แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

กรมอนามัย
DEPARTMENT OF HEALTH

กองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย

(พ.ศ. 2566)

สารบัญ

บทนำ

เทคโนโลยีสารสนเทศมีบทบาทที่สำคัญอย่างยิ่งต่อกรมอนามัยในยุคปัจจุบัน ปัจจุบันถูกนำมาใช้เป็นเครื่องมือในการจัดการข้อมูลต่าง ๆ ให้มีคุณภาพเพื่อใช้ในการปฏิบัติงานและใช้ในการตัดสินใจของผู้บริหาร นอกจากนี้ยังถูกใช้เป็นเครื่องมือช่วยในการสื่อสารภายในกรมอนามัยให้มีประสิทธิภาพและประสิทธิผล

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

วัตถุประสงค์

1. เพื่อเป็นแนวทางในการบริหารเทคโนโลยีสารสนเทศของกรมฯให้มีความมั่นคงปลอดภัยมากขึ้น
2. เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพและประสิทธิผลมากขึ้น
3. เพื่อป้องกันความเสียหายที่เกิดจากการเหตุการณ์ที่ไม่พึงประสงค์ต่อทรัพยากรด้านสารสนเทศและมีผลต่อการดำเนินงานของกรมอนามัย
4. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบสารสนเทศ ฐานข้อมูลสารสนเทศ ให้มีเสถียรภาพและพร้อมใช้งาน
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	การดำเนินงานด้านเทคโนโลยีสารสนเทศให้เป็นไปตามข้อกฎหมายที่เกี่ยวข้อง	Identification of applicable legislation and contractual requirements (A.18.1.1)
R09	การควบคุมและกำกับการพัฒนาระบบสารสนเทศในกรมฯ ให้เป็นไปตามเกณฑ์มาตรฐานของกรมฯ	Identification of applicable legislation and contractual requirements (A.14.1.1)
R10	การมีทักษะที่ทันยุคทันสมัยทางด้านเทคโนโลยีสารสนเทศ	Contact with special interest groups (A.6.1.4)
R11	ระบบบริหารจัดการทรัพย์สิน (Asset Management)	Asset Management (A.8)
R12	การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical & Environmental Security)	Physical and environmental security (A.11)
R13	การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management)	Information security incident management (A.16)
R14	การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)	Supplier relationships (A.15)

รหัสความเสี่ยง	ความเสี่ยง	มาตรการควบคุมของ ISO/IEC 27001: 2013
R15	การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity)	Information security aspects of business continuity (A.17)
R16	การเข้ารหัสข้อมูล (Cryptography)	Cryptography (A.10)
R17	การบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)	Human resource security (A.7)
R18	การจัดการข้อมูลส่วนบุคคล (PDPA)	Compliance (A.18)

ตารางที่ 2 รายละเอียดของความเสี่ยง (ปัจจัยและผลกระทบ)

รหัสความเสี่ยง	ความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R01	ความพร้อมใช้งานอย่างต่อเนื่อง (availability) ของระบบสารสนเทศภายในศูนย์ข้อมูลกลาง (data center)	ระบบสารสนเทศของกรมฯ ส่วนใหญ่ถูกติดตั้งไว้ที่ศูนย์ข้อมูลกลาง (data center) ของกรมฯ ศูนย์ข้อมูลกลางนี้มีระบบไฟฟ้าสำรองที่เก็บไว้ใน UPS เพื่อใช้ในกรณีไฟฟ้าล้มเหลว อย่างไรก็ตาม ถ้าระบบไฟฟ้าล้มเหลวเป็นเวลานานแล้วไฟฟ้าสำรองดังกล่าวจะไม่สามารถเลี้ยงอุปกรณ์ต่างๆ ได้อย่างเพียงพอ เมื่อไฟฟ้าสำรองหมดลง การทำงานของระบบสารสนเทศทั้งหมดก็จะล้มเหลว และมีผลกระทบต่อการดำเนินงานของกรมฯ	1. การทำงานตามภารกิจของกรมฯ ในส่วนที่ต้องพึงพาระบบสารสนเทศต้องหยุดชะงักและมีผลกระทบต่อการให้บริการประชาชน 2. ประชาชนไม่สามารถใช้บริการของกรมฯ ผ่านระบบเครือข่ายอินเตอร์เน็ตได้ 3. การสื่อสารของกรมฯ ที่ต้องใช้ระบบเครือข่ายไม่สามารถทำได้
R02	การเข้าถึงระบบเครือข่ายและเครือข่ายไร้สาย (wireless network) ของกรมฯ	กรมฯ มีการติดตั้งระบบเครือข่ายไร้สาย (wireless network) เพื่อให้ผู้ปฏิบัติงานของกรมฯ สามารถเข้าถึงการใช้บริการด้านสารสนเทศได้อย่างมีประสิทธิภาพและประสิทธิผลมากขึ้น อย่างไรก็ตามในกระบวนการของการยืนยันตัวบุคคล (authentication) เพื่อเข้าใช้บริการยังมีช่องโหว่ซึ่งจะทำให้ผู้ไม่ประสงค์ดีสามารถปลอมแปลงตัวตนเพื่อเข้ามาใช้บริการได้ o ผู้ใช้ระดับปฏิบัติการ ใช้วิธีการ login ด้วย ชื่อผู้ใช้ (username) และ รหัสผ่าน (password) ซึ่งกระบวนการนี้ไม่มีการเข้ารหัสลับ	1. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจใช้งานอินเตอร์เน็ตของกรมฯ ในการทำสิ่งที่ผิดกฎหมาย เช่น โพสต์ข้อความหมิ่นประมาทผู้อื่น หรือ บุกรุกระบบเครือข่ายขององค์กรอื่น ๆ อีก ซึ่งอาจจะมีผลทำให้กรมฯต้องรับผิดชอบทางกฎหมายและสูญเสียภาพลักษณ์ของกรมฯได้ 2. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจขโมยข้อมูล ดัดแปลงข้อมูลหรือทำลายข้อมูลที่สามารถเข้าถึงได้ ซึ่งอาจจะทำให้ข้อมูลที่ใช้ในการปฏิบัติงานเสียหายได้

รหัสความเสี่ยง	ความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
		(encryption) นอกจากนี้ การเข้าใช้ไม่จำเป็นต้องลงทะเบียนอุปกรณ์ที่จะใช้ o ผู้ใช้ระดับผู้บริหาร ใช้วิธีการลงทะเบียนอุปกรณ์ที่จะใช้และไม่ต้องทำการ login ใดๆ	3. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจลักลอบเข้าไปในระบบบริหารจัดการเครือข่ายเพื่อให้ได้สิทธิ์ในการควบคุมเครือข่ายไร้สายดังกล่าวได้
R03	ระบบการบริหารจัดการรหัสผ่าน (password management system)	กรมฯ ได้มีการกำหนดการใช้ชื่อผู้ใช้และรหัสผ่านเป็นการทำการยืนยันตัวบุคคลเพื่อเข้าใช้ทรัพยากรด้านสารสนเทศของกรมฯ อย่างไรก็ตาม การบริหารจัดการรหัสผ่าน (password management) ยังไม่เป็นระบบที่เป็นมาตรฐานและสามารถเป็นช่องโหว่ให้ผู้บุกรุกสามารถคาดเดารหัสผ่าน รวมทั้งการโจรกรรมรหัสผ่านได้ เช่น ข้อกำหนดในการตั้งรหัสผ่านที่สามารถป้องกันการตั้งรหัสผ่านที่อ่อนแอ (weak password) ได้ หรือ ข้อกำหนดในการจัดเก็บรหัสผ่านด้วยการเข้ารหัสลับ (encrypted passwords) ก่อนจัดเก็บในหน่วยความจำสำรอง (secondary storage) หรือ ข้อกำหนดในการสื่อสารข้อมูลที่เป็นรหัสผ่านที่ส่งระหว่างอุปกรณ์เพื่อป้องกันการแอบดักขโมย หรือ ข้อกำหนดในการปรับเปลี่ยนและตรวจสอบการใช้รหัสผ่านที่มากับอุปกรณ์ (default passwords)	1. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาครอบครองและควบคุมทรัพยากรด้านสารสนเทศกรมฯ ในการทำสิ่งต่างๆที่ไม่พึงประสงค์ 2. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจขโมยข้อมูลที่เป็นความลับ ดัดแปลงข้อมูลหรือทำลายข้อมูลที่สามารถเข้าถึงได้ ซึ่งอาจจะทำให้ข้อมูลที่ใช้ในการปฏิบัติงานเสียหายและไม่สามารถใช้งานได้ (confidentiality, integrity and availability) 3. ผู้ไม่ประสงค์ดีที่บุกรุกเข้ามาอาจลักลอบเข้าไปในระบบบริหารจัดการเครือข่ายเพื่อให้ได้สิทธิ์ในการควบคุมระบบเครือข่ายและอุปกรณ์ต่างๆ ได้
R04	การติดตั้งซอฟต์แวร์ภายในกรมฯ	ผู้ใช้งาน (end-users) สามารถที่จะติดตั้งซอฟต์แวร์ต่างๆ รวมทั้งการติดตั้งเครื่องแม่ข่าย ได้เองโดยไม่มีกระบวนการในการควบคุม (control of operational software) ซอฟต์แวร์ที่สามารถติดตั้งได้เองนี้เป็นทั้งซอฟต์แวร์ระบบ (system software) ซอฟต์แวร์ประยุกต์ (application software) รวมถึงซอฟต์แวร์อรรถประโยชน์ใดๆ (utility software)	1. การติดตั้งซอฟต์แวร์บางอย่างอาจทำให้ไม่สามารถควบคุมการรักษาความลับข้อมูลของกรมฯ ได้ 2. การติดตั้งอาจมีการเปลี่ยนแปลงการกำหนดค่ารูปแบบการทำงาน (configuration) ของอุปกรณ์และอาจจะมีผลทำให้เกิดปัญหากับการทำงานของซอฟต์แวร์ตัวอื่นๆ

รหัสความเสี่ยง	ความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
			3. การติดตั้งซอฟต์แวร์โดยไม่คำนึงถึงเรื่องลิขสิทธิ์ ซึ่งอาจจะทำให้กรมฯถูกฟ้องร้องและเกิดความเสียหายได้ 4. ซอฟต์แวร์ที่ถูกนำมาติดตั้งอาจติดไวรัสหรือซอฟต์แวร์ที่ไม่พึงประสงค์ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลและซอฟต์แวร์อื่นๆ
R05	การป้องกันซอฟต์แวร์ไม่พึงประสงค์ (malicious software)	ผู้ใช้งาน (end users) ค่อนข้างมีอิสระสูงในการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศของกรมฯ ดังนั้น ถ้าหากผู้ใช้งานขาดความระมัดระวังอาจจะส่งผลทำให้ซอฟต์แวร์ที่ไม่พึงประสงค์ (malicious software หรือ malware) สามารถเข้าสู่ระบบคอมพิวเตอร์และแพร่กระจายผ่านระบบเครือข่ายได้ ปัจจุบัน ซอฟต์แวร์ที่ไม่พึงประสงค์ดังกล่าวอาจจะผ่านเข้ามาทาง e-mail, social media, thumb-drive หรือ ซอฟต์แวร์ที่นำมาติดตั้ง	1. การใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศอาจจะไม่มีประสิทธิภาพ เช่น เครื่องคอมพิวเตอร์หรือระบบเครือข่ายทำงานช้าลง และส่งผลต่อประสิทธิภาพของงาน 2. ข้อมูลอาจจะถูกขโมยออกไปหรืออาจจะถูกทำลายหรืออาจจะถูกปิดกั้นไม่ให้สามารถเข้าถึงได้ 3. ซอฟต์แวร์ที่ใช้งานจริงที่ติดตั้งบนเครื่องคอมพิวเตอร์อาจจะถูกทำให้ใช้งานไม่ได้
R06	การสำรองข้อมูลและซอฟต์แวร์ประยุกต์ที่จัดเก็บอยู่ที่ data center ของกรมฯ และที่ส่วนอื่นๆ	ข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่ายที่ตั้งอยู่ที่ศูนย์ข้อมูลกลางได้ถูกสำเนาเก็บไว้ตามช่วงเวลาที่กำหนด อย่างไรก็ตาม ตัวสำเนาดังกล่าวกลับถูกเก็บไว้ที่ศูนย์ข้อมูลกลางเช่นเดียวกัน ดังนั้นถ้าหากเกิดไฟไหม้หรือน้ำท่วมที่ศูนย์ข้อมูลกลางแล้ว ตัวข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่าย รวมทั้งสำเนาของมันก็จะเกิดความเสียหายไปด้วยกัน นอกจากนี้ เครื่องแม่ข่ายของบางหน่วยงานก็ไม่ได้ถูกเก็บไว้ที่ศูนย์ข้อมูลกลาง ข้อมูลและซอฟต์แวร์ประยุกต์บนเครื่องแม่ข่ายดังกล่าวจึงอาจจะไม่ได้ถูกสำเนาเก็บไว้	1. กรณีที่หน่วยเก็บข้อมูลสำรอง (secondary storage) ของเครื่องแม่ข่ายเกิดความเสียหายและไม่มีสำเนาเก็บไว้ จะมีผลทำให้ข้อมูลสูญหายและซอฟต์แวร์ประยุกต์ไม่สามารถใช้งานได้อีก ถ้าเป็นระบบที่สำคัญต่อการทำธุรกรรมของหน่วยงาน ก็จะมีผลต่อการดำเนินงานทันที 2. กรณีที่เกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อศูนย์ข้อมูลกลาง เช่น ไฟไหม้ จะมีผลทำให้ข้อมูลสูญหายและซอฟต์แวร์ประยุกต์ไม่สามารถใช้งานได้อีก ถ้าเป็นระบบที่สำคัญต่อการทำธุรกรรมของหน่วยงานต่างๆ ก็จะมีผลต่อการดำเนินงานของหน่วยงานเหล่านั้นทันที

รหัสความเสี่ยง	ความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R07	การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์	การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ยังมีโอกาสเกิดขึ้นได้ในกรมฯ ทั้งนี้เนื่องจากการขาดการสร้างความตระหนักในผลลัพธ์ที่จะเกิดขึ้น รวมทั้งการขาดกลไกในการควบคุมและติดตาม จากการตรวจสอบพบว่ายังคงมีการใช้ระบบปฏิบัติการ (operating systems) ที่ไม่มีใบอนุญาต (license) อยู่	1. การใช้ระบบปฏิบัติการที่ไม่มีใบอนุญาตมีผลทำให้ขาดการบำรุงรักษาจากผู้ผลิตและอาจจะมีผลทำให้เกิดช่องโหว่ในระบบคอมพิวเตอร์ที่ผู้ไม่ประสงค์ดีอาจจะบุกรุกเข้ามาได้และสร้างความเสียหายให้กับระบบ รวมทั้งการโจรกรรมข้อมูลต่างๆ 2. การใช้ระบบปฏิบัติการที่ไม่มีใบอนุญาตเป็นสิ่งที่ผิดกฎหมายและอาจจะถูกฟ้องร้องเรียกค่าเสียหายได้ ซึ่งจะทำให้กรมฯต้องสูญเสียค่าใช้จ่ายสูงและสูญเสียภาพลักษณ์ของกรมฯ 3. ซอฟต์แวร์ที่ผิดกฎหมายอาจจะมาพร้อมกับ malware เช่น virus หรือ spyware ซึ่งสามารสร้างความเสียหายให้กับข้อมูลและทรัพยากรด้านสารสนเทศได้
R08	การดำเนินงานด้านเทคโนโลยีสารสนเทศให้เป็นไปตามข้อกฎหมายที่เกี่ยวข้อง	การดำเนินงานด้านเทคโนโลยีสารสนเทศต้องเป็นไปตามข้อกำหนดทางกฎหมาย เช่น การสร้าง log file บนเครื่องแม่ข่าย เนื่องจากกรมฯ มีหน่วยงานที่อยู่ต่างจังหวัดด้วย จึงทำให้ยังไม่สามารถควบคุมและติดตามการดำเนินงานทั้งหมดให้เป็นไปตามข้อกำหนดทางกฎหมายได้	การไม่เก็บ log file เป็นการกระทำผิดตาม พ.ร.บ ว่าด้วยเรื่องกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ซึ่งมีโทษปรับค่อนข้างสูงและทำให้เสียภาพลักษณ์ของกรมฯ
R09	การควบคุมและกำกับการพัฒนาระบบสารสนเทศในกรมฯ ให้เป็นไปตามเกณฑ์มาตรฐานของกรมฯ	การพัฒนาระบบสารสนเทศในกรมฯ เป็นลักษณะที่ผู้ใช้งาน (end-users) สามารถจัดหาหรือจัดจ้างได้เอง รวมทั้งสามารถพัฒนาระบบขึ้นมาเองด้วย ถึงแม้ว่ากรมฯ มีเอกสารที่กำหนดรูปแบบของการพัฒนาระบบฯ แต่ยังขาดควบคุมและกำกับดูแลจากศูนย์เทคโนโลยีสารสนเทศ และบางครั้งบริษัทภายนอกก็สามารถเข้ามาจัดการกับระบบของตนเองโดยผ่านระบบเครือข่ายของกรมฯ เข้ามา	1. การพัฒนาระบบไม่เป็นไปตามรูปแบบการพัฒนาระบบที่กรมฯ ได้กำหนดไว้และอาจส่งผลให้คุณภาพระบบรวมถึงความมั่นคงปลอดภัยของระบบไม่เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของกรมฯ และอาจมีความเสี่ยงต่อการถูกผู้ไม่ประสงค์ดีโจมตีผ่านทางช่องโหว่ของระบบ

รหัสความเสี่ยง	ความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
			2. บริษัทภายนอกสามารถเข้ามากำหนดรูปแบบการทำงานของระบบผ่าน VPN ซึ่งไม่มีกระบวนการในการควบคุมการดำเนินงานดังกล่าวและอาจจะเกิดช่องโหว่ด้านความมั่นคงของระบบเครือข่ายได้ 3. การเชื่อมโยงระบบเพื่อใช้ประโยชน์จากข้อมูลทำได้ยาก 4. การเกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบต่างๆ ภายในกรมฯ
R10	การมีทักษะที่ทันยุคทันสมัยทางด้านเทคโนโลยีสารสนเทศ	เทคโนโลยีสารสนเทศมีความก้าวหน้าและเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งเครื่องมือและเทคนิคใหม่ ๆ ที่มีการพัฒนาอยู่ตลอดเวลา ซึ่งสิ่งที่เกิดขึ้นดังกล่าวทำให้บุคลากรที่ดูแลด้านเทคโนโลยีสารสนเทศไม่สามารถติดตามและรู้ทันผู้ที่ไม่ประสงค์ดีในการบุกรุกเข้าสู่ระบบเครือข่ายได้ รวมทั้งไม่รู้จักเครื่องมือและเทคนิคใหม่ ๆ ที่มีประสิทธิภาพและประสิทธิผลการรับมือการโจมตีได้อย่างทันท่วงที	1. ผู้ไม่ประสงค์ดีสามารถโจมตีระบบได้สำเร็จและมีผลต่อการปฏิบัติงานและการให้บริการประชาชนของ กรมฯ 2. การบุกรุกเข้ามาใช้ประโยชน์จากทรัพยากรด้านสารสนเทศโดยเฉพาะอย่างยิ่งเครื่องแม่ข่ายที่มีช่องโหว่ เพื่อไว้ใช้ในการโจมตีเครื่องอื่นๆ เช่น การทำ Remote Execution หรือ DDOS ซึ่งนอกจากจะทำให้ประสิทธิภาพของทรัพยากรลดลงแล้ว ยังอาจจะทำให้เสียภาพลักษณ์ของกรมฯ อีกด้วย
R11	การบริหารจัดการทรัพย์สิน (Asset Management)	ผลิตภัณฑ์ End of Support หรือ End of Life ทำให้อาจพบช่องโหว่ และเกิดการโจมตีระบบสารสนเทศได้	1. ทำให้เกิดช่องโหว่ของระบบสารสนเทศต่าง ๆ และอาจเกิดการโจมตีระบบสารสนเทศที่ End of Support หรือ End of Life 2. อาจโดนขโมยข้อมูล เพื่อเรียกค่าไถ่หรือยึดระบบงานทำให้ระบบงานไม่สามารถใช้งานได้
R12	การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical & Environmental Security)	1. ระบบไฟฟ้าขัดข้อง อาจทำให้ไม่สามารถใช้งานหรือให้บริการระบบงานสารสนเทศได้อย่างต่อเนื่อง 2. เกิดการชุมนุม ยึดพื้นที่ทำให้ไม่สามารถใช้งานหรือให้บริการระบบงานสารสนเทศได้	1. ทำให้ระบบงานหรือการให้บริการหยุดชะงัก เมื่อเกิดเหตุไฟฟ้าขัดข้อง 2. อาจทำให้ไม่สามารถให้บริการหรือใช้งานระบบงานได้ เนื่องจากอาจโดนผู้ชุมนุมบุกยึดสถานที่

รหัสความเสี่ยง	ความเสี่ยง	สาเหตุของความเสี่ยง/ปัจจัยที่ทำให้เกิดความเสี่ยง	ผลกระทบ
R13	การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management)	ปัญหาของซอฟต์แวร์ อุปกรณ์ต่อพ่วง เนื่องจากระบบปฏิบัติการอัพเดท ระบบงานช้าไม่สามารถให้บริการได้	1. ทำให้ผู้ใช้งานเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ 2. ระบบงานไม่สามารถให้บริการได้
R14	การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)	การลักลอบนำข้อมูลความลับไปเปิดเผย โจมตีระบบงานได้ หากมีข้อขัดแย้งกับผู้บังคับบัญชา	1. ข้อมูลที่เป็นความลับถูกเปิดเผย 2. ข้อมูลสูญหาย ทำให้ระบบไม่สามารถใช้งานได้
R15	การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity)	ไม่ได้ทำการซักซ้อมการทบทวบกระบวนการตามแผนที่ได้วางไว้	1. อาจทำให้ระบบสำรอง ทำงานได้ล่าช้ากว่าแผนที่วางไว้ 2. อาจทำให้ระบบสำรองไม่สามารถทำงานได้เนื่องจากไม่ได้มีการทดสอบการกู้คืนระบบ
R16	การเข้ารหัสข้อมูล (Cryptography)	ข้อมูลชั้นความลับไม่มีการเข้ารหัสข้อมูล	1. อาจทำให้ข้อมูลที่เป็นชั้นความลับถูกเปิดเผยสู่สาธารณะ
R17	การบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)	ไม่ได้ทำการลบผู้ใช้ สำหรับระบบงานออกจากระบบทำให้เจ้าหน้าที่ที่ได้ลาออก สามารถเข้าถึงข้อมูลหรือระบบงานได้	1. อาจทำให้ข้อมูลที่เป็นชั้นความลับถูกเปิดเผยสู่สาธารณะ
R18	การจัดการข้อมูลส่วนบุคคล (PDPA)	ปัญหาการจัดเก็บและทำลายข้อมูลส่วนบุคคล	1. อาจทำให้ข้อมูลส่วนบุคคลถูกขโมยและเปิดเผย

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	3	5	15
R02	5	5	25
R03	5	5	25
R04	3	4	12
R05	4	5	20
R06	5	4	20
R07	5	5	25
R08	4	5	20
R09	1	4	4
R10	3	4	12
R11	4	4	16
R12	2	4	8
R13	3	5	15
R14	1	4	4
R15	3	4	12
R16	4	5	20
R17	2	4	8
R18	4	4	16

หมายเหตุ (อธิบายความหมายของคำในตารางที่ 3)

ความหมายของ “ระดับของโอกาสที่จะเกิด (P)” กำหนดได้ดังนี้

ระดับ	โอกาส	คำอธิบาย
5	สูง	เกิน 10 ครั้งต่อปี
4	ค่อนข้างสูง	ไม่เกิน 10 ครั้งต่อปี
3	ปานกลาง	ไม่เกิน 5 ครั้งต่อปี
2	ค่อนข้างน้อย	ไม่เกิน 3 ครั้งต่อปี
1	น้อย	ไม่เกิน 1 ครั้งต่อปี

ความหมายของ “ระดับของผลกระทบที่เกิดขึ้น (I)” กำหนดได้ดังนี้

ระดับ	โอกาส	คำอธิบาย
5	สูง	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	ค่อนข้างสูง	ระบบมีปัญหาและมีความสูญเสียค่อนข้างมาก
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	ค่อนข้างน้อย	เกิดเหตุร้ายที่ค่อนข้างมีความสำคัญ
1	น้อย	เกิดเหตุร้ายที่ไม่มีความสำคัญ

ตารางที่ 4 ผลการจัดลำดับความสำคัญในรูปแบบเมทริกซ์ของความทนต่อความเสี่ยง (Risk Tolerance Matrix)

ผลกระทบ	ต่ำ	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง	สูง
สูง			R1, R13	R5, R8, R16	R2, R3, R7
ค่อนข้างสูง	R9, R14	R12, R17	R4, R10, R15	R11, R18	R6
ปานกลาง					
ค่อนข้างต่ำ					
ต่ำ					

จากตารางที่ 4 แสดงให้เห็นถึงการจัดกลุ่มของความเสี่ยงตามช่วงคะแนน ซึ่งสามารถแบ่งได้เป็น 5 กลุ่มดังนี้

1. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 21 – 25 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “สูง” (แดงเข้ม) ได้แก่ความเสี่ยงที่มีรหัส R1, R3 และ R7
2. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 16 – 20 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “ค่อนข้างสูง” (สีแดง) ได้แก่ความเสี่ยงที่มีรหัส R5, R6, R8, R11, R16 และ R18
3. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 11 – 15 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “ปานกลาง” (สีส้ม) ได้แก่ความเสี่ยงที่มีรหัส R1, R4, R10, R13 และ R15
4. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 6 – 10 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “ค่อนข้างต่ำ” (สีเหลือง) ได้แก่ความเสี่ยงที่มีรหัส R12 และ R17
5. กลุ่มของความเสี่ยงที่มีคะแนนอยู่ในช่วง 1 – 5 คะแนน ซึ่งถือว่ามีระดับความเสี่ยง “ต่ำ” (สีเขียว) ได้แก่ความเสี่ยงที่มีรหัส R9 และ R14

1.3 การวางกลยุทธ์ในการจัดการความเสี่ยง (Risk Strategies)

จากคะแนนความเสี่ยงที่ได้รับจากการประเมิน จะต้องนำเสนอคณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศ (Management Committee) เพื่อพิจารณาถึงแนวทางการจัดการความเสี่ยงตามกลยุทธ์กรมฯ โดยกำหนดให้มีการจัดการความเสี่ยง ดังต่อไปนี้

หากระดับความเสี่ยง “สูง” “ค่อนข้างสูง” และ “ปานกลาง” ไม่สามารถยอมรับได้ ต้องมีการเฝ้าระวัง ควบคุม แก้ไข และจัดการเพิ่มเติมเพื่อควบคุมความเสี่ยงไม่ให้ขยายออกไป โดยให้ดำเนินการ “ควบคุมความเสี่ยง (Controlling)”

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

ตารางที่ 5 กลยุทธ์ในการจัดการความเสี่ยง (Risk Strategies)

รหัสความเสี่ยง	ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	ผู้รับผิดชอบ	แนวทาง/แผนการดำเนินงาน
R01	ความพร้อมใช้งานอย่างต่อเนื่อง (availability) ของระบบสารสนเทศภายในศูนย์ข้อมูลกลาง (data center)	ควบคุมความเสี่ยง (Controlling)	Availability of information processing facilities (A.17.2.1)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดให้มีแผนการบำรุงรักษาอุปกรณ์ UPS ให้สามารถใช้งานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา 2. กำหนดรอบระยะเวลาในการทดสอบความพร้อมใช้ของอุปกรณ์สำรอง
R02	การเข้าถึงระบบเครือข่ายและเครือข่ายไร้สาย (wireless network) ของกรมฯ	ควบคุมความเสี่ยง (Controlling)	Access to networks and network services (A.9.1.2)	เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดให้มีขั้นตอนการลงทะเบียนอุปกรณ์ที่จะเข้าใช้ระบบ wire/wireless network ของหน่วยงาน 2. กำหนดให้มีการ login ด้วยชื่อผู้ใช้ (username) และ รหัสผ่าน (password) พร้อมกับมีการเข้ารหัสลับก่อนส่งไปยัง access point เพื่อเข้าใช้ระบบ 3. เฝ้าระวังการเชื่อมต่ออุปกรณ์เข้าระบบเครือข่ายของกรมฯ และการใช้งานอุปกรณ์ดังกล่าว
R03	ระบบการบริหารจัดการรหัสผ่าน (password management system)	ควบคุมความเสี่ยง (Controlling)	Password management system (A.9.4.3)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดมาตรฐานและควบคุมการตั้งรหัสผ่านให้มีความเข้มแข็ง (strong password) ตามหลักสากล

รหัสความเสี่ยง	ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	ผู้รับผิดชอบ	แนวทาง/แผนการดำเนินงาน
					2. กำหนดให้มีการเข้ารหัสลับของรหัสผ่านในรูปแบบของการทำ hash ก่อนจัดเก็บในระบบ และระหว่างการสื่อสาร 3. กำหนดให้มีการเข้ารหัสลับของชื่อผู้ใช้ (username) และรหัสผ่าน (password) ก่อนส่งระหว่างอุปกรณ์ทุกครั้ง 4. ตั้งค่าการบริหารจัดการรหัสผ่านในระบบสารสนเทศของกรมฯ ให้บังคับให้ผู้ใช้ทบทวนรหัสผ่าน/เปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสมหรือตามที่ผู้ใช้งานต้องการ
R04	การติดตั้งซอฟต์แวร์ภายในกรมฯ	ควบคุมความเสี่ยง (Controlling)	Installation of software on operational systems (A.12.5.1)	เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดระเบียบปฏิบัติในการติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์ของกรมอนามัยให้ชัดเจน 2. ใช้เครื่องมือทางด้าน IT ในการป้องกันไม่ให้มีการติดตั้งซอฟต์แวร์โดยพละการ เช่น การกำหนด Policy ผ่านระบบ AD 3. การกำหนดสิทธิ์ของผู้ใช้งานไม่ให้สามารถติดตั้งซอฟต์แวร์ได้เอง 4. การกำหนดวิธีการรับมือเมื่อมีเหตุการณ์ผู้ใช้งานละเมิดระเบียบ เช่น การกู้คืน หรือการถอดถอน 5. การให้ความรู้เกี่ยวกับความตระหนักแก่ผู้ใช้งาน
R05	การป้องกันซอฟต์แวร์ไม่พึงประสงค์ (malicious software)	ควบคุมความเสี่ยง (Controlling)	Controls against malware (A.12.2.1)	เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ตัดการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่ติด Malware 2. ทำการค้นหา Malware จากโปรแกรม Endpoint และ Clean เครื่องคอมพิวเตอร์

รหัสความเสี่ยง	ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	ผู้รับผิดชอบ	แนวทาง/แผนการดำเนินงาน
					3. หากไม่สามารถ Clean ได้ให้ดำเนินการติดตั้งระบบปฏิบัติการใหม่
R06	การสำรองข้อมูลและซอฟต์แวร์ประยุกต์ที่จัดเก็บอยู่ที่ data center ของกรมฯ และที่ส่วนอื่นๆ	ควบคุมความเสี่ยง (Controlling)	Information backup (A.12.3.1)	เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ทำการกู้คืนข้อมูล 2. ทำการสลับไปใช้ระบบงานที่ไซต์สำรอง
R07	การใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์	ควบคุมความเสี่ยง (Controlling)	Intellectual property rights (A.18.1.2)	เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดและสื่อสารนโยบายการบริหารจัดการลิขสิทธิ์ของกรมฯ ให้ทั่วถึง 2. จัดทำ Record สำหรับบันทึกรายการซอฟต์แวร์ลิขสิทธิ์ 3. สุ่มตรวจสอบซอฟต์แวร์ลิขสิทธิ์บนเครื่องคอมพิวเตอร์ที่เกี่ยวข้อง
R08	การดำเนินงานด้านเทคโนโลยีสารสนเทศให้เป็นไปตามข้อกฎหมายที่เกี่ยวข้อง	ควบคุมความเสี่ยง (Controlling)	Identification of applicable legislation and contractual requirements (A.18.1.1)	เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ทำการค้นหา Log File ของผู้กระทำความผิด
R09	การควบคุมและกำกับการพัฒนาระบบสารสนเทศในกรมฯ ให้เป็นไปตามเกณฑ์มาตรฐานของกรมฯ	ยอมรับความเสี่ยง (Accepting)	Information security requirements analysis and specification (A.14.1.1)	หัวหน้าฝ่าย	ใช้มาตรการในการยอมรับความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. สื่อสารระเบียบปฏิบัติเกี่ยวกับรูปแบบการพัฒนาระบบของกรมฯ ให้ทราบโดยทั่วกัน 2. สุ่มตรวจสอบ TOR หรือเกณฑ์การพัฒนาระบบของแต่ละหน่วยงาน

รหัสความเสี่ยง	ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	ผู้รับผิดชอบ	แนวทาง/แผนการดำเนินงาน
R10	การมีทักษะที่ทันยุคทันสมัยทางด้านเทคโนโลยีสารสนเทศ	ควบคุมความเสี่ยง (Controlling)	Contact with special interest groups (A.6.1.4)	หัวหน้าฝ่าย	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. กำหนดช่องทางต่างๆ สำหรับติดต่อกับกลุ่มบุคคล องค์กร หรือหน่วยงานทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ 2. จัดอบรมฝึกทักษะให้กับเจ้าหน้าที่ในองค์กร
R11	การบริหารจัดการทรัพย์สิน (Asset Management)	ควบคุมความเสี่ยง (Controlling)	Asset Management (A.8)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. จัดทำรายงานสถานครุภัณฑ์ 2. วางแผนจัดหาครุภัณฑ์ทดแทน
R12	การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical & Environmental Security)	ยอมรับความเสี่ยง (Accepting)	Physical and environmental security (A.11)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการยอมรับความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ใช้ระบบสำรองไฟฟ้าและระบบ Generator ทดแทนขณะไฟฟ้าขัดข้อง 2. ใช้งานระบบงานสำรองที่ไซต์สำรองไฟฟ้าขัดข้องเป็นเวลานาน หรือเกิดเหตุการณ์ชุมนุม
R13	การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management)	ควบคุมความเสี่ยง (Controlling)	Information security incident management (A.16)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. จัดทำแผนการบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management) 2. ซักซ้อมตามขั้นตอนของแผนการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาอย่างน้อยปีละ 1 ครั้ง 3. ปฏิบัติงานตามขั้นตอนของแผนให้เป็นลำดับขั้นตอนเมื่อเกิดเหตุการณ์ผิดปกติและปัญหา
R14	การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)	ยอมรับความเสี่ยง (Accepting)	Supplier relationships (A.15)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการยอมรับความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ออกกฎข้อบังคับให้ชัดเจน และกำหนดสัญญาเรื่องการปรับหรือการฟ้องร้องเมื่อเกิดการละเมิดกฎข้อบังคับ

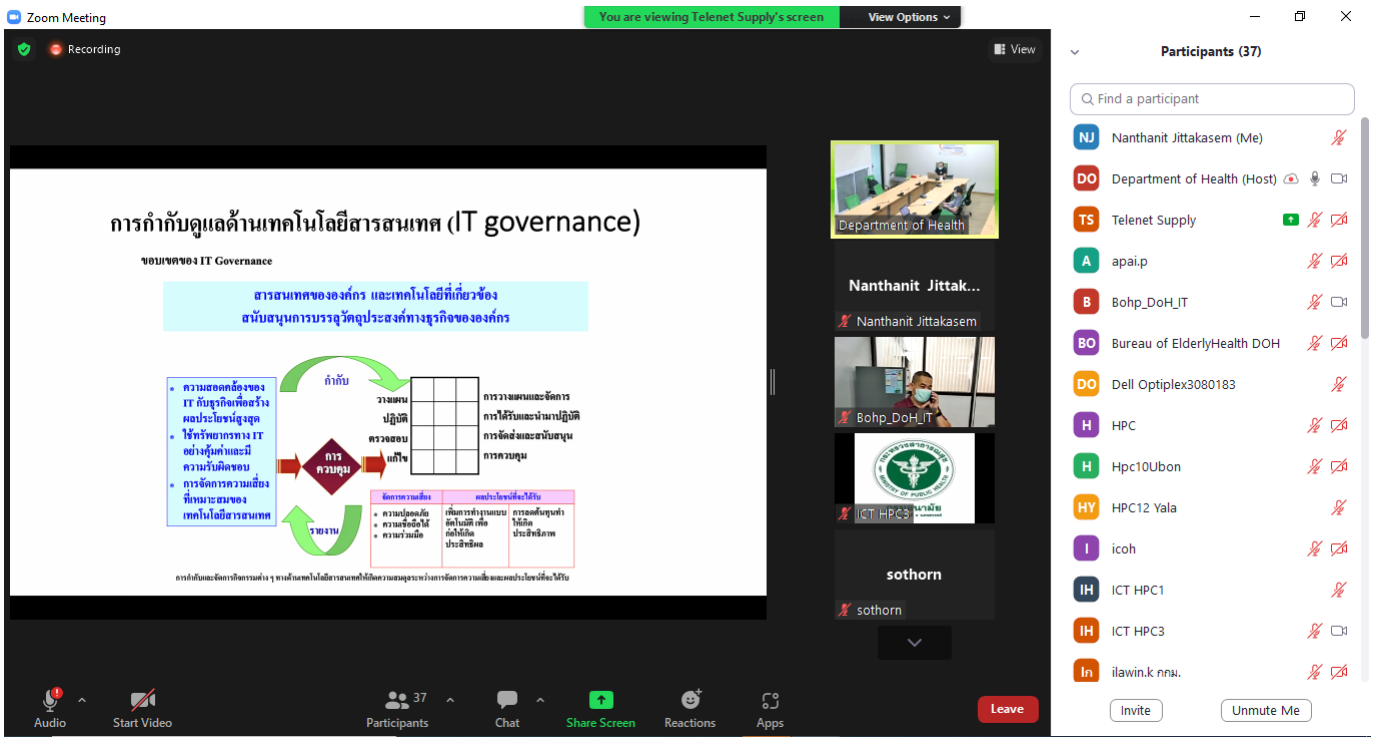
รหัสความเสี่ยง	ความเสี่ยง	กลยุทธ์	มาตรการควบคุม ISO/IEC 27001:2013	ผู้รับผิดชอบ	แนวทาง/แผนการดำเนินงาน
R15	การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Continuity)	ควบคุมความเสี่ยง (Controlling)	Information security aspects of business continuity (A.17)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. จัดทำแผน BCP 2. ซักซ้อมตามขั้นตอนการปฏิบัติของแผน BCP อย่างน้อยปีละ 1 ครั้ง
R16	การเข้ารหัสข้อมูล (Cryptography)	ควบคุมความเสี่ยง (Controlling)	Cryptography (A.10)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ดำเนินการเข้ารหัสข้อมูลบนอุปกรณ์ External Hard drive, Flash drive 2. ดำเนินการเข้ารหัสข้อมูลอุปกรณ์ Laptop ของผู้บริหาร และ Laptop ของบุคลากรที่มีข้อมูลสำคัญ
R17	การบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)	ยอมรับความเสี่ยง (Accepting)	Human resource security (A.7)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการยอมรับความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ดำเนินการลบข้อมูลเจ้าหน้าที่ ชื่อบัญชีผู้ใช้ ของระบบงานต่าง ๆ
R18	การจัดการข้อมูลส่วนบุคคล (PDPA)	ควบคุมความเสี่ยง (Controlling)	Compliance (A.18)	หัวหน้าฝ่าย, เจ้าหน้าที่ปฏิบัติการ	ใช้มาตรการในการควบคุมความเสี่ยงด้วยแนวทางการดำเนินงานต่อไปนี้ 1. ดำเนินการลบข้อมูลส่วนบุคคลตาม Consent ที่ระบุไว้ 2. กำหนดนโยบายการเข้าถึงข้อมูลส่วนบุคคลให้ชัดเจน

หมายเหตุ แนวทาง/แผนดำเนินงานข้างต้นของกรมฯควรครอบคลุมไปถึงหน่วยงานในสังกัดที่อยู่ต่างจังหวัดเพื่อให้เป็นมาตรฐานเดียวกัน ซึ่งจะทำให้สามารถควบคุมและตรวจติดตามด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและประสิทธิผล

การประชุมแผนบริหารความเสี่ยง
ด้านเทคโนโลยีและสื่อสารครั้งที่ 1

รูปภาพการประชุม Conference แผนบริหารความเสี่ยงด้านเทคโนโลยีและสื่อสารครั้งที่ 1

เนื่องจากสถาการณ์แพร่ระบาดของไวรัส Covid-19 ทางบริษัทจริงจัดประชุมผ่าน Video Conference



ซึ่งมีผู้เข้าร่วมประชุมทั้งหมด 37 คน

Information Service and Consultant Co., Ltd
55/108 KamPhaengPhet 6 Rd., Ladyao, Chatuchak, Bangkok 10900
Tel: (66) 0-2158-1188 Fax: (66) 0-2158-1189

การประชุมแผนบริหารความเสี่ยง

ด้านเทคโนโลยีและสื่อสารครั้งที่ 2

Information Service and Consultant Co., Ltd
55/108 KamPhaengPhet 6 Rd., Ladyao, Chatuchak, Bangkok 10900
Tel: (66) 0-2158-1188 Fax: (66) 0-2158-1189

รูปภาพบรรยากาศการประชุมแผนบริหารความเสี่ยงด้านเทคโนโลยีและสื่อสารครั้งที่ 2

เนื่องจากสถาการณ์แพร่ระบาดของไวรัส Covid-19 ทางบริษัทจริงจัดประชุมผ่าน Video Conference

ซึ่งมีผู้เข้าร่วมประชุมทั้งหมด 26 คน