โรงพยาบาลเขาสุกิม KHAOSUKIM HOSPITAL	**การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)**	**รหัสเอกสาร**	**KSK MOPH Identify -02**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้	**2 มี.ค. 2569**
		ชั้นความลับของเอกสาร	**ใช้ภายในเท่านั้น**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	**ผู้ตรวจทาน/ผู้ทบทวน**	**ผู้อนุมัติ**
ลายเซ็นต์			
ชื่อ-สกุล	นายวิษณุ กลางทุ่ง	นายพิทักษ์พงษ์ เพียเพ็งต้น	นายแพทย์พิริยะ ภิบาลกุล
ตำแหน่ง	นักวิชาการคอมพิวเตอร์	หัวหน้างานสุขภาพดิจิทัล (Lead Implementer)	ผู้อำนวยการโรงพยาบาลเขาสุกิม (CISO)
วันเดือนปี	24 กุมภาพันธ์ 2569	27 กุมภาพันธ์ 2569	2 มีนาคม 2569

ประวัติการแก้ไข

ครั้งที่	**วันที่ประกาศใช้**	**รายละเอียดการแก้ไข**
00	2 มีนาคม 2569	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

สารบัญ

หน้า

โรงพยาบาลเขาสุกิม KHAOSUKIM HOSPITAL	**การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)**	**รหัสเอกสาร**	**KSK MOPH Identify -02**
		แก้ไขครั้งที่	**00**
		วันที่บังคับใช้	**2 มี.ค. 2569**
		ชั้นความลับของเอกสาร	**ใช้ภายในเท่านั้น**

การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy Procedure)

อ้างอิง : พรบ ไซเบอร์ (ม.43, ม.44, ม.54), นโยบาย (ข้อ 2.1, ข้อ 2.2, ข้อ 2.3, ข้อ 3.1, ข้อ 3.2), ประมวลและกรอบ [ข้อ 18, ข้อ 18.1(ก), ข้อ 18.1(ข), ข้อ 18.1(ค), ข้อ 18.2, ข้อ 18.2(ข), ข้อ 18.3, ข้อ 18.4, ข้อ 21.1.4, ข้อ 21.2.1, ข้อ 21.2.2, ข้อ 21.3.1]

1. วัตถุประสงค์

วัตถุประสงค์เพื่อระบุและประเมินความเสี่ยงที่อาจเกิดกับบริการสำคัญ (Critical Service) ของโรงพยาบาลเขาสุกิมรวมทั้งอธิบายแนวทางการจัดการความเสี่ยง โดยความเสี่ยงดังกล่าวจะถูกประเมินจากแนวโน้มผลกระทบที่อาจจะส่งผลต่อองค์กร (Impact) และความเป็นไปได้ (Likelihood) ที่จะเกิดภัยคุกคามต่อช่องโหว่ (Threat-Vulnerability Likelihood) เพื่อให้สามารถเตรียมมาตรการป้องกันเพื่อรองรับและลดความเสี่ยงได้

โรงพยาบาลเขาสุกิมมีเป้าหมายที่จะลดระดับความเสี่ยงที่มีต่อทรัพย์สินและขั้นตอนที่เกี่ยวข้องกับทรัพย์สินทั้งหมดโดยทำให้ระดับความเสี่ยงที่ยังคงเหลืออยู่ (Residual risk) ต้องอยู่ในระดับที่สามารถยอมรับได้ (Risk appetite) ซึ่งไม่ส่งผลรุนแรงต่อการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงสาธารณสุขโดยระดับความเสี่ยงที่ยอมรับได้ดังกล่าวเป็นระดับความเสี่ยงที่ผู้บริหารกำหนดให้เป็นความเสี่ยงที่ยอมรับได้ต่อการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลเขาสุกิม

การจัดทำแนวทางการประเมินความเสี่ยงนี้มีวัตถุประสงค์เพื่อให้โรงพยาบาลเขาสุกิมสามารถดำเนินการประเมินความเสี่ยงและการจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ โดยคำนึงถึงจุดประสงค์ต่อไปนี้:

1. ละเว้นทรัพย์สินที่ไม่ต้องพึงระวัง
2. ไม่ป้องกันทรัพย์สินที่ไม่สำคัญมากเกินไปจนทำให้ที่ทรัพย์สินที่สำคัญไม่ได้รับการป้องกันที่เพียงพอ
3. สำนัก/กอง/ศูนย์/สำนักงาน/กลุ่มงาน หรือหน่วยงานเทียบเท่ากองและหน่วยงานเจ้าของโครงการ ในการประเมินความเสี่ยงด้านทรัพย์สินทั้งหมดปฏิบัติตามขั้นตอนการดำเนินงานที่ถูกกำหนดเช่นเดียวกัน

4. มาตรการรักษาความปลอดภัยใหม่หรือที่เสนอแนะเพิ่มเติมต้องสอดคล้องกับมาตรการที่มีอยู่เดิมไม่เพียงเสริมให้มีความสมบูรณ์ แต่ต้องให้ผลลัพธ์ร่วมกัน
5. มาตรการป้องกันที่นำมาใช้ต้องคำนึงถึงประสิทธิผลความคุ้มค่า (Cost Effective) ข้อจำกัดด้านทรัพยากร และต้องคำนึงถึงการป้องกันในขอบเขตที่มีความเสี่ยงสูง (High-risk Areas) เป็นลำดับแรก

2. ขอบเขต

2.1 การประเมินความเสี่ยงของกลุ่มงาน (Risk Assessment for Functions)

สำนัก/กอง/ศูนย์/สำนักงาน/กลุ่มงาน หรือหน่วยงานเทียบเท่ากอง หรือผู้ที่ได้รับมอบหมาย ของโรงพยาบาลเขาสุกิม ซึ่งมีหน้าที่รับผิดชอบบริหารจัดการ และจะดำเนินการประเมินความเสี่ยงในส่วนของทรัพย์สินที่ตนเองเป็นผู้รับผิดชอบ โดยผู้ที่ได้มอบหมายจะเป็นผู้ลงนามรับรองในในรายงานประเมินความเสี่ยงของหน่วยงานในส่วนที่ตนเองรับผิดชอบ

2.2 การประเมินความเสี่ยงของเครื่องมือเพื่อการจัดการภายใน

ความหมายของ “ทรัพย์สินเพื่อการจัดการภายใน” คือ อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์สำเร็จรูป หรือซอฟต์แวร์ประยุกต์เอกสารหรือข้อมูล ที่ใช้สำหรับการปฏิบัติงานทั่วไปภายในตามหน้าที่

ทรัพย์สินเพื่อการจัดการภายในสามารถสนับสนุนการปฏิบัติงานภายในของ โรงพยาบาลเขาสุกิม เช่น

- ข้อมูลรายชื่อผู้ดูแลระบบ
- ข้อมูลผู้รับบริการรายบุคคล (ข้อมูลคนไข้)
- ข้อมูลด้านการแพทย์และสุขภาพ
- เครื่องคอมพิวเตอร์แม่ข่าย
- อุปกรณ์เครือข่าย

- ระบบฐานข้อมูลสำหรับการจัดเก็บข้อมูล
- บุคลากร
- ผู้ใช้บริการภายนอก เช่น บริษัทดูแลบำรุงรักษาอุปกรณ์

รายการทรัพย์สินที่นำมาประเมินเหล่านี้จะนำมาจากแบบฟอร์มบัญชีทรัพย์สิน (Asset Inventory) ที่อยู่ในระเบียบปฏิบัติ เรื่อง การจัดการทรัพย์สินสารสนเทศขององค์กร (Asset Management)

2.3 การประเมินความเสี่ยงของโครงการพัฒนา/ปรับปรุงระบบสารสนเทศ

โครงการด้านการพัฒนาหรือการปรับปรุงสารสนเทศซึ่งโรงพยาบาลเขาสุกิมดำเนินการ ตัวอย่างเช่น โครงการปรับปรุงอุปกรณ์จะมีทรัพย์สินประเภทเครื่องคอมพิวเตอร์แม่ข่ายคอมพิวเตอร์ส่วนบุคคล ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่ใช้ภายในโรงพยาบาลเขาสุกิม โปรแกรมประยุกต์ที่พัฒนาขึ้นเอกสารต่าง ๆ ที่เกี่ยวกับโครงการ เช่น แผนโครงการ เอกสารการออกแบบและรายละเอียดคุณลักษณะ

3. ความรับผิดชอบในเอกสาร

<u>เจ้าของเอกสาร</u>

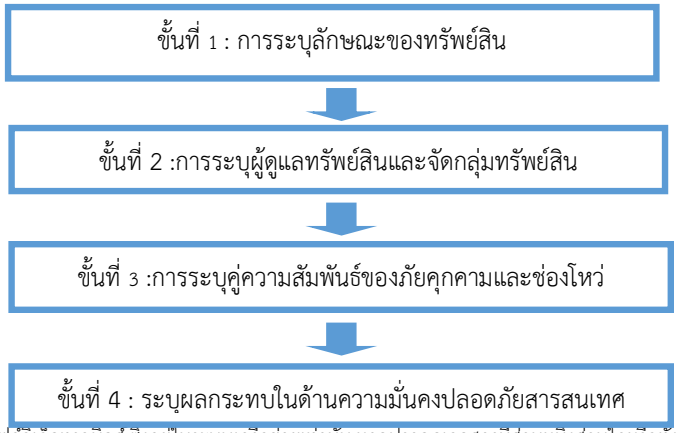
- สำนัก/กอง/ศูนย์/สำนักงาน/กลุ่มงาน หรือหน่วยงานเทียบเท่ากอง หรือผู้ที่ได้รับมอบหมาย

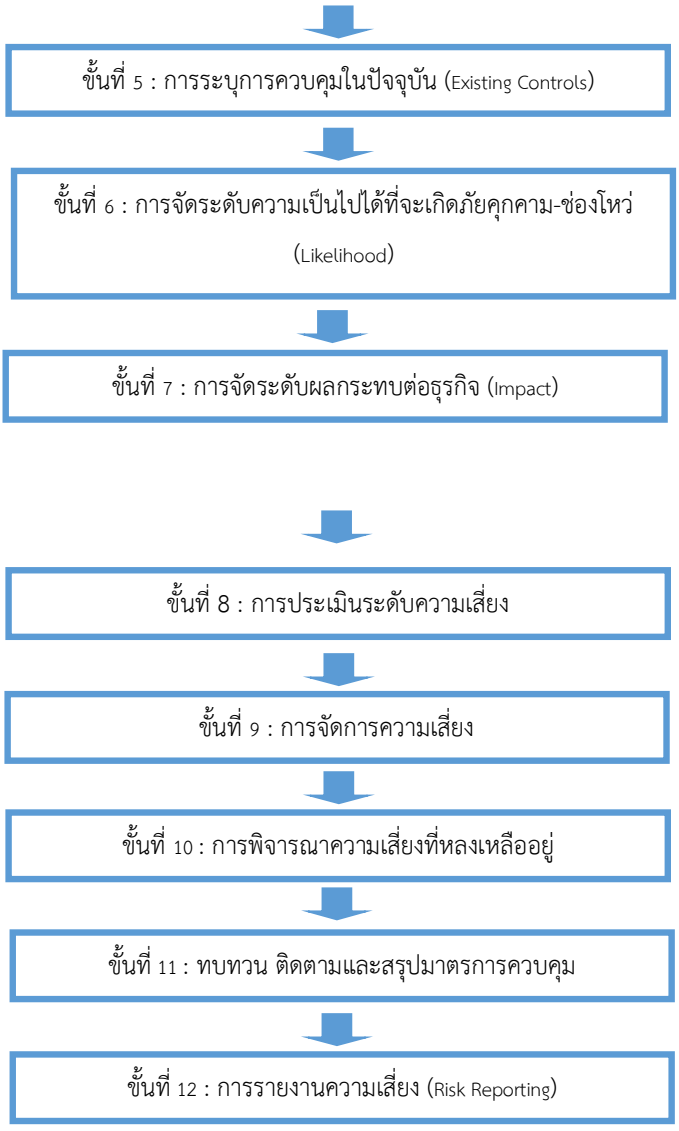
ผู้ใช้เอกสาร

- สำนัก/กอง/ศูนย์/สำนักงาน/กลุ่มงาน หรือหน่วยงานเทียบเท่ากอง หรือผู้ที่ได้รับมอบหมาย
- ผู้บริหารหรือคณะกรรมการที่มีอำนาจหน้าที่
- เจ้าของทรัพย์สิน (Asset Owner)
- เจ้าของความเสี่ยง (Risk Owner)
- คณะทำงานที่มีอำนาจหน้าที่

4. การประเมินความเสี่ยง

โรงพยาบาลเขาสุกิม จะใช้การประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง ประกอบไปด้วย 12 ขั้นตอนหลัก ดังภาพที่ 1 เพื่อนำมาประยุกต์ใช้ในการดำเนินงานของระบบบริหารจัดความมั่นคงปลอดภัยสารสนเทศ





ภาพที่ 1 ขั้นตอนการประเมินระดับความเสี่ยง

4.1 ขั้นที่ 1 : การระบุลักษณะของทรัพย์สิน

ข้อมูลและกระบวนการที่เกี่ยวข้องกับทรัพย์สินภายในสำนัก/กอง/ศูนย์/สำนักงาน/กลุ่มงาน หรือหน่วยงานเทียบเท่ากอง ทั้งหมดต้องถูกระบุเพื่อให้สามารถจัดหามาตรการป้องกันให้เหมาะสมเพียงพอตามหลักการบริหารและประเมินความเสี่ยง โดยการจัดหมวดหมู่ของทรัพย์สินและตัวอย่างประกอบการจัดในแต่ละหมวดทั้งหมด 9 ประเภท ได้แก่

1. กระบวนการทำงาน (Business Process) เช่น กระบวนการบำรุงรักษาอุปกรณ์ กระบวนการสำรองข้อมูล กระบวนการแก้ไขเหตุเสีย เป็นต้น
2. ข้อมูลสารสนเทศ (Information) เช่น ข้อมูลการตั้งค่าระบบ ข้อมูลที่บันทึกภายในเครื่องแม่ข่าย เอกสารสัญญา คู่มือการบำรุงรักษาระบบ เป็นต้น
3. ฮาร์ดแวร์ (Hardware) เช่น เครื่องแม่ข่าย เครื่องปรับอากาศ เครื่องกำเนิดไฟฟ้าอุปกรณ์ไฟฟ้าสำรอง อุปกรณ์ดับเพลิง เป็นต้น
4. คอมพิวเตอร์เสมือน (Virtual Machines) เช่น ระบบปฏิบัติการที่ใช้งานเสมือนคอมพิวเตอร์ เป็นต้น
5. ซอฟต์แวร์ (Software) เช่น ซอฟต์แวร์ของ Operating System, โปรแกรม Anti- Virus, โปรแกรมควบคุมระบบ Access Control, Security Monitoring เป็นต้น
6. อุปกรณ์เน็ตเวิร์ก (Network) เช่น อุปกรณ์เครือข่าย สายสัญญาณ เป็นต้น
7. บุคลากร (Personnel) เช่น พนักงานดูแลศูนย์คอมพิวเตอร์ เป็นต้น
8. สถานที่ (Site) เช่น อาคารสำนักงาน พื้นที่ศูนย์คอมพิวเตอร์ ศูนย์สำรอง เป็นต้น
9. กลุ่มงานสนับสนุน (Organization) เช่น ผู้ให้บริการจากภายนอก ได้แก่ บริษัทบำรุงรักษาอุปกรณ์ บริษัทผู้ให้บริการโครงข่าย เป็นต้น

4.2 ขั้นที่ 2 : การระบุผู้ดูแลทรัพย์สินและจัดกลุ่มทรัพย์สิน

เมื่อรวบรวมรายการทรัพย์สินครบถ้วนแล้ว ให้ระบุชื่อกลุ่มงานที่ทำหน้าที่ดูแลทรัพย์สินนั้น และให้ดำเนินการจัดกลุ่มรายการทรัพย์สินที่สามารถจัดให้อยู่ในกลุ่มเดียวกันได้ เช่น หากมีเครื่องแม่ข่าย (Server) หลายเครื่องในระบบโดยมีหน้าที่การทำงานเหมือนกันและติดตั้งอยู่ในสภาพแวดล้อมคล้ายคลึงกันจะสามารถจัดกลุ่มให้อยู่ในกลุ่มเดียวกันได้เพื่อความสะดวกในขั้นตอนการประเมินความเสี่ยงต่อไป ในกรณีที่ไม่สามารถจัดกลุ่มรายการทรัพย์สินได้ให้กำหนดชื่อกลุ่มรายการทรัพย์สินเป็นชื่อเดียวกับทรัพย์สินนั้น

4.3 ขั้นที่ 3 : การระบุคู่ความสัมพันธ์ของภัยคุกคามและช่องโหว่

ช่องโหว่ : เป็นจุดอ่อนที่เกี่ยวข้องกับทรัพย์สิน ซึ่งอาจจะถูกคุกคามจากภัยต่าง ๆ ก่อให้เกิดการละเมิดความปลอดภัยที่ไม่พึงปรารถนาขึ้น ซึ่งส่งผลให้มีการสูญเสีย ความเสียหาย หรืออันตรายต่อธุรกิจ (ช่องโหว่ที่มีอยู่ในตัวอุปกรณ์ไม่ก่อให้เกิดอันตราย เป็นเพียงสภาพหรือกลุ่มสภาพที่เอื้อให้ภัยคุกคามเข้ามาส่งผลต่อทรัพย์สิน)

ภัยคุกคาม : เป็นสาเหตุสำคัญที่ทำให้เกิดการละเมิดความปลอดภัยที่ไม่พึงปรารถนาซึ่งจะเป็นอันตรายต่อระบบ องค์กร และทรัพย์สินขององค์กร

ทรัพย์สินต่าง ๆ อาจได้รับผลกระทบจากภัยหลากหลายประเภทที่เข้ามาคุกคามและใช้ประโยชน์จาก ช่องโหว่ที่มีอยู่ของระบบ โปรแกรมการใช้งานเฉพาะ หรือบริการที่ใช้ในสำนักงาน

เจ้าของความเสี่ยง (Risk owner) : ระบุบุคคลหรือนิติบุคคลที่มีภาระรับผิดชอบและมีอำนาจในการบริหารความเสี่ยง

4.4 ขั้นที่ 4 : ระบุผลกระทบในด้านความมั่นคงปลอดภัยสารสนเทศ

หลังจากกำหนดภัยคุกคามและช่องโหว่ที่อาจเกิดขึ้น ให้ระบุผลกระทบของภัยคุกคามและช่องโหว่แต่ละรายการ ที่สะท้อนในด้านของความมั่นคงปลอดภัย 3 ด้านหลักต่อไปนี้

- **ด้านความลับ การเข้าถึงได้เฉพาะผู้มีสิทธิ์ (Confidentiality)** หมายถึง การรักษาหรือสงวนไว้เพื่อป้องกันทรัพย์สิน เช่น ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานสนับสนุน ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์ จากการเข้าถึง หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต
- **ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity)** หมายถึง การรักษาซึ่งความถูกต้องครบถ้วนสมบูรณ์ของทรัพย์สินเพื่อให้แน่ใจว่าทรัพย์สิน เช่น ข้อมูลที่ถูกต้องขององค์กรจะไม่ถูกแก้ไขโดยผู้ที่ไม่มีสิทธิ์ ผู้ที่ไม่ได้รับอนุญาต หรือไม่ถูกเปลี่ยนแปลง เพราะหากทรัพย์สินที่มีความสำคัญโดยเฉพาะข้อมูลที่เป็นความลับหรือข้อมูลที่มีความสำคัญนั้นถูกเปลี่ยนแปลงแก้ไขจะส่งผลเสียอย่างมากเพราะข้อมูลนั้นเชื่อถือไม่ได้หรือส่งผลกระทบต่อองค์กร
- **ด้านความพร้อมใช้งาน (Availability)** หมายถึง การรักษาสภาพความพร้อมใช้งานของข้อมูล ระบบคอมพิวเตอร์ ซึ่งครอบคลุมถึงสารสนเทศและระบบสารสนเทศ ระบบงานสนับสนุน ให้ผู้ที่มีสิทธิ์สามารถเข้าใช้งานได้ในเวลาที่ต้องการหรือตามที่ได้กำหนดไว้

4.5 ขั้นที่ 5 : การระบุการควบคุมในปัจจุบัน (Existing Controls)

ระบุมาตรการควบคุมที่เกี่ยวของกับทรัพย์สินต่าง ๆ ที่มีอยู่ในปัจจุบัน เช่น มาตรการการสำรองข้อมูล (Back-up) การจัดจ้างการบำรุงรักษาระบบ (Maintenance Agreement) การติดตั้งระบบที่มีความคงทนสูง (High Availability) เป็นต้น โดยมาตรการควบคุมที่มีประสิทธิผลจะมีผลต่อการควบคุมระดับความเสี่ยงที่เกิดขึ้นได้โดยอาจจะมีส่วนช่วยในการลดระดับโอกาสการเกิดเหตุการณ์ (Likelihood) หรือระดับของผลกระทบ (Impact) ทั้งนี้ขึ้นอยู่กับประเภทของความเสี่ยงและมาตรการควบคุมนั้น ๆ

4.6 ขั้นที่ 6 : การจัดระดับความเป็นไปได้ที่จะเกิดภัยคุกคาม-ช่องโหว่ (Likelihood)

การจัดระดับความเป็นไปได้ที่จะเกิดภัยคุกคามซึ่งใช้ประโยชน์จากช่องโหว่ที่เอื้อเฉพาะแบ่งตามตารางที่ 1

ตารางที่ 1 ตารางแสดงระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood)

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ(Likelihood)			
ระดับ	**โอกาสที่เกิด**	**เชิงปริมาณ**	**เชิงคุณภาพ**
5	สูงมาก	1 เดือนต่อครั้งหรือมากกว่า	มีโอกาสเกิดขึ้นเป็นประจำ (76% ขึ้นไป)
4	สูง	1-6 เดือนต่อครั้งแต่ไม่เกิน 5 ครั้ง	มีโอกาสเกิดขึ้นบ่อยครั้ง (51%-75%)
3	ปานกลาง	1 ปีต่อครั้ง	มีโอกาศเกิดขึ้นบางครั้ง (31%-50%)
2	น้อย	2-4 ปีต่อครั้ง	มีโอกาสเกิดขึ้นน้อยครั้ง (11%-30%)
1	น้อยมาก	5 ปีต่อครั้ง	มีโอกาสเกิดขึ้นยาก (ไม่เกิน 10%)

ในการประเมินความเป็นไปได้ของภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ จะต้องพิจารณาปัจจัยต่อไปนี้ :

- เหตุการณ์ละเมิดความปลอดภัยในอดีตที่เคยประสบ
- ภัยคุกคามจากสิ่งแวดล้อมในองค์กรภัยคุกคามที่กระทำโดยเจตนา และภัยคุกคามที่เกิดขึ้นโดยไม่ได้ตั้งใจ
- แรงจูงใจประสิทธิภาพที่รับรู้และจำเป็น ทรัพยากรที่เอื้อต่อผู้บุกรุกการรับรู้ถึงประโยชน์ที่จะได้รับ
- เตรียมการป้องกันและมาตรการควบคุมให้พร้อมเพื่อบรรเทาความเป็นไปได้ที่จะเกิดขึ้น

4.7 ขั้นที่ 7 : การจัดระดับผลกระทบต่อธุรกิจ (Impact)

ในการกำหนดระดับความเสียหายที่มีต่อองค์กรให้พิจารณาการประเมินผลมาตรการควบคุมที่ใช้งานอยู่ในปัจจุบันก่อน แล้วจึงพิจารณาผลอันอาจจะเกิดมาจากเกิดความไม่ปลอดภัยที่ส่งผลต่อข้อมูล ซึ่งระดับผลกระทบพิจารณาจากผลลัพธ์ของการสูญเสีย ดังนี้

- การสูญเสียความลับ (Loss of Confidentiality) การเปิดเผยทรัพย์สินประเภทข้อมูลหรือการเข้าถึงระบบโดยไม่ได้รับอนุญาตหรือการแทรกแซงข้อมูล
- การสูญเสียความสมบูรณ์ (Loss of Integrity) ข้อมูลหรือการทำงานระบบ ไม่ถูกต้องและสมบูรณ์
- การสูญเสียความพร้อมใช้งาน (Loss of Availability) ผู้ใช้ไม่สามารถใช้ประโยชน์จากข้อมูลหรือระบบที่สำคัญในเวลาที่ต้องการได้

โดยจะจัดระดับแยกตามทรัพย์สินหรือชุดของทรัพย์สิน และคู่ของภัยคุกคามกับช่องโหว่ และใช้แบบฟอร์มประเมินความเสี่ยงและควบคุมแก้ไขความเสี่ยง (Risk Assessment & Risk Treatment Form) ซึ่งได้กำหนดให้มีระดับผลกระทบต่อองค์กรทั้ง 5 ด้าน ดังตารางที่ 2

ตารางที่ 2 ตารางแสดงระดับผลกระทบ (Impact)

ตารางผลกระทบทางด้านตัวเงิน		
ระดับ	**ระดับผลกระทบ**	**ผลกระทบ**
5	สูงมาก	> 10 ล้านบาท
4	สูง	>2.5 แสนบาท – 10 ล้านบาท
3	ปานกลาง	>50,000 – 2.5 แสนบาท
2	น้อย	>10,000 – 50,000 บาท
1	น้อยมาก	ไม่เกิน 10,000 บาท

ตารางผลกระทบทางด้านระบบเทคโนโลยีสารสนเทศ		
ระดับ	**ระดับผลกระทบ**	**ผลกระทบ**
5	สูงมาก	เกิดความสูญเสียต่อระบบสารสนเทศ หรือไม่สามารถให้บริการระบบสารสนเทศได้ (ไม่มีแผนรองรับ ไม่มีอุปกรณ์สำรอง ไม่มีระบบทำงานหรือให้บริการทดแทน) กระทบภายในองค์กรและภายนอกองค์กร
4	สูง	เกิดความสูญเสียต่อระบบสารสนเทศ หรือไม่สามารถให้บริการระบบสารสนเทศได้ (ไม่มีแผนรองรับ ไม่มีอุปกรณ์สำรอง ไม่มีระบบทำงานหรือให้บริการทดแทน) กระทบภายในองค์กร

ตารางผลกระทบทางด้านระบบเทคโนโลยีสารสนเทศ		
ระดับ	**ระดับผลกระทบ**	**ผลกระทบ**
3	ปานกลาง	เกิดความสูญเสียต่อระบบสารสนเทศ สามารถดำเนินการแก้ไขได้ตามเวลาที่กำหนดไว้ (มีแผนรองรับ) ไม่สามารถให้บริการได้ในช่วงที่ดำเนินการแก้ไขกระทบภายในองค์กรหรือภายนอกองค์กร
2	น้อย	เกิดความสูญเสียต่อระบบสารสนเทศ สามารถดำเนินการแก้ไขได้ตามเวลา ที่กำหนดไว้ (มีอุปกรณ์สำรอง มีระบบทำงานหรือให้บริการทดแทนได้) ไม่กระทบต่อการให้บริการภายในองค์กรและภายนอกองค์กร
1	น้อยมาก	ไม่กระทบระบบสารสนเทศและการให้บริการภายในองค์กรและภายนอกองค์กร

ตารางผลกระทบทางด้านข้อมูลด้านการแพทย์และสุขภาพ/ข้อมูลส่วนบุคคล		
ระดับ	ระดับผลกระทบ	ผลกระทบ
5	สูงมาก	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลได้รับผลกระทบกับชีวิตในระดับสูงจนทำให้ไม่สามารถกลับมาใช้ชีวิตเช่นเดิมได้ เพราะข้อมูลส่วนบุคคลบางอย่างถูกเปิดเผยหรือทำให้เกิดโรคทางจิตหรือทางกายจนไปถึงขั้นเสียชีวิต

ตารางผลกระทบทางด้านข้อมูลด้านการแพทย์และสุขภาพ/ข้อมูลส่วนบุคคล		
ระดับ	ระดับผลกระทบ	ผลกระทบ
4	สูง	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลได้รับผลกระทบกับชีวิต ในระดับสูง เช่น ทำ ให้ถูกยักยอกทรัพย์ ทำให้ถูกติดแบล็คลิสต์ของสถาบันการเงิน ทรัพย์สินเกิดความ เสียหาย ถูกเลิกจ้างงาน โดนหมายเรียกในชั้นศาล สุขภาพเสื่อมถอย
3	ปานกลาง	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลรู้สึกได้ถึงความไม่สะดวกอย่างมีนัยสำคัญ หรือทำให้ทรัพย์สินเสียหาย หรือกระทบต่อจิตใจและร่างกายในระดับไม่ร้ายแรง เช่น เข้าใช้งานระบบที่ที่เคยใช้บริการไม่ได้ หรือเกิดความรู้สึกกังวล เกิดความเข้าใจผิด เกิดความเครียด หรือ เกิดความเจ็บป่วยเล็กน้อย
2	น้อย	ผลกระทบนั้นอาจจะทำให้เจ้าของข้อมูลรู้สึกได้ถึงความไม่สะดวก เช่น เคยให้ข้อมูลกับผู้ควบคุมข้อมูลไปแล้วกลับต้องให้ข้อมูลซ้ำอีกครั้งซึ่งอาจจะเกิดจากผู้ควบคุมข้อมูลทำข้อมูลสูญหายหรือข้อมูลเกิดความเสียหายทำให้ข้อมูลไม่ถูกต้อง
1	น้อยกว่า	ไม่มีผลกระทบต่อเจ้าของข้อมูล

ตารางผลกระทบทางด้านบุคลากร		
ระดับ	**ระดับผลกระทบ**	**ผลกระทบ**
5	สูงมาก	มีการบาดเจ็บถึงชีวิต
4	สูง	มีการบาดเจ็บสาหัสถึงขั้นพักงาน

ตารางผลกระทบทางด้านบุคลากร		
ระดับ	ระดับผลกระทบ	ผลกระทบ
3	ปานกลาง	มีการบาดเจ็บสาหัสถึงขั้นหยุดงาน
2	น้อย	มีการบาดเจ็บรุนแรง ยังสามารถปฏิบัติงานได้
1	น้อยมาก	ไม่มีการบาดเจ็บรุนแรง

ตารางผลกระทบทางด้านชื่อเสียง		
ระดับ	ระดับผลกระทบ	ผลกระทบ
5	สูงมาก	มีการเผยแพร่ข่าวภายนอกองค์กร และมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร ระดับภายในประเทศและต่างประเทศ
4	สูง	มีการเผยแพร่ข่าวภายนอกองค์กร และมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร ระดับภายในประเทศ
3	ปานกลาง	มีการเผยแพร่ข่าวทั่วทั้งองค์กร และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร
2	น้อย	มีการเผยแพร่ข่าวในวงจำกัดระดับกลุ่มงาน/ฝ่าย และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร
1	น้อยมาก	มีการเผยแพร่ข่าวในวงจำกัดระดับผู้ปฏิบัติงาน และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงขององค์กร

4.8 ขั้นที่ 8 : การประเมินระดับความเสี่ยง

การจัดระดับความเสี่ยงควรแบ่งตามกลุ่มทรัพย์สินที่มีประเภทเดียวกัน และคู่ของภัยคุกคามกับช่องโหว่โดยพิจารณาจากผลกระทบต่อธุรกิจและความเป็นไปได้ที่อาจจะเกิดขึ้น ดังที่แสดงในตารางที่ 3

ความเสี่ยง คือ โอกาสที่ภัยคุกคามจะอาศัยช่องโหว่ที่มีอยู่บนทรัพย์สินเพื่อก่อให้เกิดความเสียหายต่อ ทั้งทรัพย์สินหรือองค์กร ทั้งนี้ภัยคุกคามอาจมีหลากหลายหรืออาจมีเพียงแค่ภัยเดียว ที่อาจอาศัยช่องโหว่ บนทรัพย์สินเข้าทำความเสียหาย ซึ่งอาจอาศัยเพียงช่องโหว่เดียวหรือหลายช่องโหว่ที่มีอยู่ก็ได้เช่นกัน ทั้งนี้คุณลักษณะของความเสี่ยงจะอธิบายด้วยองค์ประกอบสององค์ประกอบด้วยกันคือ องค์ประกอบที่หนึ่ง โอกาสเกิดของเหตุการณ์ (Likelihood) และองค์ประกอบที่สองผลกระทบจากเหตุการณ์องค์ (Impact) โดย

ระดับความเสี่ยง = ผลกระทบจากเหตุการณ์ ที่มีค่าสูงสุด x โอกาสของเหตุการณ์

การพิจารณายอมรับความเสี่ยง และการจัดการความเสี่ยง (Risk Acceptance Level)

เมื่อได้ผลของระดับความเสี่ยงจากทรัพย์สินต่าง ๆ แล้ว ให้พิจารณาระดับความเสี่ยงที่ได้เทียบกับเกณฑ์ระดับความเสี่ยงที่ยอมรับได้ตามตารางดังต่อไปนี้

สูตรคำนวณเกณฑ์การประเมินค่าความเสี่ยง (Risk Assessment Calculation)

Risk Level = Impact Rating Level x Likelihood Rating

ตารางที่ 3 การประเมินระดับความเสี่ยง

ระดับโอกาสในการเกิดเหตุการณ์ (Likelihood)		ระดับผลกระทบ (Impact)				
		น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
		1	2	3	4	5
สูงมาก	5	5	10	15	20	25
สูง	4	4	8	12	16	20
ปานกลาง	3	3	6	9	12	15
น้อย	2	2	4	6	8	10
น้อยมาก	1	1	2	3	4	5

4.9 ขั้นที่ 9 : การจัดการความเสี่ยง

ในการจัดการความเสี่ยงต้องพิจารณาถึงการกำหนดและการคัดเลือกมาตรควบคุม (Controls) เพื่อใช้ในจัดการทรัพย์สินที่มีค่าความเสี่ยงอยู่ในระดับสูง ซึ่งในการจัดการความเสี่ยงนั้นจะพิจารณาระดับความเสี่ยงที่มีค่าระดับ ดังนี้

เกณฑ์ระดับความเสี่ยง	การจัดการความเสี่ยง	ความหมาย
ระดับความเสี่ยงสูงมาก	ลดความเสี่ยง/ควบคุมความเสี่ยง	ความเสี่ยงสูงมากจำเป็นต้องได้รับการจัดการทันทีมีความจำเป็นเร่งด่วน หรือเป็นคำสั่งจากผู้บริหาร แผนจัดการความเสี่ยงควรเริ่มต้นการปรับปรุงทันที และดำเนินการให้เสร็จสิ้นภายใน 3 เดือน นับจากวันที่ได้รับอนุมัติแผนจัดการความเสี่ยง หรือดำเนินการเร่งด่วนที่สุดตามระยะเวลาที่เหมาะสม

เกณฑ์ระดับความเสี่ยง	การจัดการความเสี่ยง	ความหมาย
ระดับความเสี่ยงสูง	ลดความเสี่ยง/ควบคุมความเสี่ยง	ความเสี่ยงสูงจะต้องได้รับการจัดการในลำดับถัดมาหรือทีนที ถ้าไม่พบความเสี่ยงสูงมากมีความจำเป็นเร่งด่วน แผนจัดการความเสี่ยงควรเริ่มต้นการปรับปรุงทันที และดำเนินการให้เสร็จสิ้นภายใน 3 - 6 เดือน นับจากวันที่ได้รับอนุมัติแผนจัดการความเสี่ยง หรือดำเนินการเร่งด่วนตามระยะเวลาที่เหมาะสม
ระดับความเสี่ยงปานกลาง	ยอมรับความเสี่ยงหรือจัดทำแผน	ความเสี่ยงปานกลาง สามารถยอมรับได้ถ้ามีมาตรการควบคุมในปัจจุบันที่ดี แต่ถ้าขาดมาตรการควบคุมในปัจจุบันต้องกำหนดแผนมาตรการเฝ้าระวังความเสี่ยงดังกล่าว ควรดำเนินการเสร็จสิ้นภายใน 6 – 12 เดือน นับจากวันที่ได้รับอนุมัติแผนจัดการความเสี่ยง หรือดำเนินการเร่งด่วนตามระยะเวลาที่เหมาะสม
ระดับความเสี่ยงต่ำ	ยอมรับความเสี่ยง	ความเสี่ยงต่ำ สามารถยอมรับความเสี่ยง ไม่ต้องดำเนินการใดๆ

หมายเหตุ : หลังจากพิจารณาระดับความเร่งด่วนแล้วไม่มีแผนลดความเสี่ยงที่มีความเร่งด่วนในระดับสูงมากให้ดำเนินการแผนลดความเสี่ยงสูงและระดับความเสี่ยงปานกลางตามลำดับได้ทันที

ความเสี่ยงของรายการประเมินความเสี่ยงที่ต้องดำเนินการจัดทำตามระเบียบปฏิบัติ เรื่อง การแก้ไขและควบคุมความเสี่ยง (Risk Treatment Procedure) โดยจะต้องมีการติดตามผล ทบทวนแผนจัดการความเสี่ยง และประเมินความเสี่ยงภายหลังการจัดการความเสี่ยง

โดยวิธีการจัดการความเสี่ยงที่เป็นไปได้ดังนี้:

1. การหลีกเลี่ยงความเสี่ยงด้วยการตัดสินใจจะไม่เดินหน้ากระทำกิจกรรมที่มีแนวโน้มก่อให้เกิดความเสี่ยง หรือเลือกวิธีการอื่น ๆ มาใช้บริหารงาน
2. การถ่ายโอนความเสี่ยงด้วยการจัดการถ่ายโอนความเสี่ยงทั้งหมดหรือเพียงบางส่วนให้หน่วยงานอื่นรับผิดชอบ
3. การลดความเสี่ยงด้วยการลดภัยคุกคามและช่องโหว่หรือแก้ไขทรัพย์สินที่มีความเสี่ยง โดยการเลือกและปฏิบัติตามมาตรการรักษาความปลอดภัยที่เหมาะสม

ในการเลือกมาตรการรักษาความปลอดภัยเพื่อนำมาพัฒนาและปฏิบัติต้องพิจารณาปัจจัยต่อไปนี้ :

- ข้อกำหนดที่เป็นกฎข้อบังคับและเป็นกฎหมาย
- ต้นทุน
- ความสะดวกในปฏิบัติงานและการให้บริการ
- การมีมาตรการรักษาความปลอดภัยที่เข้มแข็ง
- ภารกิจต่าง ๆ เพื่อการควบคุมที่ต้องดำเนินการการป้องกันการยับยั้งการตรวจจับ การกู้คืน การแก้ไข การตรวจตรา และการสร้างความตระหนัก

ในการเลือกแนวทางควบคุมอาจต้องเลือกใช้มาตรการควบคุมซึ่งรวมทั้งการควบคุมด้านปฏิบัติงานทั่วไป (Non-technical) และการควบคุมด้านเทคนิคให้สมดุลกันเพื่อสนับสนุนและเสริมให้มีความสมบูรณ์ขึ้น นอกจากนี้ควรได้ดำเนินการตรวจสอบการควบคุมที่มีอยู่การควบคุมที่ถูกวางแผนไว้ และการรักษาสภาพ (Maintenance) ของการควบคุม โดยตรวจสอบเปรียบเทียบด้านการลงทุน (Cost Comparisons) และในกรณีที่มาตรการควบคุมไม่มีประสิทธิภาพเพียงพอควรพิจารณายกเลิกหรือปรับปรุงมาตรการดังกล่าว โดยมาตรการควบคุมที่จะนำมาใช้สามารถเลือกจากมาตรฐาน พรบ ไซเบอร์ หรือ ISO/IEC 27002:2022 หรือ ISO/IEC 27002 Information Technology - Security Techniques - Code of Practice for Information Security Management หรือ อื่น ๆ ซึ่งต้องสอดคล้องกับวัตถุประสงค์ในการควบคุมหรือวิธีปฏิบัติที่มีประสิทธิภาพที่ใช้ในระบบอุตสาหกรรมอื่น ๆ

4. ระดับความเสี่ยงที่ยอมรับได้ (Acceptable Risk Level) ความเสี่ยงที่อยู่ต่ำกว่า 4 พิจารณาว่าเป็นความเสี่ยงที่ยอมรับได้

4.10 ขั้นที่ 10 : การพิจารณาความเสี่ยงที่หลงเหลืออยู่

หลังจากจัดการความเสี่ยง หากทางเลือกในการตอบสนองความเสี่ยงเป็นการ ควบคุม หลีกเลี่ยงหรือถ่ายโอน ต้องดำเนินการประมาณระดับความเสี่ยงที่เหลือ ด้วยการประมาณผลกระทบและโอกาสเกิดที่คาดว่าเมื่อเลือกแนวทางตอบสนองความเสี่ยงแล้ว จะมีผลกระทบและโอกาสเกิดของความเสี่ยงอย่างไร

4.11 ขั้นที่ 11 : ทบทวน ติดตามและสรุปมาตรการควบคุม

เมื่อประเมินความเสี่ยงและกำหนดแนวทางจัดการความเสี่ยงเสร็จสิ้นแล้ว ให้ดำเนินการทบทวนติดตามและสรุปมาตรการควบคุมในเอกสารขอบเขตการนำไปใช้งาน

4.12 ขั้นที่ 12 : การรายงานความเสี่ยง (Risk Reporting)

รายงานผลการวิเคราะห์ความเสี่ยงและผลการบริหารจัดการความเสี่ยงต่อผู้บริหารหรือคณะกรรมการที่มีอำนาจ

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

5. เอกสารอ้างอิง

1. ทะเบียนความเสี่ยง (Risk Register)
2. เอกสารการประเมินความเสี่ยงและการจัดการความเสี่ยง (Risk Assessment and Risk Treatment)
3. ดัชนีวัดความเสี่ยงที่สำคัญ (Key Risk Indicator : KRI)
4. การประเมินความเสี่ยง (Risk Assessment)
5. รายงานการประเมินความเสี่ยง (Risk Assessment Report)