บทนำ

แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศโรงพยาบาลบ้านด่านลานหอย ประจำปี 2564 จัดทำขึ้นเพื่อเป็นกรอบแนวทางการในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้บรรลุผลตามเป้าประสงค์ของหน่วยงาน เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นให้อยู่ในระดับที่องค์กรสามารถรองรับได้ และทำให้การปฏิบัติงานมีประสิทธิภาพมากยิ่งขึ้น โรงพยาบาลบ้านด่านลานหอยหวังเป็นอย่างยิ่งว่า แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศนี้ จะช่วยลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านด่านลานหอยต่อไป

หลักการและเหตุผล

ปัจจุบัน โรงพยาบาลบ้านด่านลานหอยและหน่วยงานต่างๆ ภายในโรงพยาบาลได้มีการนำระบบสารสนเทศ ซึ่งเป็นผลพวงจากความเจริญก้าวหน้าทางด้านเทคโนโลยี มาเป็นเครื่องมือช่วยในการปฏิบัติงาน ช่วยในการจัดเก็บและวิเคราะห์ข้อมูล เพื่อเป็นแนวทางในการตัดสินใจด้านการบริหารงาน เพื่อการพัฒนาแบะยกระดับการบริหารงาน ให้เป็นองค์กรที่มีสมรรถนะสูง ตอบสนองความต้องการและให้บริการกับประชาชนได้อย่างมีประสิทธิภาพ การนำเอาระบบเทคโนโลยีสารสนเทศมาช่วยในการดำเนินงานภายในองค์กร ทั้งทางด้านการเก็บข้อมูล ประมวลผลข้อมูล บริหารการจัดการในรูปแบบต่างๆ ซึ่งระบบเทคโนโลยีสารสนเทศสามารถทำได้อย่างรวดเร็ว ถูกต้อง รูปแบบการแสดงผลสามารถทำได้อย่างหลากหลาย อันเป็นตัวช่วยให้การปฏิบัติงานของเจ้าหน้าที่ภายในองค์กรนั้นๆเป็นไปด้วยความรวดเร็วและมีประสิทธิภาพ อีกทั้งยังเป็นตัวช่วยในการตัดสินใจของผู้บริหารองค์กรนั้นๆได้เป็นอย่างดี อย่างไรก็ตามระบบเทคโนโลยีสารสนเทศ เป็นเครื่องมือทางด้านอิเล็กทรอนิกส์ ที่มีทั้งข้อดีและข้อด้อย เพราะระบบการทำงานต้องอาศัยปัจจัยหลายๆอย่างร่วมมือ ทั้งทางด้าน Hardware/ Software/ Network/ User/ ปัจจัยสภาพแวดล้อมทางกายภาพ ทั้งเรื่องของไฟฟ้า อุณหภูมิ ความชื้นอีกทั้งยังมีปัจจัย ทั้งภายในและภายนอกองค์กร มาเป็นองค์ประกอบส่งเสริมหรือรบกวนการทำงานของระบบ ส่งผลต่อข้อมูลที่เก็บอยู่ในระบบและการทำงานของระบบ ซึ่งจะส่งผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่ ทั้งระดับปฏิบัติงานและระดับบริหาร ซึ่งทั้งหมดที่กล่าวมาถือเป็นความเสี่ยงในระบบสารสนเทศของโรงพยาบาล เพื่อเป็นการลดภัยดังกล่าวที่จะเกิดขึ้นในระบบสารสนเทศ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีแผนบริหารความเสี่ยงของระบบสารสนเทศ จากสถานการณ์ดังกล่าว ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ เพื่อการป้องกัน การควบคุมและบริหารความเสี่ยง แนวทางแก้ไขปัญหา ตลอดจน การฟื้นฟูให้ระบบสารสนเทศกลับสู่สภาพเดิม และใช้งานได้ตามปกติโดยเร็ว

วัตถุประสงค์

1. เพื่อให้การจัดการภายในหน่วยงานมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านด่านลานหอย

2. เพื่อให้มีการวางแผน การควบคุมแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม

3. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในโรงพยาบาลบ้านด่านลานหอย

ผลที่คาดว่าจะได้รับ

เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยง และความเสี่ยงในด้านต่างๆ ที่อาจมีผลกระทบต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และการสื่อสารของโรงพยาบาลบ้านด่านลานหอย แล้วพิจารณาหาแนวทางป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานตามแผน

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของหน่วยงาน เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต

ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง และพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชา

แผนการลดความเสี่ยง (Treatment Plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยง สำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่ง และพบว่ามีความเสี่ยงเกินกว่าระดับ ความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชาเพื่อพิจารณาอนุมัติดำเนินการ

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้วัตถุประสงค์ที่กำหนดไว้โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด เกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดการความเสี่ยงในภายหลังได้อย่างถูกต้อง

ขอบเขตการดำเนินงาน

เป็นการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของโรงพยาบาลบ้านด่านลานหอย

คำนิยาม

ระบบสารสนเทศ หมายถึง ระบบที่มีการนำคอมพิวเตอร์มาช่วยในการรวบรวม จัดเก็บ หรือจัดการกับข้อมูลข่าวสาร เพื่อให้ข้อมูลนั้นกลายเป็นสารสนเทศที่ดี สามารถนำไปใช้ประกอบการตัดสินใจในเวลาอันรวดเร็วและถูกต้อง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งสามารถส่งผลกระทบหรือสร้างความเสียหาย ทั้งที่สามารถตีมูลค่าเป็นตัวเงินได้และที่ไม่สามารถตีเป็นมูลค่าตัวเงินได้ และส่งผลกระทบและความเสียหายหรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อเป้าหมาย และวัตถุประสงค์ที่กำหนด

ลักษณะของความเสี่ยง ลักษณะของความเสี่ยงสามารถแบ่งออกได้เป็น 3 ลักษณะ ดังนี้

1) ปัจจัยเสี่ยง หมายถึง สาเหตุที่จะทำให้เกิดความเสี่ยง

2) เหตุการณ์เสียง หมายถึง เหตุการณ์ที่ส่งผลกระทบต่อการดาเนินงานหรือนโยบาย

3) ผลกระทบของความเสี่ยง หมายถึง ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจาก

การบริหารความเสี่ยง (Risk Management) หมายถึง ระบบการบริหารและควบคุม รวมทั้งกระบวนการ ดำเนินงานต่างๆ เพื่อที่จะลดสาเหตุ ของโอกาสที่จะก่อให้เกิดความเสียหาย เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ สามารถประเมินผล ควบคุม และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึง การบรรลุเป้าประสงค์ ตามภารกิจหลัก และเป้าหมายตามแผนปฏิบัติราชการขององค์กรเป็นสำคัญ การบริหารความเสี่ยงมี ความจำเป็นที่จะต้องอาศัยขั้นตอนที่ต่อเนื่อง เนื่องจากมีการระบุความเสี่ยงอันจะมีผลกระทบจากความเสี่ยงและมาตรการ หรือแผนปฏิบัติการในการจัดการความเสี่ยงนั้นได้ถูกดำเนินการตามแผนที่วางไว้

การประเมินความเสี่ยง เป็นกระบวนการที่ใช้ระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมหรือบริหารความเสี่ยง และขั้นตอนในการ ประเมินความเสี่ยงประเมินได้จากการระบุปัจจัยเสี่ยง ทั้งภายในและภายนอก การวิเคราะห์ความเสี่ยง หาสาเหตุของความเสี่ยง และการบริหารความเสี่ยง แก้ไขหรือควบคุมความเสี่ยง

ผลกระทบ (ความรุนแรง)

ผลกระทบ	ความรุนแรง	คำนิยาม
1	น้อยมาก	กระทบต่อความน่าเชื่อถือขององค์กร / ความพึงพอใจของผู้ใช้บริการน้อยมาก (มีผลกระทบน้อยมาก)
2	น้อย	กระทบต่อความน่าเชื่อถือขององค์กร / ความพึงพอใจของผู้ใช้บริการน้อย (เจ้าหน้าที่ได้รับการตำหนิ)
3	ปานกลาง	กระทบต่อความน่าเชื่อถือขององค์กร / ความพึงพอใจของผู้ใช้บริการปานกลาง (เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย)
4	สูง	กระทบต่อความน่าเชื่อถือขององค์กร / ความพึงพอใจของผู้ใช้บริการมาก (ผู้บริหารถูกตำหนิหรือถูกร้องเรียน)
5	สูงมาก	กระทบต่อความน่าเชื่อถือขององค์กร / ความพึงพอใจของผู้ใช้บริการมากที่สุด (ผู้บริหารถูกลงโทษทางวินัย)

ระดับโอกาส (ความเป็นไปได้)

ระดับ	โอกาสที่จะเกิด	คำนิยาม
1	น้อยมาก	นานๆครั้ง (โอกาสเกิดขึ้นน้อย)
2	น้อย	ไม่บ่อย (อาจเกิดขึ้นทุก 5 ปี)
3	ปานกลาง	ปานกลาง (อาจเกิดขึ้นได้ทุกปี)
4	สูง	บ่อย (อาจเกิดขึ้นได้ทุกเดือน)
5	สูงมาก	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)

กลยุทธ์ในการจัดการความเสี่ยง

1. Take (การยอมรับ) หมายถึง ยอมรับความเสี่ยงที่เกิดจากการปฏิบัติงานภายใต้ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้

2. Treat (การลด) หมายถึง การดำเนินการเพิ่มเติมเพื่อลดโอกาสเกิดหรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3. Terminate (การหลีกเลี่ยง) หมายถึง การดำเนินการเพื่อยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง ทั้งนี้หากมีการใช้กลยุทธ์นี้ อาจต้องทำการพิจารณาวัตถุประสงค์ว่าสามารถบรรลุได้หรือไม่ เพื่อทำการปรับเปลี่ยนต่อไป

4. Transfer (การร่วมจัดการหรือโอนถ่าย) หมายถึง การร่วมจัดการโดยแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์กร

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงาน สามารถแยกประเภทความเสี่ยงเป็น 8 ประเภท ดังนี้

1. ความเสี่ยงจากผู้ปฏิบัติงาน (People ware) เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การบริหารจัดการสิทธิ์ในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนที่มีอยู่ หรืออนุญาตให้ผู้อื่นใช้สิทธิ์ในการเข้าถึงระบบ อาจทำให้เกิดความเสียหายต่อระบบและข้อมูลสารสนเทศได้

2. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือหรืออุปกรณ์เทคโนโลยีสนับสนุน ถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker หรือถูกเจาะทำลายระบบจาก Cracker

3. ความเสี่ยงด้านอุปกรณ์ (Hardware) เป็นความเสี่ยงที่อาจเกิดขึ้นจากอุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย ทำหน้าที่สนับสนุนการทำงานของคอมพิวเตอร์ในลักษณะงานต่างๆ เช่น External Hard disk, Flash Drive, Switch, Router, SD Card เป็นต้น

4. ความเสี่ยงด้านระบบเชื่อมโยงเครือข่าย Internet ใช้งานไม่ได้ ทำให้ไม่สามารถเชื่อมโยงข้อมูลสารสนเทศผ่านเครือข่ายคอมพิวเตอร์ได้

5. ความเสี่ยงด้านสถานการณ์ฉุกเฉิน คือความเสี่ยงที่เกิดจากภัยพิบัติตามธรรมชาติ เช่น ไฟฟ้าดับ ไฟกระชาก ไฟไหม้ น้ำท่วม การชุมนุมประท้วง เป็นต้น

6. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน จากการเกิดไฟไหม้ อาคารถล่ม ความไม่สงบเรียบร้อยในบ้านเมืองที่อาจส่งผลกระทบต่อการดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

7. ความสี่ยงจากเครื่องคอมพิวเตอร์ลูกข่ายหรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ เป็นความเสี่ยงทางเทคนิคหรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น

8. ความเสี่ยงจากเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ เป็นความเสี่ยงทาวเทคนิคหรืออุปกรณ์ชำรุด

การประเมินความเสี่ยง

การประเมินความเสี่ยง จะพิจารณาจากปัจจัยต่าง ๆ เช่น โอกาสที่จะเกิดภัยคุกคาม ระดับผลกระทบความรุนแรงที่มีต่อระบบ

ระดับโอกาส (ความเป็นไปได้)

Risk Assessment Matrix			ต่ำมาก/น้อยมาก	ต่ำ/น้อย	ปานกลาง	สูง/บ่อย	สูงมาก/บ่อยมาก
			1	2	3	4	5
ผลกระทบ (ความรุนแรง)	สูงมาก/หายนะ	5	5	10	15	20	25
	สูง/วิกฤต	4	4	8	12	16	20
	ปานกลาง	3	3	6	9	12	15
	ต่ำ/น้อย	2	2	4	6	8	10
	ไม่เป็นสาระสำคัญ/น้อยมาก	1	1	2	3	4	5

ระดับของความเสี่ยง

เกณฑ์การยอมรับความเสี่ยง

ระดับความเสี่ยง	จัดระดับความเสี่ยง	แทนด้วยแถบสี	กลยุทธ์ในการจัดการความเสี่ยง
1-3	ต่ำ		ระดับที่ยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม (Acceptable or Limited Focus)
4-9	ปานกลาง		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังที่ระดับยอมรับไม่ได้ (Tolerable but caution or Management Discretion / Medium Risk)
10-16	สูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ (Intolerable or Attention Required / High Risk)
17-25	สูงมาก		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้ (Intolerable or Immediate Attention Required / High Risk)

มาตรการจัดการความเสี่ยง

หน่วยงานกำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ 10 ขึ้นไป ส่วนความเสี่ยงที่มีระดับต่ำกว่า 10 ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ระดับคะแนน	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
1	ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	10	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	-สร้างความตระหนักเรื่องการพึงรักษาสิทธิ์ในข้อมูลส่วนบุคคล -เปลี่ยนรหัสผ่านตามนโยบายแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศฯ -การกระตุ้นให้เกิดการปฏิบัติด้านเทคโนโลยีสารสนเทศฯ หรือระเบียบด้านสารสนเทศอย่างจริงจัง	ผู้ใช้ในหน่วยงาน/งานเทคโนโลยีสารสนเทศ	
2	ความเสี่ยงจากการนำอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	6	ลดความเสี่ยง	-จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว สามารถปฏิบัติงานได้ จัดทำแผนการตรวจสอบบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ/ สัญญาณอินเตอร์เน็ตให้ครอบคลุม	ผู้ใช้ในหน่วยงาน/งานเทคโนโลยีสารสนเทศ	
3	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับไฟกระชาก	15	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	-จัดหาเครื่องสำรองไฟฟ้าแบบมีระบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ -ประสานงานกับฝ่าย	ผู้ใช้ในหน่วยงาน/	

				อาคาร สถานที่ เพื่อจัดหาระบบสำรองไฟฟ้าสำหรับห้อง Server เพิ่มเติม	งานเทคโนโลยีสารสนเทศ	
4	ระบบเชื่อมโยงเครือข่าย Internet ใช้งานไม่ได้	9	ลดความเสี่ยง	-จัดทำเส้นทางออกสู่เครือข่าย Internet มากกว่า 1 ทาง	ผู้ใช้ในหน่วยงาน/งานเทคโนโลยีสารสนเทศ	
5	ความเสี่ยงจากการขาดทักษะความชำนาญเฉพาะด้านของบุคลากรผู้ปฏิบัติงาน/บุคคลากรไม่เพียงพอ	6	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	-จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม -จัดทำคู่มือปฏิบัติงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้	งานเทคโนโลยีสารสนเทศ	
6	ความเสี่ยงจาก -การเกิดไฟไหม้ -อาคารถล่ม -ความไม่สงบเรียบร้อยในบ้านเมือง	5	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	-ประสานกับฝ่ายอาคาร สถานที่ เพื่อจัดหาระบบเตือนภัยระบบดักจับความร้อน	ผู้ใช้ในหน่วยงาน/งานเทคโนโลยีสารสนเทศ	
7	ความเสี่ยงจากเครื่องคอมพิวเตอร์ลูกข่ายหรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้	10	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	-จัดทำแผนการตรวจสอบ บำรุงรักษาเครื่อง และอุปกรณ์อย่างสม่ำเสมอ	ผู้ใช้ในหน่วยงาน/งานเทคโนโลยีสารสนเทศ	
8	ความเสี่ยงจากเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	15	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	-ติดตั้งเครื่องแม่ข่ายภายในห้องที่มีความเหมาะสม -มีอุณหภูมิพอเหมาะควบคุมไม่ให้อุณหภูมิสูงเกินไป -จัดทำแผนการ	ผู้ใช้ในหน่วยงาน/งานเทคโนโลยีสารสนเทศ	

				ตรวจสอบบำรุงรักษาเครื่อง และอุปกรณ์อย่างสม่ำเสมอ -สำรองข้อมูล (Data Backup)		