แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
กรมอนามัย พ.ศ. 2565

กรมอนามัย
DEPARTMENT OF HEALTH

สารบัญ

บทนำ

เทคโนโลยีสารสนเทศมีบทบาทที่สำคัญอย่างยิ่งต่อกรมอนามัยในยุคปัจจุบัน ปัจจุบันถูกนำมาใช้เป็นเครื่องมือในการจัดการข้อมูลต่าง ๆ ให้มีคุณภาพเพื่อใช้ในการปฏิบัติงานและใช้ในการตัดสินใจของผู้บริหาร นอกจากนี้ยังถูกใช้เป็นเครื่องมือช่วยในการสื่อสารภายในกรมอนามัยให้มีประสิทธิภาพและประสิทธิผล

ดังนั้นการบริหารจัดการเทคโนโลยีสารสนเทศของกรมอนามัยให้มีความมั่นคงปลอดภัยจากปัจจัยต่าง ๆ จึงเป็นสิ่งที่จำเป็นอย่างยิ่งต่อการดำเนินงานของกรมอนามัย การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศฉบับนี้จึงได้ถูกจัดทำขึ้นมาเพื่อเป็นหนึ่งในเครื่องมือที่ใช้สำหรับการจัดการความมั่นคงปลอดภัยของทรัพยากรด้านสารสนเทศของกรมอนามัยในมิติต่าง ๆ ตามแนวทางของ ISO/IEC 27001: 2013

วัตถุประสงค์

แผนบริหารความเสี่ยงฯ นี้มีวัตถุประสงค์ดังต่อไปนี้

1.1 เพื่อเป็นแนวทางในการบริหารเทคโนโลยีสารสนเทศของกรมฯให้มีความมั่นคงปลอดภัยมากขึ้น

1.2 เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพและประสิทธิผลมากขึ้น

1.3 เพื่อป้องกันความเสียหายที่เกิดจากการเหตุการณ์ที่ไม่พึงประสงค์ต่อทรัพยากรด้านสารสนเทศและมีผลต่อการดำเนินงานของกรมอนามัย

1.4 เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบสารสนเทศ ฐานข้อมูลสารสนเทศให้มีเสถียรภาพและพร้อมใช้งาน

1.5 เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

ขั้นตอนการประเมินความเสี่ยง

ในส่วนนี้จะอธิบายให้เห็นถึงขั้นตอนหลัก ๆ ของกระบวนการของการประเมินความเสี่ยง ซึ่งเป็นไปตามแนวทางของมาตรฐาน COSO (Committee of Sponsoring Organization of the Treadway Commission)

การระบุความเสี่ยง (Risk Identification)

การประเมินความเสี่ยงฯนี้ได้ใช้มาตรการควบคุมของ ISO/IEC 27001: 2013 มาเป็นเกณฑ์เพื่อระบุถึงความเสี่ยงพื้นฐานที่สำคัญที่จำเป็นต้องจัดการ จากการศึกษาสถานภาพปัจจุบันของการบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศของกรมฯ เมื่อเทียบกับมาตรการควบคุมฯ ดังกล่าวพบความเสี่ยงด้านต่าง ๆ ดังตาราง ที่ 1 ซึ่งในตารางดังกล่าวมีความเสี่ยงอยู่ทั้งสิ้น 12 ความเสี่ยง (R01 - R12) ส่วนรายละเอียดที่เป็นสาเหตุหรือปัจจัยของความเสี่ยงและผลกระทบของความเสี่ยงอธิบายไว้ในตารางที่ 2

ตารางที่ 1 การระบุความเสี่ยงเทียบเคียงกับมาตรการควบคุมของ ISO/IEC 27001: 2013

รหัสความเสี่ยง	ความเสี่ยง	มาตรการควบคุมของ ISO/IEC 27001: 2013
R01	ความพร้อมใช้งานอย่างต่อเนื่อง (availability) ของระบบสารสนเทศภายในศูนย์ข้อมูลกลาง (data center)	Availability of information processing facilities (A.17.2.1)
R02	การเข้าถึงระบบเครือข่ายไร้สาย (wireless network) ของกรมฯ	Access to networks and network services (A.9.1.2)
R03	ระบบการบริหารจัดการรหัสผ่าน (password management system)	Password management system (A.9.4.3)
R04	การติดตั้งซอฟต์แวร์ภายในกรมฯ	Installation of software on operational systems (A.12.5.1)
R05	การป้องกันซอฟต์แวร์ไม่พึงประสงค์ (malicious software)	Controls against malware (A.12.2.1)
R06	การสำรองข้อมูลและซอฟต์แวร์ประยุกต์ที่จัดเก็บอยู่ที่ data center ของกรมฯ และที่ส่วนอื่น ๆ	Information backup (A.12.3.1)
R07	การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์	Intellectual property rights (A.18.1.2)
R08	การควบคุมและกำกับการพัฒนาระบบสารสนเทศในกรมฯ ให้เป็นไปตามเกณฑ์มาตรฐานของกรมฯ	Information security requirements analysis and specification (A.14.1.1)
R09	การมีทักษะที่ทันยุคทันสมัยทางด้านเทคโนโลยีสารสนเทศ	Contact with special interest groups (A.6.1.4)
R10	การป้องกันภัยคุกคามของการให้บริการด้านเทคโนโลยีสารสนเทศ	Information Security Requirements Analysis & Specification (A.14.1.1)
R11	การปรับตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย	Review of the policies for information security (A.5.1.2)

รหัสความเสี่ยง	ความเสี่ยง	มาตรการควบคุมของ ISO/IEC 27001: 2013
R12	โปรแกรมประยุกต์ (Application) ไม่มีการอัพเดท	Technical Review of Applications After Operating Platform Changes (A.14.2.3)
R13	ระบบบริหารจัดการทรัยพ์สิน (Asset Management)	Asset Management (A.8)
R14	การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical & Environmental Security)	Physical and environmental security (A.11)
R15	การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management)	Information security incident management (A.16)
R16	การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)	Supplier relationships (A.15)
R17	การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity)	Information security aspects of business continuity (A.17)
R18	การเข้ารหัสข้อมูล (Cryptography)	Cryptography (A.10)
R19	การบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)	Human resource security (A.7)

ตารางที่ 2 รายละเอียดของความเสี่ยง (ปัจจัยและผลกระทบ)

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R01	ระบบสารสนเทศของกรมฯ ส่วนใหญ่ถูกติดตั้งไว้ที่ศูนย์ข้อมูลกลาง (data center) ของกรมฯ ศูนย์ข้อมูลกลางนี้มีระบบไฟฟ้าสำรองที่เก็บไว้ใน UPS และมีเครื่องกำเนิดไฟฟ้า เพื่อใช้ในกรณีไฟฟ้าล้มเหลว อย่างไรก็ตาม อาจเกิดปัญหาเครื่องกำเนิดไฟฟ้าไม่สามารถทำงานได้	1. การทำงานตามภารกิจของกรมฯ ในส่วนที่ต้องพึงพาระบบสารสนเทศต้องหยุดชะงัก 2. ประชาชนไม่สามารถใช้บริการของกรมฯ ผ่านระบบเครือข่ายอินเตอร์เน็ตได้ 3. การสื่อสารของกรมฯ เช่น Video Conference และระบบอื่น ๆ ที่ต้องใช้ระบบเครือข่ายไม่สามารถทำได้
R02	กรมฯ มีการติดตั้งระบบเครือข่ายไร้สาย (wireless network) เพื่อให้ผู้ปฏิบัติงานของกรมฯ สามารถเข้าถึงการใช้บริการด้านสารสนเทศได้อย่างมีประสิทธิภาพและประสิทธิผลมากขึ้น อย่างไรก็ตามในกระบวนการของการยืนยันตัวบุคคล (authentication) เพื่อเข้าใช้บริการยังมีช่องโหว่ซึ่งจะทำให้ผู้ไม่ประสงค์ดีสามารถปลอมแปลงตัวตนเพื่อเข้ามาใช้บริการได้ o ผู้ใช้ระดับผู้บริหาร ใช้วิธีการลงทะเบียนอุปกรณ์ที่จะใช้ด้วย MAC-ADDRESS และไม่ต้องทำการ login ใด ๆ	1. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจใช้งานอินเตอร์เน็ตของกรมฯ ในการทำสิ่งที่ผิดกฎหมาย เช่น โพสต์ข้อความหมิ่นประมาทผู้อื่นได้ ซึ่งอาจจะมีผลทำให้กรมฯ ต้องรับผิดชอบทางกฎหมาย 2. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจขโมยข้อมูล ดัดแปลงข้อมูลหรือทำลายข้อมูลที่สามารถเข้าถึงได้ ซึ่งอาจจะทำให้ข้อมูลที่ใช้ในการปฏิบัติงานเสียหายได้ และอาจจะมีผลทำให้กรมฯ ต้องรับผิดชอบทางกฎหมาย พรบ.ส่วนบุคคล 3. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจลักลอบเข้าไปในระบบบริหารจัดการเครือข่ายเพื่อให้ได้สิทธิ์ในการควบคุมทั้งเครือข่ายทางสายและทางไร้สายดังกล่าวได้
R03	กรมฯ ได้มีการกำหนดการใช้ชื่อผู้ใช้และรหัสผ่านเป็นการทำการยืนยันตัวบุคคลเพื่อเข้าใช้ทรัพยากรด้านสารสนเทศของกรมฯ อย่างไรก็ตาม การบริหารจัดการรหัสผ่าน (password management) ยังไม่เป็นระบบที่เป็นมาตรฐานและสามารถเป็นช่องโหว่ให้ผู้บุกรุกสามารถคาดเดารหัสผ่าน รวมทั้งการโจรกรรมรหัสผ่านได้ เช่น ข้อกำหนดในการตั้งรหัสผ่านไม่เปลี่ยนทุก 90 วัน หรือ ข้อกำหนดในการสื่อสารข้อมูลที่เป็นรหัสผ่านที่ส่งระหว่างอุปกรณ์เพื่อป้องกันการแอบดักขโมย หรือ ข้อกำหนดในการปรับเปลี่ยนและตรวจสอบการใช้รหัสผ่านที่มากับอุปกรณ์ (default passwords) หรือมีการกำหนดชื่อผู้ใช้และรหัสผ่านกลาง ทำให้ไม่สามารถยืนยันได้ว่าเป็นผู้บุกรุกหรือไม่	1. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาครอบครองและควบคุมทรัพยากรด้านสารสนเทศกรมฯ ในการทำสิ่งต่างๆที่ไม่พึงประสงค์ 2. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจขโมยข้อมูลที่เป็นความลับ ดัดแปลงข้อมูลหรือทำลายข้อมูลที่สามารถเข้าถึงได้ ซึ่งอาจจะทำให้ข้อมูลที่ใช้ในการปฏิบัติงานเสียหายและไม่สามารถใช้งานได้ (confidentiality, integrity and availability)

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R04	ผู้ใช้งาน (end-users) บางคนสามารถที่จะติดตั้งซอฟต์แวร์ต่าง ๆ ได้เองโดยไม่มีกระบวนการในการควบคุม (control of operational software) ซอฟต์แวร์ที่สามารถติดตั้งได้เองนี้เป็นทั้งซอฟต์แวร์ระบบ (system software) ซอฟต์แวร์ประยุกต์ (application software) รวมถึงซอฟต์แวร์อรรถประโยชน์ใดๆ (utility software)	1. การติดตั้งซอฟต์แวร์บางอย่างอาจทำให้ไม่สามารถควบคุมการรักษาความลับข้อมูลของกรมฯ ได้ 2. การติดตั้งอาจมีการเปลี่ยนแปลงการกำหนดค่ารูปแบบการทำงาน (configuration) ของอุปกรณ์และอาจจะมีผลทำให้เกิดปัญหากับการทำงานของซอฟต์แวร์ตัวอื่น ๆ 3. การติดตั้งซอฟต์แวร์โดยไม่คำนึงถึงเรื่องลิขสิทธิ์ซึ่งอาจจะทำให้กรมฯถูกฟ้องร้องและเกิดความเสียหายได้ 4. ซอฟต์แวร์ที่ถูกนำมาติดตั้งอาจติดไวรัสหรือซอฟต์แวร์ที่ไม่พึงประสงค์ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลและซอฟต์แวร์อื่นๆ
R05	ผู้ใช้งาน (end users) ค่อนข้างมีอิสระสูงในการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศของกรมฯ ดังนั้นถ้าหากผู้ใช้งานขาดความระมัดระวัง อาจจะส่งผลทำให้ซอฟต์แวร์ที่ไม่พึงประสงค์ (malicious software หรือ malware) สามารถเข้าสู่ระบบคอมพิวเตอร์และแพร่กระจายผ่านระบบเครือข่ายได้ ปัจจุบันซอฟต์แวร์ที่ไม่พึงประสงค์ดังกล่าวอาจจะผ่านเข้ามาทาง e-mail, social media, thumb-drive หรือซอฟต์แวร์ที่นำมาติดตั้ง	1. การใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศอาจจะไม่มีประสิทธิภาพ เช่น เครื่องคอมพิวเตอร์หรือระบบเครือข่ายทำงานช้าลงและส่งผลต่อประสิทธิภาพของงาน 2. ข้อมูลอาจจะถูกขโมยออกไปหรืออาจจะถูกทำลายหรืออาจจะถูกปิดกั้นไม่ให้สามารถเข้าถึงได้ 3. ซอฟต์แวร์ที่ใช้งานจริงที่ติดตั้งบนเครื่องคอมพิวเตอร์อาจจะถูกทำให้ใช้งานไม่ได้
R06	ข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่ายที่ตั้งอยู่ที่ศูนย์ข้อมูลกลางได้ถูกสำเนาเก็บไว้ตามช่วงเวลาที่กำหนด อย่างไรก็ตาม ตัวสำเนาดังกล่าวกลับถูกเก็บไว้ที่ศูนย์ข้อมูลกลางเช่นเดียวกัน ดังนั้นถ้าหากเกิดไฟไหม้หรือน้ำท่วมที่ศูนย์ข้อมูลกลางแล้ว ตัวข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่าย รวมทั้งสำเนาของมันก็จะเกิดความเสียหายไปด้วยกัน นอกจากนี้เครื่องแม่ข่ายของบางหน่วยงานก็ไม่ได้ถูกเก็บไว้ที่ศูนย์ข้อมูลกลาง ข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่ายดังกล่าวจึงอาจจะไม่ได้ถูกสำเนาเก็บไว้	1. กรณีที่หน่วยเก็บข้อมูลสำรอง (secondary storage) ของเครื่องแม่ข่ายเกิดความเสียหายและไม่มีสำเนาเก็บไว้ จะมีผลทำให้ข้อมูลสูญหายและซอฟต์แวร์ประยุกต์ไม่สามารถใช้งานได้อีก ถ้าเป็นระบบที่สำคัญต่อการทำธุรกรรมของหน่วยงาน ก็จะมีผลต่อการดำเนินงานทันที 2. กรณีที่เกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อศูนย์ข้อมูลกลาง เช่น ไฟไหม้ จะมีผลทำให้ข้อมูลสูญหายและซอฟต์แวร์ประยุกต์ไม่สามารถใช้งานได้อีก ถ้าเป็นระบบที่สำคัญต่อการทำธุรกรรมของหน่วยงานต่างๆ ก็จะมีผลต่อการดำเนินงานของหน่วยงานเหล่านั้นทันที
R07	การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ยังมีโอกาสเกิดขึ้นได้ในกรมฯ ทั้งนี้เนื่องจากการขาดการสร้างความตระหนักในผลลัพธ์ที่จะเกิดขึ้น รวมทั้งการขาดกลไก	1. การใช้ระบบปฏิบัติการที่ไม่มีใบอนุญาตมีผลทำให้ขาดการบำรุงรักษาจากผู้ผลิตและอาจจะมีผลทำให้เกิดช่องโหว่ในระบบคอมพิวเตอร์ที่ผู้ไม่

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
	ในการควบคุมและติดตาม จากการตรวจสอบพบว่ายังคงมีการใช้ระบบปฏิบัติการ (operating systems) ที่ไม่มีใบอนุญาต (license) อยู่	ประสงค์ดีอาจจะบุกรุกเข้ามาได้และสร้างความเสียหายให้กับระบบ รวมทั้งการโจรกรรมข้อมูลต่างๆ 2. การใช้ระบบปฏิบัติการที่ไม่มีใบอนุญาตเป็นสิ่งที่ผิดกฎหมายและอาจจะถูกฟ้องร้องเรียกค่าเสียหายได้ ซึ่งจะทำให้กรมฯต้องสูญเสียค่าใช้จ่ายสูงและสูญเสียภาพลักษณ์ของกรมฯ 3. ซอฟต์แวร์ที่ผิดกฎหมายอาจจะมาพร้อมกับ malware เช่น virus หรือ spyware ซึ่งสามารถสร้างความเสียหายให้กับข้อมูลและทรัพยากรด้านสารสเทศได้
R08	การพัฒนาระบบสารสนเทศในกรมฯ เป็นลักษณะที่ผู้ใช้งาน (end-users) สามารถจัดหาหรือจัดจ้างได้เอง รวมทั้งสามารถพัฒนาระบบขึ้นมาเองด้วย ถึงแม้ว่ากรมฯ มีเอกสารที่กำหนดรูปแบบของการพัฒนาระบบฯ แต่ยังขาดควบคุมและกำกับดูแลจากศูนย์เทคโนโลยีสารสนเทศ และบางครั้งบริษัทภายนอกก็สามารถเข้ามาจัดการกับระบบของตนเองโดยผ่านระบบเครือข่ายของกรมฯ เข้ามา	1. การพัฒนาระบบไม่เป็นไปตามรูปแบบการพัฒนาระบบที่กรมฯ ได้กำหนดไว้ และอาจส่งผลให้คุณภาพระบบ รวมถึงความมั่นคงปลอดภัยของระบบไม่เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของกรมฯ และอาจมีความเสี่ยงต่อการถูกผู้ไม่ประสงค์ดีโจมตีผ่านทางช่องโหว่ของระบบ 2. การเชื่อมโยงระบบเพื่อใช้ประโยชน์จากข้อมูลทำได้ยาก 3. การเกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบต่าง ๆ ภายในกรมฯ
R09	เทคโนโลยีสารสนเทศมีความก้าวหน้าและเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งเครื่องมือและเทคนิคใหม่ ๆ ที่มีการพัฒนาอยู่ตลอดเวลา ซึ่งสิ่งที่เกิดขึ้นดังกล่าวทำให้บุคลากรที่ดูแลด้านเทคโนโลยีสารสนเทศไม่สามารถติดตามและรู้ทันผู้ที่ไม่ประสงค์ดีในการบุกรุกเข้าสู่ระบบเครือข่ายได้ รวมทั้งไม่รู้จักเครื่องมือและเทคนิคใหม่ ๆ ที่มีประสิทธิภาพและประสิทธิผลการรับมือการโจมตีได้อย่างทันท่วงที	1. ผู้ไม่ประสงค์ดีสามารถโจมตีระบบได้สำเร็จและมีผลต่อการปฏิบัติงานและการให้บริการประชาชนของกรมฯ 2. การบุกรุกเข้ามาใช้ประโยชน์จากทรัพยากรด้านสารสนเทศโดยเฉพาะอย่างยิ่งเครื่องแม่ข่ายที่มีช่องโหว่ เพื่อไว้ใช้ในการโจมตีเครื่องอื่นๆ เช่น การทำ Crytojacking หรือ DDOSหรือ ขโมยข้อมูล ซึ่งนอกจากจะทำให้ประสิทธิภาพของทรัพยากรลดลงแล้ว ยังอาจจะทำให้เสียภาพลักษณ์ของกรมฯ และอาจเกิดการฟ้องร้องอีกด้วย

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R10	เนื่องจากระบบที่ให้บริการของกรมฯ ไม่ได้ทำการอัพเดท ระบบปฏิบัติการ โปรแกรมประยุกต์ และตัวแปรภาษา (Interpreter) ซึ่งเป็นสาเหตุหลักที่ทำให้เกิดช่องโหว่ของระบบสารสนเทศของกรมฯ	1. ผู้ไม่ประสงค์ดีสามารถบุกรุกเครื่องคอมพิวเตอร์แม่ข่าย จารกรรมข้อมูล และดัดแปลงข้อมูลทำให้เกิดความเสียหายได้ 2. ผู้ไม่ประสงค์ดีบุกรุกเข้ายึดเครื่องคอมพิวเตอร์แม่ข่าย และอาจลักลอบใช้ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่ายทำให้เครื่องคอมพิวเตอร์แม่ข่ายทำงานได้ไม่เต็มประสิทธิภาพ
R11	การปรับตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย บางอุปกรณ์ ยังเปิดใช้บริการที่ไม่มีการเข้ารหัสเช่น Telnet ทำให้เกิดความเสี่ยงในการดักจับรหัสผ่านเพื่อเข้าควบคุมอุปกรณ์ได้	1. ทำให้ผู้ไม่ประสงค์ดีเข้าควบคุมอุปกรณ์ที่เปิดให้บริการที่ไม่มีการเข้ารหัสได้
R12	โปรแกรมประยุกต์ (Application) ไม่มีการอัพเดท	1. ผู้ไม่ประสงค์ดีอาศัยช่องโหว่ของโปรแกรมประยุกต์เข้าควบคุมระบบงานได้ 2. ผู้ไม่ประสงค์ดีอาศัยช่องโหว่ของโปรแกรมประยุกต์เข้าขโมยข้อมูล แก้ไข ทำให้เกิดความเสียหายกับข้อมูลได้
R13	ผลิตภัณฑ์ End of Support หรือ End of Life ทำให้อาจพบช่องโหว่ และเกิดการโจมตีระบบสารสนเทศได้	1. ทำให้เกิดช่องโหว่ของระบบสารสนเทศต่าง ๆ และอาจเกิดการโจมตีระบบสารสนเทศที่ End of Support หรือ End of Life 2. อาจโดนขโมยข้อมูล เพื่อเรียกค่าไถ่ หรือยึดระบบงานทำให้ระบบงานไม่สามารถใช้งานได้
R14	- ระบบไฟฟ้าขัดข้อง อาจทำให้ไม่สามารถใช้งานหรือให้บริการระบบงานสารสนเทศได้อย่างต่อเนื่อง - เกิดการชุมนุม ยึดพื้นที่ทำให้ไม่สามารถใช้งานหรือให้บริการระบบงานสารสนเทศได้	1. ทำให้ระบบงานหรือการให้บริการหยุดชะงัก เมื่อเกิดเหตุไฟฟ้าขัดข้อง 2. อาจทำให้ไม่สามารถให้บริการหรือใช้งานระบบงานได้ เนื่องจากอาจโดนผู้ชุมนุมบุกยึดสถานที่
R15	ปัญหาของซอฟต์แวร์ อุปกรณ์ต่อพ่วง เนื่องจากระบบปฏิบัติการอัพเดท ระบบงานช้าไม่สามารถให้บริการได้	1. ทำให้ผู้ใช้งานเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ 2. ระบบงานไม่สามารถให้บริการได้
R16	การลักลอบนำข้อมูลความลับไปเปิดเผย โจมตีระบบงานได้ หากมีข้อขัดแย้งกับผู้บังคับบัญชา	1. ข้อมูลที่เป็นความลับถูกเปิดเผย 2. ข้อมูลสูญหาย ทำให้ระบบไม่สามารถใช้งานได้

รหัสความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R17	ไม่ได้ทำการซักซ้อมการทบทวบกระบวนการตามแผนที่ได้วางไว้	1. อาจทำให้ระบบสำรอง ทำงานได้ล่าช้ากว่าแผนที่วางไว้ 2. อาจทำให้ระบบสำรองไม่สามารถทำงานได้เนื่องจากไม่ได้มีการทดสอบการกู้คืนระบบ
R18	ข้อมูลชั้นความลับไม่มีการเข้ารหัสข้อมูล	1. อาจทำให้ข้อมูลที่เป็นชั้นความลับถูกเปิดเผยสู่สาธารณะ
R19	ไม่ได้ทำการลบผู้ใช้ สำหรับระบบงานออกจากระบบทำให้เจ้าหน้าที่ที่ได้ลาออก สามารถเข้าถึงข้อมูลหรือระบบงานได้	1. อาจทำให้ข้อมูลที่เป็นชั้นความลับถูกเปิดเผยสู่สาธารณะ

การวิเคราะห์และประเมินความเสี่ยง (Risk Analysis and Assessment)

หลังจากขั้นตอนการระบุความเสี่ยง (risk identification) ด้านเทคโนโลยีสารสนเทศโดยศึกษาพิจารณาจากสถานภาพปัจจุบันแล้ว ขั้นตอนถัดมาก็เป็นการวิเคราะห์และประเมินความเสี่ยงซึ่งเป็นการวิเคราะห์โอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดจากเหตุการณ์กรณีที่ความเสี่ยงนั้นเกิดขึ้นจริง รวมไปถึงการประเมินระดับคะแนนของความเสี่ยงแต่ละความเสี่ยงและการจัดลำดับความสำคัญ การประเมินโอกาสและผลกระทบนั้นมาจากการประชุมระดมความคิดเห็นของผู้เกี่ยวข้อง (stakeholders) เป็นหลัก ซึ่งสะท้อนมาจากความรู้และประสบการณ์โดยตรง ผลลัพธ์ที่ได้แสดงไว้ในตารางที่ 3 (โดยมีหมายเหตุที่เกี่ยวข้องกำกับไว้ด้านล่างของตาราง) และตารางที่ 4

ตารางที่ 3 ผลการวิเคราะห์และประเมินความเสี่ยง (Risk Analysis and Assessment)

รหัสความเสี่ยง	ระดับของโอกาสที่จะเกิด (P)	ระดับของผลกระทบที่เกิดขึ้น (I)	ระดับคะแนนความเสี่ยง (P*I)
R01	1	2	2
R02	2	3	6
R03	2	3	6
R04	3	3	9
R05	3	3	9
R06	1	3	3
R07	3	3	9
R08	1	1	1
R09	3	2	6
R10	3	3	9
R11	2	3	6
R12	3	3	9
R13	1	3	3
R14	1	1	1
R15	3	1	3
R16	2	3	2
R17	1	2	2
R18	2	3	6
R19	1	3	3

หมายเหตุ (อธิบายความหมายของคำในตารางที่ 3)
ความหมายของ “ระดับของโอกาสที่จะเกิด (P)” กำหนดได้ดังนี้

1. สูง (3) หมายถึง การมีโอกาสที่จะเกิดขึ้นมากกว่า 3 ครั้งต่อปี
2. ปานกลาง (2) หมายถึงการมีโอกาสที่จะเกิดขึ้นเกิน 1 ครั้งแต่ไม่เกิน 3 ครั้งต่อปี
3. ต่ำ (1) หมายถึง การมีโอกาสที่จะเกิดขึ้นไม่เกิน 1 ครั้งต่อปี

ความหมายของ “ระดับของผลกระทบที่เกิดขึ้น (I)” กำหนดได้ดังนี้

1. มาก (3) หมายถึง ระบบต่างๆ ที่ใช้ในการปฏิบัติงานประจำวัน (transaction processing systems) ล้มเหลวตั้งแต่ 3 วันขึ้นไป และ/หรือ ข้อมูลที่จำเป็นต้องการปฏิบัติงานประจำถูกทำให้เกิดความเสียหาย (ถูกโจรกรรม ถูกปิดกั้นการเข้าถึง หรือ ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาติ)
2. ปานกลาง (2) หมายถึง ระบบต่างๆ ที่ใช้ในการปฏิบัติงานประจำวัน (transaction processing systems) ล้มเหลวเกิน 1 ชั่วโมงแต่ไม่เกิน 2 วันขึ้นไป
3. น้อย (1) หมายถึง ระบบต่างๆ ที่ใช้ในการปฏิบัติงานประจำวัน (transaction processing systems) ล้มเหลวไม่เกิน 1 ชั่วโมง

ตารางที่ 4 ผลการจัดลำดับความสำคัญในรูปแบบเมทริกซ์ของความทนต่อความเสี่ยง (Risk Tolerance Matrix)

ระดับของโอกาสที่จะเกิด \ ระดับของผลกระทบ	1 (ต่ำ)	2 (ปานกลาง)	3 (สูง)
3 (สูง)	R15	R09	R04, R05, R07, R10, R12
2 (ปานกลาง)		ไม่มี	R02, R03, R11, R16, R18
1 (ต่ำ)	R08, R14	R01, R17	R06, R13, R19

ตารางที่ 4 แสดงให้เห็นถึงการจัดกลุ่มของความเสี่ยงตามช่วงคะแนน ซึ่งสามารถแบ่งได้เป็น 3 กลุ่มดังนี้

1. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 6 – 9 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “สูง” (สีแดง) ได้แก่ความเสี่ยงที่มีรหัส R02, R03, R04, R05, R07, R09, R10, R11, R12, R16 และ R18
2. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 3 – 4 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “ปานกลาง” (สีส้ม) ได้แก่ความเสี่ยงที่มีรหัส R06, R013, R15 และ R19
3. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 1 – 2 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “ต่ำ” (สีเขียว) ได้แก่ความเสี่ยงที่มีรหัส R01, R08, R14, R15 และ R17

การวางกลยุทธ์ในการจัดการความเสี่ยง (Risk Strategies)

จากคะแนนความเสี่ยงที่ได้รับจากการประเมิน จะต้องนำเสนอคณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศ (Management Committee) เพื่อพิจารณาถึงแนวทางการจัดการความเสี่ยงตามกลยุทธ์กรมฯ โดยกำหนดให้มีการจัดการความเสี่ยง ดังต่อไปนี้

หากระดับความเสี่ยง “สูง” และ “ปานกลาง” ไม่สามารถยอมรับได้ ต้องมีการเฝ้าระวัง ควบคุม แก้ไข และจัดการเพิ่มเติม เพื่อควบคุมความเสี่ยงไม่ให้ขยายออกไป โดยให้ดำเนินการ “ควบคุมความเสี่ยง (Controlling)”

หากระดับความเสี่ยง “ต่ำ” ความเสี่ยงนั้นอยู่ในเกณฑ์ที่ยอมรับได้ โดยให้ดำเนินการ “ยอมรับความเสี่ยง (Accepting)”

ตารางที่ 5 กลยุทธ์ในการจัดการความเสี่ยง (Risk Strategies)

ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	แนวทาง/แผนการดำเนินงาน
R01	ควบคุมความเสี่ยง (Controlling)	Availability of information processing facilities (A.17.2.1)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดให้มีแผนการบำรุงรักษาอุปกรณ์ UPS ให้สามารถใช้งานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา 2. กำหนดให้ดำเนินการจัดหาเครื่องกำเนิดไฟฟ้าฉุกเฉินเข้ามาใช้งาน และมีแผนการบำรุงรักษาอย่างต่อเนื่อง 3. กำหนดรอบระยะเวลาในการทดสอบความพร้อมใช้ของอุปกรณ์สำรอง
R02	ควบคุมความเสี่ยง (Controlling)	Access to networks and network services (A.9.1.2)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดให้มีขั้นตอนการลงทะเบียนอุปกรณ์ที่จะเข้าใช้ระบบ wireless network ของหน่วยงาน 2. กำหนดให้มีการ login ด้วยชื่อผู้ใช้ (user name) และรหัสผ่าน (password) พร้อมกับมีการเข้ารหัสลับก่อนส่งไปยัง access point เพื่อเข้าใช้ระบบ 3. เฝ้าระวังการเชื่อมต่ออุปกรณ์เข้าระบบเครือข่ายของกรมฯ และการใช้งานอุปกรณ์ดังกล่าว
R03	ควบคุมความเสี่ยง (Controlling)	Password management system (A.9.4.3)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดมาตรฐานและควบคุมการตั้งรหัสผ่านให้มีความเข้มแข็ง (strong password) ตามหลักสากล 2. กำหนดให้มีการเข้ารหัสลับของรหัสผ่านในรูปแบบของการทำ hash ก่อนจัดเก็บในระบบ และระหว่างการสื่อสาร 3. กำหนดให้มีการเข้ารหัสลับของชื่อผู้ใช้ (user name) และ รหัสผ่าน (password) ก่อนส่งระหว่างอุปกรณ์ทุกครั้ง 4. ตั้งค่าการบริหารจัดการรหัสผ่านในระบบสารสนเทศของกรมฯ ให้บังคับให้ผู้ใช้ทบทวนรหัสผ่าน/เปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสมหรือตามที่ผู้ใช้งานต้องการ
R04	ควบคุมความเสี่ยง (Controlling)	Installation of software on	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้

ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	แนวทาง/แผนการดำเนินงาน
		operational systems (A.12.5.1)	1. กำหนดระเบียบปฏิบัติในการติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์ของกรมอนามัยให้ชัดเจน 2. ใช้เครื่องมือทางด้าน IT ในการป้องกันไม่ให้มีการติดตั้งซอฟต์แวร์โดยพละการ เช่น การกำหนด Policy ผ่านระบบ AD 3. การกำหนดสิทธิ์ของผู้ใช้งานไม่ให้สามารถติดตั้งซอฟต์แวร์ได้เอง 4. การกำหนดวิธีการรับมือเมื่อมีเหตุการณ์ผู้ใช้งานละเมิดระเบียบ เช่น การกู้คืน หรือการถอดถอน 5. การให้ความรู้เกี่ยวกับความตระหนักแก่ผู้ใช้งาน
R05	ควบคุมความเสี่ยง (Controlling)	Controls against malware (A.12.2.1)	ไม่มี
R06	ควบคุมความเสี่ยง (Controlling)	Information backup (A.12.3.1)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดและสื่อสารขั้นตอนปฏิบัติในการสำรองข้อมูลระบบสารสนเทศของกรมฯ ให้ทั่วกัน 2. จัดหาเทคโนโลยีที่เหมาะสมในการสำรองข้อมูลให้ตรงตามความต้องการของกรมฯ 3. กำหนดพื้นที่หรือสถานที่ (off-site) ในการเก็บข้อมูลสำรองนอก data center โดยจะต้องมีระยะห่างจาก data center ในระยะที่มั่นใจได้ว่าหากเกิดภัยพิภัยที่ data center แล้วข้อมูลสำรองจะไม่ได้รับความเสียหาย 4. กำหนดรอบในการทดสอบข้อมูลสำรองอย่างเหมาะสมและเพียงพอ 5. กำหนดให้มีการเข้ารหัสและจัดลำดับชั้นความลับของข้อมูลสำรอง
R07	ควบคุมความเสี่ยง (Controlling)	Intellectual property rights (A.18.1.2)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดและสื่อสารนโยบายการบริหารจัดการลิขสิทธิ์ของกรมฯ ให้ทั่วถึง 2. จัดทำ Record สำหรับบันทึกรายการซอฟต์แวร์ลิขสิทธิ์ 3. สุ่มตรวจสอบซอฟต์แวร์ลิขสิทธิ์บนเครื่องคอมพิวเตอร์ที่เกี่ยวข้อง
R08	ยอมรับความเสี่ยง (Accepting)	Identification of applicable legislation and contractual	ไม่มี

ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	แนวทาง/แผนการดำเนินงาน
		requirements (A.18.1.1)	
R09	ควบคุมความเสี่ยง (Controlling)	Contact with special interest groups (A.6.1.4)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. จัดฝึกอบรมภายใน ให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ให้กับบุคลากรของกรมฯ 2. จัดส่งเข้าหน้าที่ ที่เกี่ยวข้องกับงานเทคโนโลยีสารสนเทศ อบรมการใช้เครื่องมือที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
R10	ควบคุมความเสี่ยง (Controlling)	Information Security Requirements Analysis & Specification (A.14.1.1)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดวงรอบในการอัพเดทระบบปฏิบัติการ ระบบงานต่าง ๆ ของกรม 2. ทดสอบอัพเดทระบบงาน ระบบปฏิบัติการ ก่อนทำการอัพเดทระบบงานจริง
R11	ควบคุมความเสี่ยง (Controlling)	Review of the policies for information security (A.5.1.2)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดวงรอบในการปรับปรุงค่าคอนฟิกอุปกรณ์
R12	ควบคุมความเสี่ยง (Controlling)	Technical Review of Applications After Operating Platform Changes (A.14.2.3)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ทดสอบระบบหลังจากมีการปรับปรุงระบบปฏิบัติการก่อนทำการอัพเดทระบบปฏิบัติการจริง
R13	ควบคุมความเสี่ยง (Controlling)	Asset Management (A.8)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. จัดทำรายงานสถานครุภัณฑ์ 2. วางแผนจัดหาครุภัณฑ์ทดแทน
R14	ยอมรับความเสี่ยง (Accepting)	Physical and environmental security (A.11)	ใช้มาตรการในการยอมรับความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ใช้ระบบสำรองไฟฟ้าและระบบ Generator ทดแทนขณะไฟฟ้าขัดข้อง 2. ใช้งานระบบงานสำรองที่ไซต์สำรองไฟฟ้าขัดข้องเป็นเวลานาน หรือเกิดเหตุการณ์ชุมนุม

ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	แนวทาง/แผนการดำเนินงาน
R15	ควบคุมความเสี่ยง (Controlling)	Information security incident management (A.16)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. จัดทำแผนการบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management) 2. ซักซ้อมตามขั้นตอนของแผนการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาอย่างน้อยปีละ 1 ครั้ง 3. ปฏิบัติงานตามขั้นตอนของแผนให้เป็นลำดับขั้นตอนเมื่อเกิดเหตุการณ์ผิดปกติและปัญหา
R16	ควบคุมความเสี่ยง (Controlling)	Supplier relationships (A.15)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ออกกฎข้อบังคับให้ชัดเจน และกำหนดสัญญาเรื่องการปรับหรือการฟ้องร้องเมื่อเกิดการละเมิดกฎข้อบังคับ
R17	ควบคุมความเสี่ยง (Controlling)	Information security aspects of business continuity (A.17)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. จัดทำแผน BCP 2. ซักซ้อมตามขั้นตอนการปฏิบัติของแผน BCP อย่างน้อยปีละ 1 ครั้ง
R18	ควบคุมความเสี่ยง (Controlling)	Cryptography (A.10)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ดำเนินการเข้ารหัสข้อมูลบนอุปกรณ์ External Hard drive, Flash drive 2. ดำเนินการเข้ารหัสข้อมูลอุปกรณ์ Laptop ของผู้บริหาร และ Laptop ของบุคคลากรที่มีข้อมูลสำคัญ
R19	ควบคุมความเสี่ยง (Controlling)	Human resource security (A.7)	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ดำเนินการลบข้อมูลเจ้าหน้าที่ ชื่อบัญชีผู้ใช้ ของระบบงานต่าง ๆ

<u>หมายเหตุ</u> แนวทาง/แผนดำเนินงานข้างต้นของกรมฯควรครอบคลุมไปถึงหน่วยงานในสังกัดที่อยู่ต่างจังหวัดเพื่อให้เป็นมาตรฐานเดียวกัน ซึ่งจะทำให้สามารถควบคุมและตรวจติดตามด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและประสิทธิผล