คู่มือการจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศ



ฉบับทบทวน ๒๕๖๙

สารบัญ

หน้า

๑. ความหมายและความสำคัญของการจัดการความเสี่ยง ๓

๒. ความเสี่ยงหลักด้านระบบเทคโนโลยีสารสนเทศ ๔

๓. แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ๕

๔. กระบวนการบริหารความเสี่ยง (Risk Treatment Plan) ๑๖

๕. วิธีการจัดการความเสี่ยง (Risk treatment) ๒๑

๖. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting) ๒๑

๗. การรายงานความเสี่ยงตกค้าง (Residual risk reporting) ๒๒

๘. บทสรุป ๒๓

ภาคผนวก ๒๔

เกณฑ์การประเมินความสำคัญของระบบสารสนเทศ ๒๔

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑. ความหมายและความสำคัญของการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน ซึ่งมีโอกาสที่จะเกิดขึ้นในอนาคต และมีผลกระทบ ทั้งทางบวกและทางลบ หากเป็นทางลบจะก่อให้เกิดความผิดพลาดความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ทำให้การดำเนินงานขององค์กรไม่ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ตามขั้นตอนการดำเนินงานที่กำหนดไว้ ปัจจัยภายในองค์กร (Internal Factors) เช่น ความไม่พร้อมของโครงสร้างพื้นฐานดิจิทัล, ข้อผิดพลาดของกระบวนการทำงาน (Process Failure), พฤติกรรมและข้อจำกัดด้านทักษะของบุคลากร (Human Behavior & Competency), ช่องโหว่ของการตั้งค่าระบบ (Misconfiguration) และการขาดระบบการควบคุมภายในที่รัดกุม ปัจจัยภายนอกองค์กร (External Factors): ภัยคุกคามทางไซเบอร์และการโจมตีของแฮกเกอร์ (Cyber Attacks), ภัยธรรมชาติและอุบัติภัย (Natural & Environmental Disasters), ภาวะเศรษฐกิจ, การพึ่งพาผู้ให้บริการภายนอก (Third-Party / Supply Chain Risk) ตลอดจน ความเสี่ยงด้านการไม่ปฏิบัติตามกฎหมายและกฎระเบียบ (Compliance Risk) เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ และกฎหมายดิจิทัลภาครัฐที่เกี่ยวข้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึงสถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Risk Management) หมายถึง กระบวนการเชิงยุทธศาสตร์และการปฏิบัติการตามมาตรฐานสากล ISO/IEC 27005, ISO 31000 และ COBIT 2019 ในการระบุ วิเคราะห์ ประเมินค่า จัดการ ควบคุม เฝ้าระวัง และรายงานความเสี่ยงให้อยู่ใน ระดับความเสี่ยงที่องค์กรยอมรับได้ (IT Risk Appetite) ภายใต้กลยุทธ์การตอบสนอง ๔ แนวทาง (4Ts: Take-ยอมรับ, Treat-ลด/ควบคุม, Terminate-หลีกเลี่ยง, Transfer-โอนย้ายความเสี่ยง) เพื่อปกป้องทรัพย์สินดิจิทัลและสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสียทุกภาคส่วน

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง โดยทำตามแนวทางการตอบสนองต่อความเสี่ยงที่วางไว้ ประกอบด้วยกิจกรรมการควบคุมเกิดขึ้นในทุกระดับ ทุกหน้าที่งานและทั่วทั้งองค์กร และทำให้การดำเนินงานบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ค้นพบ การควบคุมแบบส่งเสริม และการควบคุมแบบแก้ไข

๒. ความเสี่ยงหลักด้านระบบเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ กระบวนการการทำงานที่ช่วยให้ IT Managers ขององค์กรสามารถดำเนินธุรกิจให้บรรลุผลสำเร็จของพันธกิจ และปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

๒.๑ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ (Access Risk) โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานมิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิ์ในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมิได้มีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

๒.๒ ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องหรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

๒.๓ ความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ (Availability Risk) ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้หากหน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

๒.๔ ความเสี่ยงเกี่ยวกับการที่หน่วยงานมิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี (Infrastructure Risk) รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้ อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินงาน และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

๓. แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศขององค์กรสามารถแบ่งออกเป็น ๖ ประเภท ดังนี้

๓.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติและสิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย (Server Room) เป็นต้น

การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม มีประเด็นหลัก ดังนี้

๑) ตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารหลัก การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่าง ๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น เครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย ถังดับเพลิง เป็นต้น

๒) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) ของห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของสำนักงานจำเป็นต้องมีการควบคุม เข้าได้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ในกรณีที่มีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำมีอำนาจ มีความจำเป็นต้องเข้าห้องคอมพิวเตอร์แม่ข่ายในบางครั้ง จำเป็นต้องมีการควบคุมอย่างรัดกุมและรอบคอบ เช่น การแจ้งให้เจ้าหน้าที่เทคโนโลยีสารสนเทศทราบก่อนทุกครั้ง และต้องเซ็นชื่อในสมุดบันทึกเข้าออกห้องสื่อสารทุกครั้ง เป็นต้น

๓) การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม จัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลากรณีฉุกเฉินเพื่อใช้ในการดับเพลิงเบื้องต้น

๔) การป้องกันความเสี่ยงจากระบบป้องกันไฟฟ้าลัดวงจร ทำได้โดยมีระบบป้องกันไฟฟ้ากระชากไม่ให้คอมพิวเตอร์แม่ข่ายให้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า อุปกรณ์ป้องกันไฟ จัดให้ระบบไฟฟ้าสำรองสำหรับคอมพิวเตอร์ทั้งแม่ข่ายและลูกข่าย เพื่อให้การดำเนินงานมีความต่อเนื่องกรณีกระแสไฟฟ้าดับหรือเกิดขัดข้องไม่สามารถใช้งานได้

๕) ความเสี่ยงในเรื่องของงบประมาณที่จะดำเนินการอย่างได้ประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง

๖) ความเสี่ยงในเรื่องของประเด็นนโยบายผู้บริหาร ซึ่งแนวนโยบายและวิสัยทัศน์ของแต่ละยุคสมัยเปลี่ยนแปลงไป อันส่งผลมายังแนวทางในการดำเนินงาน

๓.๒ ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงการวางแผนการตรวจสอบการทำงานการมอบหมายหน้าที่และสิทธิ์ของบุคลากร / คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน

การบริหารความเสี่ยงด้านบุคลากร มีประเด็นหลัก ดังนี้

๑) กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการด้านบุคลากร การแต่งตั้งเจ้าหน้าที่ที่มีความเหมาะสม การกำหนดโครงสร้าง การแบ่งแยกอำนาจหน้าที่ การกำหนดนโยบายและขั้นตอนการปฏิบัติงานและกำกับดูแลควบคุมการปฏิบัติงานเป็นหลัก

๒) การว่าจ้าง / จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการด้านระบบเทคโนโลยีสารสนเทศ เพราะเป็นผู้มีความรู้ ความชำนาญเฉพาะทาง มีเครื่องมือและเทคโนโลยีที่ใช้พร้อมและทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศเฉพาะด้านมากกว่าภาคราชการ โดยการว่าจ้างบุคลากรภายนอกนี้ก็จะมีความเสี่ยงในเรื่องของ ความรู้ความเข้าใจในระบบราชการ และผลสัมฤทธิ์ที่เกิดจากการทำงาน อีกทั้งในแง่ของความคุ้มค่าของการใช้จ่ายงบประมาณ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงของการว่าจ้างบุคลากรภายนอกนี้ ทำได้โดยหน่วยงานที่เป็นเจ้าของเรื่อง หรือเป็นผู้รับผิดชอบในประเด็นต่าง ๆ ต้องเป็นผู้เข้ามากำกับดูแลตั้งแต่เริ่มกระบวนการ และต่อเนื่อง โดยหลักการบริหารจัดการที่ดี อีกทั้งรักษาผลประโยชน์ของทางราชการให้มากที่สุด

๓) บุคลากรของภาคราชการ ขาดความรู้ความเข้าใจเรื่องของระบบเทคโนโลยีสารสนเทศโดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรม และนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะประสานงานและรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงในประเด็นนี้ โดยการส่งเจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศ รวมถึงการรับบุคลากรที่มีความรู้ ความเข้าใจด้านระบบเทคโนโลยีสารสนเทศมาปฏิบัติงานมากยิ่งขึ้น

๔) แผนการบริหารความเสี่ยงด้านบุคลากร คือ ต้องมีการฝึกอบรมในด้านที่เกี่ยวข้องกับระบบ ใน ๓ ระดับ คือ ระดับผู้บริหาร (CIO) ระดับผู้ดูแลระบบ (Administrator) และใช้งานทั่วไป (User) ทำให้บุคลากรของหน่วยงานสามารถใช้งานวางแผนงานระบบสารสนเทศ ดูแล ปรับปรุง และพัฒนาระบบได้ เป็นการสนับสนุนบุคลากรทางคอมพิวเตอร์ รวมทั้งผู้ใช้งานให้มีความรู้ด้านการรักษาความปลอดภัยระบบ ได้อย่างมีประสิทธิภาพ

๓.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ ไม่ว่าจะเป็นความเสี่ยงที่เกิดจากทำงานผิดพลาดของอุปกรณ์ ช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ ไวรัสคอมพิวเตอร์ เป็นต้น

การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ มีประเด็นหลัก ดังนี้

๑) ความเสี่ยงในเรื่องของจัดหาอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมกับแผนงาน / โครงการ และองค์กร ซึ่งควรให้มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมตามลักษณะของโครงการ และงบประมาณ

๒) ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Support) โดยมีข้อควรปฏิบัติ ได้แก่

- มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และการดูแลอย่างถูกต้องและต่อเนื่อง
- ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว
- การใช้อุปกรณ์ต่อพ่วง เช่น Flash Drive ควรตรวจสอบไวรัสก่อนทุกครั้ง
- ควรปัดฝุ่นหรือทำความสะอาดเครื่องคอมพิวเตอร์อยู่เสมอ เพราะเมื่อมีฝุ่นเข้าสู่เครื่องคอมพิวเตอร์มาก ๆ จะทำให้เครื่องคอมพิวเตอร์ร้อนจัดได้ง่าย เป็นสาเหตุของอาการเครื่องค้างหรือรวนได้
- ระบบปฏิบัติการ Windows ควรทำการ Update เป็นประจำ
- การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ
- การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงานเกี่ยวกับการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ เช่น การกำหนดรหัสผู้ใช้ และการใช้รหัสผ่าน
- การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ
- การสำรองข้อมูล (Backup) ข้อมูลระบบสารสนเทศ
- การบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ได้แก่ ระบบปฏิบัติการคอมพิวเตอร์ ระบบเครือข่าย และการใช้งานและประสิทธิผลของเครื่องคอมพิวเตอร์อุปกรณ์เทคโนโลยีสารสนเทศ
- กำหนดขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที
- ทำการทดสอบ Software เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ
- กำหนดบุคคลรับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนค่า Parameter ต่าง ๆ ของระบบคอมพิวเตอร์แม่ข่ายอย่างชัดเจน

๓.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่าง ๆ ที่ได้จัดทำและพัฒนาขึ้นสำหรับโครงการด้านเทคโนโลยีสารสนเทศ รวมถึงโปรแกรมประยุกต์อื่น ๆ ที่ใช้ประกอบการใช้โปรแกรมและระบบงาน ตัวอย่างเช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่ง และการถูกไม่หวังดีทำลายระบบ (Hacker) เป็นต้น

การบริหารจัดการความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ มีประเด็นหลัก ดังนี้

๑) มีการพัฒนามาตรฐานและการบริการโปรแกรมคอมพิวเตอร์พัฒนาและปรับปรุงมาตรฐาน Hardware Software, Peopleware Data และNetwork ให้เป็นฐานข้อมูลกลางของงานเทคโนโลยีสารสนเทศ และเป็นไปในทิศทางเดียวกัน

๒) พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลให้มีมาตรฐานและแบ่งสรรการให้ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้

๓.๕ ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่าง ๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่าง ๆ

การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีประเด็นหลัก ดังนี้

๑) ความเสียหายที่เกิดขึ้นจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่ายและการจัดทำระบบการกำหนดสิทธิ์ในการเข้าถึงระบบเครือข่าย ได้มีระบบการติดตามและเฝ้าดูแลการใช้เครือข่ายภายในและการเข้าออก Internet ทุกวัน รวมทั้งการสร้าง Firewall เพื่อป้องกันการเข้าถึงและการโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูลระบบ Web Server เป็นต้น

๒) เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ภายในให้มีความเสถียรและมีประสิทธิภาพรองรับกับปริมาณข้อมูล และการเคลื่อนไหวของฐานข้อมูล

๓) มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (Integrity risk) ข้อมูล หรือการทำงานของระบบเครือข่ายที่จะมีผลถึงระบบเครือข่ายที่จะมีผลถึงระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสี่ยง (availability risk) แก้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

๔) กำหนดมาตรการรักษาความปลอดภัยข้อมูล เช่น กรณีนำเครื่องคอมพิวเตอร์ส่งซ่อม

๕) กำหนดชั้นความสำคัญในการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงการเข้าถึงข้อมูลผ่านเครือข่ายในการรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล

๖) การควบคุมการกำหนดสิทธิ์ให้แก่ผู้ใช้งาน (User Privilege) เช่น สิทธิ์ในการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ให้แก่ ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ

๗) กำหนดระยะเวลาการใช้งานของ User พร้อม Password และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๘) กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบ และมีความลับ

๙) ในการที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่นให้มีสิทธิ์ในการใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่าง ๆ ต้องมีการอนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นรวมถึงกำหนดระยะเวลาในการใช้งาน

๑๐) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด หรือทันทีเมื่อสงสัยว่ารหัสผ่านถูกเปิดเผย
- ผู้ใช้งานต้องกำหนดรหัสผ่านด้วยความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษ
- ไม่กำหนดรหัสผ่านมาจากสิ่งที่สื่อถึงตัวผู้ใช้งาน เช่น ชื่อ นามสกุล วันเกิด เบอร์โทรศัพท์ หรือบุคคลในครอบครัว หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- ไม่จดรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น เช่น กระดาษโน้ตแปะติดหน้าจอคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่เข้าใช้งาน
- หลีกเลี่ยงการใช้รหัสผ่านเดิมเมื่อเปลี่ยนรหัสผ่านใหม่ (ระบบจะไม่อนุญาตให้ใช้รหัสผ่านซ้ำกับรหัสผ่านเดิมที่เคยใช้ไปแล้ว)
- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๓ เดือน หรือ ๙๐ วัน

๑๑) กำหนดแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายในส่วนเครือข่ายภายนอก

๑๒) ติดตั้งระบบป้องกันการบุกรุก เช่น Firewall ระหว่างเครือข่ายในกับเครือข่ายนอก โดยการติดตั้งผ่านอุปกรณ์คอมพิวเตอร์ ติดตั้งระบบป้องกันการบุกรุกในระบบเครือข่ายด้วยซอฟต์แวร์และฮาร์ดแวร์ที่ดูแลระบบจะติดตั้งและกำหนดรูปแบบการอนุญาตให้เข้าใช้เครือข่ายอินเทอร์เน็ต

๑๓) จัดทำแผนผังระบบเครือข่าย / แผนผังการเชื่อมโยงระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งในและภายนอกและอุปกรณ์ให้เป็นปัจจุบันอยู่เสมอ

๑๔) ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส เป็นต้น

๑๕) กำหนดบุคคลผู้รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของอุปกรณ์เครือข่าย

๑๖) กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น การปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่งคือ ผู้ใช้งานในระบบจะต้องคอยดูแล และป้องกันไม่ให้ตนเองเป็นช่องทาง ผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตามและหากหาวิธีการป้องกัน และแก้ไขจุดบกพร่องของซอฟต์แวร์ที่ใช้งาน เพราะไม่มีระบบเครือข่ายใดที่ปลอดภัยสมบูรณ์แบบ ดังนั้นต้องมีระบบป้องกันที่ดีโดยมีวิธีการ ดังนี้

- ติดตั้งโปรแกรมกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
- มีระบบสำรองข้อมูลอัตโนมัติแบบ Immutable Backup / Cloud
- อัพเดทข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดท
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ
- กำหนดให้ระบบอัปเดต Signature/Agent และสแกนระบบอัตโนมัติ (Full Scan สัปดาห์ละ ๑ ครั้ง และสแกนแบบ Real-time ตลอดเวลา)

๑๗) การป้องกันจากการเปิดไฟล์จากบันทึกข้อมูลก่อนใช้งานทุกครั้ง

- แผ่น CD เทปต่าง ๆ, USB Flash Drive, External HDD/SSD, SD Card
- บังคับใช้ระบบ Endpoint DLP และสแกนไวรัสทันทีที่เชื่อมต่อ
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลก ๆ ที่น่าสงสัย เช่น .pif , .scr, .vbs, .bat, .iso, .xlsm, .zip[cite: 1] เป็นต้น
- ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

๑๘) การป้องกันจากการเปิด E-Mail

- อย่าเปิดไฟล์ E-Mail จากผู้ส่งที่ไม่รู้จัก และไม่ทราบที่มา
- อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ

- ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทั้งทันที หรือ กดปุ่ม "Report Phishing" แจ้งไอที และห้ามกรอกรหัสผ่านใดๆ

- อัพเดทโปรแกรม E-Mail สม่ำเสมอ

๑๙) การป้องกันจาการดาวน์โหลดจาก Internet

- ระวังลิงก์และไฟล์แนบจาก Line, Teams, Zoom, Chat ต่างๆ เปิดให้เฉพาะลิงก์หรือไฟล์แนบที่ได้มาจากเจ้าหน้าที่หรือวิทยากร เท่านั้น

- ไม่ควรเข้า Website ที่มากับ E-Mail

- ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่น่าเชื่อถือ

- ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลด้านความปลอดภัยเสมอ

- หลีกเลี่ยงการแชร์ไฟล์ไม่จำเป็น

- หลีกเลี่ยงการแชร์ไฟล์ประเภท Peer to Peer

- ห้ามใช้โปรแกรม BitTorrent และห้ามโหลดลง Cloud ส่วนตัว

- แชร์ไฟล์ข้อมูลผ่านระบบ Cloud Drive / SharePoint ขององค์กร

๓.๖ ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุก การโจรกรรมข้อมูลสำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล

การบริหารจัดการความเสี่ยงด้านข้อมูล มีประเด็นหลัก ดังนี้

๑) ฐานข้อมูล มีความเสี่ยงกับการเข้าถึงข้อมูล (Access Risk) และระบบคอมพิวเตอร์ในส่วน ที่เกี่ยวข้องหรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งทางหน่วยงานไม่มีวิธีการจัดการและควบคุมความเสี่ยง (Access Risk) ที่รอบคอบและรัดกุมอาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับข้อมูลและนำข้อมูลไปใช้ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ก็อาจถูกแก้ไขเปลี่ยนแปลงได้

๒) ฐานข้อมูล มีความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) และการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่ ที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access Risk) ซึ่งส่งผลให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์อาจถูกแก้ไขเปลี่ยนแปลงได้ หรือสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ

๓) ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้สำรองข้อมูลและระบบงานคอมพิวเตอร์และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน

นอกจากนี้หากไม่มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่รัดกุมเพียงพอแล้ว (Access Risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์เสียหายได้

๔) ฐานข้อมูล มีความเสี่ยงกับการที่หน่วยงานไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี (Infrastructure Risk) รวมทั้งไม่ได้จัดให้มีระบบคอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการทำงานของหน่วยงาน รวมถึงไม่มีการจัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่าง ๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานสำคัญทุกด้าน และการจัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรู้และความเชี่ยวชาญในงานที่รับผิดชอบสำหรับการควบคุมการปฏิบัติงาน

๕) ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back up) ที่สำคัญของศูนย์เทคโนโลยีสารสนเทศ นั้น เพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติ ในการบริหารจัดการ ในการเก็บข้อมูล (Back up) การกู้คืนข้อมูล (Recovery) ตลอดจนสถานที่จัดเก็บข้อมูลที่เหมาะสมและปลอดภัย ดังนั้นการสำรองข้อมูลและการเตรียมข้อมูลให้พร้อมกรณีฉุกเฉินจึงมีวัตถุประสงค์เพื่อให้ข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและในเวลาที่ต้องการ (Availability Risk) โดยที่เนื้อหาครอบคลุมเกี่ยวข้องกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

- การกำหนดการสำรองข้อมูล (Back up)
- การทดสอบ กำหนดทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบได้ว่าข้อมูลรวมทั้งโปรแกรมต่าง ๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้การเก็บรักษาที่เจ้าหน้าที่จัดเก็บข้อมูลโดยตรง และมีการจัดเก็บข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัย และติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง
- การกู้คืนข้อมูลสู่ระบบ มีกำหนดบุคลากรผู้ได้รับสิทธิ์กู้คืนข้อมูลที่ได้ทำการสำรองไว้โดย Login ผ่าน Username & Password ที่กำหนดไว้

๓.๗ ความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมาย หมายถึง ความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคลและการปฏิบัติตามกฎหมาย หมายถึง เหตุการณ์ความไม่แน่นอน ช่องโหว่ หรือข้อผิดพลาดในกระบวนการประมวลผลข้อมูล (การเก็บรวบรวม ใช้ หรือเปิดเผย) ผ่านระบบเทคโนโลยีดิจิทัล โครงสร้างเครือข่าย หรือฐานข้อมูลขององค์การสะพานปลา ที่อาจนำไปสู่การสูญหาย การเข้าถึงโดยมิชอบ การทำลาย การแก้ไขเปลี่ยนแปลง หรือการรั่วไหลของข้อมูลส่วนบุคคลของเกษตรกรชาวประมง ผู้เพาะเลี้ยงสัตว์น้ำ ผู้ประกอบการแพปลา คู่ค้า ผู้รับบริการ ณ สะพานปลาและท่าเทียบเรือประมงทั้ง ๑๗ แห่ง ตลอดจนบุคลากรของ อสป. อันก่อให้เกิดความเสียหายทั้งในมิติตัวเงินจากการถูกปรับ

ทางปกครอง โทษทางอาญา ความรับผิดทางแพ่ง และความเสียหายที่ไม่เป็นตัวเงิน เช่น ภาพลักษณ์ ชื่อเสียง และความเชื่อมั่นต่อการให้บริการของรัฐวิสาหกิจ ซึ่งกำหนดกรอบแนวทางปฏิบัติและมาตรการควบคุมความเสี่ยงตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนี้

การกำหนดฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล หมายถึง การประมวลผลข้อมูลส่วนบุคคลในทุกระบบงานดิจิทัล (เช่น ระบบ ERP, ระบบควบคุมการเข้าออกท่าเทียบเรือ, ระบบประมูลสินค้าสัตว์น้ำ, ระบบทะเบียนผู้ประกอบการแพปลา, และระบบสินเชื่อชาวประมง) ต้องกำหนดฐานทางกฎหมายรองรับอย่างชัดเจนก่อนเริ่มกิจกรรม ห้ามประมวลผลข้อมูลโดยปราศจากฐานทางกฎหมาย โดยจำแนกตามภารกิจของ อสป. ได้แก่

๑) ฐานสัญญา ใช้สำหรับการให้บริการขนถ่ายสัตว์น้ำ การเช่าพื้นที่อาคารพาณิชย์ท่าเทียบเรือประมง สัญญาเงินกู้และสินเชื่อหมุนเวียนเพื่อการประมง ตลอดจนสัญญาจ้างงานและสัญญาจัดซื้อจัดจ้างคู่ค้าภายนอก

๒) ฐานหน้าที่ตามกฎหมาย ใช้สำหรับการจัดทำและส่งมอบข้อมูลบัญชี ภาษีอากร รายงานตามพระราชบัญญัติจัดระเบียบกิจการแพปลา พ.ศ. ๒๔๙๖, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และคำสั่งศาลหรือพนักงานเจ้าหน้าที่ตามกฎหมาย

๓) ฐานภารกิจของรัฐ ใช้สำหรับการปฏิบัติหน้าที่ในการจัดระเบียบกิจการแพปลา การส่งเสริมอาชีพประมง และการดำเนินงานตามวัตถุประสงค์แห่งพระราชบัญญัติจัดตั้งองค์การสะพานปลาเพื่อประโยชน์สาธารณะ

๔) ฐานความยินยอม ใช้เฉพาะกรณีที่ไม่มีฐานทางกฎหมายอื่นรองรับ เช่น กิจกรรมการสื่อสารข้อมูลทางการตลาด โครงการส่งเสริมภาพลักษณ์ หรือการใช้คุกกี้ติดตามพฤติกรรมบนเว็บไซต์ อสป. โดยการขอความยินยอมต้องทำเป็นลายลักษณ์อักษรหรือผ่านระบบอิเล็กทรอนิกส์ มีข้อความชัดเจน เข้าใจง่าย และเจ้าของข้อมูลสามารถถอนความยินยอมได้โดยสะดวกทุกเมื่อ

การบริหารจัดการและตอบสนองต่อสิทธิของเจ้าของข้อมูล หมายถึง กำหนดกลไกและขั้นตอนการดำเนินงานเพื่อรองรับการใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคล (ได้แก่ สิทธิได้รับการแจ้งให้ทราบ, สิทธิเข้าถึงและขอรับสำเนา, สิทธิขอให้โอนย้ายข้อมูล, สิทธิคัดค้านการประมวลผล, สิทธิขอให้ลบ ทำลาย หรือทำเป็นข้อมูลนิรนาม, สิทธิระงับการใช้ และสิทธิแก้ไขข้อมูลให้ถูกต้อง) ดังนี้

๑) ระยะเวลาดำเนินการ หน่วยงานเจ้าของข้อมูล (Data Owner) ร่วมกับสำนักงานเทคโนโลยีสารสนเทศ ต้องตรวจสอบและดำเนินการตามคำร้องขอให้แล้วเสร็จภายใน ๓๐ วัน นับแต่วันที่ได้รับคำร้องขอที่ถูกต้องครบถ้วน

๒) การปฏิเสธคำขอ การปฏิเสธสิทธิของเจ้าของข้อมูลจะกระทำได้เฉพาะกรณีที่มีข้อยกเว้นตามกฎหมายหรือคำสั่งศาลเท่านั้น โดยต้องบันทึกเหตุผลการปฏิเสธเป็นลายลักษณ์อักษรในทะเบียนคำร้องขอใช้สิทธิ (Data Subject Request Log) เพื่อการตรวจสอบย้อนหลัง

มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

๑) การจำกัดสิทธิ์เข้าถึง (Access Control) บังคับใช้หลักการให้สิทธิเท่าที่จำเป็นต่อหน้าที่ โดยจัดทำระบบพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับผู้ดูแลระบบ (Administrator) และผู้มีสิทธิ์เข้าถึงฐานข้อมูลที่มีข้อมูลส่วนบุคคลระดับอ่อนไหว

๒) การเข้ารหัสข้อมูล ข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูง เช่น ข้อมูลบัตรประจำตัวประชาชน ข้อมูลชีวมิติ ข้อมูลบัญชีธนาคารชาวประมง ต้องได้รับการเข้ารหัสทั้งในขณะจัดเก็บ ด้วยมาตรฐานสากล (เช่น AES-256) และขณะรับส่งผ่านโครงข่ายสารสนเทศ ด้วยโปรโตคอลความปลอดภัย TLS ๑.๓ หรือเทียบเท่าขึ้นไป

๓) การควบคุมอุปกรณ์ปลายทางและการป้องกันข้อมูลรั่วไหล ติดตั้งระบบสกัดกั้นการถ่ายโอนข้อมูล ห้ามคัดลอกหรือถ่ายโอนข้อมูลส่วนบุคคลลงในอุปกรณ์บันทึกข้อมูลพกพา (USB Flash Drive, External Drive) โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร

๔) การจัดเก็บบันทึกประวัติเหตุการณ์ ระบบสารสนเทศที่มีการประมวลผลข้อมูลส่วนบุคคลต้องเก็บบันทึกประวัติการเข้าถึง (Access Log), ประวัติการทำธุรกรรม (Transaction Log) และประวัติการเปลี่ยนแปลงแก้ไขข้อมูลไว้อย่างมั่นคงปลอดภัย ไม่น้อยกว่า ๙๐ วัน เพื่อรองรับการสืบสวนตามกฎหมาย

ระยะเวลาการจัดเก็บและการทำลายข้อมูลส่วนบุคคล

๑) ระยะเวลาจัดเก็บ ข้อมูลส่วนบุคคลจะถูกจัดเก็บไว้เพียงเท่าที่จำเป็นตามวัตถุประสงค์ของการประมวลผล หรือตามที่กฎหมายกำหนดไว้เป็นการเฉพาะ (อาทิ ข้อมูลสัญญาและเอกสารธุรกรรมการเงินให้จัดเก็บเป็นระยะเวลา ๑๐ ปี ตามกฎหมายการบัญชีและภาษีอากร, ข้อมูลทะเบียนผู้ใช้บริการท่าเทียบเรือจัดเก็บตลอดระยะเวลาที่ยังใช้บริการและต่อเนื่องอีก ๕ ปีหลังสิ้นสุดสัญญา)

๒) แนวทางการทำลายข้อมูล เมื่อสิ้นสุดระยะเวลาจัดเก็บตามที่กำหนด ให้เจ้าหน้าที่ร่วมกับหน่วยงานเจ้าของข้อมูล ดำเนินการลบ ทำลาย ข้อมูลอิเล็กทรอนิกส์อย่างถาวร หรือดำเนินการแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวบุคคลได้อีกต่อไป พร้อมทั้งจัดทำทะเบียนบันทึกการทำลายข้อมูลเพื่อเก็บไว้เป็นหลักฐาน

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ในการออกแบบ พัฒนา หรือจัดหาระบบเทคโนโลยีดิจิทัลใหม่ หรือเมื่อมีการเปลี่ยนแปลงทางสถาปัตยกรรมระบบงานหลักที่มีการประมวลผลข้อมูลส่วนบุคคลของเกษตรกร ชาวประมง และคู่ค้าเป็นจำนวนมาก (เช่น การติดตั้งระบบกล้องวงจรปิดตรวจจับใบหน้า ณ ท่าเทียบเรือ, การพัฒนาแอปพลิเคชันตลาดกลางสัตว์น้ำดิจิทัล) เจ้าหน้าที่ต้องดำเนินการจัดทำรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ร่วมกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ก่อนการเริ่มใช้งานระบบจริงทุกครั้ง เพื่อระบุปัจจัยเสี่ยงและกำหนดมาตรการลดทอนความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

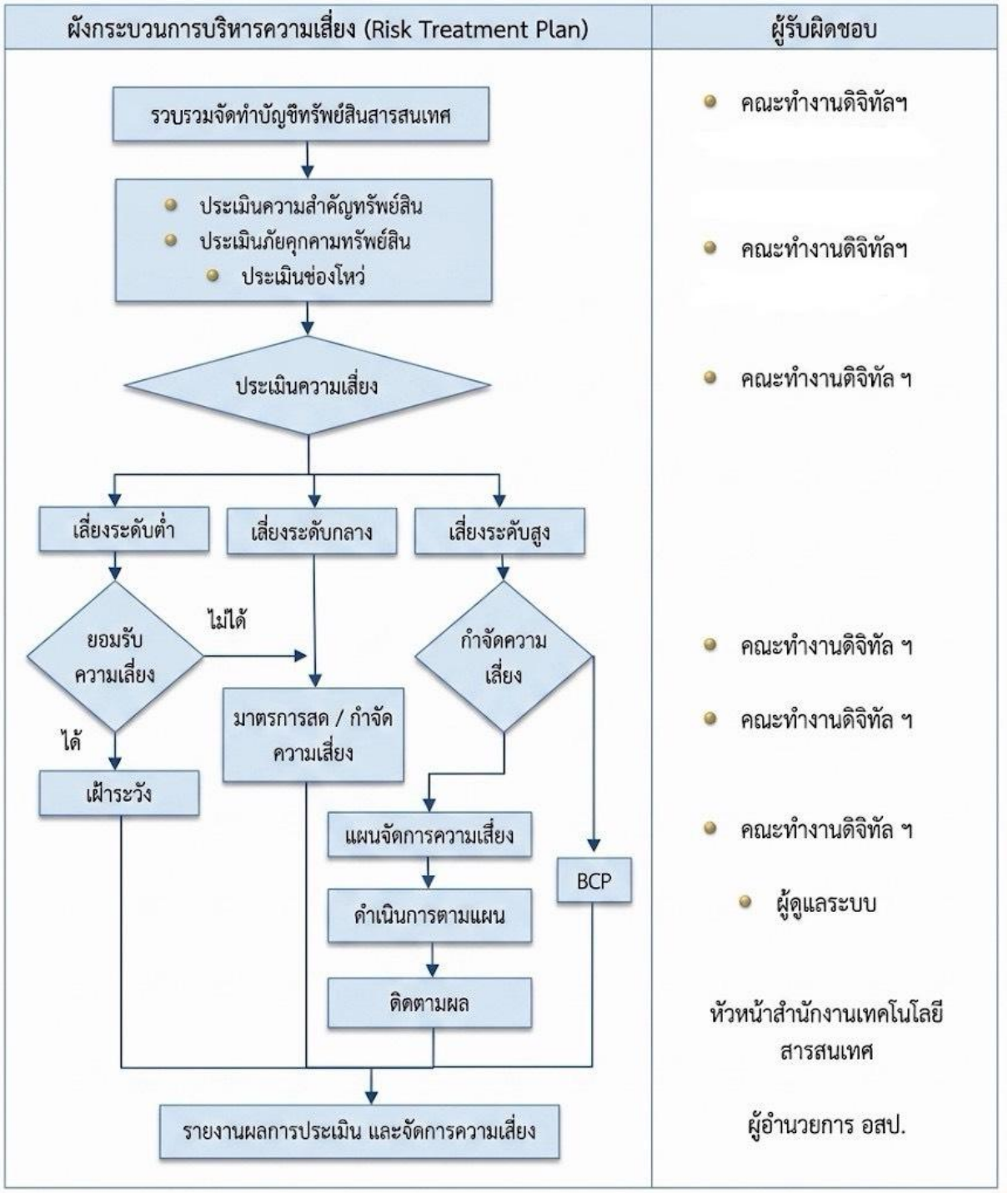
แผนการตอบสนองและแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

๑) เมื่อเกิดเหตุการณ์การละเมิดข้อมูลส่วนบุคคล หรือมีข้อสงสัยว่าข้อมูลส่วนบุคคลเกิดการรั่วไหล ผู้พบเหตุต้องแจ้งต่อผู้ดูแลระบบและ DPO ทันทีภายใน ๑ ชั่วโมง นับแต่ตรวจพบเหตุ

๒) ทีมตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัย ต้องเข้าควบคุมเหตุการณ์ ประเมินระดับความรุนแรง และดำเนินการยับยั้งความเสียหาย

๓) หากการละเมิดมีความเสี่ยงที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล อสป. ต้องแจ้งเหตุละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) โดยไม่ชักช้าภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ และหากมีความเสี่ยงสูงมากที่จะกระทบต่อเจ้าของข้อมูล ต้องแจ้งเหตุพร้อมแนวทางการเยียวยาให้เจ้าของข้อมูลทราบโดยทันทีผ่านช่องทางที่เหมาะสม

๔. กระบวนการบริหารความเสี่ยง (Risk Treatment Plan)



๔.๑ รวบรวมจัดทำบัญชีทรัพย์สินในระบบสารสนเทศ

ระบบการเผยแพร่ข้อมูลราคากลางสินค้าสัตว์น้ำผ่านเว็บไซต์องค์การสะพานปลา ตามประเภทของทรัพย์สินแบ่งได้ ๖ ประเภท ดังนี้ (๑) กระบวนการ (๒) ข้อมูล/สารสนเทศ (๓) ฮาร์ดแวร์ (๔) ซอฟต์แวร์ (๕) บุคลากร (๖) บริการ โดยรายละเอียดประเภททรัพย์สิน และตัวอย่างทรัพย์สินแสดง ดังตาราง

ลำดับ	ประเภททรัพย์สิน	รายการทรัพย์สิน
๑	Business Process (กระบวนการ)	๑.๑ กระบวนการสำรองข้อมูล ๑.๒ กระบวนการนำเข้า/แก้ไขข้อมูล
๒	Information (ข้อมูล/สารสนเทศ)	๒.๑ ข้อมูล Diagram ๒.๒ ข้อมูล Backup ๒.๓ ข้อมูล configuration ๒.๔ ข้อมูล Log (Network & System)
๓	Hardware (ฮาร์ดแวร์)	๓.๑ เครื่องคอมพิวเตอร์แม่ข่ายระบบสารสนเทศ ๓.๒ เครื่องคอมพิวเตอร์ PC / Note Book ๓.๓ อุปกรณ์สนับสนุนที่ทำงานร่วมกับคอมพิวเตอร์ ๓.๔ อุปกรณ์เครือข่าย
๔	Software (ซอฟต์แวร์)	๔.๑ ระบบปฏิบัติการ ๔.๒ โปรแกรมอรรถประโยชน์ ๔.๓ โปรแกรมจัดเก็บ Log File ๔.๔ Web Application
๕	Personnel (บุคลากร)	๕.๑ ผู้ดูแลระบบ ๕.๒ เจ้าหน้าที่ของหน่วยงาน ๕.๓ นักศึกษาฝึกงาน
๖	Service (บริการ)	๖.๑ บริการอินเทอร์เน็ต

๔.๒ จัดทำบัญชีทรัพย์สินสารสนเทศ (Assets List) FM-ISMS-๐๑ ในกรณีที่ทรัพย์สินหลายรายการมีความคล้ายคลึงกัน ผู้รับผิดชอบทรัพย์สิน สามารถจัดกลุ่มทรัพย์เพื่อลดจำนวนรายการทรัพย์สินในการประเมินความเสี่ยง โดยประเมินเป็นกลุ่มทรัพย์สินแทน ซึ่งประกอบด้วยข้อมูลของทรัพย์สินดังนี้

๑) ประเภททรัพย์สิน
๒) กลุ่มทรัพย์สิน
๓) รายการทรัพย์สิน
๔) ผู้รับผิดชอบทรัพย์สิน

๔.๓ การประเมินระดับความสำคัญทรัพย์สิน โดยใช้หลักเกณฑ์ด้านความลับ (Confidential) ความถูกต้อง (Integrity) และความพร้อมใช้ (Available) เพื่อจัดระดับความสำคัญของทรัพย์สินในระบบสารสนเทศในแต่ละประเด็นดังนี้

๑) **ความลับ (Confidentiality)** หมายถึง ภัยคุกคามและช่องโหว่ของความเสี่ยงที่ระบุไว้ อาจทำให้ทรัพย์สินถูกเปิดเผยต่อผู้ไม่มีสิทธิ์รับรู้

๒) **ความถูกต้อง (Integrity**) หมายถึง ภัยคุกคามและช่องโหว่ของความเสี่ยงที่ระบุไว้ อาจทำให้ทรัพย์สินถูกเปลี่ยนแปลง แก้ไข โดยผู้ไม่มีสิทธิ์หรือไม่เจตนา

๓) **ความพร้อมใช้ (Availability)** หมายถึง ภัยคุกคามและช่องโหว่ของความเสี่ยงที่ระบุไว้ อาจทำให้ผู้มีสิทธิ์ใช้งานทรัพย์สินไม่สามารถใช้งานทรัพย์สินได้ หรือทรัพย์สินอาจอยู่ในสภาพไม่พร้อมให้ใช้งาน

โดยการพิจารณาจากค่ามากที่สุดในเกณฑ์ทั้ง ๓ หากรายการทรัพย์สินใดที่มีค่าความสำคัญตั้งแต่ระดับ ๒ ขึ้นไป ให้ถือว่าทรัพย์สินนั้นมีความสำคัญและจะต้องนำมาประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ เกณฑ์การประเมินตามภาคผนวกท้ายขั้นตอนปฏิบัตินี้

๔.๔ ประเมินความเสี่ยงในรายการทรัพย์สินในระบบสารสนเทศของระบบการเผยแพร่ข้อมูลราคากลางสินค้าสัตว์น้ำผ่านเว็บไซต์องค์การสะพานปลา ในแบบฟอร์มประเมินความเสี่ยง Risk Assessment (FM-ISMS-๐๒) โดยมีขั้นตอนดังนี้

๔.๔.๑ กำหนดภัยคุกคามที่เป็นความเสี่ยงส่งผลกระทบต่อการให้บริการด้านสารสนเทศ โดยภัยคุกคามดังกล่าวอาจแบ่งได้ เป็นลักษณะต่าง ๆ ดังตัวอย่าง

ลักษณะภัยคุกคาม		สิ่งแวดล้อม	ธรรมชาติ	ความตั้งใจ	อุบัติเหตุ
๑	ขโมย	-	-	✓	-
๒	ผู้ไม่มีสิทธิ์เข้าถึงทรัพย์สิน	-	-	✓	-
๓	ไฟฟ้าขัดข้อง	✓	-	✓	✓
๔	โรคระบาด	✓	-	-	-
๕	น้ำท่วม	-	✓	-	-
๖	อุปกรณ์ล้มเหลว	-	-	✓	✓
๗	ความผิดพลาดในการใช้งาน	-	-	-	✓
๘	ข้อมูลเสียหาย	✓	-	✓	✓
๙	ละเมิดลิขสิทธิ์	-	-	✓	-

๔.๔.๒ ประเมินระดับความรุนแรงของผลกระทบ **(Impact)** จากความเสี่ยงนั้น โดยแบ่งออกเป็น ๔ ระดับ และมีเกณฑ์ในการประเมินความรุนแรงของผลกระทบดังนี้

ระดับของผลกระทบ	รายละเอียด
มาก (๔)	มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ขาดความต่อเนื่องในการให้บริการมากกว่า ๑๒ ชั่วโมง ส่งผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของผู้ใช้บริการทั้งภายในและภายนอกองค์กร
ค่อนข้างมาก (๓)	มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การให้บริการหยุดชะงักชั่วคราวเป็นระยะเวลา ๓ - ๕ ชั่วโมง ส่งผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของผู้ใช้บริการภายในองค์กร
ปานกลาง (๒)	มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การให้บริการหยุดชะงักชั่วคราวเป็นระยะเวลาไม่เกิน ๑ ชั่วโมง ไม่มีผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของผู้ใช้บริการ
น้อย (๑)	มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การให้บริการหยุดชะงักชั่วคราวเป็นระยะเวลา ๑๕ - ๓๐ นาที ไม่มีผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของผู้ใช้บริการ

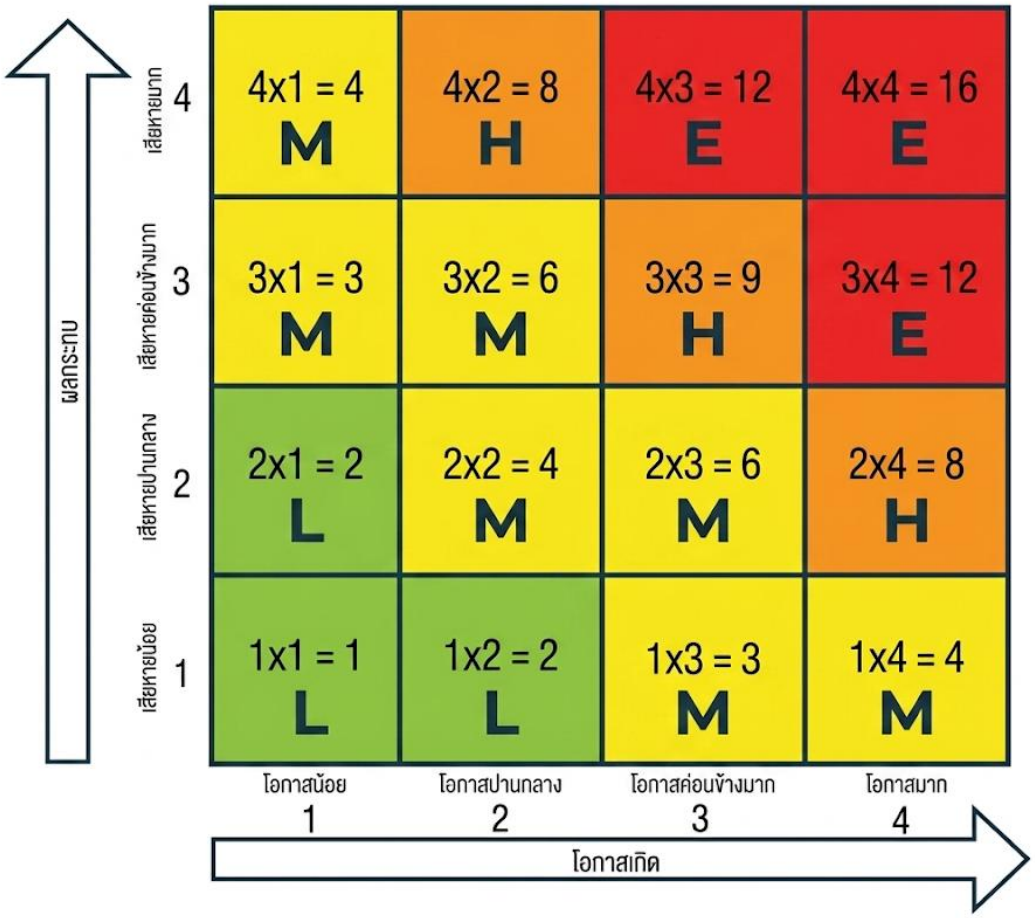
๔.๔.๓ ประเมินโอกาสในการเกิดภัยคุกคาม หรือ ความเสี่ยง **(Likelihood)** โดยแบ่งโอกาสมากน้อยตามจำนวนครั้งของการเกิดภัยคุกคาม หรือความเสี่ยงนั้น โดยระดับความเสี่ยงแบ่งออกเป็น ๔ ระดับ ดังนี้

ระดับโอกาสเกิดเหตุการณ์	ความหมาย
มาก (๔)	มีโอกาสเกิดเหตุการณ์ >= ๑๒ ครั้ง ภายในระยะเวลา ๑ ปี
ค่อนข้างมาก (๓)	มีโอกาสเกิดเหตุการณ์ระหว่าง ๓ – ๖ ครั้ง ภายในระยะเวลา ๑ ปี
ปานกลาง (๒)	มีโอกาสเกิดเหตุการณ์ระหว่าง ๑ – ๒ ครั้ง ภายในระยะเวลา ๒ ปี
น้อย (๑)	มีโอกาสเกิดเหตุการณ์ไม่เกิน ๑ ครั้ง ภายในระยะเวลา ๓ ปี

๔.๔.๔ คำนวณหาระดับความเสี่ยง (Risk Level) โดยใช้ข้อมูลของระดับผลกระทบ (Impact) คูณกับระดับโอกาสของการเกิดเหตุการณ์ที่จะเกิด (Likelihood) ดังนี้

ระดับความเสี่ยง = ระดับผลกระทบ X ระดับโอกาสการเกิด
Risk Level (Impact) (Likelihood)

ระดับความเสี่ยง (Risk Level) สามารถแบ่งได้ตามผลการคูณผลกระทบ และ โอกาสเกิดได้ตามแผนภาพดังนี้



คะแนนความเสี่ยง	ระดับความเสี่ยง	แนวทางการจัดการความเสี่ยง
๑-๒	ความเสี่ยงต่ำ **Low**	๑) ยอมรับความเสี่ยง Risk Accept ๒) เฝ้าระวังความเสี่ยง Risk Monitor
๓-๖	ความเสี่ยงปานกลาง **Medium**	๑) กำหนดมาตรการเพื่อควบคุมความเสี่ยง Risk Controlling ๒) ถ่ายโอนความเสี่ยง Risk Transferring
๘-๙	ความเสี่ยงสูง **High**	๑) วางแผนเพื่อกำจัด Risk Avoid หรือลดความเสี่ยง Risk Reduce โดยจัดทำในแผนการจัดการความเสี่ยง (Risk Treatment Plan) FM-ISMS-0๓ ๒) จัดทำแผนต่อเนื่องทางธุรกิจ BCP
๑๒-๑๖	ความเสี่ยงสูงสุด **Extremely high**	

๔.๕ การประเมินความเสี่ยงที่เหลือ (Assessment of Residual Risk) โดยการประเมิน impact และความถี่อีกครั้งเพื่อทบทวนว่า ระดับความเสี่ยงตอบสนองต่อมาตรการการควบคุมความเสี่ยงตามที่วางแผนไว้หรือไม่

๔.๖ รายงานผลการดำเนินการจัดการความเสี่ยง (Risk Treatment Report) ต่อที่ประชุมทบทวนฝ่ายบริหาร โดยหัวหน้าสำนักงานเทคโนโลยีสารสนเทศ

๕. วิธีการจัดการความเสี่ยง (Risk treatment)

การกำหนดวิธีการจัดการความเสี่ยง เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์การจัดการความเสี่ยงอย่างใดอย่างหนึ่งผสมผสานกันดังต่อไป

๕.๑ Take – การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับให้มีความเสี่ยง เนื่องจากค่าใช้จ่ายในการจัดการหรือสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ก็ควรมีมาตรการติดตามและดูแล เช่น การกำหนดระดับของผลกระทบที่ยอมรับได้ เตรียมแผนการตั้งรับ/จัดการความเสี่ยง เป็นต้น

๕.๒ Treat – การลด/ควบคุมความเสียง (Risk Reduction/Control) การออกแบบระบบควบคุม การแก้ไขปรับปรุงการทำงาน เพื่อป้องกันหรือจำกัดผลกระทบ และโอกาสเกิดความเสียหาย เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะวางมาตรการเชิงรุก เป็นต้น

๕.๓ Terminate – การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหยุดหรือเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการทำงาน ลดขอบเขตการดำเนินการ เป็นต้น

การยุติ เปลี่ยนแปลง หรือยกเลิกกิจกรรม โครงการ หรือระบบงานที่ก่อให้เกิดความเสี่ยงระดับวิกฤติที่ไม่สามารถควบคุมได้ เช่น การยกเลิกการใช้ระบบปฏิบัติการหรือโปรแกรมที่หมดอายุการรับประกันความปลอดภัยจากผู้ผลิต (End of Support)

๕.๔ Transfer – การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading) การกระจายทรัพย์สินหรือกระบวนการต่าง ๆ เพื่อลดความเสี่ยงจากการสูญเสีย เช่น การประกันทรัพย์สิน เพื่อโอนความเสี่ยงไปยังบริษัทประกัน การจ้างบริษัทภายนอกให้ทำงานบางส่วนแทน การทำสำเนาเอกสารหลายๆ ชุด การกระจายที่เก็บทรัพย์สินมีค่า เป็นต้น

๖. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

เมื่อประเมินความเสี่ยงแล้วเสร็จ จำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่นสามารถอ่านได้เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้ รายงานประกอบด้วยรายละเอียดอย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง และการออกรายงานมีวัตถุประสงค์ให้ส่วนต่างๆ ได้รับรู้ดังต่อไปนี้

๖.๑ ฝ่ายบริหาร ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

๖.๑.๑ รับรู้ความเสี่ยงที่องค์กรเผชิญอยู่

๖.๑.๒ เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่างๆในกรณีที่เกิดมีเหตุ หรือเหตุการณ์และเกิดผลเสียต่อภารกิจและผลประกอบการ

๖.๑.๓ ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร

๖.๑.๔ เข้าใจผลกระทบที่อาจมีต่อความมั่นใจของผู้ที่ได้รับผลกระทบ

๖.๑.๕ ให้แน่ใจว่ากระบวนการบริหารความเสี่ยงกำลังเป็นไปอย่างได้ผล

๖.๑.๖ ออกนโยบายบริหารความเสี่ยงและความรับผิดชอบของหน่วยงานและบุคลากรต่างๆในการบริหารความเสี่ยง

๖.๒ หัวหน้างาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

๖.๒.๑ ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อหน่วยงานอื่น หรือกิจกรรมอื่นในองค์กร

๖.๒.๒ มีดัชนีชี้วัดสมรรถนะของกิจกรรมในหน่วยงานเพื่อดูว่าระบบงานของตนเองได้รับผลกระทบจากความเสี่ยงมากน้อยเพียงใด

๖.๒.๓ รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางการแก้ไข

๖.๒.๔ รายงานความเสี่ยงใดๆที่เกิดใหม่หรือความล้มเหลวใดๆ ในมาตรการการควบคุมหรือป้องกันอารักขาสารสนเทศที่มีอยู่

๖.๓ ผู้ปฏิบัติงาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น

๖.๓.๑ เข้าใจบทบาทภาระหน้าที่และความรับผิดชอบในความเสี่ยงแต่ละรายการ

๖.๓.๒ เข้าใจบทบาทในการดำเนินการพัฒนาอย่างต่อเนื่องด้านการบริหารความเสี่ยง

๖.๓.๓ เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรมองค์กรที่สำคัญอย่างหนึ่ง

๗. การรายงานความเสี่ยงตกค้าง (Residual risk reporting)

เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการประเมิน และการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมาใช้ได้ผลหรือไม่เพียงไร วิธีการมาตรฐานที่ใช้กันโดยทั่วไป คือการมีหน่วยงานภายในหรือภายนอกทำการตรวจสอบโดยกระบวนการ IT auditing ที่เหมาะสม เนื่องจากสิ่งแวดล้อมและกฎระเบียบ มีการเปลี่ยนแปลงเกิดขึ้นตลอดเวลา จำเป็นต้องมีการบริหารความเสี่ยงและการตรวจสอบเป็นประจำ

๘. บทสรุป

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ เป็นกลไกหลักในการกำกับดูแลด้านดิจิทัล (Digital Governance) ขององค์การสะพานปลา เพื่อรักษาเสถียรภาพ ความมั่นคงปลอดภัย และความพร้อมใช้งานของระบบแม่ข่าย เครือข่าย ฐานข้อมูล และแอปพลิเคชัน ให้อยู่ภายใต้กรอบระดับความเสี่ยงที่ยอมรับได้ (IT Risk Appetite) โดยขับเคลื่อนผ่านการเฝ้าระวังเชิงรุกด้วยดัชนีชี้วัดความเสี่ยงหลัก (KRI) การเตรียมพร้อมรับมือภัยพิบัติ (IT-BCP/DRP) และการตรวจประเมินความมั่นคงปลอดภัย พร้อมทั้งรายงานผลและแนวโน้มความเสี่ยงต่อคณะอนุกรรมการที่กำกับดูแลด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อสนับสนุนการบริหารจัดการทรัพยากรไอทีและการดำเนินงานตามภารกิจขององค์กรได้อย่างมีประสิทธิภาพ มั่นคง และต่อเนื่อง

ภาคผนวก

เกณฑ์การประเมินความสำคัญของระบบสารสนเทศ

๑) การประเมินระดับความสำคัญของทรัพย์สินประเภทกระบวนการ (Business Process)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความลับ (Confidentiality)	เป็นกิจกรรมที่เกี่ยวข้องกับข้อมูลทั่วไปที่สามารถเปิดเผยให้รับรู้ได้ หรือเข้าถึงได้ ไม่มีความสำคัญต่อองค์กร และไม่จำเป็นต้องควบคุม	เป็นกิจกรรมที่เกี่ยวข้องกับข้อมูลที่สำคัญ หรือจำเป็นต่อการปฏิบัติงาน หรือจำเป็นต่อการให้บริการภายในองค์กร ต้องควบคุมให้เฉพาะกลุ่มบุคคลที่สามารถรับรู้หรือเข้าถึงได้	เป็นกิจกรรมที่เกี่ยวข้องกับข้อมูลที่เป็นความลับ หรือความสำคัญ หรือมีค่าต่อองค์กรในระดับสูง ต้องควบคุมให้รับรู้ได้เฉพาะผู้มีสิทธิ์เท่านั้น หรือจำกัดจำนวนผู้รับรู้ / เข้าถึง
ความถูกต้อง (Integrity)	เป็นกิจกรรมที่ไม่เป็นต้องเน้นความถูกต้อง แม่นยำ ยอมให้เกิดความผิดพลาดได้ โดยไม่ส่งผลกระทบต่อองค์กร หรือต่อการปฏิบัติงาน การให้บริการ	เป็นกิจกรรมที่จำเป็นต้องเน้นความถูกต้อง แม่นยำ ยอมให้เกิดความผิดพลาดได้บ้างเล็กน้อยในส่วนที่ไม่ใช่สาระสำคัญ	เป็นกิจกรรมที่มีสำคัญสูง จำเป็นต้องควบคุมความถูกต้อง แม่นยำ และไม่สามารถยอมให้เกิดความผิดพลาดได้
ความพร้อมใช้ (Availability)	เป็นกิจกรรมที่หากไม่ปฏิบัติหรือปฏิบัติล่าช้าก็ไม่ส่งผลกระทบต่อการให้บริการ	เป็นกิจกรรมที่หากไม่ปฏิบัติหรือปฏิบัติล่าช้าจะส่งผลกระทบต่อการให้บริการบางส่วน	เป็นกิจกรรมที่หากไม่ปฏิบัติหรือปฏิบัติล่าช้าจะส่งผลกระทบต่อการให้บริการทั้งหมด

๒) การประเมินระดับความสำคัญของทรัพย์สินประเภทข้อมูล/สารสนเทศ (Information)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความลับ (Confidentiality)	ข้อมูลทั่วไปที่สามารถเปิดเผยให้รับรู้ หรือเข้าถึงได้ ไม่มีความสำคัญต่อองค์กร และไม่จำเป็นต้องควบคุม	ข้อมูลที่สำคัญ หรือจำเป็นต่อการปฏิบัติงาน หรือจำเป็นต่อการให้บริการภายในองค์กร ต้องควบคุมให้เฉพาะกลุ่มบุคคลที่สามารถรับรู้หรือเข้าถึงได้	ข้อมูลที่เป็นความลับ หรือความสำคัญ หรือมีค่าต่อองค์กรในระดับสูง ต้องควบคุมให้รับรู้ได้เฉพาะผู้มีสิทธิ์เท่านั้น หรือจำกัดจำนวนผู้รับรู้/เข้าถึง

๒) การประเมินระดับความสำคัญของทรัพย์สินประเภทข้อมูล/สารสนเทศ (Information)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความถูกต้อง (Integrity)	ข้อมูลที่ไม่สำคัญ และไม่ได้เน้นที่ความถูกต้องแม่นยำ ยอมให้เกิดความผิดพลาดได้ โดยไม่ส่งผลกระทบต่อองค์กร หรือต่อการปฏิบัติงาน การให้บริการเช่น ข้อมูลชั่วโมงการเปิดใช้เครื่อง เป็นต้น	เป็นข้อมูลที่มีความสำคัญจำเป็นต้องควบคุมความถูกต้องของข้อมูล สามารถส่งผลกระทบต่อการปฏิบัติงาน การให้บริการ เช่น ข้อมูลใบคำร้องขอใช้งานระบบฯ ข้อมูลการติดตามสมรรถนะของระบบ	ข้อมูลที่มีสำคัญสูงจำเป็นต้องควบคุมความถูกต้องแม่นยำ และไม่สามารถยอม ให้เกิดความผิดพลาดได้ ความถูกต้องของข้อมูลส่งผล กระทบต่อการปฏิบัติงาน การให้บริการขององค์กร เช่น ค่าคอนฟิกูเรชั่นของระบบ เป็นต้น
ความพร้อมใช้ (Availability)	ข้อมูลที่มีความสำคัญน้อย หรือแทบไม่มีความสำคัญต่อองค์กร หรือต่อการปฏิบัติ งาน การให้บริการ	ข้อมูลที่มีความสำคัญต่อองค์กร หรือต่อการปฏิบัติงาน การให้บริการ หากขาด ความพร้อมใช้อาจส่งผลทำให้ปฏิบัติงานล่าช้า	ข้อมูลที่มีความสำคัญต่อองค์กร หรือต่อการปฏิบัติงาน การให้บริการในระดับสูง หากขาดความพร้อมใช้อาจส่งผลทำให้ไม่สามารถปฏิบัติงานได้

๓) การประเมินระดับความสำคัญของทรัพย์สินประเภทฮาร์ดแวร์ (Hardware)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความลับ (Confidentiality)	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งมีการจัดเก็บข้อมูลทั่วไปที่สามารถเปิดเผยให้รับรู้หรือเข้าถึงได้	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งมีการจัดเก็บข้อมูลที่สำคัญ หรือจำเป็นต่อการปฏิบัติงาน หรือจำเป็นต่อการให้บริการภายในองค์กร	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งมีการจัดเก็บข้อมูลที่เป็นความลับหรือความสำคัญ หรือมีค่าต่อองค์กรในระดับสูง
ความถูกต้อง (Integrity)	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากระบบทำงานหรือประมวล ผลผิดพลาดจะไม่ส่งผล กระทบต่อการให้บริการ	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากระบบทำงานหรือประมวลผลผิดพลาด จะส่งผลกระทบต่อการให้บริการเพียงบางส่วน	อุปกรณ์ใช้สนับสนุนการทำงานของระบบ ซึ่งหากระบบทำงานหรือประมวลผลผิดพลาด จะส่ง ผลกระทบต่อการให้บริการทั้งหมด

๓) การประเมินระดับความสำคัญของทรัพย์สินประเภทฮาร์ดแวร์ (Hardware)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความพร้อมใช้ (Availability)	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากไม่พร้อมใช้งานจะไม่ส่งผลกระทบต่อการให้บริการ	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากไม่พร้อมใช้งานจะส่งผลกระทบต่อการให้บริการบางส่วน	อุปกรณ์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากไม่พร้อมใช้งานจะส่งผลกระทบ ต่อการให้บริการทั้งหมด

๔) การประเมินระดับความสำคัญของทรัพย์สินประเภทซอฟต์แวร์ (Software)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความลับ (Confidentiality)	ซอฟต์แวร์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งมีการจัดเก็บข้อมูลทั่วไปที่สามารถเปิดเผยได้ให้รับรู้หรือเข้าถึงได้	ซอฟต์แวร์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งมีการจัดเก็บข้อมูลที่สำคัญ หรือจำเป็นต่อการปฏิบัติงาน หรือจำเป็นต่อการให้บริการภายในองค์กร	ซอฟต์แวร์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งมีการจัดเก็บข้อมูลที่เป็นความลับหรือความสำคัญ หรือมีค่าต่อองค์กรในระดับสูง
ความถูกต้อง (Integrity)	ซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการจัดการข้อมูลที่มีความ สำคัญ หรือจำเป็นต่อการ ปฏิบัติงาน	ซอฟต์แวร์ที่ใช้ในการจัดการข้อมูลที่มีความสำคัญ หรือจำเป็นต่อการปฏิบัติงาน เช่น ซอฟต์แวร์ในการควบคุม AccessControl ซอฟต์แวร์ ควบคุมกล้องวงจรปิด เป็นต้น	ซอฟต์แวร์ที่ใช้ในการประมวลผลข้อมูล หรือใช้ในการจัดการข้อมูลที่มีความ สำคัญ หรือมีค่าต่อองค์กรในระดับสูง
ความพร้อมใช้ (Availability)	ซอฟต์แวร์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากไม่พร้อมใช้งาน จะไม่ส่งผลกระทบต่อการให้บริการ	ซอฟต์แวร์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากไม่พร้อมใช้งานจะส่งผลกระทบต่อการให้บริการเพียงบางส่วน	ซอฟต์แวร์ที่ใช้สนับสนุนการทำงานของระบบ ซึ่งหากไม่พร้อมใช้งานจะส่งผลกระทบต่อการให้บริการทั้งหมด

๕) การประเมินระดับความสำคัญของทรัพย์สินประเภทบุคลากร (Personnel)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความลับ (Confidentiality)	บุคลากรที่ไม่ได้รับรู้ หรือไม่ได้เข้าถึงข้อมูลที่มีความสำคัญกับองค์กร	บุคลากรที่สามารถรับรู้หรือสามารถเข้าถึงข้อมูลที่สำคัญซึ่งต้องควบคุมให้เฉพาะกลุ่มบุคคลที่สามารถ รับรู้หรือเข้าถึงได้	บุคลากรที่สามารถรับรู้หรือสามารถเข้าถึงข้อมูลที่เป็นความลับ หรือความสำคัญหรือมีค่าต่อองค์กรในระดับ สูง
ความถูกต้อง (Integrity)	บุคลากรที่ไม่เกี่ยวข้องกับกิจกรรมที่จำเป็นต้องเน้นความถูกต้อง แม่นยำ	บุคลากรที่เกี่ยวข้องกับกิจกรรมที่จำเป็นต้องเน้นความถูกต้อง แม่นยำ ยอมให้เกิดความผิดพลาดได้บ้างเล็กน้อย	บุคลากรที่เกี่ยวข้องกับกิจกรรมที่สำคัญสูงจำเป็นต้องควบคุมความถูกต้อง แม่นยำ และไม่สามารถยอมให้เกิดความผิดพลาดได้
ความพร้อมใช้ (Availability)	หากขาดบุคลากร จะไม่ส่งผลกระทบต่อการให้บริการ	หากขาดบุคลากร จะส่งผลกระทบต่อการให้บริการบางส่วน	หากขาดบุคลากร จะส่งผลกระทบต่อการให้บริการทั้งหมด

๖) การประเมินระดับความสำคัญของทรัพย์สินประเภทบริการ (Service)			
ด้าน	**ระดับต่ำ (๑)**	**ระดับปานกลาง (๒)**	**ระดับสูง (๓)**
ความลับ (Confidentiality)	เป็นหน่วยงานที่ไม่สามารถเข้าถึงข้อมูลที่สำคัญได้ หรือไม่จำเป็นต้องควบคุม	เป็นหน่วยงานที่สามารถเข้าถึงข้อมูลที่สำคัญ หรือจำเป็นต่อการให้บริการภายในองค์กร	เป็นหน่วยงานที่สามารถเข้าถึงข้อมูลที่เป็นความลับหรือความสำคัญ หรือมีค่าต่อองค์กรในระดับสูง
ความถูกต้อง (Integrity)	เป็นหน่วยงานที่ไม่มีสิทธิ์ในการแก้ไขข้อมูล หรือการตั้งค่าระบบ	เป็นหน่วยงานที่มีสิทธิ์ในการแก้ไขข้อมูล หรือตั้งค่าระบบเช่นเดียวกับเจ้าหน้าที่ขององค์กร	เป็นหน่วยงานที่มีสิทธิ์ในการแก้ไขข้อมูล หรือตั้งค่าระบบโดยที่เจ้าหน้าที่ขององค์กรไม่มีสิทธิ์ในการแก้ไข
ความพร้อมใช้ (Availability)	เป็นหน่วยงานซึ่งหากไม่เข้าปฏิบัติงานจะไม่ส่งผลกระทบต่อการปฏิบัติงานขององค์กร หรือส่งผลกระทบเล็กน้อย	เป็นหน่วยงานซึ่งหากไม่เข้าปฏิบัติงาน อาจส่งผลทำให้การปฏิบัติงานขององค์กรล่าช้า	เป็นหน่วยงานที่หากไม่พร้อมให้บริการ จะส่งผลทำให้องค์กรไม่สามารถปฏิบัติงานได้

การบันทึกคุณภาพ

เลขเอกสาร	ชื่อบันทึก	ประเภทสื่อ	ระยะเวลาจัดเก็บ
FM-ISMS-๐๑	บัญชีรายชื่อทรัพย์สิน (Assets List)	Electronic	๒ ปี
FM-ISMS-๐๒	แบบประเมินความเสี่ยง (Risk Assessment)	Electronic	๒ ปี
FM-ISMS-๐๓	แผนการจัดการความเสี่ยง RTP	Electronic	๒ ปี