วยงานให้มีประสิทธิภาพ (Efficiency) และประสิทธิผล (Effectiveness)

๒๑๑. หน่วยงานวิเคราะห์ข้อมูลตามตัวชี้วัดประสิทธิภาพของระบบการจัดการ โดยพิจารณาให้ครอบคลุมถึงความเชื่อมโยงต่อตัวชี้วัดของหน่วยงานและองค์กร สรุปผลการวิเคราะห์ข้อมูลปัญหาที่เกี่ยวข้อง และคำแนะนำในการปรับปรุงแก้ไขให้ดียิ่งขึ้น

๒๑๒. หน่วยงานวิเคราะห์ถึงการกำหนดโครงการภายใต้แผนปฏิบัติงานของหน่วยงานว่ามีความครบถ้วนและสอดรับกับผลการวิเคราะห์ข้อมูล เพื่อพิจารณาถึงช่องทางและโอกาสในการพัฒนาปรับปรุงตามผลการวิเคราะห์ ความเป็นไปได้ ตลอดจนงบประมาณที่ถูกจัดสรรให้หน่วยงานมีความเพียงพอต่อการพัฒนาปรับปรุง

๒๑๓. หน่วยงาน นำเสนอข้อมูลสรุปผลการวิเคราะห์และความเชื่อมโยงต่อแผนปฏิบัติการของหน่วยงาน แก่คณะกรรมการภายหลังการอนุมัติ หน่วยงานดำเนินการตามแผนงานโครงการ และรายงานให้ผู้บริหารหรือผู้บังคับบัญชาในสายงานและคณะกรรมการ ได้รับทราบเป็นระยะ ๆ พร้อมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบตามความจำเป็น จนกระทั่งเสร็จสิ้นตามแผน โดยให้เป็นไปตามกลไกและระเบียบการจัดการโครงการของรัฐวิสาหกิจและกฎระเบียบอื่น ๆที่เกี่ยวข้องในระดับองค์กร

๒๑๔. ในกรณีที่ผลการดำเนินการในโครงการใด ๆ กระทบหรือส่งผลต่อระบบการจัดการและองค์ประกอบของระบบการจัดการส่วนหนึ่งส่วนใดหรือทั้งหมด อาทิ การส่งผลให้ต้องมีการปรับปรุง นโยบาย กระบวนการ ขั้นตอนปฏิบัติหรือเอกสารอื่นให้ผู้จัดการโครงการนั้น ๆ แจ้งแก่ผู้แทนคณะกรรมการ เพื่อการวางแผนการปรับปรุงต่อไป

๒๑๕. กรณีผลของการดำเนินโครงการใด ๆ เป็นข้อมูลสำคัญของตัวชี้วัดประสิทธิภาพของระบบการจัดการ หรือมีส่วนเกี่ยวข้องให้ผู้จัดการโครงการแจ้งผู้แทนคณะกรรมการเพื่อปรับปรุงผลการวัดประเมิน

๒๑๖. ผลการวัดประเมินต้องถูกนำมาพิจารณาในการปรับปรุงค่าเป้าหมายหรือกลไกการวัดประเมินประสิทธิภาพของระบบการจัดการให้เหมาะสม

๒๑๗. ประสิทธิภาพของระบบการจัดการสามารถถูกวัดประเมินโดยตัวชี้วัดความสำเร็จของโครงการภายใต้แผนปฏิบัติการ และตัวชี้วัดความสำเร็จของโครงการก็สามารถถูกวัดประเมินโดยผลผลิตของระบบการจัดการได้เช่นกัน ขึ้นอยู่กับบริบทและการกำหนดความเชื่อมโยงระหว่างระบบการจัดการและการบริหารโครงการนั้น ๆ อย่างไรก็ตามตัวชี้วัดต้องถูกกำหนดแยกไว้อย่างชัดเจนระหว่างตัวชี้วัดของระบบการจัดการและตัวชี้วัดของโครงการ ไม่สามารถนำมากล่าวอ้างหรือใช้ผลอ้างอิงแก่กันและกันได้

๒๑๘. การแก้ไข (Corrective Action) จากผลการตรวจสอบทั้งจากภายในและภายนอก (Audit Findings) สามารถพิจารณาเป็นส่วนหนึ่งของการพัฒนาปรับปรุงภายใต้ระบบการจัดการได้ ก็ต่อเมื่อผลการตรวจสอบนั้นมิได้เกิดจากการพลั้งเผลอ ละเลย หรือความบกพร่องต่อหน้าที่ของบุคลากร

แนวปฏิบัติการใช้ระบบ Help Desk

Use of Helpdesk System for Datacenter Operation

แนวปฏิบัตินี้เพื่อให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศสามารถใช้ระบบ Help Desk ทดแทนการใช้กระดาษเพื่อการบันทึก สอบทาน อนุมัติ และวิเคราะห์ผลการดำเนินงาน

๒๑๙. ระบบ Help Desk เป็นระบบสารสนเทศภายในที่สามารถใช้ในการรองรับการบันทึกดังต่อไปนี้

๒๑๙.๑ การบันทึกอุบัติการณ์

๒๑๙.๒ การบันทึกปัญหาคงค้าง

๒๑๙.๓ การบันทึกคำขอบริการ

๒๑๙.๔ การบันทึกความเสี่ยง

๒๑๙.๕ การบันทึกประเด็นตรวจสอบ

๒๑๙.๖ การบันทึกตัวชี้วัดประสิทธิภาพ

๒๑๙.๗ การบันทึกการเปลี่ยนแปลง

๒๒๐. การบันทึกอุบัติการณ์ ให้พิจารณาว่าเป็นเหตุเสีย เหตุขัดข้องหรือเหตุอันเกิดจากความผิดปกติ หรือผิดไปจากสภาวะปกติหรือไม่ อาทิ การแจ้งเหตุเสีย การไม่สามารถเข้าใช้งานระบบตลอดจนเหตุผิดปกติของระบบหรือเครือข่ายจากการเฝ้าระวัง ในการบันทึกอุบัติการณ์ ต้องประกอบด้วย (อย่างน้อย)

๒๒๐.๑ รายละเอียดเหตุเสีย

๒๒๐.๒ ระดับความรุนแรง

๒๒๐.๓ แนวทางการแก้ไขปัญหา (Solution/Work around)

๒๒๐.๔ สาเหตุของอุบัติการณ์ (กรณีทราบสาเหตุแน่ชัด)

๒๒๑. อุบัติการณ์ที่ไม่ทราบสาเหตุแน่ชัดให้พิจารณาเป็นปัญหาคงค้าง (บันทึกเพิ่มเติม) และนำหมายเลขปัญหาคงค้างเพิ่มลงในบันทึกอุบัติการณ์

๒๒๒. กรณีที่การแก้ไขอุบัติการณ์ต้องมีการเปลี่ยนแปลง (change) ให้จัดทำบันทึกการเปลี่ยนแปลง (change) และนำหมายเลขการเปลี่ยนแปลงเพิ่มลงในบันทึกอุบัติการณ์

๒๒๓. การบันทึกปัญหาคงค้าง ให้พิจารณาว่าเป็นเหตุขัดข้องที่ยังไม่สามารถแก้ไขที่สาเหตุได้ หรือเหตุขัดข้องที่ยังไม่ทราบสาเหตุได้ (known error) ประกอบด้วย (อย่างน้อย)

๒๒๓.๑ เหตุเสียที่ทราบและไม่สามารถแก้ไขได้

๒๒๓.๒ แนวทางการแก้ไขเบื้องต้น

๒๒๓.๓ ระดับความรุนแรง (ใช้เกณฑ์เดียวกับอุบัติการณ์)

๒๒๔. การบันทึกการเปลี่ยนแปลง ให้พิจารณาว่าเป็นการเปลี่ยนแปลงองค์ประกอบของทรัพย์สินสารสนเทศส่วนหนึ่งส่วนใด หรือทั้งหมด อาทิ การเปลี่ยนแปลงการตั้งค่าอุปกรณ์เครือข่าย การติดตั้ง critical patch หรือ patch ที่ทำให้เกิด downtime การเปลี่ยนแปลงเอกสาร ISMS-PR / IS-PR การเปลี่ยนแปลงรายชื่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ และบุคคลอื่น ๆ ที่เกี่ยวข้อง ในการบันทึกต้องประกอบด้วย (อย่างน้อย)

๒๒๔.๑ ข้อมูลการเปลี่ยนแปลงที่ต้องดำเนินการ

๒๒๔.๒ ระดับความรุนแรงของการเปลี่ยนแปลง

๒๒๔.๓ แผนการกู้คืนถ้าผิดพลาด (ถ้ามี) กรณีไม่มีให้ระบุว่าไม่มี ห้ามเว้นว่าง

๒๒๔.๔ รายละเอียดหรือขั้นตอนการเปลี่ยนแปลง (เฉพาะ major change)

๒๒๔.๕ ระยะเวลาที่คาดว่าจะดำเนินการและระยะเวลาที่คาดว่าแล้วเสร็จ

๒๒๕. การบันทึกประเด็นตรวจสอบ ให้พิจารณาว่าเป็นผลจากการตรวจสอบหรือการทำงานที่ผิดนโยบาย แนวปฏิบัติ ระเบียบ หรือกฎหมาย รวมเรียกว่า “ความไม่สอดคล้อง” หรือการพัฒนาปรับปรุงที่ต้องการในระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ อาทิ ประเด็นความไม่สอดคล้องจากผู้ตรวจสอบภายใน ประเด็นความไม่สอดคล้องจากผู้ตรวจสอบภายนอก ในการบันทึกต้องประกอบด้วย (อย่างน้อย)

๒๒๕.๑ ประเด็นความไม่สอดคล้องที่พบ

๒๒๕.๒ ข้อกำหนดที่เป็นประเด็นความไม่สอดคล้อง

๒๒๕.๓ ข้อเสนอแนะ (ถ้ามี)

๒๒๖. การดำเนินการแก้ไข (corrective action) ให้เป็นการบันทึกลงในบันทึกประเด็นความไม่สอดคล้อง โดยผู้ที่ได้รับมอบหมายให้ดำเนินการแก้ไข ในการบันทึก (ตอบกลับ) ประเด็นความไม่สอดคล้องต้องประกอบด้วย (อย่างน้อย)

๒๒๖.๑ แนวทางการแก้ไขเบื้องต้น (ถ้ามี)

๒๒๖.๒ แนวทางการแก้ไขที่สาเหตุของความไม่สอดคล้อง (การแก้ไขที่จะขจัดซึ่งความไม่สอดคล้องและไม่เกิดซ้ำ)

๒๒๖.๓ สาเหตุแห่งความไม่สอดคล้อง

๒๒๖.๔ ระยะเวลาที่คาดว่าจะดำเนินการแล้วเสร็จ

๒๒๗. การบันทึกตัวชี้วัดประสิทธิภาพ ให้เป็นการบันทึกตามตัวชี้วัดประสิทธิภาพของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ในการบันทึกตัวชี้วัดประกอบด้วย (อย่างน้อย)

๒๒๗.๑ ตัวชี้วัด

๒๒๗.๒ ค่าเป้าหมาย

๒๒๗.๓ การมอบหมายผู้ดำเนินการวัด

๒๒๗.๔ ความถี่ในการสรุปผลและรายงานผล

๒๒๗.๕ แหล่งข้อมูลที่มาที่ใช้ในการวัดผล (ถ้ามี)

๒๒๘. ในการวัดค่าตัวชี้วัดประสิทธิภาพ ให้ดำเนินการตอบกลับค่าการวัด (ผลการประเมินหรือความคืบหน้า) โดยพิจารณาตามรอบความถี่ของการสรุปผล ดังนี้

๒๒๘.๑ หากตัวชี้วัดมีความถี่ในการสรุปผลเป็นรายปี ให้จัดทำรายงานความคืบหน้าหรือผลเบื้องต้นภายในวันที่ 5 ของทุกเดือน

๒๒๘.๒ หากตัวชี้วัดมีความถี่ในการสรุปผลเป็นรายเดือน ให้ตอบกลับค่าการวัดทุกวันศุกร์สุดท้ายของเดือน

๒๒๘.๓ หากตัวชี้วัดมีความถี่ในการสรุปผลเป็นรายสัปดาห์ ให้ตอบกลับค่าการวัดทุกวันศุกร์ของแต่ละสัปดาห์

๒๒๙. ในการบันทึกความเสี่ยง ให้พิจารณาแยกเป็น 2 ระดับ ความเสี่ยงจากทรัพย์สิน หรือความเสี่ยงจากการจัดการ

๒๓๐. ในการบันทึกความเสี่ยงจากทรัพย์สิน เป็นผลจากการรายงานช่องโหว่ของทรัพย์สินสารสนเทศ ซึ่งอาจเกิดจากกลไกการตรวจทานช่องโหว่ (VA Scan) หรือการทำ Threat Intelligence ในการบันทึกประกอบด้วย (อย่างน้อย)

๒๓๐.๑ ทรัพย์สินสารสนเทศที่มีช่องโหว่

๒๓๐.๒ ช่องโหว่ที่เกิดขึ้น

๒๓๐.๓ แนวทางการแก้ไขช่องโหว่

๒๓๐.๔ ระดับความเสี่ยง (อ้างอิงค่า CVE Score) ถ้าไม่มีให้ระบุโดยใช้เกณฑ์ของความเสี่ยงการจัดการ

๒๓๑. ในการวางแผนการแก้ไขความเสี่ยง (treatment plan) ของความเสี่ยงในทรัพย์สินสารสนเทส ให้บันทึก (ตอบกลับ) บนบันทึกความเสี่ยง โดยผู้ที่ได้รับมอบหมายให้ดำเนินการแก้ไขอย่างน้อยประกอบด้วย

๒๓๑.๑ แนวทางการแก้ไขช่องโหว่

๒๓๑.๒ ระยะเวลาที่คาดว่าจะแล้วเสร็จ

๒๓๑.๓ กรณีไม่สามารถจัดการได้ให้เจ้าของความเสี่ยง (ปัจจุบันคือหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ) ตอบกลับว่า “ยอมรับความเสี่ยง” แล้วทำการเปลี่ยนสถานะบันทึก

๒๓๒. ในการบันทึกความเสี่ยงการจัดการ ให้ผู้ประเมินบันทึกอย่างน้อย

๒๓๒.๑ ความเสี่ยงที่บ่งชี้

๒๓๒.๒ ภัยคุกคาม (ถ้ามี) ที่อาจเกิดขึ้น หรือผลกระทบจากการเกิดขึ้นของความเสี่ยงนั้นทางตรง

๒๓๒.๓ ระดับโอกาสการเกิดของความเสี่ยง

๒๓๒.๔ ค่าคะแนนเฉลี่ยระดับผลกระทบ

๒๓๒.๕ ระดับความเสี่ยง

๒๓๓. ในการวางแผนการแก้ไขความเสี่ยง (treatment plan) ของความเสี่ยงการจัดการให้บันทึก (ตอบกลับ) บนบันทึกความเสี่ยง โดยผู้ที่ได้รับมอบหมายให้ดำเนินการแก้ไข อย่างน้อยประกอบด้วย

๒๓๓.๑ กลยุทธ์การจัดการความเสี่ยง

๒๓๓.๒ แนวทางการรับมือและแผนการจัดการความเสี่ยง

๒๓๓.๓ ระดับความเสี่ยงคงเหลือ (residual risk) ที่คาดว่าจะเหลือ

๒๓๓.๔ ระยะเวลาที่คาดว่าจะแล้วเสร็จ

๒๓๔. ทุกบันทึกความเสี่ยงให้บันทึกและมอบหมายถึง “หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ” ในฐานะเจ้าของความเสี่ยงเสมอ และให้ถือว่าเป็นการอนุมัติบันทึกนั้นโดยปริยาย

ตัวอย่างมาตรฐานบันทึกข้อความ

(ตามแนวปฏิบัติข้อ ๒๑๙–๒๓๔)

◆ **๑. การบันทึกอุบัติการณ์ (Incident Record) (๒๒๐–๒๒๒)**

Incident ID: INC-2024-00987
วันที่/เวลา: 25 กันยายน 2567, 22:34 น.
รายละเอียดเหตุเสีย (Incident Detail): ระบบ HIS ไม่สามารถใช้งานได้ – พบ web server ไม่ตอบสนอง
ระดับความรุนแรง (Severity Level): High – ส่งผลกระทบต่อบริการผู้ป่วย
แนวทางการแก้ไขปัญหา (Solution/Workaround): รีสตาร์ท Apache Service และตรวจสอบ log
สาเหตุของอุบัติการณ์ (Root Cause): RAM เต็มจาก process ที่ไม่ยุติ
หมายเลขปัญหาคงค้าง (Linked Problem ID): PRB-2024-00034
หมายเลขการเปลี่ยนแปลง (Linked Change ID): CHG-2024-00012

◆ **๒. การบันทึกปัญหาคงค้าง (Problem Record) (๒๒๓)**

Problem ID: PRB-2024-00034
เหตุเสียที่ทราบแต่ยังไม่สามารถแก้ไข (Known Error): RAM บน web server ใช้สูงเกิน 90%
แนวทางการแก้ไขเบื้องต้น (Temporary Fix): ตั้ง cron job ให้รีสตาร์ท service อัตโนมัติ
ระดับความรุนแรง (Severity): Medium

◆ **๓. การบันทึกคำขอบริการ (Service Request) (๒๑๙.๓)**

Request ID: SRV-2024-00087
คำขอ (Requested Service): ติดตั้ง Server Dell R750 ในพื้นที่ Colocation
รายละเอียด (Request Detail): ขนาด 2U, น้ำหนัก 25 กก., ใช้ไฟ 800W พร้อม UPS
สถานะ (Status): อนุมัติแล้ว

◆ **๔. การบันทึกความเสี่ยงจากทรัพย์สิน (Asset-Based Risk Record) (๒๒๙–๒๓๑)**

Risk ID: RSK-2024-00135
ทรัพย์สินสารสนเทศ (Information Asset): Web Server – HIS Production
ช่องโหว่ที่พบ (Vulnerability): CVE-2024-12345 – Apache Path Traversal
แนวทางการแก้ไขช่องโหว่ (Remediation Plan): อัปเดต Apache และปิด Directory Listing
ระดับความเสี่ยง (Risk Level): High (CVSS 8.6)
แผนการแก้ไข (Treatment Plan):

- **แนวทาง:** ติดตั้ง patch, ปรับ permission
- **กำหนดเวลาแล้วเสร็จ:** ภายใน 7 วัน

เจ้าของความเสี่ยง (Risk Owner): หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

◆ **๕. การบันทึกความเสี่ยงจากการจัดการ (Management-Based Risk Record) (๒๓๒–๒๓๓)**

Risk ID: RSK-2024-00221
ความเสี่ยง (Identified Risk): ขาดเจ้าหน้าที่เวรกลางคืน
ผลกระทบ (Impact): การตอบสนองต่อเหตุขัดข้องล่าช้า
โอกาสเกิด (Likelihood): 4 / **ผลกระทบเฉลี่ย:** 3
ระดับความเสี่ยง (Calculated Risk Score): 12 (High)
แผนจัดการความเสี่ยง (Risk Treatment):

- **กลยุทธ์:** ลดความเสี่ยง
- **แนวทาง:** จัดเวรชดเชย
- **ระดับความเสี่ยงคงเหลือ (Residual Risk):** ปานกลาง
- **ระยะเวลาดำเนินการ:** ไตรมาส 4/2567

เจ้าของความเสี่ยง (Risk Owner): หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

◆ **๖. การบันทึกการเปลี่ยนแปลง (Change Record) (๒๒๔)**

Change ID: CHG-2024-00012
ข้อมูลการเปลี่ยนแปลง (What Changed): ติดตั้ง Critical Patch CVE-2024-12345
ระดับความรุนแรง (Change Impact Level): High – มี downtime
แผนกู้คืน (Rollback Plan): Snapshot VM + Backup ก่อนเปลี่ยน
รายละเอียดขั้นตอน (Steps for Major Change): ทดสอบบน staging, ติดตั้งบน production
ระยะเวลาดำเนินการ (Scheduled Time): 15 ต.ค. 2567, 21:00–21:15

◆ **๗. การบันทึกประเด็นตรวจสอบ (Audit Issue Record) (๒๒๕)**

Audit Issue ID: AUD-2024-0032
ประเด็นความไม่สอดคล้อง (Nonconformity): ไม่มีเอกสารประกอบการตั้งค่า Firewall
ข้อกำหนดที่เกี่ยวข้อง (Related Requirement): ISMS-PR ข้อ 4.4.8 / Annex A.5.15

ข้อเสนอแนะ (Recommendation): จัดทำเอกสาร config และควบคุมตามขั้นตอน

🔸 **๘. การดำเนินการแก้ไขประเด็นตรวจสอบ (Corrective Action Record) (๒๒๖)**

แนวทางแก้ไขเบื้องต้น (Initial Action): สำรวจ config ปัจจุบัน
แนวทางแก้ไขสาเหตุ (Root Cause Fix): จัดทำ SOP และควบคุมเวอร์ชันเอกสาร
สาเหตุของความไม่สอดคล้อง (Cause): ไม่มีการบังคับใช้ระบบ Document Control
กำหนดเวลาแล้วเสร็จ (Due Date): ภายใน 30 กันยายน 2567

🔸 **๙. การบันทึกตัวชี้วัดประสิทธิภาพ (KPI Record) (๒๒๗–๒๒๘)**

KPI ID: KPI-2024-0002
ตัวชี้วัด (KPI Name): ความพร้อมใช้งานของระบบ Data Center
ค่าเป้าหมาย (Target): 99.95% ต่อปี
ผู้รับผิดชอบ (Assignee): หัวหน้าทีมระบบเครือข่าย
ความถี่รายงานผล (Frequency): รายเดือน (ส่งก่อนวันที่ 5)
แหล่งข้อมูล (Data Source): Zabbix, Service Desk report
ค่าที่วัดได้ล่าสุด (Latest Result): 99.98% (มิ.ย. 2567)

🔸 **๑๐. การบันทึกเหตุการณ์เชื่อมโยง Incident ⟶ Problem ⟶ Change ⟶ KPI (Incident Chain Record) (๒๒๐–๒๒๔, ๒๒๗)**

Incident ID: INC-2025-00012
วันที่/เวลา: 18 มกราคม 2568, 07:30–08:10 น.
รายละเอียดเหตุเสีย (Incident Detail): ระบบ SSO Authentication ล่ม ทำให้ไม่สามารถล็อกอินเข้าใช้ระบบต่าง ๆ ได้
ระดับความรุนแรง (Severity Level): High – ส่งผลต่อหลายระบบวิกฤต
แนวทางการแก้ไขปัญหา (Solution/Workaround): รีสตาร์ท SSO Gateway
สาเหตุของอุบัติการณ์ (Root Cause): log เต็มที่ /var/log ทำให้ session timeout
หมายเลขปัญหาคงค้าง (Linked Problem ID): PRB-2025-00009
หมายเลขการเปลี่ยนแปลง (Linked Change ID): CHG-2025-00007
หมายเลขตัวชี้วัด (Linked KPI ID): KPI-2025-00001

🔸 **๑๑. การบันทึกย้อนหลัง และการตรวจสอบ (Late Change & Audit Record) (๒๒๕–๒๒๖)**

Audit Issue ID: AUD-2025-0011
ประเด็นความไม่สอดคล้อง (Nonconformity): มีการติดตั้ง FortiClient VPN รุ่นใหม่ในเดือนพฤศจิกายน โดยไม่ได้เปิด Change Request ล่วงหน้า
ข้อกำหนดที่เกี่ยวข้อง (Related Requirement): ISMS-PR ข้อ 4.4.10 / Annex A.8.32
ข้อเสนอแนะ (Recommendation): ต้องจัดทำบันทึก Change Calendar ล่วงหน้าสำหรับงานประจำ
แนวทางแก้ไขเบื้องต้น (Initial Action): บันทึกการเปลี่ยนแปลงย้อนหลัง พร้อมระบุสาเหตุ
แนวทางแก้ไขสาเหตุ (Root Cause Fix): จัดระบบสื่อสารล่วงหน้าในกรณีเจ้าหน้าที่ลาหยุดยาว พร้อมจัดทำแบบฟอร์ม Job Delegation
สาเหตุของความไม่สอดคล้อง (Cause): เจ้าหน้าที่หลักลาหยุดโดยไม่มีผู้แทน
กำหนดเวลาแล้วเสร็จ (Due Date): 31 มีนาคม 2568

🔸 **๑๒. การบันทึกความเสี่ยงด้านบุคลากร (Management-Based Risk Record) (๒๓๒–๒๓๓)**

Risk ID: RSK-2025-00045
ความเสี่ยง (Identified Risk): เจ้าหน้าที่ Technical Support 2 คนจะสิ้นสุดสัญญาจ้างปลายไตรมาส 2
ผลกระทบ (Impact): ความล่าช้าในการ deploy ระบบใหม่ และการตอบสนองเหตุขัดข้อง
โอกาสเกิด (Likelihood): 5 / **ผลกระทบเฉลี่ย:** 3
ระดับความเสี่ยง (Calculated Risk Score): 15 (High)
แผนจัดการความเสี่ยง (Risk Treatment):

- **กลยุทธ์:** ลดความเสี่ยง
- **แนวทาง:** ดำเนินการสรรหาบุคลากรล่วงหน้า พร้อมฝึกอบรมข้อนตำแหน่ง
- **ระดับความเสี่ยงคงเหลือ (Residual Risk):** Low
- **ระยะเวลาดำเนินการ:** ภายใน 15 เมษายน 2568

เจ้าของความเสี่ยง (Risk Owner): หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

🔸 **๑๓. การบันทึกความเสี่ยงจากทรัพย์สิน – ความเสี่ยงทางกายภาพ (Asset-Based Risk Record – Physical) (๒๓๐–๒๓๑)**

Risk ID: RSK-2025-00051
ทรัพย์สินสารสนเทศ (Information Asset): UPS ชั้น 2 ห้อง Data Center
ช่องโหว่ที่พบ (Vulnerability): ไม่มีระบบแจ้งเตือนเมื่อ Battery เสื่อม
แนวทางการแก้ไขช่องโหว่ (Remediation Plan): ติดตั้งอุปกรณ์ Remote Monitoring Module
ระดับความเสี่ยง (Risk Level): High
แผนการแก้ไข (Treatment Plan):

- **แนวทาง:** ประสานจัดซื้ออุปกรณ์เสริม และเชื่อมต่อระบบตรวจสอบศูนย์
- **กำหนดเวลาแล้วเสร็จ:** ภายในเดือนมีนาคม 2568

หมายเลขการเปลี่ยนแปลง (Linked Change ID): CHG-2025-00010
เจ้าของความเสี่ยง (Risk Owner): หัวหน้าทีมระบบไฟฟ้าและอุปกรณ์สำรองไฟ

แนวปฏิบัติ Threat Intelligence

Threat Intelligence Procedure

แนวปฏิบัตินี้มีขึ้นเพื่อให้มีการบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์อย่างเป็นระบบ โดยดำเนินการรวบรวม วิเคราะห์ ประเมิน และเผยแพร่ข้อมูลเชิงลึกด้านภัยคุกคาม (Threat Intelligence) เพื่อใช้ในการบริหารจัดการความเสี่ยง การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพและทันเวลา โดยสอดคล้องตามมาตรฐาน ISO/IEC 27001:2022 ข้อ 6.1 (การดำเนินการกับความเสี่ยงและโอกาส), ข้อ 8.2 (การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ), ข้อ 8.3 (การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ), และ Control A.5.7 (Threat Intelligence) รวมถึงกรอบปฏิบัติที่ได้รับการยอมรับในระดับสากล ทั้งนี้ ให้ฝ่ายเทคโนโลยีสารสนเทศมอบหมายผู้รับผิดชอบที่ชัดเจนในแต่ละกิจกรรม (ผู้รวบรวม ผู้วิเคราะห์ และผู้อนุมัติรายงาน) เพื่อให้สามารถติดตามและตรวจสอบการปฏิบัติได้

๒๓๕. จัดให้มีการรวบรวมข้อมูลภัยคุกคามจากแหล่งข้อมูลที่เชื่อถือได้ โดยระบุระดับความน่าเชื่อถือ (Reliability) และความเกี่ยวข้อง (Relevance) ของข้อมูลที่นำมาใช้ประกอบการวิเคราะห์ภัยคุกคาม เพื่อให้สามารถระบุและจัดลำดับความสำคัญของภัยคุกคามได้อย่างเหมาะสมและทันเวลา ทั้งนี้ ควรพัฒนา

ไปสู่การรับข้อมูลแบบอัตโนมัติผ่านมาตรฐาน STIX/TAXII หรือ Threat Intelligence Feed เพื่อลดการพึ่งพาการดำเนินการด้วยตนเองและรองรับการขยายตัวในระยะยาว

๒๓๖. จัดให้มีการวิเคราะห์ภัยคุกคามเชิงลึกในมิติทางเทคนิคและกลยุทธ์ (Technical & Strategic Analysis) จากแหล่งข้อมูลที่มีความเชี่ยวชาญเฉพาะทาง โดยการวิเคราะห์นั้นต้องเชื่อมโยงกับ Tactics, Techniques, and Procedures (TTPs) ของ MITRE ATT&CK Framework หรือกรอบมาตรฐานอื่น ๆ ที่เป็นที่ยอมรับ เพื่อให้สามารถระบุลักษณะเฉพาะของภัยคุกคามที่อาจส่งผลกระทบต่อองค์กรได้อย่างชัดเจน

๒๓๗. จัดทำรายงานสรุปภัยคุกคาม (Threat Intelligence Report) เป็นประจำทุกเดือน โดยในรายงานต้องระบุประเภทภัยคุกคาม แนวโน้มภัยคุกคามที่สำคัญ รายละเอียดของเทคนิคการโจมตีที่พบเป็นประจำ (Common Techniques) ตัวอย่างเหตุการณ์จริงที่เกี่ยวข้อง (Incident Case Study) รวมถึงข้อเสนอแนะในการป้องกันและรับมือภัยคุกคามอย่างชัดเจน เพื่อสนับสนุนการตัดสินใจของผู้บริหารและผู้รับผิดชอบงานด้านความมั่นคงปลอดภัยสารสนเทศ

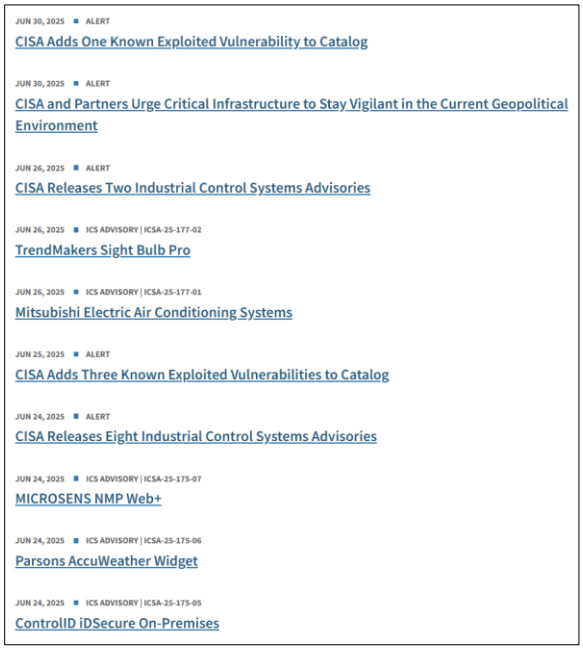
๒๓๘. จัดให้มีการเชื่อมโยงข้อมูลภัยคุกคาม (Threat Intelligence) กับกระบวนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident Response Process) เพื่อให้การนำข้อมูลภัยคุกคามไปใช้ในการตรวจจับ ตอบสนองและฟื้นฟูระบบสามารถดำเนินการได้อย่างมีประสิทธิภาพ รวมถึงนำตัวบ่งชี้การโจมตี (Indicators of Compromise: IOC) ที่ได้รับการตรวจสอบแล้วไปกำหนดค่าในอุปกรณ์ป้องกัน เช่น Firewall, IPS/IDS และ EDR เพื่อปิดกั้นภัยคุกคามเชิงรุกโดยอัตโนมัติเท่าที่เป็นไปได้

๒๓๙. จัดให้มีการติดตามและวัดประสิทธิภาพของกระบวนการ Threat Intelligence อย่างสม่ำเสมอ โดยการกำหนดตัวชี้วัดที่ชัดเจน เช่น ความรวดเร็วในการตรวจจับภัยคุกคาม (Time to Detection), จำนวนภัยคุกคามที่สามารถตรวจจับและป้องกันได้ (Detection & Prevention Rate) โดยกำหนดค่าฐาน (Baseline) และค่าเป้าหมาย (Target/Threshold) ของแต่ละตัวชี้วัดให้ชัดเจน รวมถึงการประเมินคุณภาพของข้อมูลภัยคุกคามที่ถูกนำมาใช้งาน เพื่อปรับปรุงกระบวนการให้มีประสิทธิภาพอย่างต่อเนื่อง

๒๔๐. จัดให้มีการฝึกอบรมและพัฒนาทักษะด้าน Threat Intelligence ให้แก่บุคลากรที่เกี่ยวข้องอย่างต่อเนื่อง เพื่อให้มีขีดความสามารถที่เหมาะสมกับบทบาทหน้าที่ในการรวบรวม วิเคราะห์ และดำเนินการกับข้อมูลภัยคุกคามได้อย่างมีประสิทธิภาพ

๒๔๑. จัดให้มีการบริหารจัดการข้อมูลภัยคุกคามอย่างเป็นระบบ และมีการควบคุมการเข้าถึงข้อมูลภัยคุกคามตามระดับชั้นข้อมูล (Data Classification) เพื่อรักษาความมั่นคงปลอดภัย และป้องกันไม่ให้ข้อมูลภัยคุกคามที่มีความสำคัญรั่วไหลสู่ผู้ไม่ได้รับอนุญาต

๒๔๒. จัดให้มีการรวบรวมและตรวจสอบข้อมูลภัยคุกคาม (Threat Intelligence) จากแหล่ง Cybersecurity Alerts & Advisories (เช่น ThaiCERT , CISA หรือแหล่งอื่นตามที่หน่วยงานกำหนด) โดยดำเนินการอย่างสม่ำเสมอเป็นรายสัปดาห์ พร้อมทั้งวิเคราะห์ข้อมูลที่เกี่ยวข้องกับระบบหรือบริการภายใน และหากพบประเด็นที่มีความเสี่ยงหรือมีแนวโน้มส่งผลกระทบ ให้รายงานต่อหัวหน้าฝ่ายเทคโนโลยีสารสนเทศโดยเร็ว เพื่อพิจารณาดำเนินการแก้ไขหรือป้องกันเชิงรุก


JUN 30, 2025 ■ ALERT
CISA Adds One Known Exploited Vulnerability to Catalog

JUN 30, 2025 ■ ALERT
CISA and Partners Urge Critical Infrastructure to Stay Vigilant in the Current Geopolitical Environment

JUN 26, 2025 ■ ALERT
CISA Releases Two Industrial Control Systems Advisories

JUN 26, 2025 ■ ICS ADVISORY | ICSA-25-177-02
TrendMakers Sight Bulb Pro

JUN 26, 2025 ■ ICS ADVISORY | ICSA-25-177-01
Mitsubishi Electric Air Conditioning Systems

JUN 25, 2025 ■ ALERT
CISA Adds Three Known Exploited Vulnerabilities to Catalog

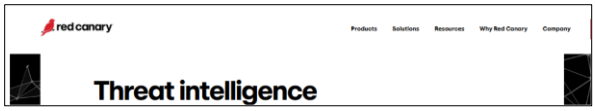
JUN 24, 2025 ■ ALERT
CISA Releases Eight Industrial Control Systems Advisories

JUN 24, 2025 ■ ICS ADVISORY | ICSA-25-175-07
MICROSENS NMP Web+

JUN 24, 2025 ■ ICS ADVISORY | ICSA-25-175-06
Parsons AccuWeather Widget

JUN 24, 2025 ■ ICS ADVISORY | ICSA-25-175-05
ControlID iDSecure On-Premises

๒๔๓. จัดให้มีการติดตามและสรุปข้อมูลภัยคุกคามจาก Red Canary Threat Detection Report หรือแหล่งข้อมูลเชิงลึกด้านภัยคุกคาม (เช่น Unit 42, MITRE ATT&CK, Microsoft Threat Intelligence) โดยสรุปผลการวิเคราะห์แนวโน้มไว้ในรายงานสรุปภัยคุกคามรายเดือนฉบับเดียวกับข้อ ๒๓๗ เพื่อหลีกเลี่ยงการจัดทำรายงานซ้ำซ้อน และเพื่อส่งเสริมความเข้าใจในภัยคุกคามเชิงลึก และเสนอแนะแนวทางรับมือให้กับทีมบริหารจัดการระบบที่เกี่ยวข้อง



แหล่งข้อมูลเชิงลึกด้านภัยคุกคาม

1. Red Canary – Threat Detection Report

รายงานภัยคุกคามประจำปีที่จัดอันดับเทคนิค MITRE ATT&CK ที่พบมากที่สุด

2. Unit 42 – Threat Research (Palo Alto Networks)

รายงานภัยคุกคามลึกระดับแคมเปญ เช่น ransomware, malware families, APT

3. MITRE ATT&CK - Threat Intelligence

ฐานข้อมูลพฤติกรรมการโจมตีที่ใช้โดย Threat Intelligence และ SOC ทั่วโลก

4. Microsoft Security Blog – Threat intelligence

หน้าแท็บ "Threat intelligence" ในบล็อกความปลอดภัยของ Microsoft

๒๔๔. จัดให้มีการตรวจสอบบันทึกไฟล์จากระบบ SIEM โดยใช้เครื่องมือตรวจสอบ IOC ที่ได้รับอนุมัติ (ดูรายการในเอกสารวิธีปฏิบัติงาน Work Instruction) เช่น https://www.threatstop.com/check-ioc และสรุปผลไว้ในรายงานเฝ้าระวังภัยคุกคามรายสัปดาห์ฉบับเดียวกับข้อ ๒๔๒