โรงพยาบาลพระศรีมหาโพธิ์

ระเบียบปฏิบัติ

เรื่อง การประเมินความเสี่ยงปลอดภัย ของข้อมูลสารสนเทศ

QP – ISMS - 09

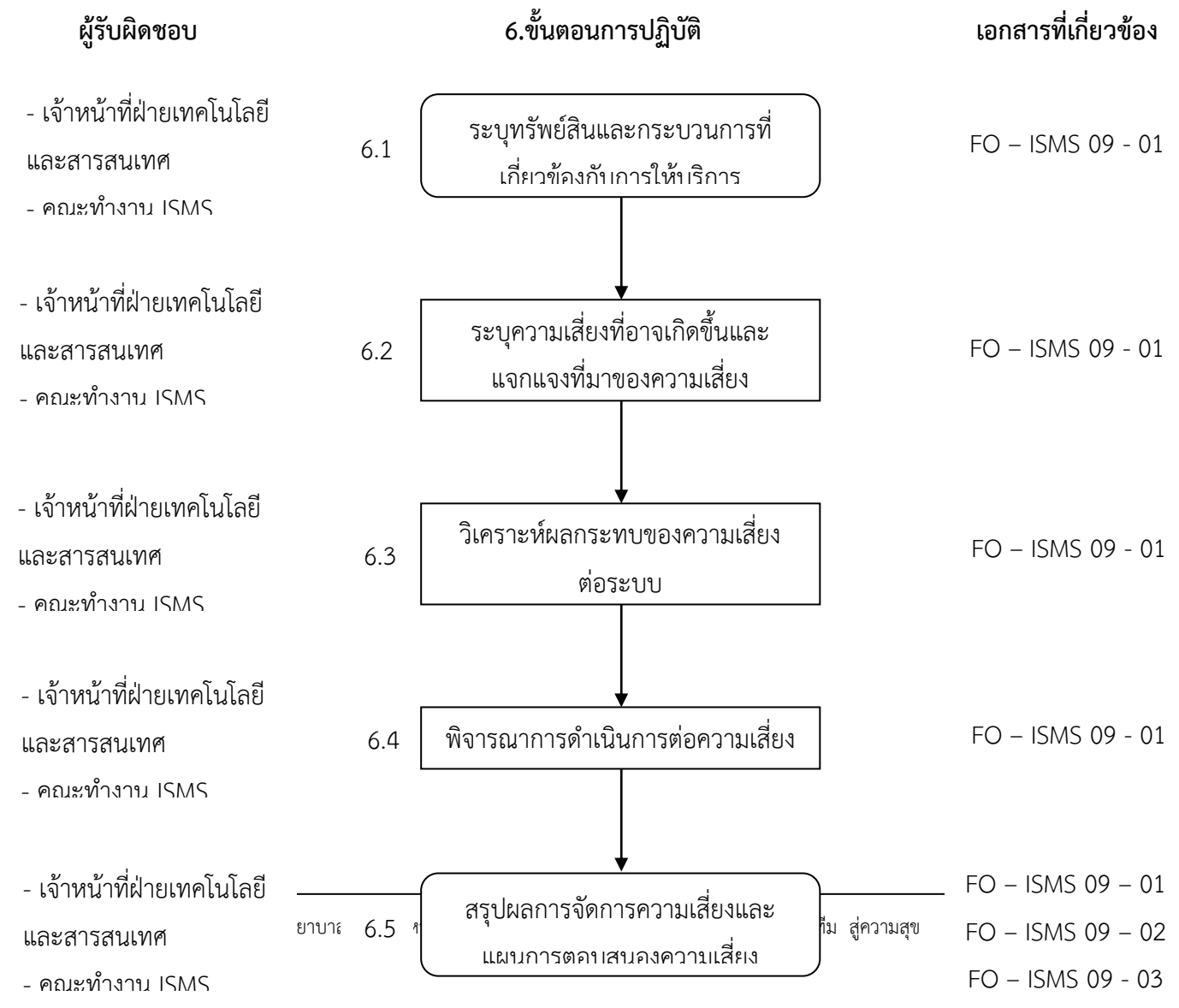
	ชื่อ - สกุล	ลายเซ็น	วัน / เดือน / ปี
จัดทำ/แก้ไขโดย	นายวุฒิไกร พิมพ์หล่อ นักวิชาการคอมพิวเตอร์ปฏิบัติการ		21 มีนาคม 2565
รับรองโดย	นายวีระยุทธ มายุศิริ เลขานุการคณะทำงาน ISMS		21 มีนาคม 2565
ทบทวนโดย	นางวิรีย์อร จูมพระบุตร ประธานคณะทำงาน ISMS		21 มีนาคม 2565
อนุมัติโดย	นายประภาส อุครานันท์ ผู้อำนวยการโรงพยาบาล		21 มีนาคม 2565
สำเนาฉบับที่..... เอกสารฉบับ (/) ควบคุม ( ) ไม่ควบคุม			

สารบัญ

บันทึกการประกาศใช้

ฉบับ	แก้ไขครั้งที่	วัน/เดือน/ปี	รายละเอียด	จัดทำ/แก้ไขโดย	อนุมัติโดย
A	00	21 มี.ค. 2565	- ประกาศใช้ฉบับแรก	นายวุฒิไกร พิมพ์หล่อ	นายประภาส อุครานันท์

1. ผังการไหลของกระบวนการประเมินความเสี่ยงปลอดภัยของข้อมูลสารสนเทศ



2 วัตถุประสงค์

2.1 เพื่อกำหนดขั้นตอนมาตรฐานในการประเมินความเสี่ยง และแก้ไขควบคุมความเสี่ยงขององค์กร ให้มีการดำเนินการอย่างสอดคล้องกันในขอบเขตของการขอการรับรอง

2.2 เพื่อให้ทราบและเข้าใจถึงแนวคิด กรอบการทำงาน บทบาทหน้าที่ความรับผิดชอบ ในกระบวนการการจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยสารสนเทศ

2.3 เพื่อกำหนดแนวทางการวัดผลของกระบวนการจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยสารสนเทศและการปรับปรุงประสิทธิภาพของกระบวนการอย่างต่อเนื่อง

3 **ขอบเขต**

ผู้มีหน้าที่รับผิดชอบในขอบเขตนี้จะต้องดำเนินการรวบรวมแหล่งที่มาของข้อมูลที่เกี่ยวข้องกับทางด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อนำมากำหนดประเภทของความเสี่ยง แล้วจัดลำดับความสำคัญ ความรุนแรง ที่จะมีผลกระทบต่อทรัพยากรและการให้บริการของระบบสารสนเทศ พร้อมทั้งนำข้อมูลดังกล่าวมาบริหารจัดการเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมทั้งดำเนินการเฝ้าระวัง และประเมินผลการจัดการความเสี่ยงด้านสารสนเทศเป็นระยะ อย่างต่อเนื่อง พร้อมทั้งปรับปรุงกระบวนการบริหารจัดการด้านความเสี่ยงสารสนเทศให้มีประสิทธิภาพมากยิ่งขึ้น

4 คำนิยาม

4.1 ความมั่นคงปลอดภัยด้านสารสนเทศ (INFORMATION SECURITY)	หมายถึง การป้องกันสารสนเทศจากภัยคุกคามต่าง ๆ เพื่อทำให้มั่นใจว่าการดำเนินงานจะธำรงไว้ซึ่งความลับความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศรวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ
4.2 ความเสี่ยง (RISK)	หมายถึงเหตุการณ์ที่ไม่มีความแน่นอนที่อาจเกิดขึ้นได้ในอนาคตและอาจส่งผลกระทบเชิงลบ สร้างความสูญเสีย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน เช่น ชื่อเสียงองค์กร ความเชื่อมั่นของผู้ใช้บริการ) หรือลดโอกาสที่จะบรรลุเป้าหมายที่องค์กรกำหนดไว้
4.3 การประเมินความเสี่ยง (RISK ASSESSMENT)	หมายถึง การวิเคราะห์และประเมินโอกาสเกิดของภัยคุกคามจุดอ่อนหรือช่องโหว่และผลกระทบที่มีต่อทรัพย์สิน (Asset) ขององค์กร
4.4 ความน่าจะเป็นในการเกิดเหตุการณ์ (PROBABILITY)	หมายถึง โอกาสเกิดความเสี่ยงหรือความถี่ในการเกิดความเสี่ยงเพื่อนำไปใช้ในการตัดสินใจในการบริหารจัดการความเสี่ยง
4.5 จุดอ่อนหรือช่องโหว่ (VULNERABILITY)	หมายถึง สาเหตุหรือข้อบกพร่องที่เป็นช่องทางที่ก่อให้เกิดภัยคุกคาม
4.6 ภัยคุกคาม (THREAT)	หมายถึง เหตุการณ์หรือสิ่งที่เกิดขึ้นจากภายในองค์กรหรือภายนอกและส่งผลเสียต่อทรัพย์สินขององค์กร
4.7 ผลกระทบ (IMPACT LEVEL)	หมายถึง เกณฑ์ของเหตุการณ์ที่เกิดจากความเสี่ยงซึ่งส่งผลกระทบต่อการดำเนินธุรกิจ การเงินและชื่อเสียงขององค์กร
4.8 STATEMENT OF APPLICABILITY: SOA	หมายถึง เอกสารระบุว่ามาตรการใน Annex: A ข้อที่องค์กรได้มีการนำมาใช้งานและเหตุผลของการนำมาใช้ รวมถึงมาตรการข้อใดที่ไม่ได้นำมาใช้งานและเหตุผลที่ไม่ได้นำมาใช้งาน
4.9 EXISTING CONTROL	หมายถึง มาตรการจัดการความเสี่ยงที่นำมาใช้ควบคุมภัยคุกคามหรือช่องโหว่ต่าง ๆ

5 ความรับผิดชอบ

5.1 เจ้าหน้าที่ฝ่ายเทคโนโลยีและ	มีหน้าที่รับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

สารสนเทศ

5.2 ISMS	มีหน้าที่ ตัดสินใจเกี่ยวกับการยอมรับความเสี่ยงระบบสารสนเทศขององค์กร จัดทำทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ นำเสนอผู้บริหารอนุมัติ โดยคำนึงถึงกฎหมาย ข้อบังคับ สัญญาจ้างมาเป็นส่วนหนึ่งในการกำหนดนโยบายรวมถึงการสื่อสารความสำคัญของนโยบาย แนวปฏิบัติให้กับบุคลากรที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร เช่น ผู้ใช้งาน ผู้รับจ้าง ผ่านการประกาศในเว็บไซต์ การอบรม การทำสัญญา เป็นต้น
5.3 ผู้บริหาร	พิจารณาอนุมัตินโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

6 ขั้นตอนการปฏิบัติงาน

6.1 ระบุทรัพย์สิน (Asset) และกระบวนการที่เกี่ยวข้องกับการให้บริการ (IdentifyAsset / Process)

คณะกรรมการบริหาร จัดให้มีการประชุมเพื่อทำการพิจารณาทรัพย์สินหรือกระบวนการ (Process) การให้บริการขององค์กรที่เกี่ยวข้องกับขอบเขตการขอการรับรองเมื่อคณะกรรมการพิจารณาเสร็จ ให้บันทึกรายละเอียดลงในรายงานการประเมินความเสี่ยง (FO – ISMS 09 - 01)

6.2 ระบุความเสี่ยงที่อาจเกิดขึ้นและแจกแจงที่มาของความเสี่ยง

6.2.1 ระบุความเป็นไปได้ของภัยคุกคามของกระบวนการ (Identify Possible Threat to Process)

คณะกรรมการบริหาร ร่วมกันพิจารณาและระบุภัยคุกคาม (Threat) ที่สามารถเกิดขึ้นได้กับทรัพย์สิน (Asset) หรือกระบวนการ (Process) ที่กำลังพิจารณานั้นก่อให้เกิดผลกระทบ ในด้านใดของ Confidentiality, Integrity, Availability โดยมีแหล่งข้อมูล เช่น อุบัติการณ์ที่เคยพบ, ข้อมูลข่าวสารเกี่ยวกับปัญหาด้านความปลอดภัยข้อมูลเป็นต้น

6.2.2 ระบุจุดอ่อนและการควบคุมปัจจุบัน (Identify Vulnerability& Existing Control)

คณะกรรมการบริหาร ร่วมกันพิจารณาว่ามีจุดอ่อนหรือช่องโหว่ (Vulnerability) ใดบ้าง ที่อาจถูกภัยคุกคามเข้าก่อให้เกิดความเสียหายต่อทรัพย์สิน (Asset) หรือกระบวนการ (Process) ที่กำลังพิจารณาได้ และปัจจุบันองค์กรมีการควบคุม (Control) ใดอยู่บ้าง ที่ช่วยป้องกันไม่ให้ภัยคุกคามสามารถสร้างความเสียหายทรัพย์สิน (Asset) หรือกระบวนการ (Process) ได้

6.3 วิเคราะห์ผลกระทบของความเสี่ยงต่อระบบ

6.3.1 ผลกระทบต่อทรัพย์สินหรือกระบวนการ (Asset /Process Impact)

คณะกรรมการบริหาร ร่วมกันประเมินระดับผลกระทบ (Impact) ของแต่ละภัยคุกคามและจุดอ่อนในการให้บริการขององค์กร โดยพิจารณาจากผลกระทบ ดังนี้

- ความลับ (Confidentiality) หากข้อมูลถูกเปิดเผยไปสู่ผู้ที่ไม่ได้รับอนุญาต

- ความถูกต้องครบถ้วน (Integrity) หากข้อมูลถูกบิดเบือน ไม่ครบถ้วน ถูกแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาตจนเกิดความเสียหาย
- ความมีพร้อมใช้(Availability) หากข้อมูลไม่สามารถเข้าใช้งานได้เมื่อต้องการ โดยการประเมินผลกระทบ ตามรายละเอียดในตาราง Impact Level โดยเลือกคะแนนจากที่มีผลกระทบสูงสุด

ตารางอ้างอิง Impact Level

ผลกระทบหากสูญเสียในด้าน C,I,A					
Impact Level	คะแนน	ความต่อเนื่องของธุรกิจ (I1)	ภาพลักษณ์องค์กร (I2)	ผลกระทบกับระบบอื่นๆ ที่เกี่ยวข้อง ((I3)	กฎหมายหรือข้อบังคับ (I4)
Very High	5	ไม่สามารถให้บริการได้ตามปกติมากกว่า 48 ชม.	ภาพลักษณ์สูญเสียถาวร ผู้รับบริการ หมดความเชื่อถือ ออกสื่อต่างประเทศ	มีผลกระทบกับ มากกว่า 2 ระบบขึ้นไป ไม่สามารถทำงานได้	ขัดต่อข้อกฎหมายหรือพระราชบัญญัติคอมพิวเตอร์
High	4	ไม่สามารถให้บริการได้ตามปกติมากกว่า 24 ถึง 48 ชม.	ส่งผลกับภาพลักษณ์ขององค์กรค่อนข้างสูง ออกสื่อภายในประเทศ	มีผลกระทบกับ 2 ระบบ ไม่สามารถทำงานได้	ขัดต่อนโยบายหรือข้อปฏิบัติขององค์กร
Medium	3	ไม่สามารถให้บริการได้ตามปกติมากกว่า 4 ถึง 24 ชม.	กระทบกับภาพลักษณ์ขององค์กรเล็กน้อย สู่ภายนอก	มีผลกระทบกับ 1 ระบบ ไม่สามารถทำงานได้	ขัดต่อข้อปฏิบัติของหน่วยงาน
Low	2	ไม่สามารถให้บริการได้ตามปกติมากกว่า 2 ถึง 4 ชม.	แทบจะไม่กระทบภาพลักษณ์ขององค์กร รู้กันภายในองค์กร	มีผลกระทบทำให้ระบบอื่นทำงานช้าลง	ขัดต่อกระบวนการในการปฏิบัติงานเฉพาะในทีม
Very Low	1	ไม่สามารถให้บริการได้ตามปกติน้อยกว่า 2 ชม.	ไม่กระทบภาพลักษณ์	ไม่มีผลกระทบกับระบบอื่น	ไม่ขัดต่อกฎข้อบังคับต่างๆ รวมถึงนโยบายและระเบียบปฏิบัติ

6.3.2 ระดับความน่าจะเป็น (Likelihood Probability)

คณะกรรมการบริหาร ร่วมกันประเมินระดับความน่าจะเป็น (Probability) ที่ภัยคุกคามจะสามารถเข้าก่อให้เกิดความเสียหายต่อการให้บริการผ่านจุดอ่อนหรือช่องโหว่ (Vulnerability) ที่มีอยู่ โดยให้พิจารณาจาก 2 ปัจจัยหลัก ดังนี้

- **แนวโน้มการเกิดขึ้นของ Threat**พิจารณาจากแรงจูงใจหรือค่าทางสถิติที่มีการบันทึกไว้ที่มีผลต่อ Confidentiality, Integrity, Availability ของการให้บริการองค์กรที่ผ่านมา เช่น ผู้ไม่มีสิทธิเข้าถึงโดยไม่ได้รับอนุญาต, มีคนนำข้อมูลที่ไม่อนุญาตให้เปิดเผยโดยไม่รับอนุญาต หรือส่งผลเสียหายให้องค์กร, การนำข้อมูลจัดเก็บในจุดที่ไม่ถูกต้อง เป็นต้น
- **ความยากง่ายที่จะถูกกระทำ** พิจารณาจาก จุดอ่อนหรือช่องโหว่ (Vulnerability) ที่มี และ Control ที่มีในปัจจุบัน หากมีจุดอ่อนหรือช่องโหว่ (Vulnerability) มาก และไม่มีการควบคุมค่าความน่าจะเป็นที่ Threat จะเข้ากระทำความเสียหายกับการให้บริการจะสูงกว่าในกรณีที่มี Control ควบคุมอยู่

ตารางอ้างอิง Probability

Probability	คะแนน	Criteria / Description
Almost Certain	5	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้ประจำ ทุกสัปดาห์หรือบ่อยกว่า
Likely	4	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้บ่อย ประมาณเดือนละครั้ง
Possible	3	Threat มีความน่าจะเป็นที่จะเกิดขึ้นปานกลาง ประมาณ 3-5 ครั้งในรอบปี
Unlikely	2	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้ยาก ประมาณ 1–2 ครั้งในรอบปี
Rare	1	Threat มีความน่าจะเป็นที่จะเกิดขึ้นได้ยากมากอาจจะเกิดขึ้น 1-2 ครั้งในรอบ 3 ปี

6.3.3 คำนวณค่าความเสี่ยง (Calculate Risk Level)

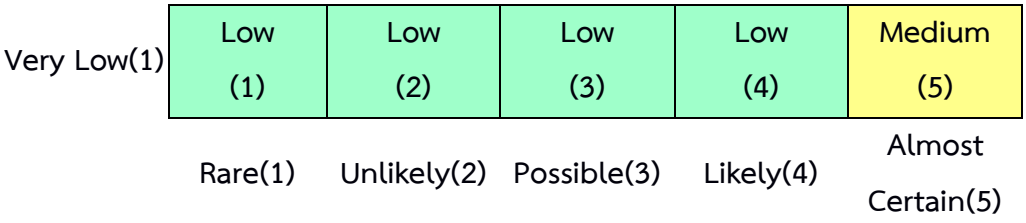
คณะกรรมบริหาร ร่วมกันประเมินค่าความเสี่ยง (Risk Level) โดยวิธีการคำนวณ ดังนี้

Risk Level = Impact x Probability

จากนั้นนำค่าที่ได้มาหา Risk Level ที่กำหนดไว้ตามตารางด้านล่างนี้

ตารางอ้างอิง Risk Level

Impact					
Very High(5)	Medium (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
High(4)	Low (4)	Medium (8)	High (12)	High (16)	Extreme (20)
Medium(3)	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
Low(2)	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)



เมื่อได้ค่า Risk Level แล้ว ให้ดำเนินการพิจารณาจากผลความเสี่ยงนั้น ว่าจำเป็นต้องหาวิธีในการแก้ไขและควบคุมความเสี่ยงอย่างไรหรือไม่

โดยค่าความเสี่ยง (Risk Level) ที่องค์กรสามารถยอมรับได้ อ้างอิงตามตารางด้านล่าง ดังนี้

ตารางแสดงความหมายของความเสี่ยงในแต่ละระดับ

Risk Level	Required Action
Extreme	**ความเสี่ยงในระดับสูง** ไม่สามารถยอมรับได้ ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง และดำเนินการทันที
High	**ความเสี่ยงในระดับค่อนข้างสูงไม่สามารถยอมรับได้** ต้องพิจารณาหาวิธีการแก้ไขความเสี่ยง และดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสม
Medium	**ความเสี่ยงในระดับปานกลาง** ทำการติดตามผลความเสี่ยงและพิจารณาปรับปรุงมาตรการควบคมปัจจุบันที่มีอยู่ แต่หากมีเหตุจำเป็นก็สามารถพิจารณายอมรับความเสี่ยงได้
Low	**ความเสี่ยงในระดับที่ต่ำมาก** สามารถยอมรับได้โดยไม่ต้องดำเนินการใดๆ เพิ่มเติมที่มีในปัจจุบัน

6.4 พิจารณาการดำเนินการต่อความเสี่ยง

6.4.1 พิจารณาการแก้ไขและควบคุมความเสี่ยง (Determine Risk Treatment Solution)

คณะกรรมการบริหาร ร่วมกันพิจารณาหาวิธีการที่เหมาะสมสำหรับแก้ไขและควบคุมความเสี่ยงลงในแบบฟอร์ม Risk Treatment Plan (FO-ISMS-09-02) โดยมีประเด็นที่ควรพิจารณา ดังนี้

- รายละเอียดของวิธีการที่เลือกใช้ ความยากง่ายในการดำเนินการ ความเหมาะสม และความเข้ากันได้กับสภาพปัจจุบันขององค์กร
- ที่ต้องใช้ทั้งในแง่ของ งบประมาณ, บุคลากร และเวลา ฯลฯ

6.4.2 กฎหมาย ระเบียบ นโยบาย หรือข้อตกลงที่เกี่ยวข้อง

6.4.3 ประสิทธิภาพในการแก้ไขและควบคุมความเสี่ยงที่เกิดขึ้น

6.4.4 ความเป็นไปได้และความคุ้มค่าของวิธีการแก้ไขควบคุมความเสี่ยง (Possible &

Valuable Treatment)

คณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยข้อมูล ร่วมกันพิจารณาความเป็นไปได้และความคุ้มค่าของวิธีการแก้ไขควบคุมความเสี่ยง (Treatment) และนำเสนอเข้าขอความเห็นชอบจากผู้บริหารตามความเหมาะสม

- ถ้าวิธีการแก้ไขควบคุมความเสี่ยงมีความเป็นไปได้และคุ้มค่าต่อการดำเนินการ ให้ปฏิบัติตาม Risk Treatment Plan
- ถ้าไม่สามารถหาวิธีการแก้ไขควบคุมความเสี่ยงได้ หรือไม่คุ้มค่าต่อการดำเนินการ ให้ปฏิบัติตาม Accept Risk

6.5 สรุปผลการจัดการความเสี่ยงและแผนการตอบสนองความเสี่ยง

6.5.1 สรุปและจัดทำแผนแก้ไขความเสี่ยง (Summarize Risk Treatment Plan)

คณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยข้อมูล ร่วมกันสรุปและจัดทำแผนแก้ไขความเสี่ยง (Risk Treatment Plan) เพื่อนำเข้าขอความสนับสนุนและอนุมัติโดยผู้บริหาร โดยข้อมูลที่ต้องระบุในแผนแก้ไขความเสี่ยง ลงในแบบฟอร์ม Risk Treatment Plan

ซึ่งรวมถึงการที่ทำข้อตกลงและมีการกำหนดมาตรการควบคุมหน่วยงานภายนอกที่เข้ามาในพื้นที่ เพื่อเป็นการลดความเสี่ยงที่เกี่ยวข้องกับองค์กรและหน่วยงานภายนอก

6.5.2 พิจารณาอนุมัติแผนแก้ไขความเสี่ยง (Approve Risk Treatment Plan)

ผู้บริหารพิจารณาอนุมัติแผนแก้ไขความเสี่ยงและให้ความสนับสนุนทรัพยากรต่าง ๆ ในการดำเนินการตามแผนแก้ไขความเสี่ยง

6.5.3 ติดตามผลของกิจกรรมการลดความเสี่ยง (Perform Risk Treatment Activity)

คณะกรรมบริหารความเสี่ยงด้านความปลอดภัยข้อมูลประสานงานกัน เพื่อดำเนินการตามวิธีการที่ระบุไว้ในแผนแก้ไขความเสี่ยง โดยใช้ทรัพยากรตามที่กำหนดไว้ในแผน และดำเนินการให้แล้วเสร็จภายในระยะเวลาที่กำหนดไว้ พร้อมทั้งรายงานความคืบหน้าและปัญหาที่พบในการดำเนินการให้ผู้บริหารทราบเป็นระยะ ซึ่งจะมีการติดตามทบทวนมาตรการควบคุมปลอดภัยข้อมูลสารสนเทศปีละ 1 ครั้ง

6.5.4 ตัดสินใจการยอมรับความเสี่ยง (Accept Risk Decision)

คณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยข้อมูล ร่วมกันสรุปรายการของความเสี่ยงที่จำเป็นต้องยอมรับข้อจำกัด และเหตุผลที่ทำให้ไม่สามารถดำเนินการแก้ไขและควบคุมความเสี่ยงนั้น ๆ ได้ โดยให้บันทึกข้อมูลลงในรายงานการประเมินความเสี่ยง (FO-ISMS-09-01) เพื่อเสนอ ผู้บริหารพิจารณาและลงนามยอมรับความเสี่ยง

ซึ่งจะดำเนินการยอมรับความเสี่ยงจะพิจารณาได้กรณีความเสี่ยงปานกลางหรือต่ำเท่านั้น ถ้าเป็นความเสี่ยงสูงหรือสูงมากจะต้องมีการมาตรควบคุม

หมายเหตุ: คณะกรรมการบริหารความเสี่ยงด้านความปลอดภัยข้อมูล ดำเนินการสรุปรายละเอียดของ Control ต่าง ๆ ตาม Annex A มาสรุปไว้ในเอกสาร Statement of Applicability(FO-ISMS-09-03)

7 เอกสารที่เกี่ยวข้อง

7.2 FO - ISMS 09 - 01 Risk Assessment Report

7.3 FO – ISMS 09 - 02 Risk Treatment Plan

7.4 FO - ISMS 09 - 03 Statement of Applicability (SoA)

8. การจัดเก็บบันทึกคุณภาพ

ชื่อเอกสาร	สถานที่เก็บ		ผู้รับผิดชอบ	การจัดเก็บ	ระยะเวลา	ผู้เข้าถึงเอกสาร
	เอกสาร	ไฟล์				
8.1 FO - ISMS 09 - 01 Risk Assessment Report	ตู้เอกสารฝ่ายเทคโนโลยีและสารสนเทศ ชั้น 2	-	เจ้าหน้าที่ฝ่ายเทคโนโลยีและสารสนเทศ	เรียงตามลำดับก่อนหลัง	ตลอดอายุการใช้งาน	1.เจ้าหน้าที่ฝ่ายเทคโนโลยีและสารสนเทศ 2.หัวหน้าฝ่ายเทคโนโลยีและสารสนเทศ
8.2 FO - ISMS 09 - 02 Risk Treatment Plan	ตู้เอกสารฝ่ายเทคโนโลยีและสารสนเทศ ชั้น 2	-	เจ้าหน้าที่ฝ่ายเทคโนโลยีและสารสนเทศ	เรียงตามลำดับก่อนหลัง	ตลอดอายุการใช้งาน	1.เจ้าหน้าที่ฝ่ายเทคโนโลยีและสารสนเทศ 2.หัวหน้าฝ่ายเทคโนโลยีและสารสนเทศ
8.3 FO - ISMS 09 - 03	ตู้เอกสารฝ่าย	-	เจ้าหน้าที่ฝ่าย	เรียง	ตลอดอายุการ	1.เจ้าหน้าที่ฝ่ายเทคโนโลยี

Statement of Applicability (SoA)	เทคโนโลยีและสารสนเทศ ชั้น 2		เทคโนโลยีและสารสนเทศ	ตามลำดับก่อนหลัง	ใช้งาน	และสารสนเทศ 2.หัวหน้าฝ่ายเทคโนโลยีและสารสนเทศ

ภาคผนวก

การประเมินความเสี่ยงที่มีผลต่อข้อมูลการให้บริการลูกค้า (Risk Assessment Report)													
พื้นที่/หน่วยงาน			วันที่จัดทำ						ผู้จัดทำ		ผู้อนุมัติ		
Asset / Process	Threats	Vulnerability	Impact			Evaluate		Risk Level ระดับความเสี่ยง	Existing Control (ระบุมาตรการควบคุมที่มี)	Related Risk Treatement Plan แผนจัดการความเสี่ยง	Plan Status สถานะ	Residual	Risk Level ระดับความเสี่ยง
			Confidentiality	Integrity	Availability	Probability	Impact					Probability / Impact	
Computer PC / Lab top กล้องวงจรปิด													
Server External hard disk													
การดูแล Network Security													
การจัดทำ Backup													
- บุคลากร - ผู้รับจ้างภายนอก													

แผนดำเนินการความเสี่ยง Risk Treatment Plan โรงพยาบาลพระศรีมหาโพธิ์						
Treatment ID	Treatment Explanation	Responsible Person/Dept.	Duration		Status	Actual Finish Date
			Start	Finish		