การประเมินความเสี่ยงด้านสารสนเทศ

การประเมินความเสี่ยงด้านสารสนเทศทางการแพทย์ โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ได้ประเมินความเสี่ยงที่เกิดจากบุคคล จากทางด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ เป็นแนวทางในการดำเนินงาน โดย โรงพยาบาลพระอาจารย์มั่น ภูริทัตโต ได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของ งานสารสนเทศทางการแพทย์ ปรากฏ ดังนี้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
ความเสี่ยงที่เกิดจากบุคคล (People)						
เหตุการณ์หรือภัยที่เกิดจากบุคลากร ภายในโรงพยาบาลพระอาจารย์มั่น ภูริทัตโต	- ระบบคอมพิวเตอร์ติดไวรัส หรือหนอนอินเตอร์เน็ตจากอินเตอร์เน็ต หรือไฟล์ที่คัดลอกจากอุปกรณ์ บันทึกข้อมูลแบบพกพา เช่น Flash Driver และ External Harddisk,Storage ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศประมวลผล ข้อมูลได้ช้าลงหรืออาจทำงานผิดพลาดได้	๓	๓	๙	ค่อนข้างสูง	-ผู้ดูแลระบบ(System Administrator) ตัดการเชื่อมต่อเครื่องที่ติดไวรัสดังกล่าว ออกจากระบบเครือข่าย ภายใน และดำเนินการสแกนไวรัสเพื่อกำจัดไวรัสเครื่องดังกล่าว -หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)
เหตุการณ์หรือภัย ที่เกิดจากผู้ไม่ประสงค์ดี	-ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบหน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบคอมพิวเตอร์ และระบบสารสนเทศล่มได้	๑	๓	๓	ต่ำ	ตรวจสอบพอร์ตทั้งหมดที่ใช้เชื่อมต่อแล้วให้ปิดพอร์ตที่ไม่ใช้งาน โดยทันที
ความเสี่ยงที่เกิดจากกระบวนการ (Process)						
เหตุการณ์หรือภัย ที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผล (Process Device)	-อุปกรณ์ประมวลผลข้อมูล (Process Device) สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผลข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ โรงพยาบาล ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิ ในห้องServer และสารสนเทศสูงขึ้นทำให้อุปกรณ์ประมวลผลข้อมูล	๑	๓	๓	ต่ำ	-ผู้พบเหตุแจ้งให้หัวหน้างานสารสนเทศทางการแพทย์ทราบ เพื่อรายงานตามลำดับขั้นและสั่งการต่อไป -ผู้ดูแลระบบ(System Administrator) ตรวจสอบความครบถ้วนและความเสียหายและระบบ ปรับอากาศ พร้อมทั้งรายงานให้ หัวหน้างาน ทราบ เพื่อสั่งการต่อไป

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
	(Process Device) ได้รับความเสียหาย					- หัวหน้างาน ประชาสัมพันธ์ให้กับ บุคลากรได้รับทราบถึงการหยุดให้บริการชั่วคราว - หัวหน้างาน ประสานงานกับกลุ่มเทคโนโลยีสารสนเทศเพื่อสอบถามปัญหา และระยะเวลา การแก้ไขที่จะสามารถกลับมาให้บริการ -ผู้ดูแลระบบ(System Administrator) เปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมทั้งรายงานให้ หัวหน้างาน และผู้บริหารทราบตามลำดับ -หัวหน้างานประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้ปกติ
	เหตุการณ์อัคคีภัย - สินทรัพย์ (Asset) ที่ย้ายไม่ทันอาจถูกไฟไหม้ - อุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องเซิร์ฟเวอร์ ไม่สามารถให้บริการได้	๑	๓	๓	ต่ำ	แนวทางการปฏิบัติตามแผนป้องกันและระงับอัคคีภัยในการรักษาความมั่นคงปลอดภัยสารสนเทศ <u>กรณีที่ ๑</u> ไฟเริ่มไหม้หรือสามารถดับไฟได้ -ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับ - ผู้พบเหตุรายงานให้ผู้อำนวยการทราบโดยเร็ว -ผู้ดูแลระบบ (System Administrator) ประเมินสถานการณ์ในเบื้องต้นว่า ควรหยุดให้บริการระบบคอมพิวเตอร์ และระบบสารสนเทศหรือไม่ - ถ้าหยุดให้บริการ หัวหน้างาน สั่งการให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการ ชั่วคราวเนื่องจากเหตุไฟไหม้ -ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device)

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
						ระบบปรับอากาศ และสภาพภายในห้องเซิร์ฟเวอร์ พร้อมทั้งรายงานให้ผู้อำนวยการ หัวหน้างาน ทราบตามลำดับชั้นและสั่งการต่อไป -หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ(System Administrator) ดำเนินการแก้ไข และเปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ -หัวหน้า ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้แล้ว -หากเสียหายมากให้ผู้ดูแลระบบ(System Administrator) รายงานให้หัวหน้างานสารสนเทศทางการแพทย์ทราบ ตามลำดับชั้นและสั่งการต่อไป <u>กรณีที่ ๒</u> ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง - ให้ผู้พบเหตุโทรแจ้งหน่วยดับเพลิง เป็นลำดับแรก และแจ้งให้ หัวหน้างานสารสนเทศทางการแพทย์ทราบโดยเร็ว - ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณไฟที่เริ่มลุกลามและบริเวณโดยรอบ หากไม่สามารถระงับเหตุได้ ให้ออกจากพื้นที่โดยเร็ว -หัวหน้างาน ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุด ให้บริการเนื่องจากเหตุไฟไหม้
	เหตุการณ์ที่เกิดจาก ภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง - เช่น กรณีการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมืองอาจถูกปิดกั้นการเข้า	**๑**	**๒**	๒	**ต่ำ**	- หากสามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator)ตรวจสอบความเสียหาย ผลกระทบและความพร้อมใช้งานของอุปกรณ์ประมวลผลข้อมูล (Process Device)ระบบปรับอากาศ และสภาพภายในห้องเซิร์ฟเวอร์ รายงานให้หัวหน้างาน

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
	ออกและอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำบริเวณโรงพยาบาล					สารสนเทศทางการแพทย์ทราบ ตามลำดับชั้นและสั่งการต่อไป - หากไม่สามารถระงับเหตุได้ ให้ผู้ดูแลระบบ (System Administrator)รายงานให้หัวหน้างานสารสนเทศทางการแพทย์ทราบ ตามลำดับชั้นและสั่งการต่อไป - ถ้าเกิดเหตุการณ์ไฟฟ้าดับ ให้ดำเนินการตามแนวทางแก้ไข - กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย
ทรัพย์สินครุภัณฑ์ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software)	-ไม่เพียงพอต่อการใช้งาน -ไม่พร้อมใช้งาน	๓	๓	**๙**	**ค่อนข้างสูง**	-จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งานตามแผนที่กำหนด - กำหนดแนวทางการควบคุม กำกับ ติดตาม ประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ปรับปรุงระบบการยืม-คืน เมื่อนำอุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอกสำนักงาน - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
โครงข่ายการสื่อสาร (Communication Network)	-ไม่เพียงพอต่อการใช้งาน -ไม่พร้อมใช้งาน	๓	๓	**๙**	**ค่อนข้างสูง**	- กำหนดแนวทางการควบคุม กำกับ ติดตาม ประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ข้อมูลและสารสนเทศ		๒	๒	**๔**	**ค่อนข้างต่ำ**	- กำหนดแนวทางการควบคุม กำกับ ติดตาม ประเมิน

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
(Information)						การใช้งาน การเข้ารหัส - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมายเหตุ เกณฑ์การประเมินการให้คะแนนโอกาสที่จะเกิดและผลกระทบ

ระดับ ๑ = รุนแรงน้อยที่สุด / โอกาสเกิดน้อยที่สุด

ระดับ ๒ = รุนแรงน้อย / โอกาสเกิดน้อย

ระตับ ๓ = รุนแรงปานกลาง / โอกาสเกิดปานกลาง

ระดับ ๔ = รุนแรงมาก / โอกาสเกิดมาก

ระตับ ๕ = รุนแรงมากที่สุด / โอกาสเกิดมากที่สุด