๕. การประเมินความเสี่ยงด้านสารสนเทศ

การประเมินความเสี่ยงด้านสารสนเทศ กรมสนับสนุนบริการสุขภาพ ได้ประเมินความเสี่ยงที่เกิดจากบุคคล จากทางด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ ตามข้อ ๓ และ ๔ เป็นแนวทางในการดำเนินงาน โดย กรมสนับสนุนบริการสุขภาพ ได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพแล้ว ปรากฏ ดังนี้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕.๑ ความเสี่ยงที่เกิดจากบุคคล (People)						
(๑) เหตุการณ์หรือภัยที่เกิดจากบุคลากร ภายในกรมสนับสนุนบริการสุขภาพ	- ระบบคอมพิวเตอร์ติดไวรัส หรือหนอนอินเทอร์เน็ตจากอินเตอร์เน็ต หรือไฟล์ที่คัดลอกจากอุปกรณ์ บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externel Harddisk, Storage ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศประมวลผล ข้อมูลได้ช้าลงหรืออาจทำงานผิดพลาดได้	๕	๕	๒๕	สูง	- ผู้ดูแลระบบ (System Administrator) ตัดการเชื่อมต่อเครื่องที่ติดไวรัสดังกล่าว ออกจากระบบเครือข่าย ภายใน และดำเนินการสแกนไวรัสเพื่อกำจัดไวรัสเครื่องดังกล่าว - หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)
(๒) เหตุการณ์หรือภัย ที่เกิดจากผู้ไม่ประสงค์ดี	- ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบหน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์ และระบบสารสนเทศล่มได้	๕	๕	๒๕	สูง	ตรวจพอร์ตทั้งหมดที่ใช้เชื่อมต่อแล้วให้ปิดพอร์ตที่ไม่ได้ใช้งาน โดยทันที
๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process)						
(๑) เหตุการณ์หรือภัย ที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)	- อุปกรณ์ประมวลผลข้อมูล (Process Device) สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ กรมสนับสนุนบริการสุขภาพ	๓	๕	๑๕	ค่อนข้างสูง	- ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - ผู้ดูแลระบบ (System Administrator) ตรวจสอบความครบถ้วนและความเสียหาย

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ)						
(๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ)	- ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิในห้องศูนย์ข้อมูลและสารสนเทศสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้รับความเสียหาย					และระบบปรับอากาศ พร้อมทั้ง รายงานให้ DCIO ทราบ เพื่อสั่งการต่อไป - DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการชั่วคราวเนื่องจากไฟฟ้าดับ - DCIO ประสานงานกับกลุ่มเทคโนโลยีสารสนเทศเพื่อสอบถามปัญหา และระยะเวลา การแก้ไขที่จะสามารถกลับมาให้บริการได้ - ผู้ดูแลระบบ (System Administrator) เปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมทั้งรายงานให้ DCIO และ อธิบดีทราบตามลำดับ - DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้ปกติ
	(๓.๒) เหตุการณ์อัคคีภัย - สินทรัพย์ (Asset) ที่ย้ายไม่ทันอาจถูกไฟไหม้ - อุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ไม่สามารถให้บริการได้	๑	๕	๕	ค่อนข้างต่ำ	แนวทางปฏิบัติตามแผนป้องกันและระงับอัคคีภัย ในการรักษาความมั่นคงปลอดภัยสารสนเทศ <u>กรณีที่ ๑</u> ไฟเริ่มไหม้หรือสามารถดับไฟได้ - ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
(๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ)	(๓.๒) เหตุการณ์อัคคีภัย (ต่อ)					- ผู้พบเหตุรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ และให้แจ้งให้อธิบดีทราบโดยเร็ว - ผู้ดูแลระบบ (System Administrator) ประเมินสถานการณ์ในเบื้องต้นว่า ควรหยุดให้บริการระบบคอมพิวเตอร์ และระบบสารสนเทศหรือไม่ - ถ้าหยุดให้บริการ DCIO สั่งการให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการ ชั่วคราวเนื่องจากเหตุไฟไหม้ - ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ พร้อมทั้งรายงานให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ DCIO และอธิบดีทราบตามลำดับชั้น และสั่งการต่อไป - หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ (System Administrator) ดำเนินการ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ)						
(๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ)	(๓.๒) เหตุการณ์อัคคีภัย (ต่อ)					แก้ไข และเปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ - DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้แล้ว - หากเสียหายมากให้ผู้ดูแลระบบ (System Administrator) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยี และ DCIO ทราบ ตามลำดับขั้นและสั่งการต่อไป <u>กรณีที่ ๒</u> ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง - ให้ผู้พบเหตุโทรแจ้งหน่วยดับเพลิง เป็นลำดับแรก และแจ้งให้ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ และ DCIO ทราบโดยเร็ว - ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณไฟที่เริ่มลุกลามและบริเวณโดยรอบ หากไม่สามารถระงับเหตุได้ ให้ออกจากพื้นที่โดยเร็ว -DCIO ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุด ให้บริการเนื่องจากเหตุไฟไหม้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕.๒ ความเสี่ยงที่เกิดจากกระบวนการ (Process) (ต่อ)						
(๓) ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ (ต่อ)	(๓.๓) เหตุการณ์ที่เกิดจาก ภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง - เช่น กรณีการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง อาจถูกปิดกั้นการเข้าออกและอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำบริเวณกระทรวงสาธารณสุข ซึ่งส่งผลกระทบต่อห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ หรือสถานที่ปฏิบัติงานบริเวณอาคาร กรมสนับสนุนบริการสุขภาพ .	๑	๕	๕	ค่อนข้างต่ำ	- หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายในภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยี และ DCIO ทราบ ตามลำดับชั้นและสั่งการต่อไป - หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator) รายงานให้ผู้อำนวยการกลุ่มเทคโนโลยี และ DCIO ทราบ ตามลำดับชั้นและสั่งการต่อไป - ถ้าเกิดเหตุการณ์ไฟฟ้าดับ ให้ดำเนินการตามแนวทางแก้ไขตาม ข้อ ๕ - กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย ตามที่ กรมสนับสนุนบริการสุขภาพกำหนด

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕.๓ ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology)						
๕.๓.๑ ทรัพย์สินครุภัณฑ์ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software)	- ไม่เพียงพอต่อการใช้งาน - ไม่พร้อมใช้งาน	๒	๕	๑๐	ค่อนข้างสูง	- จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ - สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งานตามแผนที่กำหนด - กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ปรับปรุงระบบการยืม-คืน เมื่อนำอุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอกสำนักงาน - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
๕.๓.๒ เครือข่ายสารสนเทศ และเครือข่ายเสมือน (Information Network and Virtual Machine)	- ไม่เพียงพอต่อการใช้งาน - ไม่พร้อมใช้งาน	๒	๕	๑๐	ค่อนข้างสูง	- กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕.๓ ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) (ต่อ)						
๕.๓.๓ โครงข่ายการสื่อสาร (Communication Network)	- ไม่เพียงพอต่อการใช้งาน - ไม่พร้อมใช้งาน	๒	๕	๑๐	ค่อนข้างสูง	- กำหนดแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งาน การเข้ารหัสในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
๕.๓.๔ ข้อมูลและสารสนเทศ (Information)		๒	๕	๑๐	ค่อนข้างสูง	- กำหนดแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งาน การเข้ารหัส - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

<u>หมายเหตุ</u> เกณฑ์การประเมินการให้คะแนนโอกาสที่จะเกิดและผลกระทบ

ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด
ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย
ระดับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง
ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก
ระดับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด

แผนผังประเมินความเสี่ยง

ผลกระทบของความเสี่ยง					
๕	๑๐	๑๕	๒๐	๒๕
๔	๘	๑๒	๑๖	๒๐
๓	๖	๙	๑๒	๑๕
๒	๔	๖	๘	๑๐
๑	๒	๓	๔	๕

สีแดง ระดับความเสี่ยงสูง ค่าระหว่าง ๑๕ - ๒๕
สีเหลือง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง ๘ - ๑๔
สีเขียว ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง ๔ - ๗
สีฟ้า ระดับความเสี่ยงต่ำ ค่าระหว่าง ๑ - ๓