แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
(IT Risk Management Plan)

วัตถุประสงค์

1. เพื่อให้การจัดการภายในโรงพยาบาลเก้าเลี้ยว ให้มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลง ของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบเทคโนโลยี สารสนเทศและการสื่อสาร

2. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และการสื่อสารของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

3. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

5. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมี ผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

การประเมินความเสี่ยง (Risk assessment)

การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของกรมสามารถแยกประเภทความเสี่ยงเป็น 4 ประเภท ดังนี้

- ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์เครื่องมือและอุปกรณ์เองอาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดีถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

- ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการ เข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศและการ สื่อสาร หรือใช้ข้อมูลต่างๆ ของกรมฯ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อ ข้อมูลสารสนเทศได้

- ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

- ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ ทั้งนี้ ลักษณะรายละเอียดของความเสี่ยง (Description of risk)

ตารางรายละเอียดของความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๑	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ
๒. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT๐๒	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร หรือแผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วน หรือได้รับความเสียหายทั้งหมด หรือการเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ
๓. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๓	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล	- Hacker/Cracker - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๔. ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	RIT๐๔	ความเสี่ยงด้านเทคนิค	กรมฯ ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับ-ส่งข้อมูลต่างๆ ได้	- ความล้มเหลวทางเทคนิค - การดำเนินการของหน่วยงานภายนอกที่มีผลกระทบต่อระบบเครือข่ายของกรมฯ	ระบบเครือข่ายสื่อสาร ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ
๕. ความเสี่ยงจากการละเมิดลิขสิทธิ์	RIT๐๕	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของกรมฯ ส่งผลให้กรมฯ อาจถูกฟ้องร้องได้	- กรมฯ ถูกฟ้องร้องการละเมิดลิขสิทธิ์	เครื่องคอมพิวเตอร์ อธิบดีกรม ผู้ดูแลระบบ
๖. ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบงานสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุง (Update) ให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบ หรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ความล้มเหลวทางเทคนิค - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล	เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ดูแลระบบ
๗. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	RIT๐๗	ความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวัง ทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี หรือถูกดักจับข้อมูลสำคัญ หรือการส่งข้อมูลคำสั่งเจตนาร้าย หรือการติดไวรัสหรือเวิร์ม ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของกรมฯ	- Hacker/Cracker - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ไวรัส/เวิร์ม	เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบงานสารสนเทศ ระบบเครือข่าย ผู้ใช้งาน ผู้ดูแลระบบ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๘. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบงานสารสนเทศ ระบบเครือข่าย ผู้ใช้งาน ผู้ดูแลระบบ
๙. ความเสี่ยงจากการติดตั้งระบบงานและฐานข้อมูลไว้ที่เครือข่ายภายนอกกรมฯ	RIT๐๙	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล รวมไปถึงการที่ระบบงานไม่สามารถใช้งานได้ อันเกิดจากความบกพร่องของผู้ดูแลระบบภายนอกกรมฯ	- Hacker/Cracker - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/ เวิร์ม - ความล้มเหลวทางเทคนิค	เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ

การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาส ที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบและระดับความเสี่ยง ซึ่งใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	> ๔ ครั้ง/ปี
๔	สูง	๔ ครั้ง/ปี
๓	ปานกลาง	๓ ครั้ง/ ปี
๒	น้อย	๒ ครั้ง/ปี
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

ตารางการประมาณความเสี่ยง (Risk estimation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ /ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๑. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๑	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ	๑	๕
๒. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT๐๒	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร หรือแผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วน หรือได้รับความเสียหายทั้งหมด หรือการเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ	๓	๕
๓. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๓	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส หรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล	- Hacker/Cracker - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/ เวิร์ม	เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ	๓	๓

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ /ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๔. ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	RIT๐๔	ความเสี่ยงด้านเทคนิค	กรมฯ ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับ-ส่งข้อมูลต่างๆ ได้	- ความล้มเหลวทางเทคนิค - การดำเนินการของหน่วยงานภายนอกที่มีผลกระทบต่อระบบเครือข่ายของกรมฯ	ระบบเครือข่ายสื่อสารระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ	๓	๓
๕. ความเสี่ยงจากการละเมิดลิขสิทธิ์	RIT๐๕	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของกรมฯ ส่งผลให้กรมอาจถูกฟ้องร้องได้	- กรมฯ ถูกฟ้องร้องการละเมิดลิขสิทธิ์	เครื่องคอมพิวเตอร์ อธิบดีกรม ผู้ดูแลระบบ	๓	๑
๖. ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบงานสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุง (Update) ให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบหรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ความล้มเหลวทางเทคนิค - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล	เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ดูแลระบบ	๓	๓
๗. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	RIT๐๗	ความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวังทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี หรือถูกดักจับข้อมูลสำคัญ หรือการส่งข้อมูลคำสั่งเจตนาร้าย หรือการติดไวรัสหรือเวิร์ม ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของกรมฯ	- Hacker/Cracker - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ไวรัส/เวิร์ม	เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบงานสารสนเทศ ระบบเครือข่าย ผู้ใช้งาน ผู้ดูแลระบบ	๕	๓

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ /ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๘. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบงานสารสนเทศ ระบบเครือข่าย ผู้ใช้งาน ผู้ดูแลระบบ	๓	๔
๙. ความเสี่ยงจากการติดตั้งระบบงานและฐานข้อมูลไว้ที่เครือข่ายภายนอกกรมฯ	RIT๐๙	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล รวมไปถึงการที่ระบบงานไม่สามารถใช้งานได้ อันเกิดจากความบกพร่องของผู้ดูแลระบบภายนอกกรมฯ	- Hacker/Cracker - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/ เวิร์ม - ความล้มเหลวทางเทคนิค	เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบงานสารสนเทศ ผู้ใช้งาน ผู้ดูแลระบบ	๓	๔

การประเมินค่าความเสี่ยง (Risk evaluation)

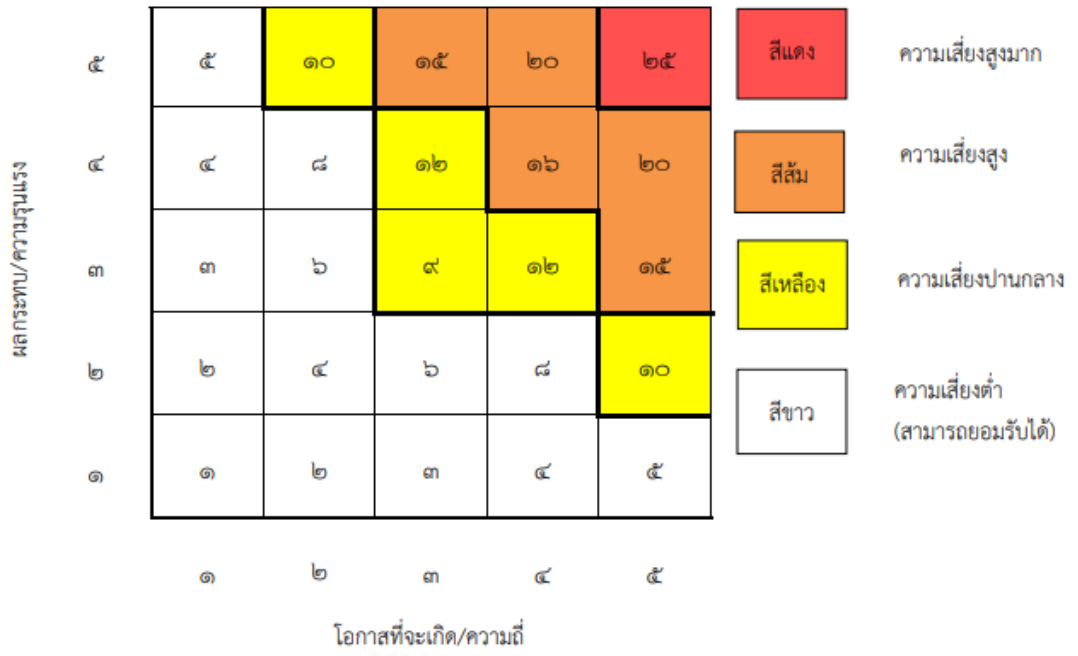
การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้นและขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ (ความถี่) X ความรุนแรงของเหตุการณ์ต่างๆ (ผลกระทบ)

ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ – ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๕ – ๑๔	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗ – ๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ส้ม
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

การประเมินความเสี่ยง

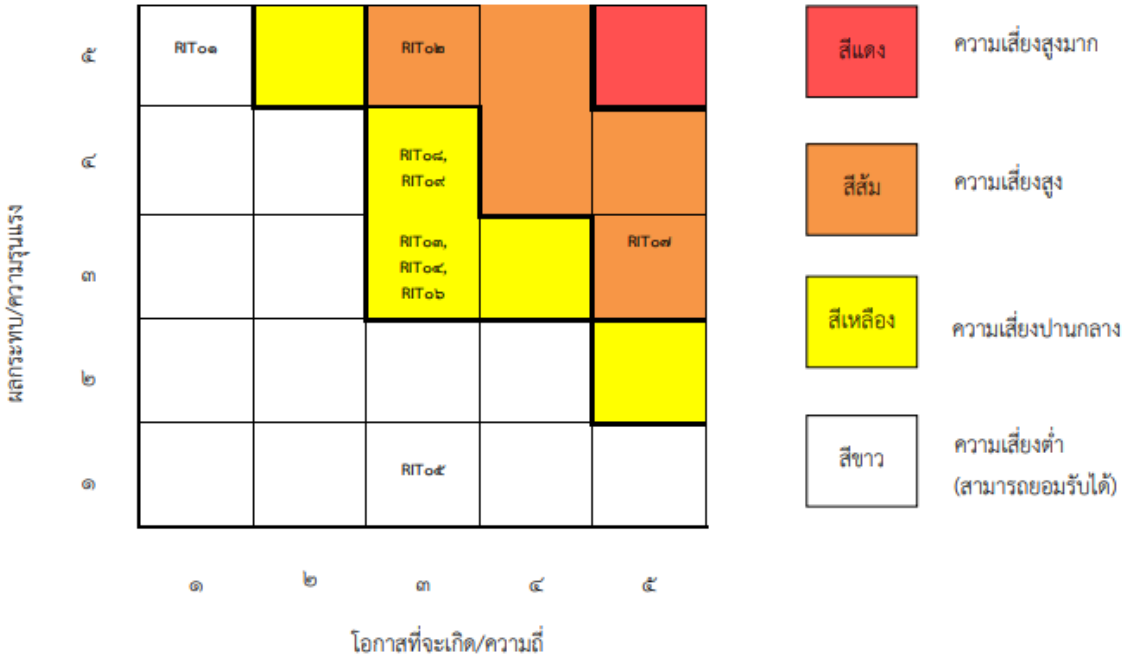


สรุปผลการประเมินค่าความเสี่ยง (Risk evaluation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาสที่จะเกิด/ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๑	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๑	๕	๕
๒. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	RIT๐๒	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร หรือแผ่นดินไหว จนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วน หรือได้รับความเสียหายทั้งหมด หรือการเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	๓	๕	๑๕
๓. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	RIT๐๓	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล	๓	๓	๙
๔. ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	RIT๐๔	ความเสี่ยงด้านเทคนิค	กรมฯ ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับ-ส่งข้อมูลต่างๆ ได้	๓	๓	๙
๕. ความเสี่ยงจากการละเมิดลิขสิทธิ์	RIT๐๕	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของกรมฯ ส่งผลให้กรมอาจถูกฟ้องร้องได้	๓	๑	๓

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาสที่จะเกิด/ความถี่	ความรุนแรง	ระดับคะแนน
๖. ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบงานสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุง (Update) ให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบหรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงจากการถูกบุกรุก โจมตีได้	๓	๓	๙
๗. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	RIT๐๗	ความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวังทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี หรือถูกดักจับข้อมูลสำคัญ หรือการส่งข้อมูลคำสั่งเจตนาร้าย หรือการติดไวรัสหรือเวิร์ม ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของกรมฯ	๕	๓	๑๕
๘. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๓	๔	๑๒
๙. ความเสี่ยงจากการติดตั้งระบบงานและฐานข้อมูลไว้ที่เครือข่ายภายนอกกรมฯ	RIT๐๙	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล รวมไปถึงระบบงานไม่สามารถใช้งานได้ ที่เกิดจากความบกพร่องของผู้ดูแลระบบภายนอกกรมฯ	๓	๔	๑๒

แผนภูมิความเสี่ยงด้านสารสนเทศ (Risk Map)



ผลการวิเคราะห์ความเสี่ยง (Risk analysis)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศในการบริหารจัดการได้อย่างมีประสิทธิภาพ

ตารางผลการวิเคราะห์ความเสี่ยง (Risk analysis)

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑.	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร หรือแผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วนหรือได้รับความเสียหายทั้งหมด หรือการเกิดน้ำท่วมจนต้องดำเนินการตัดกระแสไฟฟ้าและไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	๑๕
๒.	ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	ความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวัง ทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี หรือถูกดักจับข้อมูลสำคัญ หรือการส่งข้อมูลคำสั่งเจตนาร้าย หรือการติดไวรัสหรือเวิร์ม ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของกรมฯ	๑๕
๓.	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๑๒
๔.	ความเสี่ยงจากการติดตั้งระบบงานและฐานข้อมูลไว้ที่เครือข่ายภายนอกกรมฯ	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล รวมไปถึงระบบงานไม่สามารถใช้งานได้ ที่เกิดจากความบกพร่องของผู้ดูแลระบบภายนอกกรมฯ	๑๒

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๕.	ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล	๙
๖.	ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	ความเสี่ยงด้านเทคนิค	กรมฯ ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับ-ส่งข้อมูลต่างๆ ได้	๙
๗.	ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบงานสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุง (Update) ให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบหรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	๙
๘.	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๕
๙.	ความเสี่ยงจากการละเมิดลิขสิทธิ์	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของกรม ส่งผลให้กรมฯ อาจถูกฟ้องร้องได้	๓

การจัดการความเสี่ยง (Risk management)

นโยบายของโรงพยาบาลเก้าเลี้ยว ค่าระดับความเสี่ยงที่ยอมรับได้ ≤ 5 ซึ่ง กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยงคือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ 15 ขึ้นไป ส่วนความเสี่ยง ที่มีระดับความเสี่ยงต่ำกว่า 15 ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการ สื่อสารหรือไม่ก็ได้การดำเนินการจัดการความเสี่ยง

ตารางการจัดการความเสี่ยง (Risk management)

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑.	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	๑๕	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
๒.	ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	๑๕	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ฝึกอบรม เผยแพร่และประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องของความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของกรมอย่างต่อเนื่อง - กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด
๓.	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สำรวจและจัดหาระบบสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - ตรวจสอบความพร้อมของระบบสำรองไฟฟ้าอย่างสม่ำเสมอ
๔.	ความเสี่ยงจากการติดตั้งระบบงานและฐานข้อมูลไว้ที่เครือข่ายภายนอกกรมฯ	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- ตรวจสอบระบบงานให้ได้มาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP-Top ๑๐ Web Application Security Risks เพื่อลดความเสี่ยง - ระบบงานใดๆ ที่ติดตั้งภายนอกกรมฯ ให้ดำเนินการติดตั้งระบบงานภายใต้โครงการบริการคลาวด์ภาครัฐของสำนักงานรัฐบาลอิเล็กทรอนิกส์เป็นหลัก เพื่อความปลอดภัยและเพื่อให้สอดคล้องกับนโยบายภาครัฐ

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๕.	ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	๙	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- ตรวจสอบการตั้งค่าของ firewall, IPS อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ
๖.	ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	๙	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาระบบเครือข่ายอินเทอร์เน็ตสำรองเพื่อเป็นช่องทางให้ระบบอินเทอร์เน็ตใช้งานได้อย่างต่อเนื่อง - ตรวจสอบการเชื่อมต่อเครือข่ายอินเทอร์เน็ต
๗.	ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบงานสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	๙	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- มีการสำรวจและรวบรวมความต้องการงบประมาณอย่างต่อเนื่องเพื่อการจัดทำงบประมาณในแต่ละปี - มีการหารือ ชี้แจง และทำความเข้าใจกับผู้บังคับบัญชาในเรื่องงบประมาณที่ต้องใช้อย่างชัดเจน - วางแผนการใช้งบกองทุนเป็นแหล่งเงินทุนสำรอง ในกรณีไม่ได้รับงบประมาณตามที่ได้วางแผนไว้
๘.	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๕	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบงานสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
๙.	ความเสี่ยงจากการละเมิดลิขสิทธิ์	๓	- ยอมรับความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง

แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

จากการจัดการความเสี่ยง สามารถนำมาจัดทำแผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีหน่วยงานรับผิดชอบคือ งานสารสนเทศทางการแพทย์ โรงพยาบาลเก้าเลี้ยว ระยะเวลาดำเนินการระหว่างเดือนตุลาคม 2564 – กันยายน 2565

ตาราง แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีพ.ศ. 2564			ปีพ.ศ. 2565								
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๑. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	- ตรวจสอบความพร้อมใช้ของอุปกรณ์ดับเพลิง	- ทุก ๖ เดือน	●						●					
	- จัดทำแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	- เดือน ต.ค.	●											
	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	- เดือน พ.ย. - เดือน มี.ค.		←	→			←	→					
๒. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	- ฝึกอบรม เผยแพร่และประชาสัมพันธ์เรื่องความมั่นคงปลอดภัยสารสนเทศ	- ตลอดปี	←	→										→
	- กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	- ตลอดปี	←	→										→

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีพ.ศ. 2564			ปีพ.ศ. 2565								
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- สำรวจและจัดหาระบบสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - ตรวจสอบความพร้อมของระบบสำรองไฟฟ้า	- เดือนมิ.ย.ถึงก.ย. - ทุก ๖ เดือน	●						●		◄———	———	———	———►
๔. ความเสี่ยงจากการติดตั้งระบบงานและฐานข้อมูลไว้ที่เครือข่ายภายนอกกรมฯ	- ตรวจสอบระบบงานให้ได้มาตรฐาน OWASP-Top ๑๐ - สำรวจระบบงานที่ติดตั้งภายนอกกรมฯ เพื่อโอนย้ายมายังเครื่องแม่ข่ายกรมฯ หรือเครื่องแม่ข่ายคลาวด์ภาครัฐ	- ทุกครั้งที่ตรวจรับระบบงาน - ทุก ๖ เดือน	●						●					
๕. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	- ตรวจสอบการตั้งค่าของ Firewall, IPS อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ	- ทุกเดือน - ทุกเดือน - ทุกเดือน - ทุกเดือน	◄------	------	------	------	------	------	------	------	------	------	------	------►

ประเภทความเสี่ยง	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีพ.ศ. 2564			ปีพ.ศ. 2565								
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๖. ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	- สำรวจและจัดหาระบบเครือข่ายอินเทอร์เน็ตสำรองเพื่อเป็นช่องทางให้ระบบอินเทอร์เน็ตใช้งานได้อย่างต่อเนื่อง	- เดือน มิ.ย. ถึง ก.ย.									←			→
	- ตรวจสอบการเชื่อมต่อเครือข่ายอินเทอร์เน็ต	- ทุก ๓ เดือน	●			●			●			●		
๗. ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบงานสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	- มีการสำรวจและรวบรวมความต้องการงบประมาณอย่างต่อเนื่อง เพื่อการจัดทำงบประมาณในแต่ละปี	- เดือน มิ.ย. ถึง ก.ย.									←			→
	- มีการหารือ ชี้แจงและทำความเข้าใจกับผู้บังคับบัญชาในเรื่องงบประมาณที่ต้องใช้อย่างชัดเจน	- เดือน ก.ย.												●
	- วางแผนการใช้งบกองทุนเป็นแหล่งเงินทุนสำรอง ในกรณีไม่ได้รับงบประมาณตามที่ได้วางแผนไว้													