



ศูนย์สนับสนุนบริการสุขภาพที่ 1
กรมสนับสนุนบริการสุขภาพ

เอกสารแนวทางการดำเนินงาน
ด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber Security)
ตามมาตรฐานระบบบริการสุขภาพ HS4

HS4 : Health Service Support Standards System

ข้อมูลเปิด มาตรฐาน HS4 โรงพยาบาลอยุธยา ข้อมูลสรุป มาตรฐานบริการ คู่มือการใช้งาน

ระบบประเมินมาตรฐานสุขภาพ

HS4 ยกระดับ มาตรฐานสุขภาพไทย

ระบบประเมินมาตรฐานสุขภาพที่ทันสมัย ช่วยยกระดับการให้บริการด้านสุขภาพในประเทศไทย ด้วยการประเมินที่เป็นระบบและมีมาตรฐาน

เข้าสู่ระบบประเมิน (สำหรับสถานพยาบาล)

เข้าสู่ระบบประเมิน (สำหรับผู้ตรวจประเมิน)

ระบบประเมินที่ทันสมัย

HS4
Health Service Support Standard System

HS4 ช่วยให้โรงพยาบาลและหน่วยบริการสุขภาพสามารถประเมินและยกระดับมาตรฐานการบริการให้มีประสิทธิภาพ

ครอบคลุมทุกมิติของมาตรฐานสุขภาพ

ศูนย์สนับสนุนบริการสุขภาพที่ 1
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข
ประจำปีงบประมาณ พ.ศ. 2569

สารบัญ

หน้า

- **มาตรฐานระบบบริการสุขภาพ ด้าน 9 การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)**
จัดทำโดยกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขาธิการกรม กรมสนับสนุนบริการสุขภาพ
ประจำปีงบประมาณ พ.ศ. 2569
- **ตัวอย่างเอกสาร / แบบฟอร์ม**
จัดทำโดยงานเทคโนโลยีสารสนเทศและการประชาสัมพันธ์ กลุ่มบริหารงานทั่วไป ศูนย์สนับสนุนบริการ
สุขภาพที่ 1

หมวดที่ 1

การกำกับดูแลด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ (IT & Cyber Governance)

- | | |
|---|----|
| 1.1 โครงสร้างการกำกับดูแลระบบสารสนเทศ (CS.1.1) | 1 |
| <ul style="list-style-type: none">• คำสั่งแต่งตั้งคณะกรรมการ/ผู้รับผิดชอบ• บทบาท อำนาจหน้าที่ และความรับผิดชอบ | |
| 1.2 แผนแม่บทและแผนพัฒนาเทคโนโลยีสารสนเทศ (CS.1.2) | 3 |
| <ul style="list-style-type: none">• แผนแม่บท IT & Cybersecurity• เป้าหมาย แนวทาง และแผนพัฒนา | |
| 1.3 นโยบายและแผนงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CS.1.3) | 5 |
| <ul style="list-style-type: none">• นโยบาย Cybersecurity• แผนงานด้าน Cybersecurity | |
| 1.4 โครงสร้างและอัตรากำลังหน่วยงานสารสนเทศ (CS.1.4) | 8 |
| <ul style="list-style-type: none">• ผังโครงสร้างองค์กร IT• บทบาทหน้าที่บุคลากร | |
| 1.5 มาตรการ นโยบาย และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ (CS.1.5) | 10 |
| <ul style="list-style-type: none">• Information Security Policy• PDPA / Data Governance• Network & System Security Policy | |

หมวดที่ 2

การบริหารจัดการความเสี่ยงด้านระบบสารสนเทศ (IT & Cyber Risk Management)

- | | |
|---|----|
| 2.1 การประเมินและให้คะแนนความเสี่ยงระบบสารสนเทศ (CS.2.1) | 14 |
| <ul style="list-style-type: none">• ทะเบียนทรัพย์สินสารสนเทศ (Asset Inventory)• ตารางประเมินความเสี่ยง | |

สารบัญ (ต่อ)

	หน้า
2.2 แผนจัดการความเสี่ยงด้านระบบสารสนเทศ (CS.2.2)	17
• Risk Treatment Plan	
2.3 การดำเนินการตามแผนจัดการความเสี่ยง (CS.2.3)	20
• รายงานการดำเนินงาน	
• หลักฐานการดำเนินการจริง	
2.4 การติดตามและประเมินผลการจัดการความเสี่ยง (CS.2.4)	23
• การเปรียบเทียบความเสี่ยงก่อน-หลัง	
2.5 การปรับปรุงแผนจัดการความเสี่ยงอย่างต่อเนื่อง (CS.2.5)	26
• PDCA / Continuous Improvement	

หมวดที่ 3

การสร้างความมั่นคงปลอดภัยสารสนเทศและความตระหนักรู้ (Information Security & Awareness)

3.1 แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศ (CS.3.1)	29
• Access Control	
• Backup & Availability	
• Risk Assessment	
3.2 มาตรการจัดการรหัสผ่านและการคุ้มครองข้อมูล (CS.3.2)	32
• Password Management	
• PII / Patient Confidentiality	
3.3 แผนและกิจกรรม Cybersecurity Awareness (CS.3.3)	34
• แผนงานการสร้างความตระหนัก	
• ตารางกิจกรรมและสื่อประกอบ	
3.4 การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติ (CS.3.4)	37
• ประกาศ / หนังสือเวียน	
3.5 การตรวจสอบและประเมินการปฏิบัติตาม (CS.3.5)	39
• Compliance Assessment	
• การปรับปรุงอย่างต่อเนื่อง	

หมวดที่ 4

การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resources Management)

4.1 ทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ (CS.4.1)	42
--	----

สารบัญ (ต่อ)

	หน้า
4.2 การวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis (CS.4.2)	45
• Hardware / Software / Network / People	
4.3 แผนเพิ่มและจัดการศักยภาพทรัพยากร IT (CS.4.3)	48
4.4 สมรรถนะบุคลากรด้าน IT และแผนพัฒนารายบุคคล (CS.4.4)	51
4.5 การปรับปรุงแผนเพิ่มศักยภาพอย่างต่อเนื่อง (CS.4.5)	54
หมวดที่ 5	
ความมั่นคงปลอดภัยทางกายภาพและความต่อเนื่องของระบบ (Physical & System Security)	
5.1 มาตรการรักษาความปลอดภัยทางกายภาพ Data Center (CS.5.1)	58
5.2 การสำรองและกู้คืนข้อมูล (CS.5.2)	61
5.3 ระบบป้องกันอัคคีภัยใน Data Center (CS.5.3)	64
5.4 มาตรการป้องกันความเสียหายของข้อมูลและระบบ (CS.5.4)	66
• UPS / RAID / Redundant System	
5.5 ระบบเฝ้าระวังความปลอดภัยทางกายภาพ (CS.5.5)	69
หมวดที่ 6	
การตรวจสอบและแผนรับมือภัยคุกคามทางไซเบอร์ (Audit & Incident Response)	
6.1 แผนการตรวจสอบด้าน Cybersecurity (CS.6.1)	72
6.2 แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) (CS.6.2)	75
6.3 การฝึกซ้อมและทบทวนแผน Incident Response (CS.6.3)	78

อ้างอิงเกณฑ์จาก หมวดที่ 1 ข้อ CS.1.1

“มีการจัดโครงสร้างการดูแลระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ พร้อมกำหนดอำนาจหน้าที่ และความรับผิดชอบ”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.1.1 การจัดโครงสร้างและบทบาทการดูแลระบบสารสนเทศ

หน่วยงานได้จัดโครงสร้างการดูแลระบบสารสนเทศของสถานพยาบาล โดยมีคำสั่งแต่งตั้งผู้บริหารและคณะทำงานด้านเทคโนโลยีสารสนเทศอย่างเป็นทางการ ประกอบด้วยผู้บริหารระดับผู้อำนวยการโรงพยาบาล ผู้รับผิดชอบด้านเทคโนโลยีสารสนเทศ และผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

มีการกำหนดบทบาท อำนาจหน้าที่ และความรับผิดชอบของแต่ละตำแหน่งอย่างชัดเจนเป็นลายลักษณ์อักษร เพื่อกำกับดูแลระบบสารสนเทศ ระบบเครือข่าย และการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้เป็นไปตามนโยบายและกฎหมายที่เกี่ยวข้อง

2 ตัวอย่าง “คำสั่งแต่งตั้ง” (เอกสารหลักฐานสำคัญ)

คำสั่งโรงพยาบาล.....

ที่/25xx

เรื่อง แต่งตั้งคณะกรรมการและผู้รับผิดชอบด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การบริหารจัดการระบบเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล เป็นไปอย่างมีประสิทธิภาพ สอดคล้องตามมาตรฐานระบบบริการสุขภาพ ด้านที่ 9 และกฎหมายที่เกี่ยวข้อง

อาศัยอำนาจตาม

จึงแต่งตั้งบุคคลดังต่อไปนี้

1. ผู้อำนวยการโรงพยาบาล ประธานกรรมการ
2. หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ กรรมการ
3. ผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (CISO/ผู้แทน) กรรมการ
4. เจ้าหน้าที่เทคโนโลยีสารสนเทศ กรรมการและเลขานุการ

หน้าที่และความรับผิดชอบ

- กำกับดูแลและบริหารจัดการระบบสารสนเทศของโรงพยาบาล
- กำหนดนโยบายและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์
- ติดตาม ประเมิน และรายงานสถานะความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหาร
- ประสานงานเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

3 ตัวอย่าง “ตารางสรุปบทบาท (แนบตอบกรรมการตรวจ)”

ตำแหน่ง	บทบาทหน้าที่หลัก
ผู้อำนวยการโรงพยาบาล	กำกับนโยบาย อนุมัติแผนด้าน IT/Cyber
หัวหน้าฝ่าย IT	บริหารจัดการระบบสารสนเทศและโครงสร้างพื้นฐาน
ผู้รับผิดชอบด้าน Cyber (CISO/เทียบเท่า)	กำกับมาตรการความมั่นคงปลอดภัยไซเบอร์
เจ้าหน้าที่ IT	ดูแลระบบ Server, Network, Backup

4 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มี คำสั่งแต่งตั้งเป็นลายลักษณ์อักษร
- ☒ ระบุ บทบาท + หน้าที่ชัดเจน
- ☒ มี ลายเซ็นผู้บริหาร
- ☒ แนบเอกสารประกอบในระบบประเมิน

อ้างอิงเกณฑ์ หมวดที่ 1 ข้อ CS.1.2

“มีการจัดทำแผนแม่บทหรือแผนพัฒนาของสถานพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนา และการใช้งานเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.1.2 การจัดทำแผนแม่บท / แผนพัฒนาเทคโนโลยีสารสนเทศ

หน่วยงานได้จัดทำแผนแม่บทและแผนพัฒนาเทคโนโลยีสารสนเทศของสถานพยาบาล โดยกำหนดเป้าหมาย แนวทางการพัฒนา และการใช้งานเทคโนโลยีสารสนเทศให้สอดคล้องกับภารกิจด้านสาธารณสุข และเป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

แผนดังกล่าวครอบคลุมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยง และการกำหนดนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ โดยได้รับการอนุมัติจากผู้บริหาร และนำไปใช้เป็นกรอบในการดำเนินงานของหน่วยงาน

2 ตัวอย่างโครงสร้างเอกสาร

“แผนแม่บท / แผนพัฒนาเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์”

ชื่อเอกสาร

แผนแม่บทเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาล.....

ระยะเวลา พ.ศ. 25xx – 25xx

1. บทนำ

อธิบายความสำคัญของการใช้เทคโนโลยีสารสนเทศในการให้บริการสาธารณสุข และความจำเป็นในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อคุ้มครองข้อมูลผู้ป่วยและความต่อเนื่องของระบบบริการ

2. วัตถุประสงค์ของแผน

1. เพื่อกำหนดทิศทางการพัฒนาและใช้งานเทคโนโลยีสารสนเทศของโรงพยาบาล
2. เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ
3. เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

3. ขอบเขตของแผน

ครอบคลุมระบบสารสนเทศด้านสาธารณสุข เช่น HIS, LIS, ระบบเครือข่าย, ฐานข้อมูลผู้ป่วย และระบบสนับสนุนการบริหาร

4. แนวทางการดำเนินงาน (ความสำคัญของ CS.1.2)

(ก) การกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

- แต่งตั้งคณะกรรมการ/ผู้รับผิดชอบด้าน IT และ Cybersecurity
- กำหนดนโยบายและโครงสร้างการกำกับดูแล
- รายงานผลต่อผู้บริหารเป็นระยะ

(ข) การบริหารความเสี่ยง

- ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์
- จัดทำแผนจัดการความเสี่ยง (Risk Management Plan)
- ติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง

(ค) นโยบายและแนวปฏิบัติ

- นโยบายความมั่นคงปลอดภัยสารสนเทศ
- นโยบายคุ้มครองข้อมูลส่วนบุคคล (PDPA)
- แนวปฏิบัติการสำรองและกู้คืนข้อมูล

5. แผนพัฒนาเทคโนโลยีสารสนเทศ (ตัวอย่างตาราง)

ลำดับ	โครงการ	เป้าหมาย	ระยะเวลา (ปี)	ผู้รับผิดชอบ
1	ปรับปรุงระบบ HIS	เพิ่มความเร็วและความปลอดภัย	25xx	ฝ่าย IT
2	จัดทำระบบ Backup	ป้องกันข้อมูลสูญหาย	25xx	System Admin
3	อบรม Cybersecurity	เพิ่มความรู้ตระหนักรู้บุคลากร	25xx	IT / HR

6. การติดตามและประเมินผล

- ติดตามความก้าวหน้าโครงการตามแผน
- ประเมินผลและรายงานผู้บริหารอย่างน้อยปีละ 1 ครั้ง
- ปรับปรุงแผนตามผลการประเมิน

7. การอนุมัติแผน

แผนแม่บทฉบับนี้ได้รับความเห็นชอบและอนุมัติจากผู้บริหาร เพื่อใช้เป็นแนวทางในการดำเนินงาน

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ เป็นเอกสาร “แผน” อย่างเป็นทางการ
- ☒ ครอบคลุม 3 เรื่องหลัก (กำกับดูแล / ความเสี่ยง / นโยบาย)
- ☒ ระบุเป้าหมาย + แนวทางการพัฒนา IT ชัดเจน
- ☒ มีลายเซ็นผู้บริหารอนุมัติ

อ้างอิงเกณฑ์ หมวดที่ 1 ข้อ CS.1.3

“มีนโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.1.3 นโยบายและแผนงานการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานได้จัดทำนโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล อย่างเป็นลายลักษณ์อักษร เพื่อใช้เป็นกรอบและแนวทางในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

นโยบายและแผนงานดังกล่าวครอบคลุมการควบคุมการเข้าถึงระบบสารสนเทศ การคุ้มครองข้อมูลผู้ป่วย และข้อมูลส่วนบุคคลตามกฎหมาย การบริหารความเสี่ยง การสำรองและกู้คืนข้อมูล รวมถึงการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และได้รับการอนุมัติจากผู้บริหารของหน่วยงานแล้ว

2 ตัวอย่างเอกสารหลัก

“นโยบายและแผนงานการรักษาความมั่นคงปลอดภัยไซเบอร์”

ชื่อเอกสาร

ประกาศ นโยบายและแผนงานการรักษาความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาล.....

1. หลักการและเหตุผล

เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลมีความมั่นคงปลอดภัย ปกป้องข้อมูลผู้ป่วย ข้อมูลส่วนบุคคล และระบบบริการสาธารณสุขจากภัยคุกคามทางไซเบอร์ รวมทั้งสร้างความเชื่อมั่นแก่ประชาชน ผู้รับบริการ

2. วัตถุประสงค์

1. เพื่อกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล
2. เพื่อป้องกัน ลดความเสี่ยง และรับมือภัยคุกคามทางไซเบอร์
3. เพื่อให้การใช้งานระบบสารสนเทศเป็นไปอย่างปลอดภัยและต่อเนื่อง

3. ขอบเขต

ครอบคลุมระบบสารสนเทศทั้งหมดของโรงพยาบาล เช่น ระบบ HIS, LIS, ระบบเครือข่าย, ฐานข้อมูลผู้ป่วย, อุปกรณ์คอมพิวเตอร์ และช่องทางการสื่อสารทางอิเล็กทรอนิกส์

4. นโยบายหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Core Policies)

4.1 การควบคุมการเข้าถึง (Access Control)

- กำหนดสิทธิ์การเข้าถึงระบบตามบทบาทหน้าที่ (Role-based Access Control)
- ใช้รหัสผ่านที่มีความปลอดภัย และทบทวนสิทธิ์เป็นระยะ

4.2 การจัดการข้อมูลและทรัพย์สินสารสนเทศ

- จัดทำทะเบียนทรัพย์สินสารสนเทศ
- ควบคุมการจัดเก็บ ใช้ และเปิดเผยข้อมูลผู้ป่วยและข้อมูลส่วนบุคคล

4.3 การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

- ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- ป้องกันการรั่วไหลของข้อมูลผู้ป่วยทุกช่องทาง รวมถึงสื่อสังคมออนไลน์

4.4 การบริหารความเสี่ยงด้านไซเบอร์

- ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
- จัดทำและทบทวนแผนจัดการความเสี่ยง

4.5 การสำรองและกู้คืนข้อมูล (Backup & Recovery)

- กำหนดรอบการสำรองข้อมูลอย่างสม่ำเสมอ
- ทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

4.6 การตอบสนองต่อเหตุการณ์ (Incident Response)

- จัดทำแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์
- กำหนดช่องทางการแจ้งเหตุและผู้รับผิดชอบชัดเจน

5. แผนงานการดำเนินงาน (ตัวอย่าง)

ลำดับ	กิจกรรม	รายละเอียด	ผู้รับผิดชอบ
1	จัดทำนโยบาย Cyber	ประกาศใช้นโยบายอย่างเป็นทางการ	ผู้บริหาร
2	ประเมินความเสี่ยง	วิเคราะห์ความเสี่ยงระบบ IT	ฝ่าย IT
3	สำรองข้อมูล	สำรองข้อมูลระบบ HIS/LIS	System Admin
4	อบรมบุคลากร	สร้างความตระหนักรู้ด้าน Cyber	IT / HR

6. การบังคับใช้และทบทวน

นโยบายและแผนงานฉบับนี้ให้ใช้บังคับกับบุคลากรทุกระดับ และมีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

7. การอนุมัติ

นโยบายและแผนงานฉบับนี้ได้รับการอนุมัติให้ใช้บังคับโดยผู้บริหารของหน่วยงาน

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

- 3** Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)
- ✓ มีทั้ง “นโยบาย” และ “แผนงาน”
 - ✓ เป็นลายลักษณ์อักษร
 - ✓ ครอบคลุม Access Control, PDPA, Risk, Backup, Incident
 - ✓ มีลายเซ็นผู้บริหารอนุมัติ

อ้างอิงเกณฑ์ หมวดที่ 1 ข้อ CS.1.4

“มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.1.4 การจัดโครงสร้างและอัตรากำลังหน่วยงานสารสนเทศ

หน่วยงานได้จัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศให้เหมาะสมกับภารกิจด้านสาธารณสุข และการให้บริการของสถานพยาบาล โดยมีการกำหนดตำแหน่ง บทบาทหน้าที่ และความรับผิดชอบของบุคลากร ด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน

โครงสร้างดังกล่าวครอบคลุมการบริหารจัดการระบบสารสนเทศ ระบบเครือข่าย การดูแลความมั่นคง ปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งมีเอกสารแสดงโครงสร้างองค์กรและเอกสารกำหนด บทบาทหน้าที่เป็นลายลักษณ์อักษร

2 ตัวอย่างเอกสารหลัก

“โครงสร้างและอัตรากำลังหน่วยงานสารสนเทศ”

ชื่อเอกสาร

ผังโครงสร้างและอัตรากำลังหน่วยงานสารสนเทศ

โรงพยาบาล.....

1. วัตถุประสงค์

เพื่อกำหนดโครงสร้าง อัตรากำลัง และบทบาทหน้าที่ของหน่วยงานสารสนเทศให้เหมาะสมกับการบริหารจัดการระบบเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล

2. โครงสร้างหน่วยงานสารสนเทศ (Organizational Structure)

โครงสร้างการบังคับบัญชา (ตัวอย่าง)

- ผู้อำนวยการโรงพยาบาล
 - ↳ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
 - ↳ เจ้าหน้าที่ระบบ (System Administrator)
 - ↳ เจ้าหน้าที่เครือข่าย (Network Administrator)
 - ↳ เจ้าหน้าที่สนับสนุนงาน IT (IT Support)
 - ↳ ผู้รับผิดชอบด้านคุ้มครองข้อมูลส่วนบุคคล (DPO/ผู้แทน)

หมายเหตุ: สำหรับหน่วยงานขนาดเล็ก สามารถมอบหมายบทบาทหลายหน้าที่ให้บุคลากรคนเดียวได้ โดยมีคำสั่ง แต่งตั้งชัดเจน

3. ตารางอัตรากำลังและบทบาทหน้าที่ (Roles & Responsibilities)

ตำแหน่ง	จำนวน	บทบาทหน้าที่หลัก
หัวหน้าฝ่าย IT / CIO	1	วางแผนและกำกับการบริหารระบบสารสนเทศและนโยบายไซเบอร์
System Administrator	1	ดูแล Server, HIS, Backup, Patch
Network Administrator	1	ดูแล Network, Firewall, VPN
IT Support	1	สนับสนุนผู้ใช้งาน แก้ไขปัญหาเบื้องต้น
DPO / ผู้แทน	1	กำกับการคุ้มครองข้อมูลส่วนบุคคลตาม PDPA

4. การมอบหมายหน้าที่และความรับผิดชอบ

หน่วยงานได้มีคำสั่งแต่งตั้งบุคลากรตามโครงสร้างข้างต้น พร้อมกำหนดบทบาทหน้าที่ ความรับผิดชอบ และสายการบังคับบัญชาอย่างชัดเจน เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

5. การทบทวนโครงสร้างและอัตรากำลัง

มีการทบทวนโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงภารกิจ เทคโนโลยี หรือความเสี่ยงด้านไซเบอร์

6. การอนุมัติ

เอกสารฉบับนี้ได้รับการอนุมัติให้ใช้เป็นโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศ

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

3 เอกสารแนบที่ควรส่ง

- ☒ ผังโครงสร้างองค์กร (Organizational Chart)
- ☒ ตาราง Roles & Responsibilities
- ☒ คำสั่งแต่งตั้งบุคลากรด้าน IT / Cyber
- ☒ เอกสารทบทวนอัตรากำลัง (ถ้ามี)

4 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มีโครงสร้างหน่วยงานชัดเจน
- ☒ ระบุอัตรากำลังครบถ้วน
- ☒ มีบทบาทหน้าที่เป็นลายลักษณ์อักษร
- ☒ มีลายเซ็นผู้บริหารอนุมัติ

อ้างอิงเกณฑ์ หมวดที่ 1 ข้อ CS.1.5

“มีการกำหนดมาตรการ/นโยบาย/แนวปฏิบัติด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกฎหมายและกฎระเบียบที่เกี่ยวข้อง เช่น พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2565 กฎหมายและกฎระเบียบที่เกี่ยวข้องอื่น”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.1.5 การกำหนดมาตรการ/นโยบาย/แนวปฏิบัติด้านเทคโนโลยีสารสนเทศ

หน่วยงานได้กำหนดมาตรการ นโยบาย และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศที่จำเป็นอย่างเป็นลายลักษณ์อักษร เพื่อใช้เป็นกรอบในการบริหารจัดการระบบสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล

นโยบายและแนวปฏิบัติดังกล่าวสอดคล้องกับกฎหมายและกฎระเบียบที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายด้านเทคโนโลยีสารสนเทศอื่นที่เกี่ยวข้อง โดยได้รับการอนุมัติจากผู้บริหารและประกาศใช้อย่างเป็นทางการ พร้อมแจ้งให้บุคลากรรับทราบและถือปฏิบัติ

2 ชุดเอกสารหลัก (แนะนำให้แนบเป็น “รวมชุดเอกสาร”)

เอกสารที่ 1 : นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

สาระสำคัญ

- หลักการรักษา ความลับ (Confidentiality), ความถูกต้อง (Integrity), ความพร้อมใช้ (Availability)
- ขอบเขตการบังคับใช้กับบุคลากรทุกระดับ
- โครงสร้างการกำกับดูแลและความรับผิดชอบ

ตัวอย่างข้อความ

โรงพยาบาลกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ เพื่อปกป้องระบบสารสนเทศและข้อมูลผู้ป่วยจากการเข้าถึง ใช้ เผยแพร่ แก่ไข หรือทำลายโดยไม่ได้รับอนุญาต และให้การให้บริการสาธารณสุขเป็นไปอย่างต่อเนื่อง

เอกสารที่ 2 : นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy / PDPA)

สาระสำคัญ

- หลักการเก็บ ใช้ เผยแพร่ข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูล
- การแจ้งเหตุข้อมูลรั่วไหล

ตัวอย่างหัวข้อ

- การจำแนกข้อมูล (ทั่วไป/อ่อนไหว)
- การขอความยินยอม
- ช่องทางติดต่อ DPO

เอกสารที่ 3 : แนวปฏิบัติการบริหารจัดการข้อมูล (Data Governance Guidelines)

สาระสำคัญ

- การจำแนกประเภทข้อมูล (Public / Confidential / Sensitive)
- การจัดเก็บ ทำลาย และสำรองข้อมูล
- การควบคุมการเข้าถึงข้อมูล

เอกสารที่ 4 : นโยบาย/แนวปฏิบัติความปลอดภัยระบบเครือข่ายและระบบสารสนเทศ

(Network & System Security Policy)

สาระสำคัญ

- Firewall / IDS-IPS

(เชิงนโยบาย) หน่วยงานต้องจัดให้มีระบบควบคุมและป้องกันการเข้าถึงเครือข่ายจากภายนอกและภายใน เพื่อป้องกันการบุกรุก การโจมตี และการใช้งานเครือข่ายที่ไม่เหมาะสม

ตัวอย่าง แนวปฏิบัติ

1. ติดตั้ง Firewall เพื่อควบคุมการรับ-ส่งข้อมูลระหว่างเครือข่ายภายในกับเครือข่ายภายนอก
2. กำหนดกฎ (Rule) การอนุญาตและปฏิเสธการเชื่อมต่ออย่างเหมาะสมกับภารกิจ
3. ใช้ระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อเฝ้าระวังพฤติกรรมผิดปกติ
4. ทบทวนและปรับปรุงการตั้งค่า Firewall และ IDS/IPS อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีความเสี่ยงใหม่

กรรมการตรวจ : แสดงว่า มีการป้องกันเชิงรุก ไม่ใช่แค่ต่ออินเทอร์เน็ตเฉย ๆ

- Patch Management

(เชิงนโยบาย) หน่วยงานต้องควบคุมและจัดการการอัปเดตซอฟต์แวร์และระบบปฏิบัติการ เพื่อป้องกันช่องโหว่ด้านความปลอดภัยที่อาจถูกนำไปใช้โจมตีระบบ

ตัวอย่าง แนวปฏิบัติ

1. ติดตามข่าวสารช่องโหว่ด้านความปลอดภัยของระบบปฏิบัติการและซอฟต์แวร์ที่ใช้
2. อัปเดต Patch ด้านความปลอดภัยอย่างสม่ำเสมอ ตามระดับความสำคัญของความเสี่ยง
3. ทดสอบ Patch ในระบบทดสอบก่อนนำไปใช้งานจริง (ถ้ามี)
4. บันทึกการอัปเดต Patch เป็นหลักฐานการดำเนินงาน

กรรมการตรวจ : แสดงว่า หน่วยงานไม่ปล่อยระบบล้ำสมัยจนเสี่ยงถูกโจมตี

- Encryption (การเข้ารหัสข้อมูล)

(เชิงนโยบาย) หน่วยงานต้องคุ้มครองข้อมูลสำคัญ โดยเฉพาะข้อมูลผู้ป่วยและข้อมูลส่วนบุคคล ด้วยมาตรการเข้ารหัส เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

ตัวอย่าง แนวปฏิบัติ

1. เข้ารหัสข้อมูลสำคัญขณะจัดเก็บ (Data at Rest) และขณะส่งผ่านเครือข่าย (Data in Transit)
2. ใช้โปรโตคอลที่ปลอดภัยในการรับ-ส่งข้อมูล เช่น HTTPS, VPN
3. ควบคุมการเข้าถึงกุญแจเข้ารหัส (Encryption Key) เฉพาะผู้ที่ได้รับอนุญาต
4. ทบทวนมาตรการเข้ารหัสให้เหมาะสมกับระดับความเสี่ยงของข้อมูล

กรรมการตรวจ : เชื่อมตรงกับ PDPA และการปกป้องข้อมูลผู้ป่วย

- การตรวจสอบและบันทึก Log (Log Monitoring)

(เชิงนโยบาย) หน่วยงานต้องมีการบันทึกและตรวจสอบการใช้งานระบบสารสนเทศและเครือข่าย เพื่อใช้ตรวจสอบเหตุการณ์ผิดปกติ และเป็นหลักฐานเมื่อเกิดเหตุด้านความมั่นคงปลอดภัยไซเบอร์

ตัวอย่าง แนวปฏิบัติ

1. บันทึก Log การใช้งานระบบที่สำคัญ เช่น การเข้า-ออกระบบ การแก้ไขข้อมูล และการตั้งค่าระบบ
2. จัดเก็บ Log อย่างปลอดภัยและกำหนดระยะเวลาเก็บรักษาที่เหมาะสม
3. ตรวจสอบ Log เป็นระยะ เพื่อค้นหาพฤติกรรมผิดปกติหรือเหตุการณ์ผิดพลาด
4. ใช้ Log เป็นข้อมูลสนับสนุนการสอบสวนเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

กรรมการตรวจ : แสดงว่า หน่วยงาน “ตรวจสอบย้อนหลังได้” ไม่ใช่รู้ตัวหลังเกิดเหตุอย่างเดียว

3 ตัวอย่าง “ตารางสรุปนโยบาย (แนบตอบกรรมการตรวจ)”

ลำดับ	ชื่อนโยบาย/แนวปฏิบัติ	ครอบคลุมเรื่อง	สถานะ
1	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)	ความมั่นคงปลอดภัยสารสนเทศ	ประกาศใช้
2	นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy (PDPA))	คุ้มครองข้อมูลส่วนบุคคล	ประกาศใช้
3	แนวปฏิบัติการบริหารจัดการข้อมูล (Data Governance)	การจัดการข้อมูล	ประกาศใช้
4	นโยบาย/แนวปฏิบัติความปลอดภัยระบบเครือข่ายและระบบสารสนเทศ (Network & System Security)	ระบบเครือข่าย/ระบบ	ประกาศใช้

4 ตัวอย่างหน้าลงนามประกาศใช้

ประกาศโรงพยาบาล.....

เรื่อง ให้ใช้บังคับนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ

ให้ใช้นโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศฉบับนี้ ตั้งแต่วันที่ เป็นต้นไป

บุคลากรทุกระดับต้องถือปฏิบัติโดยเคร่งครัด

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

5 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มี นโยบาย/มาตรการ/แนวปฏิบัติ ครบ
- ☒ สอดคล้องกฎหมาย (PDPA ฯลฯ)
- ☒ ประกาศใช้อย่างเป็นทางการ
- ☒ มีลายเซ็นผู้บริหาร
- ☒ มีหลักฐานการแจ้งบุคลากร (หนังสือเวียน/อีเมล)

อ้างอิงเกณฑ์ หมวดที่ 2 ข้อ CS.2.1

“มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.2.1 การประเมินและให้คะแนนความเสี่ยงระบบสารสนเทศ

หน่วยงานได้จัดให้มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยครอบคลุมทรัพย์สินสารสนเทศทั้งหมดที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุข ได้แก่ ระบบสารสนเทศด้านการรักษาพยาบาล ระบบเครือข่าย อุปกรณ์เทคโนโลยีสารสนเทศ และข้อมูลผู้ป่วย

การประเมินความเสี่ยงดำเนินการโดยมีส่วนร่วมของผู้บริหาร ฝ่ายเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง มีการจัดทำทะเบียนทรัพย์สินสารสนเทศ การวิเคราะห์ภัยคุกคามและช่องโหว่ การประเมินโอกาสและผลกระทบ พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอต่อผู้บริหาร

2 เอกสารหลักที่ใช้ตอบ

“กระบวนการประเมินความเสี่ยงระบบสารสนเทศ (IT Risk Assessment Process)”

1. วัตถุประสงค์

เพื่อระบุ วิเคราะห์ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อใช้เป็นข้อมูลในการวางแผนควบคุมและลดความเสี่ยง

2. ขอบเขต

ครอบคลุมทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการให้บริการสาธารณสุขทั้งหมด เช่น

- ระบบ HIS / LIS / เวชระเบียน
- ระบบเครือข่ายและอินเทอร์เน็ต
- Server, Computer, Network Device
- ข้อมูลผู้ป่วยและข้อมูลส่วนบุคคล

3. กระบวนการประเมินความเสี่ยง

ขั้นตอนที่ 1 : จัดทำทะเบียนทรัพย์สินสารสนเทศ (IT Asset Inventory)

รวบรวมรายการทรัพย์สินด้าน Hardware, Software, Network และ Data พร้อมระบุเจ้าของทรัพย์สินและระดับความสำคัญ

ขั้นตอนที่ 2 : ระบุภัยคุกคามและช่องโหว่

พิจารณาภัยคุกคาม เช่น Malware, Ransomware, การเข้าถึงโดยไม่ได้รับอนุญาต, ระบบล่ม

ขั้นตอนที่ 3 : ประเมินโอกาสและผลกระทบ

กำหนดคะแนน

- โอกาสเกิด (Likelihood) ระดับ 1–5
- ผลกระทบ (Impact) ระดับ 1–5

ขั้นตอนที่ 4 : คำนวณและจัดระดับความเสี่ยง

ความเสี่ยง = โอกาส × ผลกระทบ

แบ่งระดับความเสี่ยงเป็น สูง / ปานกลาง / ต่ำ

ขั้นตอนที่ 5 : การมีส่วนร่วมของหน่วยงานที่เกี่ยวข้อง

จัดประชุมร่วมระหว่างผู้บริหาร ฝ่าย IT และหน่วยงานผู้ใช้งาน เพื่อพิจารณาความเสี่ยงร่วมกัน

ขั้นตอนที่ 6 : รายงานผลการประเมิน

จัดทำรายงานผลการประเมินความเสี่ยง เสนอต่อผู้บริหารเพื่อรับทราบ

3 ตัวอย่าง “ทะเบียนทรัพย์สินสารสนเทศ (IT Asset Inventory)”

ลำดับ	ประเภท	รายการทรัพย์สิน	เจ้าของ	ความสำคัญ
1	Software	ระบบ HIS	ฝ่าย IT	สูง
2	Hardware	Server หลัก	ฝ่าย IT	สูง
3	Network	Firewall	ฝ่าย IT	สูง
4	Data	ข้อมูลผู้ป่วย	เวชระเบียน	สูง

4 ตัวอย่าง “ตารางประเมินความเสี่ยง (Risk Assessment Matrix)”

ทรัพย์สิน	ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ
Server HIS	ไฟฟ้าดับ	4	5	20	สูง
ระบบเครือข่าย	ถูกโจมตี	3	4	12	ปานกลาง
ข้อมูลผู้ป่วย	เข้าถึงโดยมิชอบ	2	5	10	ปานกลาง

5 เอกสารประกอบที่ควรแนบให้กรรมการ

- ☒ ทะเบียนทรัพย์สินสารสนเทศ (Asset Inventory)
- ☒ ตารางประเมินความเสี่ยง (Risk Register)
- ☒ รายงานการประชุมการประเมินความเสี่ยง
- ☒ รายงานผลการประเมินเสนอต่อผู้บริหาร

Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

-  มี “กระบวนการ” ชัดเจน
-  ครอบคลุม Asset Inventory ทั้งหมด
-  มี การให้คะแนนความเสี่ยง
-  มี ส่วนร่วมหลายฝ่าย
-  มีรายงานเสนอผู้บริหาร

อ้างอิงเกณฑ์ หมวดที่ 2 ข้อ CS.2.2

“มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการหรือกระบวนการ ระยะเวลา ดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.2.2 แผนจัดการความเสี่ยงระบบสารสนเทศ

หน่วยงานได้จัดทำแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร โดยอ้างอิงผลการประเมินความเสี่ยงตามข้อ CS.2.1 กำหนดกลยุทธ์และมาตรการจัดการความเสี่ยงที่เหมาะสม ระบุระยะเวลาดำเนินการและผู้รับผิดชอบอย่างชัดเจน

แผนดังกล่าวได้รับการอนุมัติจากผู้บริหาร และนำไปใช้เป็นกรอบในการลดความเสี่ยงและรักษาความต่อเนื่องของบริการสาธารณสุขของหน่วยงาน

2 เอกสารหลัก

“แผนจัดการความเสี่ยงระบบสารสนเทศ (IT Risk Management Plan)”

ชื่อเอกสาร

แผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาล.....

ระยะเวลา พ.ศ. 25xx

1. บทนำ

เอกสารฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางและมาตรการในการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ โดยใช้ผลการประเมินความเสี่ยงเป็นฐาน เพื่อป้องกัน ลดผลกระทบ และควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

2. วัตถุประสงค์

1. ลดความเสี่ยงที่อาจกระทบต่อระบบสารสนเทศและข้อมูลผู้ป่วย
2. กำหนดมาตรการควบคุมความเสี่ยงอย่างเป็นระบบ
3. รักษาความต่อเนื่องของการให้บริการสาธารณสุข

3. ขอบเขต

ครอบคลุมความเสี่ยงของระบบ HIS/LIS, ระบบเครือข่าย, Server, อุปกรณ์ IT และข้อมูลผู้ป่วย ภายใต้การให้บริการสาธารณสุขของหน่วยงาน

4. กลยุทธ์การจัดการความเสี่ยง (Risk Treatment Options)

หน่วยงานใช้แนวทางการจัดการความเสี่ยงดังนี้

- ลดความเสี่ยง (Mitigation)
- ยอมรับความเสี่ยง (Acceptance)
- โอนความเสี่ยง (Transfer) เช่น การทำประกัน
- หลีกเลี่ยงความเสี่ยง (Avoidance)

5. ตารางแผนจัดการความเสี่ยง (Risk Treatment Plan)

ลำดับ	ความเสี่ยงที่ประเมิน	ระดับ	กลยุทธ์	มาตรการจัดการ	ระยะเวลา	ผู้รับผิดชอบ
1	Server HIS ไม่มี UPS	สูง	ลด	จัดซื้อและติดตั้ง UPS	พ.ค. 25xx	ฝ่าย IT
2	ไม่มี Firewall ภายนอก	สูง	ลด	จัดหา Firewall และตั้งค่า	มิ.ย. 25xx	หัวหน้า IT
3	บุคลากรขาดความรู้ PDPA	ปานกลาง	ลด	อบรมความรู้ PDPA	ก.ค. 25xx	HR/IT
4	DR ใช้เวลานาน	ปานกลาง	ลด	ทบทวนแผน DR	ส.ค. 25xx	System Admin

หมายเหตุ: ตารางนี้เป็นหัวใจของ CS.2.2 และต้องอ้างอิงจากผล CS.2.1

6. การติดตามและรายงานผล

ฝ่าย IT จะติดตามความคืบหน้าการดำเนินการตามแผนจัดการความเสี่ยง และจัดทำรายงานเสนอต่อผู้บริหารอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุสำคัญ

7. การอนุมัติแผน

แผนจัดการความเสี่ยงฉบับนี้ได้รับการพิจารณาและอนุมัติจากผู้บริหาร เพื่อใช้เป็นแนวทางในการดำเนินงาน (ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

3 เอกสารแนบที่ควรส่งพร้อม CS.2.2

- ✓ รายงานผลการประเมินความเสี่ยง (จาก CS.2.1)
- ✓ ตารางแผนจัดการความเสี่ยง (Risk Treatment Plan)
- ✓ หนังสือ/คำสั่งอนุมัติแผน

-  Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)
-  ✓ เป็นเอกสาร “แผน” เป็นลายลักษณ์อักษร
-  ✓ ระบุ กลยุทธ์/มาตรการ/ระยะเวลา/ผู้รับผิดชอบ
-  ✓ อ้างอิงความเสี่ยงจาก CS.2.1
-  ✓ มี ลายเซ็นผู้บริหารอนุมัติ

อ้างอิงเกณฑ์ หมวดที่ 2 ข้อ CS.2.3

“การดำเนินการตามแผนจัดการความเสี่ยง”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.2.3 การดำเนินการตามแผนจัดการความเสี่ยง

หน่วยงานได้ดำเนินการตามแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ตามที่กำหนดไว้ในแผนจัดการความเสี่ยง (CS.2.2) โดยมีการนำมาตรการควบคุมความเสี่ยงไปปฏิบัติจริงอย่างเป็นระบบ

มีการติดตามความคืบหน้าและบันทึกผลการดำเนินงาน พร้อมจัดทำเอกสารหลักฐานประกอบ เช่น รายงานผลการดำเนินงาน ภาพถ่าย ใบสั่งซื้อ ใบบันทึกการตั้งค่าระบบ และรายงานการอบรม เพื่อยืนยันว่า มาตรการลดความเสี่ยงได้ถูกนำไปใช้จริง

2 เอกสารหลัก

“รายงานการดำเนินการตามแผนจัดการความเสี่ยง

(Risk Mitigation Implementation Report)”

ชื่อเอกสาร

รายงานการดำเนินการตามแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โรงพยาบาล.....

ประจำปี พ.ศ. 25xx

1. บทนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อแสดงผลการดำเนินการตามแผนจัดการความเสี่ยง (CS.2.2) โดยแสดงให้เห็นว่า มาตรการควบคุมและลดความเสี่ยงที่กำหนดไว้ ได้ถูกนำไปปฏิบัติจริง พร้อมหลักฐานที่สามารถตรวจสอบได้

2. ขอบเขตการดำเนินงาน

ครอบคลุมการดำเนินการตามแผนจัดการความเสี่ยงของระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการสาธารณสุข ได้แก่ ระบบ HIS/LIS, ระบบเครือข่าย, Server, การคุ้มครองข้อมูลผู้ป่วย และการพัฒนาศักยภาพบุคลากร

3. ตารางแสดงผลการดำเนินการตามแผนจัดการความเสี่ยง

(หัวใจของ CS.2.3)

ลำดับ	ความเสี่ยง	มาตรการตามแผน (CS.2.2)	ผลการดำเนินการจริง	หลักฐานประกอบ	สถานะ
1	Server HIS ไม่มี UPS	จัดซื้อและติดตั้ง UPS	ติดตั้ง UPS ขนาด 2,000 VA แล้ว	รูปถ่าย / ใบส่งมอบ	เสร็จสิ้น
2	ไม่มี Firewall ภายนอก	จัดหา Firewall	ติดตั้ง Firewall และตั้งค่า Policy	ใบสั่งซื้อ / Screenshot	เสร็จสิ้น
3	บุคลากรขาดความรู้ PDPA	อบรมความรู้ PDPA	อบรมบุคลากร 30 คน	รายชื่ออบรม / รูปถ่าย	เสร็จสิ้น
4	ไม่มี Auto Backup	ติดตั้งระบบ Backup	ตั้งค่า Backup อัตโนมัติ	Log ระบบ / คู่มือ	ดำเนินการ

ข้อสำคัญ : ต้องแสดงว่า “แผนถูกนำไปปฏิบัติจริง” ไม่ใช่แค่วางแผน

4. สรุปผลการดำเนินงาน

จากการดำเนินการตามแผนจัดการความเสี่ยง พบว่ามาตรการส่วนใหญ่ได้ดำเนินการแล้วเสร็จ และช่วยลดระดับความเสี่ยงของระบบสารสนเทศให้อยู่ในระดับที่ยอมรับได้ โดยความเสี่ยงที่ยังอยู่ระหว่างดำเนินการจะถูกติดตามและรายงานในรอบถัดไป

5. ปัญหา อุปสรรค และข้อเสนอแนะ (ถ้ามี)

- ความล่าช้าในการจัดซื้อบางรายการ
- ข้อจำกัดด้านงบประมาณหรือบุคลากร

6. การรับรองผลการดำเนินงาน

รายงานฉบับนี้จัดทำเพื่อเสนอผู้บริหารรับทราบผลการดำเนินการตามแผนจัดการความเสี่ยง

(ลงชื่อ)

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

3 เอกสารหลักฐานที่ควรแนบ (แนบจริง = ได้คะแนน)

- ✓ รูปถ่ายอุปกรณ์ / การติดตั้งระบบ
- ✓ Screenshot การตั้งค่า Firewall / Backup
- ✓ ใบส่งชื่อ / ใบส่งมอบ
- ✓ รายชื่อและเอกสารการอบรม
- ✓ Log ระบบ / รายงานผลการตั้งค่า

4 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ✓ อ้างอิงแผนจาก CS.2.2
- ✓ แสดง “การดำเนินการจริง” ครบถ้วน
- ✓ มีหลักฐานตรวจสอบได้
- ✓ มีรายงานเป็นลายลักษณ์อักษร

อ้างอิงเกณฑ์ หมวดที่ 2 ข้อ CS.2.4

“มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน เสนอต่อผู้บริหาร”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.2.4 การติดตามและประเมินผลการจัดการความเสี่ยง

หน่วยงานได้มีการติดตาม ประเมินผล และรายงานผลการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ โดยอ้างอิงจากผลการดำเนินการตามแผนจัดการความเสี่ยง (CS.2.2 และ CS.2.3)

มีการประเมินสถานะความเสี่ยงหลังการดำเนินมาตรการ เปรียบเทียบระดับความเสี่ยงก่อนและหลังการจัดการ และจัดทำรายงานผลเสนอต่อผู้บริหารเพื่อใช้ประกอบการตัดสินใจและกำกับดูแล

2 เอกสารหลัก

“รายงานการติดตามและประเมินผลการจัดการความเสี่ยง

(Risk Monitoring & Evaluation Report)”

ชื่อเอกสาร

รายงานการติดตามและประเมินผลการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โรงพยาบาล.....

รอบการประเมิน พ.ศ. 25xx

1. บทนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อแสดงผลการติดตามและประเมินผลการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์ หลังจากหน่วยงานได้ดำเนินการตามแผนจัดการความเสี่ยงแล้ว

2. ขอบเขตการติดตามและประเมินผล

ครอบคลุมความเสี่ยงของระบบสารสนเทศที่เกี่ยวข้องกับบริการสาธารณสุข ได้แก่ ระบบ HIS/LIS, ระบบเครือข่าย Server, ข้อมูลผู้ป่วย และบุคลากรที่เกี่ยวข้อง

3. วิธีการติดตามและประเมินผล

- ตรวจสอบสถานะการดำเนินงานตามแผนจัดการความเสี่ยง
- ประเมินระดับความเสี่ยง ก่อน และ หลัง การดำเนินมาตรการ
- ตรวจสอบหลักฐานการดำเนินงาน
- ประชุมร่วมกับหน่วยงานที่เกี่ยวข้อง

4. ตารางเปรียบเทียบระดับความเสี่ยง (Before – After)

(หัวใจของ CS.2.4)

ลำดับ	ความเสี่ยง	ระดับก่อนจัดการ	มาตรการที่ดำเนินการ	ระดับหลังจัดการ	สถานะ
1	Server HIS ไม่มี UPS	สูง	ติดตั้ง UPS	ต่ำ	ควบคุมได้
2	ไม่มี Firewall	สูง	ติดตั้ง Firewall	ปานกลาง	ควบคุมได้
3	บุคลากรขาดความรู้ PDPA	ปานกลาง	อบรมบุคลากร	ต่ำ	ควบคุมได้
4	Backup ไม่สม่ำเสมอ	ปานกลาง	ตั้งค่า Auto Backup	ปานกลาง	ติดตาม

กรรมการตรวจจะมองตารางนี้เป็นหลัก ต้องเห็นชัดว่า “ความเสี่ยงลดลง”

5. สรุปผลการประเมิน

จากการติดตามและประเมินผล พบว่าการดำเนินมาตรการตามแผนจัดการความเสี่ยงช่วยลดระดับความเสี่ยงของระบบสารสนเทศให้อยู่ในระดับที่ยอมรับได้ อย่างไรก็ตาม ยังมีบางความเสี่ยงที่ต้องติดตามและปรับปรุงอย่างต่อเนื่อง

6. การรายงานต่อผู้บริหาร

รายงานผลการติดตามและประเมินผลฉบับนี้ได้นำเสนอผู้บริหารเพื่อรับทราบ และใช้ประกอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

7. การรับรองรายงาน

(ลงชื่อ)

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

3 เอกสารแนบที่ควรส่งพร้อม CS.2.4

- ✓ รายงานผล CS.2.3
- ✓ ตารางเปรียบเทียบความเสี่ยง (Before–After)
- ✓ บันทึกการประชุมติดตาม
- ✓ หนังสือเสนอผู้บริหาร

Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

-  มีการ “ติดตาม + ประเมินผล”
-  เปรียบเทียบระดับความเสี่ยงก่อน-หลัง
-  มีรายงานเสนอต่อผู้บริหาร
-  เป็นเอกสารลายลักษณ์อักษร

อ้างอิงเกณฑ์ หมวดที่ 2 ข้อ CS.2.5

“มีการนำผลการประเมินหรือความเสี่ยงที่ยังคงเหลืออยู่ มาปรับปรุงแผนการจัดการความเสี่ยงอย่างต่อเนื่อง”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.2.5 การปรับปรุงแผนจัดการความเสี่ยง

หน่วยงานได้นำผลการติดตามและประเมินผลการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ (CS.2.4) มาวิเคราะห์และใช้ในการปรับปรุงแผนจัดการความเสี่ยงและมาตรการควบคุมความเสี่ยงให้เหมาะสมกับสถานการณ์ปัจจุบัน

มีการทบทวนระดับความเสี่ยงที่ยังคงอยู่หรือเกิดขึ้นใหม่ ปรับปรุงมาตรการ ระยะเวลาดำเนินการ และผู้รับผิดชอบ พร้อมจัดทำเอกสารแผนปรับปรุงและเสนอผู้บริหารพิจารณา

2 เอกสารหลัก

“รายงานการปรับปรุงแผนจัดการความเสี่ยง

(Risk Management Plan Improvement Report)”

ชื่อเอกสาร

รายงานการปรับปรุงแผนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โรงพยาบาล.....

ประจำปี พ.ศ. 25xx

1. บทนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อแสดงการนำผลการติดตามและประเมินผลการจัดการความเสี่ยง (CS.2.4) มาปรับปรุงแผนจัดการความเสี่ยงและมาตรการควบคุมความเสี่ยง เพื่อให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศมีความเหมาะสมและต่อเนื่อง

2. ข้อมูลอ้างอิง

- ผลการประเมินความเสี่ยง (CS.2.1)
- แผนจัดการความเสี่ยง (CS.2.2)
- รายงานการดำเนินการตามแผน (CS.2.3)
- รายงานติดตามและประเมินผล (CS.2.4)

3. ประเด็นที่ต้องปรับปรุงจากผลการประเมิน

ลำดับ	ความเสี่ยง	ผลการประเมินล่าสุด	ประเด็นที่พบ
1	Backup ไม่สม่ำเสมอ	ยังอยู่ระดับปานกลาง	บุคลากรไม่เพียงพอ
2	Firewall ตั้งค่าเบื้องต้น	ลดความเสี่ยงได้บางส่วน	ยังไม่ครอบคลุมทุกระบบ
3	ภัยคุกคามใหม่ (Phishing)	ความเสี่ยงใหม่	บุคลากรขาดความตระหนัก

4. ตารางแสดง “การปรับปรุงแผนจัดการความเสี่ยง”

(หัวใจของ CS.2.5)

ลำดับ	ความเสี่ยง	มาตรการเดิม	มาตรการที่ปรับปรุง	ระยะเวลา	ผู้รับผิดชอบ
1	Backup ไม่สม่ำเสมอ	Backup รายสัปดาห์	เพิ่ม Auto Backup รายวัน	มิ.ย. 25xx	System Admin
2	Firewall ไม่ครอบคลุม	ตั้งค่าเฉพาะหลัก	เพิ่ม Rule สำหรับระบบย่อย	ก.ค. 25xx	Network Admin
3	Phishing	ไม่มีมาตรการ	อบรม + Phishing Test	ส.ค. 25xx	IT / HR

จุดสำคัญ : ต้องแสดงว่า “มีการเปลี่ยน/เพิ่มมาตรการจากบทเรียนที่ได้”

5. ผลที่คาดว่าจะได้รับ

- ลดระดับความเสี่ยงที่ยังคงอยู่
- เพิ่มความพร้อมรับมือภัยคุกคามใหม่
- พัฒนาความต่อเนื่องของระบบบริการสาธารณสุข

6. การอนุมัติและนำไปใช้

การปรับปรุงแผนจัดการความเสี่ยงฉบับนี้ได้รับการพิจารณาและเห็นชอบจากผู้บริหาร เพื่อใช้เป็นแนวทางในการดำเนินงานรอบถัดไป

(ลงชื่อ)

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

(ลงชื่อ)

ผู้อำนวยการโรงพยาบาล

วันที่

3 เอกสารแนบที่ควรส่งพร้อม CS.2.5

- ☒ รายงาน CS.2.4
- ☒ ตารางปรับปรุงแผนจัดการความเสี่ยง
- ☒ บันทึกการประชุมทบทวนความเสี่ยง
- ☒ หนังสือเสนอ/อนุมัติผู้บริหาร

Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

-  นำผล CS.2.4 มาใช้จริง
-  มีการ “ปรับปรุงแผน/มาตรการ” ชัดเจน
-  เป็นเอกสารลายลักษณ์อักษร
-  มีการอนุมัติจากผู้บริหาร

สรุปภาพรวมหมวดที่ 2

- CS.2.1 ประเมินความเสี่ยง
- CS.2.2 วางแผนจัดการ
- CS.2.3 ดำเนินการ
- CS.2.4 ติดตาม/ประเมิน
- CS.2.5 ปรับปรุงต่อเนื่อง (PDCA ครบวงจร)

อ้างอิงเกณฑ์ หมวดที่ 3 ข้อ CS.3.1

“มีการจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific information security policy) มีหัวข้ออย่างน้อยต่อไปนี้

- 1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)
- 2) การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งานและการจัดทำแผนเตรียมความพร้อมรับมือภัยคุกคาม
- 3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.3.1 มีการจัดทำ แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific information security policy)

หน่วยงานมีการจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific Information Security Policy) เป็นลายลักษณ์อักษร และประกาศใช้โดยได้รับการลงนามจากผู้บริหารเรียบร้อยแล้ว

แนวปฏิบัติดังกล่าวครอบคลุมหัวข้อสำคัญ ได้แก่

1. การเข้าถึงและการควบคุมการใช้งานสารสนเทศ (Access Control) โดยกำหนดสิทธิ์การใช้งานระบบตามบทบาทหน้าที่ของผู้ใช้งาน
2. การสำรองข้อมูลเพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน รวมถึงการจัดทำแผนเตรียมความพร้อมรับมือเหตุขัดข้องและภัยคุกคามทางไซเบอร์
3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ เพื่อใช้เป็นข้อมูลในการกำหนดมาตรการควบคุมและลดความเสี่ยง

แนวปฏิบัตินี้ใช้บังคับกับบุคลากรทุกระดับและระบบสารสนเทศทั้งหมดของหน่วยงาน เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและสนับสนุนความต่อเนื่องของการให้บริการด้านสาธารณสุข

2 ตัวอย่างเอกสารที่ใช้ตอบ

แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific Information Security Policy)

โรงพยาบาล.....

ฉบับที่/25xx

1. หลักการและเหตุผล

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลมีความมั่นคงปลอดภัย ปกป้องข้อมูลผู้ป่วยและข้อมูลสารสนเทศจากการเข้าถึงโดยมิชอบ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และสนับสนุนความต่อเนื่องของการให้บริการด้านสาธารณสุข

2. วัตถุประสงค์

1. กำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศ
2. ควบคุมการเข้าถึงและการใช้งานระบบอย่างเหมาะสม
3. เตรียมความพร้อมรับมือเหตุขัดข้องและภัยคุกคามทางไซเบอร์
4. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างเป็นระบบ

3. ขอบเขต

ใช้บังคับกับบุคลากรทุกระดับ และระบบสารสนเทศทั้งหมดของโรงพยาบาล เช่น ระบบ HIS, ระบบเวชระเบียน, ระบบเครือข่าย, Server และข้อมูลผู้ป่วย

4. แนวปฏิบัติด้านความมั่นคงปลอดภัย

(หัวใจของ CS.3.1 — ต้องมีครบ 3 หัวข้อนี้)

4.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)

- กำหนดสิทธิ์การเข้าถึงระบบตามบทบาทหน้าที่ (Role-based Access Control)
- ผู้ใช้งานต้องมีบัญชีผู้ใช้ส่วนบุคคล ห้ามใช้บัญชีร่วมกัน
- มีขั้นตอนการขออนุมัติ การปรับเปลี่ยน และการยกเลิกสิทธิ์การใช้งาน
- ทบทวนสิทธิ์ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อเปลี่ยนหน้าที่

4.2 การสำรองข้อมูล ความพร้อมใช้งาน และการเตรียมความพร้อมรับมือภัยคุกคาม

- จัดให้มีการสำรองข้อมูลระบบสารสนเทศและข้อมูลผู้ป่วยอย่างสม่ำเสมอ
- กำหนดรอบการสำรองข้อมูล และจัดเก็บข้อมูลสำรองในสถานที่ที่ปลอดภัย
- จัดทำแผนเตรียมความพร้อมรับมือเหตุฉุกเฉินและภัยคุกคามทางไซเบอร์
- ทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสามารถใช้งานได้จริง

4.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

- จัดให้มีการประเมินความเสี่ยงด้านระบบสารสนเทศอย่างเป็นระบบ
- ครอบคลุมระบบสารสนเทศ อุปกรณ์ และข้อมูลที่เกี่ยวข้องกับบริการสาธารณสุข
- บันทึกผลการประเมินความเสี่ยง และจัดทำแผนจัดการความเสี่ยง
- รายงานผลการประเมินต่อผู้บริหารเพื่อใช้ประกอบการกำกับดูแล

5. ความรับผิดชอบ

- **ผู้บริหาร** : กำกับดูแลและให้การสนับสนุน
- **ฝ่ายเทคโนโลยีสารสนเทศ** : ดำเนินการตามแนวปฏิบัติ
- **บุคลากรทุกระดับ** : ปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด

6. การบังคับใช้และทบทวน

แนวปฏิบัตินี้ให้ใช้บังคับตั้งแต่วันที่ประกาศ และทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านเทคโนโลยีหรือภัยคุกคาม

7. การประกาศใช้

ประกาศ ณ วันที่

ลงชื่อ

(ผู้อำนวยการโรงพยาบาล)

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

☒ เป็น “แนวปฏิบัติ” ไม่ใช่แค่แผน

☒ มี ครบ 3 หัวข้อ ตามเกณฑ์

☒ เป็นเอกสารทางการ

☒ มีลายเซ็นผู้บริหาร

อ้างอิงเกณฑ์ หมวดที่ 3 ข้อ CS.3.2

“มีนโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคล (PII) ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.3.2

หน่วยงานมีการจัดทำนโยบายและระเบียบปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (PII) และความลับผู้ป่วยเป็นลายลักษณ์อักษร โดยครอบคลุมการป้องกันการรั่วไหลของข้อมูลทุกช่องทาง รวมถึงการใช้สื่อสังคมออนไลน์ (Social Media)

นโยบายดังกล่าวได้รับการลงนามประกาศใช้โดยผู้บริหาร และมีการแจ้งให้เจ้าหน้าที่ภายในหน่วยงานรับทราบและถือปฏิบัติ เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลและความลับผู้ป่วย

2 ตัวอย่าง

นโยบายและระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและความลับผู้ป่วย (Personal Data & Patient Confidentiality Policy)

โรงพยาบาล.....

ฉบับที่/25xx

1. หลักการและเหตุผล

เพื่อคุ้มครองข้อมูลส่วนบุคคล (PII) และข้อมูลสุขภาพของผู้ป่วยไม่ให้เกิดการเข้าถึง ใช้ เปิดเผย หรือรั่วไหลโดยไม่ได้รับอนุญาต รวมถึงการป้องกันการเปิดเผยข้อมูลผ่านสื่อสังคมออนไลน์ (Social Media) ซึ่งอาจส่งผลกระทบต่อสิทธิของผู้ป่วยและความน่าเชื่อถือของหน่วยงาน

2. วัตถุประสงค์

1. คุ้มครองข้อมูลส่วนบุคคลและความลับผู้ป่วย
2. ป้องกันการรั่วไหลของข้อมูลทุกช่องทาง รวมถึง Social Media
3. กำหนดแนวปฏิบัติให้บุคลากรถือปฏิบัติอย่างเป็นมาตรฐานเดียวกัน

3. ขอบเขต

ใช้บังคับกับบุคลากรทุกระดับ รวมถึงพนักงาน ลูกจ้าง และผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูลผู้ป่วยและข้อมูลส่วนบุคคลของโรงพยาบาล

4. แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและความลับผู้ป่วย

4.1 การจัดการข้อมูลส่วนบุคคล (PII)

- เก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อการปฏิบัติงาน
- จำกัดการเข้าถึงข้อมูลเฉพาะผู้ที่ได้รับมอบหมาย
- ห้ามคัดลอกหรือส่งต่อข้อมูลโดยไม่ได้รับอนุญาต

4.2 การคุ้มครองความลับผู้ป่วย

- ห้ามเปิดเผยข้อมูลผู้ป่วยแก่บุคคลภายนอกโดยไม่ได้รับความยินยอม
- ห้ามนำข้อมูลผู้ป่วยไปใช้เพื่อประโยชน์ส่วนตน
- ใช้ข้อมูลผู้ป่วยเพื่อวัตถุประสงค์ทางการแพทย์และการบริการเท่านั้น

4.3 การใช้ Social Media

- ห้ามเผยแพร่ภาพ ข้อความ หรือข้อมูลใด ๆ ที่สามารถระบุตัวผู้ป่วยได้
- ห้ามถ่ายภาพผู้ป่วยหรือข้อมูลทางการแพทย์เพื่อเผยแพร่บน Social Media
- การสื่อสารผ่าน Social Media ต้องได้รับอนุญาตจากหน่วยงานก่อน

5. การแจ้งและการถือปฏิบัติ

โรงพยาบาลได้แจ้งนโยบายและระเบียบปฏิบัตินี้ให้บุคลากรทุกระดับรับทราบ ผ่านหนังสือเวียน/การประชุม/การอบรม และให้ถือปฏิบัติอย่างเคร่งครัด

6. การบังคับใช้

ผู้ใดฝ่าฝืนนโยบายนี้ อาจถูกพิจารณาดำเนินการทางวินัยตามระเบียบของหน่วยงาน

7. การประกาศใช้

ประกาศ ณ วันที่

ลงชื่อ

(ผู้อำนวยการโรงพยาบาล)

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มีคำว่า PII / ความลับผู้ป่วย / Social Media ชัดเจน
- ☒ เป็น นโยบายหรือระเบียบปฏิบัติ (ไม่ใช่แค่แนวคิด)
- ☒ แจ้งเจ้าหน้าที่รับทราบและถือปฏิบัติ
- ☒ มี ลายเซ็นผู้บริหาร

อ้างอิงเกณฑ์ หมวดที่ 3 ข้อ CS.3.3

“มีการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) อย่างสม่ำเสมอ”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.3.3

หน่วยงานมีการจัดทำแผนงานการสร้างความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) อย่างสม่ำเสมอ โดยครอบคลุมการให้ความรู้แก่บุคลากรทุกกลุ่ม ได้แก่ พนักงานใหม่ ผู้ใช้งานทั่วไป ผู้บริหาร และเจ้าหน้าที่ด้านโครงสร้างพื้นฐาน

แผนงานดังกล่าวครอบคลุมการกำหนดบทบาทและความรับผิดชอบของแต่ละกลุ่ม การสร้างความรู้ด้านกฎหมาย กฎ ระเบียบ และภัยคุกคามทางไซเบอร์ รวมถึงการสื่อสารแจ้งเตือนอย่างต่อเนื่องและทันเวลา พร้อมมีการจัดกิจกรรมและสื่อประกอบตามแผน

2 ตัวอย่าง

1. แผนงานการสร้างความรู้ด้าน Cybersecurity
2. ตารางรายละเอียดแผนงาน (ก) – (ง) ครบถ้วน
3. หลักฐานกิจกรรม (อบรม/สื่อ/แจ้งเตือน)

เอกสารที่ 1

แผนงานการสร้างความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness Plan)

โรงพยาบาล.....

ประจำปีงบประมาณ พ.ศ. 25xx

1. หลักการและเหตุผล

หน่วยงานตระหนักว่าบุคลากรทุกระดับเป็นปัจจัยสำคัญต่อความมั่นคงปลอดภัยไซเบอร์ จึงจัดทำแผนงานการสร้างความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสริมสร้างความรู้ ความเข้าใจ และพฤติกรรมที่ถูกต้องในการใช้งานระบบสารสนเทศ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2. วัตถุประสงค์

- สร้างความตระหนักรู้ด้าน Cybersecurity แก่บุคลากรทุกกลุ่ม
- ป้องกันข้อมูลรั่วไหลและเหตุการณ์ทางไซเบอร์
- สนับสนุนการปฏิบัติตามกฎหมายและนโยบายที่เกี่ยวข้อง

3. กลุ่มเป้าหมาย

บุคลากรทุกระดับ ได้แก่ พนักงานใหม่ ผู้ใช้งานทั่วไป ผู้บริหาร และเจ้าหน้าที่ด้านโครงสร้างพื้นฐาน IT

เอกสารที่ 2

ตารางรายละเอียดแผนงานการสร้างความรู้ความตระหนัก

หมวด	รายละเอียด	ตัวอย่างหลักฐาน
(ก) กลุ่มเป้าหมายที่ได้รับความรู้	- พนักงานใหม่ (Orientation) - ผู้ใช้งานทั่วไปและผู้บริหาร - เจ้าหน้าที่โครงสร้างพื้นฐาน (IT/ระบบ)	- เอกสารอบรม - แบบทดสอบ/Quiz
(ข) การเผยแพร่ความรับผิดชอบของแต่ละกลุ่ม	- ผู้บริหารรับผิดชอบนโยบาย - IT ดูแลระบบและความปลอดภัย - บุคลากรทั่วไปไม่คลิกลิงก์แปลก	- Poster บทบาทหน้าที่ - Infographic
(ค) การสร้างความรู้เรื่องกฎหมาย กฎระเบียบ	- PDPA - พ.ร.บ.ไซเบอร์ - นโยบายโรงพยาบาล - ภัย Social Engineering	- วิดีโอความยาว 5 นาที - Line Group แจ้งข่าวภัย
(ง) การสื่อสารอย่างสม่ำเสมอและทันเวลา	- อบรมประจำปี / รายไตรมาส - แจ้งเตือน Phishing Simulation - ป้ายประกาศ / LINE Broadcast	- ตารางกิจกรรม - Screenshot การแจ้งเตือน

ตารางนี้คือหัวใจของ CS.3.3 กรรมการจะเทียบ “ทีละข้อ (ก)–(ง)” จากตารางนี้

เอกสารที่ 3

ตัวอย่างตารางกิจกรรม Cybersecurity Awareness

ลำดับ	กิจกรรม	กลุ่มเป้าหมาย	ระยะเวลา
1	อบรม Cybersecurity Awareness	บุคลากรทุกระดับ	ม.ค. 25xx
2	แจก Infographic Phishing	บุคลากรทั่วไป	ก.พ. 25xx
3	แจ้งเตือนภัยผ่าน LINE	ทุกหน่วยงาน	ตลอดปี
4	ทบทวนบทเรียน / Quiz	พนักงานใหม่	ทุกไตรมาส

Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

-  มีคำว่า Cybersecurity Awareness
-  มี แผนงานเป็นลายลักษณ์อักษร
-  มีรายละเอียดครบ (ก)-(ง)
-  มี ตารางกิจกรรม + ตัวอย่างสื่อ
-  ไม่ใช่กิจกรรมครั้งเดียว แต่ “ต่อเนื่อง”

อ้างอิงเกณฑ์ หมวดที่ 3 ข้อ CS.3.4

“มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติสร้างความรู้ความเข้าใจ ให้บุคลากรทุกคนได้รับทราบ และถือปฏิบัติ”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.3.4

หน่วยงานมีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ให้บุคลากรทุกคนได้รับทราบ โดยครอบคลุมนโยบายตามข้อ 1.3 และแนวปฏิบัติตามข้อ 3.1 – 3.2

มีการออกประกาศภายในและหนังสือเวียนแจ้งนโยบายอย่างเป็นทางการ เพื่อให้บุคลากรรับทราบ ทำความเข้าใจ และถือปฏิบัติอย่างเคร่งครัด

2 เอกสารที่ 1 : (เอกสารหลัก – สำคัญที่สุด)

ประกาศภายใน เรื่อง การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาล.....

ประกาศ ณ วันที่

เรื่อง การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

เพื่อให้บุคลากรทุกระดับของโรงพยาบาลมีความรู้ ความเข้าใจ และถือปฏิบัติตามนโยบายและระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์อย่างถูกต้อง โรงพยาบาลจึงขอประชาสัมพันธ์นโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง ดังนี้

1. นโยบายและแผนงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ข้อ 1.3)
2. แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (ข้อ 3.1)
3. นโยบายและระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลและความลับผู้ป่วย (ข้อ 3.2)

ขอให้บุคลากรทุกระดับศึกษา ทำความเข้าใจ และถือปฏิบัติตามนโยบายและระเบียบปฏิบัติดังกล่าวอย่างเคร่งครัด หากมีข้อสงสัยสามารถสอบถามได้ที่ฝ่ายเทคโนโลยีสารสนเทศ

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ลงชื่อ

(ผู้อำนวยการโรงพยาบาล)

เอกสารที่ 2 : (เอกสารประกอบ)

หนังสือเวียนแจ้งนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง แจ้งนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

เรียน บุคลากรทุกฝ่าย

ตามที่โรงพยาบาลได้กำหนดนโยบายและระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ เพื่อคุ้มครองข้อมูลผู้ป่วยและข้อมูลส่วนบุคคล จึงขอแจ้งให้บุคลากรทุกฝ่ายรับทราบและถือปฏิบัติตามนโยบายและระเบียบปฏิบัติดังกล่าวโดยเคร่งครัด

ทั้งนี้ ขอให้หัวหน้าหน่วยงานแจ้งให้บุคลากรในสังกัดรับทราบโดยทั่วกัน

ขอแสดงความนับถือ

.....

ฝ่ายเทคโนโลยีสารสนเทศ

3 หลักฐานแนบเพิ่มเติม (เลือกแนบได้)

- Screenshot Email / LINE กลุ่มหน่วยงาน
- รายชื่อผู้รับหนังสือเวียน
- ภาพการประชุมชี้แจงนโยบาย
- เอกสารลงนามรับทราบ (ถ้ามี)

4 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มี ประกาศภายใน
- ☒ มี หนังสือเวียน
- ☒ ระบุชัด ข้อ 1.3, 3.1, 3.2
- ☒ แสดงว่า “บุคลากรทุกคนรับทราบ”

อ้างอิงเกณฑ์ หมวดที่ 3 ข้อ CS.3.5

“มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด และนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติ อย่างต่อเนื่อง”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.3.5

หน่วยงานมีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ และยอมรับการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการแจ้งนโยบายอย่างเป็นทางการ การประเมินความเข้าใจและการยอมรับ รวมถึงการตรวจติดตามการปฏิบัติตามจริง มีการวิเคราะห์ผลการประเมิน และนำผลไปใช้ในการปรับปรุงนโยบาย แนวปฏิบัติ และกระบวนการบังคับใช้อย่างต่อเนื่อง

2 เอกสารที่ 1 (เอกสารหลัก)

รายงานการตรวจสอบและประเมินการปฏิบัติตามระเบียบปฏิบัติ

ด้านความมั่นคงปลอดภัยสารสนเทศ (Cybersecurity Compliance Report)

โรงพยาบาล.....

ประจำปีงบประมาณ พ.ศ. 25xx

1. หลักการและเหตุผล

เพื่อให้มั่นใจว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด หน่วยงานจึงจัดให้มีการตรวจสอบและประเมินผลการปฏิบัติตาม (Compliance) และนำผลการประเมินไปใช้ในการปรับปรุงกระบวนการบังคับใช้ระเบียบปฏิบัติอย่างต่อเนื่อง

2. วัตถุประสงค์

1. ตรวจสอบความเข้าใจและการยอมรับนโยบายของบุคลากร
2. ประเมินการปฏิบัติตามระเบียบปฏิบัติด้าน Cybersecurity
3. ปรับปรุงนโยบายและแนวปฏิบัติให้เหมาะสมและมีประสิทธิภาพ

3. ขอบเขตการประเมิน

ครอบคลุมระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศตาม

- นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ (ข้อ 1.3)
- ข้อ 3.1 – 3.4

4. ตารางโครงสร้างการดำเนินงาน

ขั้นตอน	รายละเอียด	เอกสารประกอบ
1. แจ้งนโยบายอย่างเป็นทางการ	แจ้งให้บุคลากรรับทราบผ่าน Email / LINE / ประชุม	ประกาศภายใน, เอกสารลงนามรับทราบ
2. ตรวจสอบว่า “เข้าใจ-ยอมรับ”	แบบประเมินความเข้าใจ / แบบยอมรับ Compliance	แบบประเมินออนไลน์, แบบลงนาม
3. ประเมินการปฏิบัติตามจริง	ตรวจ log, สุ่มตรวจพฤติกรรม, ตรวจความเสี่ยง	Audit log, แบบประเมิน supervisor
4. วิเคราะห์ผลการประเมิน	วิเคราะห์ช่องโหว่/การไม่ปฏิบัติตาม	รายงานผล, สถิติการฝ่าฝืน
5. ปรับปรุงระเบียบ/แนวปฏิบัติ	ปรับนโยบาย เพิ่มอบรม แก่กระบวนการ	นโยบายเวอร์ชันใหม่, บันทึกประชุม

เอกสารที่ 2 : แบบฟอร์มสำคัญ

แบบฟอร์มยืนยันความเข้าใจและการยอมรับระเบียบปฏิบัติ (Compliance Agreement)

ข้าพเจ้าได้อ่าน ทำความเข้าใจ และยอมรับการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานแล้ว

ชื่อ-สกุล	ตำแหน่ง	หน่วยงาน	ลงชื่อ	วันที่

แบบฟอร์มตรวจติดตามการปฏิบัติตาม (Compliance Monitoring)

รายการตรวจ	ปฏิบัติ	ไม่ปฏิบัติ	หมายเหตุ
ใช้งานระบบตามสิทธิ์	✓		
ไม่เปิดเผยข้อมูลผู้ป่วย	✓		
ไม่ใช้ Social Media ผิดนโยบาย	✓		
ปฏิบัติตาม Password Policy	✓		

3 ต้องมีครบ 5 ขั้นตอนนี้ พร้อมเอกสารหลักฐาน

1. แจ้งนโยบายอย่างเป็นทางการ
2. ตรวจสอบว่า “เข้าใจ-ยอมรับ”
3. ประเมินการปฏิบัติตามจริง (Compliance Monitoring)
4. วิเคราะห์ผลการประเมิน
5. ปรับปรุงระเบียบ/แนวปฏิบัติอย่างต่อเนื่อง

-  Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)
-  ไม่ใช่แค่ “แจ้ง” แต่มี ตรวจสอบ-ประเมิน-ปรับปรุง
-  มี Compliance Agreement
-  มี Monitoring / Audit
-  มี การปรับปรุงจากผลประเมิน
-  สอดคล้องแนวคิด PDCA / Continuous Improvement

อ้างอิงเกณฑ์ หมวดที่ 4 ข้อ CS.4.1

“มีการจัดทำทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ (Critical services) ของหน่วยงาน”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.4.1

หน่วยงานมีการจัดทำทะเบียนทรัพย์สินด้านสารสนเทศ (IT Asset Inventory) ที่เกี่ยวข้องกับบริการสำคัญ (Critical services) ของหน่วยงาน โดยครอบคลุมทรัพย์สินด้าน Hardware, Software, Network และ ข้อมูล/เอกสารสำคัญ

มีการระบุเจ้าของทรัพย์สิน ระดับความสำคัญ และระดับความเสี่ยงของทรัพย์สินแต่ละรายการ เพื่อใช้เป็นฐานข้อมูลในการบริหารจัดการและควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

2 เอกสารที่ 1 (เอกสารหลัก)

ทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ (IT Asset Inventory for Critical Services)

โรงพยาบาล.....

ปรับปรุงล่าสุด ณ วันที่

1. หลักการและเหตุผล

เพื่อให้หน่วยงานสามารถบริหารจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ (Critical services) ได้อย่างเหมาะสม หน่วยงานจึงจัดทำทะเบียนทรัพย์สินด้านสารสนเทศ (IT Asset Inventory) เพื่อใช้เป็นข้อมูลพื้นฐานในการกำหนดมาตรการควบคุมและบริหารความเสี่ยง

2. วัตถุประสงค์

1. ระบุและจัดทำรายการทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ
2. กำหนดเจ้าของทรัพย์สินและระดับความสำคัญ
3. ใช้เป็นฐานข้อมูลสำหรับการบริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์

3. ขอบเขต

ครอบคลุมทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการสำคัญของหน่วยงาน ได้แก่ ระบบให้บริการทางการแพทย์ ระบบข้อมูลผู้ป่วย ระบบเครือข่าย และเอกสาร/ข้อมูลสำคัญ

4. ตารางทะเบียนทรัพย์สินด้านสารสนเทศ

ลำดับ	ประเภททรัพย์สิน	รายการ	เจ้าของทรัพย์สิน (Asset Owner)	ความสำคัญ (Critical / Non)	ความเสี่ยง	สถานะ	หมายเหตุ
1	Hardware	Server HIS #1	หัวหน้า IT	Critical	High	ใช้งานอยู่	อายุใช้งาน > 7 ปี
2	Software	ระบบ HIS (v5.0)	หัวหน้า IT	Critical	Medium	ใช้งานอยู่	ไม่มีสัญญาบำรุง
3	Network	Firewall FortiGate	ผู้ดูแลระบบ	Critical	High	ใช้งานอยู่	ต้อง Renew license
4	Document	นโยบาย Data Backup	CISO	Critical	Low	ล่าสุด 2566	ยังไม่อัปเดต

ตารางนี้คือหัวใจของ CS.4.1

กรรมการจะดูว่า มี Critical + Asset Owner + ครบ 4 ประเภท หรือไม่

เอกสารที่ 2 (เอกสารประกอบ – แนะนำ)

แบบฟอร์มขึ้นทะเบียนทรัพย์สินด้านสารสนเทศ (IT Asset Registration Form)

รายการ	รายละเอียด
ประเภททรัพย์สิน	Hardware / Software / Network / Data / Document
ชื่อทรัพย์สิน	
บริการสำคัญที่เกี่ยวข้อง	
เจ้าของทรัพย์สิน (Asset Owner)	
ระดับความสำคัญ	Critical / Non-Critical
ระดับความเสี่ยง	High / Medium / Low
สถานะการใช้งาน	
หมายเหตุ	

3 ต้องแสดงให้เห็นว่า โรงพยาบาล

✓ มี ทะเบียนทรัพย์สินด้านสารสนเทศ (IT Asset Inventory)

✓ เชื่อมโยงกับ บริการสำคัญ (Critical services)

✓ ครอบคลุม 4 ประเภทหลัก

- Hardware
- Software
- Network
- People / Data / Document ระบุ เจ้าของทรัพย์สิน (Asset Owner) และระดับความสำคัญ

4 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

✓ มีคำว่า Critical services

✓ ครอบคลุม 4 ประเภททรัพย์สิน

✓ ระบุ Asset Owner

✓ ระบุความสำคัญและความเสี่ยง

✓ เป็นทะเบียนทรัพย์สินจริง ไม่ใช่แค่รายการครุภัณฑ์ทั่วไป

อ้างอิงเกณฑ์ หมวดที่ 4 ข้อ CS.4.2

“มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.4.2

หน่วยงานมีการวิเคราะห์สถานการณ์ปัจจุบันและจัดทำ Gap Analysis ของทรัพยากรด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมด้าน Hardware, Software, Network และ People อย่างครบถ้วน ผลการวิเคราะห์ถูกนำมาใช้ในการระบุช่องว่างและกำหนดแนวทางพัฒนา เพื่อให้ทรัพยากรด้านเทคโนโลยีสารสนเทศมีความเพียงพอและเหมาะสมต่อการให้บริการสำคัญของหน่วยงาน

2 เอกสารหลัก

รายงานการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้านเทคโนโลยีสารสนเทศ

โรงพยาบาล.....

ประจำปีงบประมาณ พ.ศ. 25xx

1. หลักการและเหตุผล

เพื่อให้ทรัพยากรด้านเทคโนโลยีสารสนเทศของหน่วยงานมีความเพียงพอ เหมาะสม และสามารถรองรับการให้บริการด้านสาธารณสุขที่สำคัญได้อย่างต่อเนื่อง หน่วยงานจึงจัดทำการวิเคราะห์สถานการณ์ปัจจุบัน (As-is) และการวิเคราะห์ช่องว่าง (Gap Analysis) ของทรัพยากรด้าน Hardware, Software, Network และ People

2. วัตถุประสงค์

1. ประเมินความพร้อมและความเพียงพอของทรัพยากร IT ปัจจุบัน
2. เปรียบเทียบกับความต้องการในการให้บริการสำคัญ
3. ระบุช่องว่างและประเด็นที่ต้องพัฒนาเพิ่มเติม

3. ขอบเขตการวิเคราะห์

ครอบคลุมทรัพยากรด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบริการสำคัญของหน่วยงาน ได้แก่

- Hardware
- Software
- Network
- People (บุคลากรด้าน IT)

4. ตารางสรุปผลการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis

(หัวใจของ CS.4.2 — กรรมการจะดูตารางนี้เป็นหลัก)

4.1 ด้าน Hardware

รายการ	สถานการณ์ปัจจุบัน	ความต้องการ	Gap ที่พบ	แนวทางพัฒนา
Server HIS	อายุใช้งาน > 7 ปี	ควรไม่เกิน 5 ปี	ประสิทธิภาพต่ำ	วางแผนจัดซื้อใหม่
UPS	มีเฉพาะเครื่องหลัก	ควรครอบคลุมทุก Server	ยังไม่เพียงพอ	เพิ่ม UPS

4.2 ด้าน Software

รายการ	สถานการณ์ปัจจุบัน	ความต้องการ	Gap ที่พบ	แนวทางพัฒนา
ระบบ HIS	เวอร์ชันเก่า	เวอร์ชันล่าสุด	ขาดฟีเจอร์ใหม่	วางแผนอัปเดต
Antivirus	License ใกล้เคียงหมด	License ต่อเนื่อง	เสี่ยงขาดการป้องกัน	ต่ออายุ License

4.3 ด้าน Network

รายการ	สถานการณ์ปัจจุบัน	ความต้องการ	Gap ที่พบ	แนวทางพัฒนา
Firewall	ใช้งานอยู่	ต้องอัปเดตเสมอ	ใกล้หมด License	ต่ออายุ / ปรับแผน
Bandwidth	เพียงพอเฉพาะเวลาปกติ	รองรับ Peak	ความเร็วไม่พอ	เพิ่ม Bandwidth

4.4 ด้าน People

รายการ	สถานการณ์ปัจจุบัน	ความต้องการ	Gap ที่พบ	แนวทางพัฒนา
บุคลากร IT	1 คน	อย่างน้อย 2 คน	กำลังไม่เพียงพอ	ขออัตรากำลังเพิ่ม
ทักษะ Cyber	ระดับพื้นฐาน	ทักษะเฉพาะทาง	ขาดการอบรม	จัดอบรม Cyber

5. สรุปผลการวิเคราะห์

จากการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis พบว่าทรัพยากรด้านเทคโนโลยีสารสนเทศของหน่วยงานยังมีบางด้านที่ต้องพัฒนาเพิ่มเติม เพื่อให้สามารถรองรับการให้บริการสำคัญได้อย่างมีประสิทธิภาพ โดยเฉพาะด้าน Hardware และ People ซึ่งจำเป็นต้องได้รับการปรับปรุงในระยะต่อไป

6. การนำผลการวิเคราะห์ไปใช้

ผลการวิเคราะห์นี้จะถูกนำไปใช้ประกอบการวางแผนจัดสรรงบประมาณ การพัฒนาทรัพยากร และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงาน

การรับรองรายงาน

ลงชื่อ

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

ผู้อำนวยการโรงพยาบาล

วันที่

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ✓ มีคำว่า วิเคราะห์สถานการณ์ปัจจุบัน
- ✓ มี Gap Analysis ชัดเจน
- ✓ ครอบคลุม Hardware / Software / Network / People
- ✓ มีเอกสารสรุปผลเป็นลายลักษณ์อักษร

อ้างอิงเกณฑ์ หมวดที่ 4 ข้อ CS.4.3

“มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากร ด้าน Hardware, Software, Network”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.4.3

หน่วยงานได้นำผลการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ตามข้อ CS.4.2 มาใช้จัดทำแผนพัฒนาทรัพยากรด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมด้าน Hardware, Software, Network และ People อย่างครบถ้วน

แผนดังกล่าวมีการกำหนดแนวทางพัฒนา ลำดับความสำคัญ ระยะเวลาดำเนินการ และผู้รับผิดชอบ เพื่อให้ทรัพยากรด้านเทคโนโลยีสารสนเทศมีความเพียงพอและเหมาะสมต่อการให้บริการสำคัญของหน่วยงาน

2 เอกสารหลัก

แผนการเพิ่มและจัดการศักยภาพของทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resource Capacity Improvement Plan)

โรงพยาบาล.....

ปีงบประมาณ พ.ศ. 25xx

1. หลักการและเหตุผล

จากผลการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้านเทคโนโลยีสารสนเทศตามข้อ CS.4.2 พบว่าทรัพยากรบางด้านยังไม่เพียงพอหรือมีข้อจำกัดในการรองรับการให้บริการสำคัญ หน่วยงานจึงจัดทำแผนการเพิ่มและจัดการศักยภาพของทรัพยากรด้าน Hardware, Software และ Network เพื่อให้มีความพร้อม เหมาะสม และลดความเสี่ยงต่อการให้บริการ

2. วัตถุประสงค์

1. เพิ่มศักยภาพและความพร้อมของทรัพยากรด้าน IT
2. ลดความเสี่ยงจากทรัพยากรที่ล้าสมัยหรือไม่เพียงพอ
3. รองรับการให้บริการสำคัญของหน่วยงานอย่างต่อเนื่อง

3. ขอบเขตแผน

ครอบคลุมการจัดการศักยภาพทรัพยากรด้าน

- Hardware
- Software
- Network

4. ตารางแผนจัดการศักยภาพทรัพยากร

(โครงสร้างตัวอย่าง)

ด้าน	รายการ	แนวทางพัฒนา	ระยะเวลา ดำเนินการ	ผู้รับผิดชอบ	หมายเหตุ
Hardware	Server HIS	จัดซื้อ/ติดตั้ง Server Dell R650	มิ.ย.-ก.ค. 25xx	หัวหน้า IT	ดำเนินการแล้ว
Software	Antivirus	ติดตั้ง Bitdefender GravityZone	มิ.ย.-ก.ค. 25xx	IT Support	รอเสนอราคา
Network	Firewall	จัดซื้อ FortiGate และ แยก VLAN	ส.ค.-ก.ย. 25xx	System Admin	ขออนุมัติ กรรมการ

ตารางนี้คือ หัวใจหลักของ CS.4.3 กรรมการจะดูว่า ครบ 3 ด้าน และเป็นแผนจริง หรือไม่

5. การติดตามและทบทวนแผน

หน่วยงานจะติดตามความก้าวหน้าของการดำเนินงานตามแผน และทบทวนแผนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงภารกิจหรือความเสี่ยงด้านเทคโนโลยีสารสนเทศ

6. การอนุมัติแผน

แผนฉบับนี้ได้รับความเห็นชอบจากผู้บริหาร และใช้เป็นกรอบในการพัฒนาทรัพยากรด้านเทคโนโลยีสารสนเทศของหน่วยงาน

ลงชื่อ

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

ผู้อำนวยการโรงพยาบาล

วันที่

แบบฟอร์มติดตามแผนเพิ่มศักยภาพทรัพยากร IT

รายการ	สถานะ	ปัญหา / อุปสรรค	การดำเนินการ
อัปเดต Server หลักสำหรับ ระบบ HIS	ดำเนินการแล้ว	ต้องหยุดระบบชั่วคราว นอกเวลาราชการ	ติดตั้ง Server ใหม่ ย้ายข้อมูล และทดสอบระบบเรียบร้อยแล้ว
ติดตั้งระบบ Antivirus และ Patch Management	อยู่ระหว่าง ดำเนินการ	รออนุมัติงบประมาณค่า License	เสนอขออนุมัติงบประมาณและ เตรียมแผนติดตั้ง
อบรมบุคลากรด้าน Cybersecurity	ดำเนินการ บางส่วน	บุคลากรติดภารกิจ ไม่ ครบตามเป้าหมาย	จัดอบรมเพิ่มเติมรอบถัดไปและ อบรมออนไลน์เสริม

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ✓ เป็น “แผน” ไม่ใช่แค่รายการ
- ✓ ครบ Hardware / Software / Network
- ✓ มีระยะเวลา + ผู้รับผิดชอบ
- ✓ เชื่อมโยงจาก CS.4.2
- ✓ ใช้งานจริงได้

อ้างอิงเกณฑ์ หมวดที่ 4 ข้อ CS.4.4

“มีการกำหนดสมรรถนะตามบทบาทหน้าที่ที่จำเป็น (Functional Competency) ของบุคลากรด้าน IT ทุกคน และประเมินสมรรถนะตามบทบาทหน้าที่ และจัดทำแผนเพิ่มสมรรถนะรายบุคคล”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.4.4

หน่วยงานมีการกำหนดสมรรถนะตามบทบาทหน้าที่ที่จำเป็น (Functional Competency) ของบุคลากรด้านเทคโนโลยีสารสนเทศทุกคน มีการประเมินสมรรถนะตามบทบาทหน้าที่ และจัดทำแผนเพิ่มสมรรถนะรายบุคคล เพื่อพัฒนาความรู้และทักษะให้เหมาะสมกับภารกิจและความรับผิดชอบ

2 ตัวอย่างเอกสาร

เอกสารที่ 1

ตารางกำหนดสมรรถนะตามบทบาทหน้าที่บุคลากรด้าน IT (IT Functional Competency Framework)

โรงพยาบาล.....

ปีงบประมาณ พ.ศ. 25xx

ตารางที่ 1 : สมรรถนะตามบทบาทหน้าที่

บทบาทหน้าที่	สมรรถนะที่จำเป็น	ระดับที่คาดหวัง
หัวหน้าฝ่าย IT	IT Governance, Cybersecurity Management, PDPA	สูง
System Admin	Server, Network, Backup, Incident Response	สูง
IT Support	User Support, Endpoint Security, Patch	กลาง
Programmer / HIS	HIS, Database, Secure Coding	กลาง

ตารางนี้แสดงว่า “กำหนดสมรรถนะตามบทบาท” ครบทุกคน

เอกสารที่ 2

ผลการประเมินสมรรถนะตามบทบาทหน้าที่บุคลากรด้าน IT

ตารางที่ 2 : ผลการประเมินสมรรถนะรายบุคคล

ชื่อ-สกุล	บทบาท	สมรรถนะที่ประเมิน	ระดับปัจจุบัน	ระดับที่คาดหวัง	ช่องว่าง
นาย ก	System Admin	Network / Security	กลาง	สูง	ต้องอบรมเพิ่ม
น.ส. ข	IT Support	Endpoint Security	ต่ำ	กลาง	ขาดประสบการณ์

เอกสารที่ 3

แผนเพิ่มสมรรถนะรายบุคคล (Individual Development Plan : IDP)

ตารางที่ 3 : แผนพัฒนารายบุคคล

ชื่อ	บทบาท	ช่องว่างสมรรถนะ	แนวทางพัฒนา	ระยะเวลา	ผู้รับผิดชอบ
นาย ก	System Admin	Cybersecurity ขั้นสูง	อบรม Cyber / Cert	ปี 25xx	หัวหน้า IT
น.ส. ข	IT Support	Endpoint Security	On-the-job + อบรม	ปี 25xx	หัวหน้า IT

ตัวอย่าง แบบฟอร์มประกอบ จำนวน 2 แบบฟอร์ม

1. แบบฟอร์มประเมินสมรรถนะตามบทบาทหน้าที่

ชื่อ-สกุล : นาย ก.กิตติ

ตำแหน่ง : System Administrator

หน่วยงาน : ฝ่ายเทคโนโลยีสารสนเทศ

สมรรถนะ	ระดับ 1	ระดับ 2	ระดับ 3	คะแนน
การบริหารจัดการระบบ Server	เข้าใจพื้นฐาน	ดูแลได้ตามคู่มือ	วิเคราะห์/แก้ปัญหาเชิงลึก	2
การจัดการระบบเครือข่าย	รู้โครงสร้าง	ตั้งค่า VLAN / Firewall ได้	ออกแบบ Network	2
ความมั่นคงปลอดภัยไซเบอร์	รู้แนวคิดพื้นฐาน	ปฏิบัติตาม Policy	วิเคราะห์ Incident	1
การสำรองและกู้คืนข้อมูล	ทำตามขั้นตอน	วางแผน Backup	ทดสอบ DR Plan	2

สรุปผล : สมรรถนะด้าน Cybersecurity ยังต่ำกว่าระดับที่คาดหวัง → ต้องจัดทำ IDP

2. แบบฟอร์มแผนพัฒนารายบุคคล (IDP)

(ตัวอย่าง) แบบฟอร์มแผนพัฒนารายบุคคล (Individual Development Plan : IDP)

ชื่อ-สกุล : นาย ก.กิตติ

บทบาทหน้าที่ : System Administrator

เป้าหมายพัฒนา	วิธีพัฒนา	ระยะเวลา	ผลที่คาดหวัง
เพิ่มสมรรถนะด้าน Cybersecurity	อบรมหลักสูตร Cybersecurity สำหรับ System Admin	ภายในปี 25xx	มีความรู้ด้าน Incident Response
พัฒนาทักษะ Network Security	ฝึกปฏิบัติจริงร่วมกับผู้เชี่ยวชาญ / Vendor	6 เดือน	สามารถตั้งค่า Firewall / VLAN ได้
เสริมความรู้ด้าน PDPA	เรียนออนไลน์ + ทบทวนนโยบายองค์กร	3 เดือน	ปฏิบัติงานสอดคล้อง PDPA

ตัวอย่างเพิ่มเติม (อีก 1 บทบาท)

1. แบบฟอร์มประเมินสมรรถนะตามบทบาทหน้าที่

ชื่อ-สกุล : น.ส. ข.ขวัญใจ

ตำแหน่ง : IT Support

สมรรถนะ	ระดับ 1	ระดับ 2	ระดับ 3	คะแนน
การสนับสนุนผู้ใช้งาน	ทำตามคำสั่ง	แก้ปัญหาเบื้องต้น	วิเคราะห์ปัญหา	2
Endpoint Security	รู้พื้นฐาน	ตั้งค่า Antivirus	วิเคราะห์ Malware	1
การใช้นโยบาย IT	รับทราบ	ปฏิบัติตาม	แนะนำผู้อื่นได้	2

2. แบบฟอร์มแผนพัฒนารายบุคคล (IDP)

เป้าหมายพัฒนา	วิธีพัฒนา	ระยะเวลา	ผลที่คาดหวัง
เพิ่มทักษะ Endpoint Security	อบรม Endpoint / Antivirus	6 เดือน	ลดความเสี่ยง Malware
เสริมความรู้ Cyber Awareness	อบรมภายในหน่วยงาน	ต่อเนื่อง	ปฏิบัติตามนโยบายได้ถูกต้อง

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ✓ กำหนด Functional Competency ทุกบทบาท
- ✓ มี ผลการประเมินจริง
- ✓ มี IDP รายบุคคล
- ✓ ครบทั้ง 3 เอกสาร
- ✓ ใช้พัฒนาได้จริง

อ้างอิงเกณฑ์ หมวดที่ 4 ข้อ CS.4.5

“มีผลการวิเคราะห์ สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People มาปรับปรุงจัดทำแผนเพิ่มศักยภาพ อย่างต่อเนื่อง”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.4.5

หน่วยงานมีการนำผลการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People มาใช้จัดทำแผนเพิ่มศักยภาพ และมีการติดตามประเมินผลการดำเนินงานตามแผนอย่างต่อเนื่อง มีการจัดทำรายงานสรุปความก้าวหน้า ระบุผลการดำเนินงานจริง ปัญหาและอุปสรรค พร้อมนำผลการติดตามไปใช้ในการปรับแผนและกำหนดแนวทางดำเนินการในระยะถัดไป

โรงพยาบาล ดำเนินการ ทำแผน → ลงมือทำ → ติดตามผล → รู้ปัญหา → ปรับแผนได้จริง

2 เอกสารหลัก

รายงานการนำผลการวิเคราะห์และ Gap Analysis ไปใช้ปรับปรุงและพัฒนาศักยภาพทรัพยากรด้านเทคโนโลยีสารสนเทศ

โรงพยาบาล.....

ปีงบประมาณ พ.ศ. 25xx

1. หลักการและเหตุผล

จากการวิเคราะห์สถานการณ์ปัจจุบันและการทำ Gap Analysis ของทรัพยากรด้านเทคโนโลยีสารสนเทศ (Hardware, Software, Network และ People) ตามข้อ CS.4.2 หน่วยงานได้นำผลการวิเคราะห์ดังกล่าวมาใช้เป็นข้อมูลในการปรับปรุงและพัฒนาศักยภาพทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง เพื่อให้มีความเพียงพอ เหมาะสม และรองรับภารกิจและบริการสำคัญของหน่วยงาน

2. วัตถุประสงค์

1. นำผลการวิเคราะห์และ Gap Analysis ไปใช้ในการปรับปรุงทรัพยากร IT
2. เพิ่มศักยภาพและลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ
3. สนับสนุนการให้บริการสำคัญของหน่วยงานอย่างต่อเนื่อง

3. สรุปผลการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis

(สรุปจากรายงาน CS.4.2)

ด้านทรัพยากร	ความสามารถที่มี	ข้อจำกัด / ความเสี่ยง
Hardware	มี Server 2 ชุด, UPS 30 นาที	Server อายุเกิน 7 ปี, UPS ไม่ครอบคลุม
Software	มี HIS, Antivirus, Backup	ไม่มี Auto Update, OS ล้าสมัย
Network	มี Firewall, แยก Guest WiFi	ไม่มี IDS/IPS, Redundancy ไม่พอ
People	มี IT Officer 1 คน	ขาดบุคลากรเฉพาะด้าน Cyber

4. ตารางการนำผลวิเคราะห์ไปปรับปรุงและพัฒนา

ด้าน	Gap ที่พบ	การปรับปรุง/พัฒนา	ระยะเวลา	สถานะ
Hardware	Server เก่า / UPS ไม่พอ	จัดซื้อ Server ใหม่ + เพิ่ม UPS	ปี 25xx	ดำเนินการแล้ว
Software	ไม่มี Patch Management	ติดตั้งระบบอัปเดตอัตโนมัติ	ปี 25xx	อยู่ระหว่างดำเนินการ
Network	ไม่มี IDS/IPS	จัดหา Firewall ที่มี IDS/IPS	ปี 25xx	วางแผน
People	ขาดทักษะ Cyber	อบรม Cyber / ทำ IDP	ต่อเนื่อง	ดำเนินการแล้ว

ตารางนี้คือ จุดชี้ขาดของ CS.4.5 กรรมการจะดูว่า Gap → การปรับปรุงจริง หรือไม่

5. การปรับปรุงอย่างต่อเนื่อง

หน่วยงานมีการติดตามผลการดำเนินงานตามแผนพัฒนาทรัพยากรด้านเทคโนโลยีสารสนเทศ และทบทวนผลการดำเนินงานอย่างน้อยปีละ 1 ครั้ง เพื่อนำผลไปใช้ในการปรับปรุงแผนและมาตรการให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลง

6. การรับรอง

รายงานฉบับนี้ได้รับการรับรองจากผู้บริหาร และใช้เป็นข้อมูลประกอบการพัฒนาและจัดสรรทรัพยากรด้านเทคโนโลยีสารสนเทศของหน่วยงาน

ลงชื่อ

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

ผู้อำนวยการโรงพยาบาล

วันที่

3 แบบฟอร์มแนบประกอบ

(ตัวอย่าง) แบบฟอร์มติดตามการปรับปรุงศักยภาพทรัพยากร IT

ด้าน	กิจกรรมพัฒนา	ผลการดำเนินงาน	ปัญหา / อุปสรรค	แนวทางปรับปรุง
Hardware	จัดซื้อและติดตั้ง Server ใหม่สำหรับระบบ HIS	ดำเนินการแล้ว 100% และย้ายระบบสำเร็จ	ไม่มี	ติดตามประสิทธิภาพหลังใช้งานจริงทุกไตรมาส
Software	ติดตั้งระบบ Antivirus และ Patch Management	ดำเนินการแล้ว 80%	ขาด License Key บางส่วน	เร่งจัดซื้อ License เพิ่มและวางแผนอัปเดตให้ครบ
Network	ติดตั้งระบบ IDS/IPS	ยังไม่เริ่มดำเนินการ	งบประมาณอนุมัติล่าช้า	ปรับแผนดำเนินการในไตรมาสถัดไป
People	อบรม Cybersecurity ให้บุคลากร IT	อบรมแล้ว 3 จาก 4 คน	บุคลากร 1 คนติดภารกิจ	จัดอบรมเพิ่มเติมในรอบถัดไป
Policy	ทบทวนและปรับปรุงแผน IRP	ร่างแผนแล้ว เสนอผู้บริหาร	ผู้บริหารยังไม่ลงนาม	นัดประชุมเพื่อติดตามการอนุมัติ

(ตัวอย่าง) เอกสารรายงานการติดตามและประเมินผลการดำเนินงานตามแผนเพิ่มศักยภาพทรัพยากร IT

โรงพยาบาล.....

รอบการติดตาม : ไตรมาส 2/25xx

สรุปภาพรวม

จากการติดตามผลการดำเนินงานตามแผนเพิ่มศักยภาพทรัพยากรด้านเทคโนโลยีสารสนเทศ พบว่า บางกิจกรรมดำเนินการแล้วเสร็จ ขณะที่บางกิจกรรมอยู่ระหว่างดำเนินการหรือมีความล่าช้า เนื่องจากข้อจำกัดด้านงบประมาณ บุคลากร และการอนุมัติ

แนวทางปรับปรุง

- เร่งรัดการจัดซื้อ License Software
- ปรับแผนการติดตั้ง IDS/IPS ให้สอดคล้องรอบงบประมาณ
- จัดตารางอบรมบุคลากรเพิ่มเติม

(ตัวอย่าง) บันทึกการประชุมติดตามแผนเพิ่มศักยภาพ (Meeting Notes)

วาระ : ติดตามผลการดำเนินงาน CS.4.5

ผู้เข้าร่วม : ผู้บริหาร / IT / HR

มติที่ประชุม

1. เห็นชอบผลการจัดซื้อ Server ใหม่
2. มอบฝ่าย IT เร่งดำเนินการจัดหา License Software
3. ปรับแผนอบรม Cybersecurity ให้ครอบคลุมครบทุกคนภายในไตรมาสถัดไป

Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

-  มีแผน (จาก CS.4.3)
-  มีการติดตามผลจริง
-  มีรายงานความก้าวหน้า
-  ระบุปัญหา/อุปสรรคได้
-  มีหลักฐานการประชุม/รายงาน

อ้างอิงเกณฑ์ หมวดที่ 5 ข้อ CS.5.1

“กำหนดมาตรการการรักษาความปลอดภัยทางกายภาพ การทบทวนสิทธิ์บุคลากรที่ได้รับอนุญาตให้เข้าถึง Data Center และการกำหนดหน้าที่ความรับผิดชอบในการดูแล Data Center ของหน่วยงาน”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.5.1

หน่วยงานมีการกำหนดมาตรการรักษาความปลอดภัยทางกายภาพของ Data Center อย่างชัดเจน ครอบคลุมการควบคุมการเข้า-ออกพื้นที่ การป้องกันการบุกรุก มีการทบทวนสิทธิ์บุคลากรที่ได้รับอนุญาตให้เข้าถึง Data Center อย่างสม่ำเสมอ และมีการกำหนดหน้าที่ความรับผิดชอบในการดูแล Data Center โดยมีเอกสาร และหลักฐานที่สามารถตรวจสอบได้

โรงพยาบาลดำเนินการ 3 ส่วนหลัก ได้แก่

1. มาตรการรักษาความปลอดภัยทางกายภาพของ Data Center
2. การทบทวนสิทธิ์บุคลากรที่ได้รับอนุญาตให้เข้าถึง Data Center อย่างสม่ำเสมอ
3. การกำหนดหน้าที่และความรับผิดชอบในการดูแล Data Center อย่างชัดเจน

2 เอกสารที่ 1

มาตรการรักษาความปลอดภัยทางกายภาพของ Data Center (Physical Security Measures for Data Center)

โรงพยาบาล.....

สถานที่ Data Center

วันที่ประกาศใช้

1. การควบคุมการเข้า-ออกพื้นที่ Data Center

- Data Center เป็นพื้นที่ควบคุมเฉพาะ (Restricted Area)
- ใช้กุญแจ/บัตรผ่านเฉพาะผู้ได้รับอนุญาต
- ติดตั้งกล้องวงจรปิด (CCTV) บันทึกภาพย้อนหลังอย่างน้อย 30 วัน
- บุคคลภายนอกต้องมีเจ้าหน้าที่ควบคุมตลอดเวลา
- มีการบันทึก Log การเข้า-ออก (สมุดหรือระบบดิจิทัล)

2. การป้องกันการบุกรุกและความเสี่ยงทางกายภาพ

- ห้อง Data Center แยกจากพื้นที่ใช้งานทั่วไป
- ติดตั้งระบบล็อกประตู และอุปกรณ์แจ้งเตือน
- ห้ามจัดเก็บวัสดุไวไฟหรือของที่ไม่เกี่ยวข้อง

3. การทบทวนสิทธิการเข้าถึง Data Center

- ทบทวนรายชื่อผู้มีสิทธิ์เข้า Data Center อย่างน้อย ทุก 6 เดือน
- ยกเลิกสิทธิ์ทันทีเมื่อบุคลากรลาออก/เปลี่ยนหน้าที่
- การขอเพิ่มสิทธิ์ต้องได้รับอนุมัติจากหัวหน้าหน่วยงาน

4. การกำหนดหน้าที่และความรับผิดชอบ

- กำหนดผู้รับผิดชอบหลักในการดูแล Data Center
- กำหนดผู้ตรวจสอบการเข้า-ออกและอุปกรณ์ความปลอดภัย
- มีคำสั่งแต่งตั้งหรือเอกสารมอบหมายหน้าที่เป็นลายลักษณ์อักษร

ลงชื่อ

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

ผู้อำนวยการโรงพยาบาล

เอกสารที่ 2

รายงานการทบทวนสิทธิการเข้าถึง Data Center (Access Rights Review Report)

รอบการทบทวน : ☐ 6 เดือน ☐ ประจำปี

วันที่ทบทวน :

ชื่อ-สกุล	ตำแหน่ง	เหตุผลที่ได้รับสิทธิ์	คงสิทธิ์	ยกเลิกสิทธิ์	หมายเหตุ
นาย ก.กิตติ	System Admin	ดูแลระบบ	✓	☐	–
น.ส. ข.ขวัญใจ	IT Support	สนับสนุนระบบ	✓	☐	–
นาย ค.	เจ้าหน้าที่ทั่วไป	ไม่มีความจำเป็น	☐	✓	ย้ายงาน

ผู้ทบทวน

ผู้อนุมัติ

เอกสารที่ 3

เอกสารกำหนดหน้าที่และความรับผิดชอบในการดูแล Data Center (Roles & Responsibilities)

บทบาท	หน้าที่
ผู้ดูแลหลัก (Primary Operator)	ควบคุมสิทธิ์เข้า-ออก ดูแลอุปกรณ์
ผู้ตรวจสอบ (Auditor)	ตรวจสอบ Log, CCTV, การเข้า-ออก
ผู้บริหาร IT	อนุมัติสิทธิ์และบริหารความเสี่ยง

แบบฟอร์มประกอบ

แบบฟอร์มบันทึกการเข้า-ออก Data Center

วันที่	ชื่อ-สกุล	เวลา เข้า	เวลา ออก	เหตุผลในการเข้า	ผู้ควบคุม (ลงชื่อ)
10 ม.ค. 25xx	นาย ก.กิตติ	09:00	10:30	ตรวจสอบ Server HIS และสถานะ Backup	หัวหน้าฝ่าย IT
15 ม.ค. 25xx	น.ส. ขวัญใจ	13:00	14:00	เปลี่ยน UPS และตรวจสอบระบบ ไฟฟ้า	System Admin
20 ม.ค. 25xx	นาย ช. (Vendor)	10:00	11:30	ซ่อมบำรุงอุปกรณ์ Network Firewall	เจ้าหน้าที่ IT

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ✓ มาตรการทางกายภาพเป็นลายลักษณ์อักษร
- ✓ ควบคุมการเข้า-ออก + Log
- ✓ ทบทวนสิทธิ์เป็นรอบ
- ✓ ระบุผู้รับผิดชอบชัดเจน
- ✓ มีเอกสารตรวจสอบได้

อ้างอิงเกณฑ์ หมวดที่ 5 ข้อ CS.5.2

“การกำหนดรอบการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูล รวมถึงป้องกันสื่อบันทึกการสำรองข้อมูล จากความเสียหายและการสูญหาย และการเข้าถึงโดยไม่ได้รับอนุญาต”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.5.2

หน่วยงานมีการจัดทำแผนการสำรองและกู้คืนข้อมูล (Data Backup & Recovery Plan) อย่างชัดเจน ครอบคลุมระบบสารสนเทศที่สำคัญ มีการกำหนดรอบการสำรองข้อมูล การจัดเก็บข้อมูลอย่างปลอดภัยทั้งภายใน และภายนอกหน่วยงาน รวมถึงมีการทดสอบการกู้คืนข้อมูลเป็นระยะ พร้อมบันทึกผลการทดสอบและมาตรการ ป้องกันสื่อบันทึกข้อมูล ได้แก่

1. แผนการสำรองข้อมูล (Backup Plan / Schedule)
2. การทดสอบการกู้คืนข้อมูล (Recovery Testing / Drill)
3. มาตรการป้องกันสื่อสำรองข้อมูล
4. หลักฐานเป็นเอกสารตรวจสอบได้

2 เอกสารหลัก

แผนการสำรองและกู้คืนข้อมูล (Data Backup & Recovery Plan)

โรงพยาบาล.....

วันที่ประกาศใช้

1. วัตถุประสงค์

เพื่อให้ข้อมูลสารสนเทศที่สำคัญของหน่วยงานสามารถกู้คืนได้อย่างถูกต้อง ปลอดภัย และต่อเนื่อง ในกรณีเกิด เหตุขัดข้อง เหตุฉุกเฉิน หรือภัยคุกคามทางไซเบอร์

2. ขอบเขตข้อมูลที่ต้องสำรอง

- ระบบ HIS
- ระบบ LIS (LAB)
- ข้อมูลเวชระเบียนอิเล็กทรอนิกส์
- เอกสารสำคัญทางราชการ

3. แผนการสำรองข้อมูล (Backup Schedule)

ระบบ	ความถี่	วิธีการ	สถานที่เก็บ
HIS	รายวัน	Full + Incremental	Onsite Server + Cloud
LAB (LIS)	รายวัน	Scheduled Script	External NAS
เอกสารเวชระเบียน	รายสัปดาห์	Manual Backup	External HDD (ลิ้นชัก)

4. การจัดเก็บข้อมูลสำรอง

- เก็บข้อมูลอย่างน้อย 2 ชุด
 - Onsite ภายในหน่วยงาน
 - Offsite (Cloud / External Storage)
- จำกัดสิทธิ์การเข้าถึงเฉพาะผู้รับผิดชอบ
- จัดเก็บในสถานที่ปลอดภัย

5. การทดสอบการกู้คืนข้อมูล (Data Recovery Testing)

- ดำเนินการทดสอบกู้คืนข้อมูล อย่างน้อยปีละ 1 ครั้ง
- ใช้ข้อมูลจริงในสภาพแวดล้อมจำลอง
- บันทึกผลการทดสอบ เช่น ระยะเวลา ความสมบูรณ์ และปัญหาที่พบ

6. มาตรการป้องกันสื่อบันทึกข้อมูลสำรอง

- เข้ารหัสข้อมูล (Encryption)
- ควบคุมการเข้าถึง Flash Drive / External HDD
- ตรวจสอบสภาพอุปกรณ์อย่างสม่ำเสมอ
- สื่อที่เสื่อมสภาพ ดำเนินการทำลายอย่างปลอดภัย (Secure Destruction)

ลงชื่อ

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

ผู้อำนวยการโรงพยาบาล

เอกสารที่ 2

บันทึกการทดสอบการกู้คืนข้อมูล (Recovery Drill Record)

วันที่ทดสอบ	ระบบ	ระยะเวลากู้คืน	ผลลัพธ์	ผู้ทำการทดสอบ (ลงชื่อ)
30 มิ.ย. 2568	HIS	2 ชม. 30 นาที	กู้คืนสมบูรณ์ 100%	System Admin

3 แบบฟอร์มประกอบ

แบบฟอร์มตรวจสอบการสำรองข้อมูลประจำงวด

ระบบ	สำรองตามแผน	ปัญหาที่พบ	แนวทางแก้ไข	ผู้ตรวจ
HIS	สำรองข้อมูลรายวันครบถ้วน	ไม่พบปัญหา	ติดตามและตรวจสอบ Log การสำรองข้อมูลต่อเนื่อง	นาย ก. กิตติ
LAB (LIS)	สำรองข้อมูลรายวัน	สำรองข้อมูลล่าช้า 1 ครั้ง	ปรับเวลา Scheduled Script และตรวจสอบระบบอีกครั้ง	นาย ก. กิตติ

Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

-  มี Backup Schedule
-  เก็บข้อมูล 2 แหล่ง (Onsite + Offsite)
-  มี Recovery Drill อย่างน้อยปีละ 1 ครั้ง
-  มีบันทึกผลการทดสอบ
-  มีมาตรการป้องกันสื่อสารองข้อมูล

อ้างอิงเกณฑ์ หมวดที่ 5 ข้อ CS.5.3

“มีระบบป้องกันอัคคีภัย เช่น ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงหรือระบบดับเพลิงอัตโนมัติ ให้เหมาะสมกับความเสี่ยง”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.5.3

หน่วยงานมีการติดตั้งระบบป้องกันอัคคีภัยในพื้นที่ Data Center/ห้อง Server อย่างเหมาะสมกับความเสี่ยง ประกอบด้วยระบบตรวจจับควัน ระบบสัญญาณเตือนภัย และเครื่องดับเพลิง รวมถึงมีการจัดทำแผนตรวจสอบและบำรุงรักษาอย่างสม่ำเสมอ พร้อมบันทึกผลการตรวจสอบเป็นหลักฐาน

2 ตัวอย่าง

เอกสารที่ 1

แผนการป้องกันอัคคีภัยใน Data Center / ห้อง Server (Fire Protection Plan)

โรงพยาบาล :

สถานที่ : ห้อง Server / Data Center

วันที่ประกาศใช้ :

1) วัตถุประสงค์

เพื่อป้องกันความเสียหายจากอัคคีภัยต่อระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญของหน่วยงาน

2) ระบบป้องกันอัคคีภัยที่ติดตั้ง

- ระบบตรวจจับควัน (Smoke Detector)
- ระบบสัญญาณเตือนภัย (Fire Alarm System)
- เครื่องดับเพลิงชนิด Dry Chemical / CO₂
- ระบบดับเพลิงอัตโนมัติ (เช่น FM-200 / CO₂ / Nitrogen) ตามความเหมาะสมของพื้นที่

3) แนวทางตอบสนองเมื่อเกิดเหตุ

1. ระบบแจ้งเตือนทำงาน (แจ้งเจ้าหน้าที่)
2. ตัดกระแสไฟฟ้าในพื้นที่
3. ใช้เครื่องดับเพลิงเบื้องต้น
4. อพยพและแจ้งหน่วยงานที่เกี่ยวข้อง

4) ผู้รับผิดชอบ

- ผู้ดูแลห้อง Server
- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ (หัวหน้า IT)

ลงชื่อ (ผู้บริหาร)

เอกสารที่ 2

แผนการตรวจสอบและบำรุงรักษาระบบป้องกันอัคคีภัย (Fire Protection Maintenance Plan)

รายการ	ความถี่	ผู้รับผิดชอบ
ตรวจสอบเครื่องดับเพลิง	ทุก 6 เดือน	IT
ตรวจสอบ Smoke Detector	ปีละ 1 ครั้ง	งานอาคาร
ทดสอบ Fire Alarm	ปีละ 1 ครั้ง	งานอาคาร/IT

แบบฟอร์มการบันทึกการตรวจสอบระบบป้องกันอัคคีภัย (Fire System Inspection Log)

ตัวอย่างข้อมูลกรอกจริง 3 รายการ

วันที่ตรวจ	ระบบ/อุปกรณ์	สภาพ	ผลการตรวจ	ผู้ตรวจ
10 ม.ค. 25xx	Smoke Detector	ปกติ	ตรวจจับควันได้	นาย ก.กิตติ
10 ม.ค. 25xx	Fire Alarm	ปกติ	สัญญาณเตือนดัง	นาย ก.กิตติ
10 ม.ค. 25xx	เครื่องดับเพลิง CO ₂	ปกติ	พร้อมใช้งาน	นาย ก.กิตติ

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มี Smoke Detector
- ☒ มี Alarm
- ☒ มี Fire Extinguisher / ระบบดับเพลิงอัตโนมัติ (ตามบริบท)
- ☒ มีแผนบำรุงรักษา
- ☒ มี บันทึกการตรวจสอบระบบป้องกันอัคคีภัย

อ้างอิงเกณฑ์ หมวดที่ 5 ข้อ CS.5.4

“มีมาตรการหรือระบบป้องกันความเสียหายของข้อมูล และระบบ เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server ให้เหมาะสมกับความเสี่ยง”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.5.4

หน่วยงานมีมาตรการและระบบป้องกันความเสียหายของข้อมูลและระบบอย่างเหมาะสมกับความเสี่ยง โดยมีการใช้ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID ระบบ Redundant Power Supply และระบบ Server สำรอง สำหรับระบบสารสนเทศที่สำคัญ พร้อมทั้งมีการตรวจสอบ ทดสอบ และบำรุงรักษาระบบดังกล่าวอย่างสม่ำเสมอ และมีบันทึกผลการตรวจสอบเป็นหลักฐาน

2 ตัวอย่าง

เอกสารที่ 1

มาตรการและระบบป้องกันความเสียหายของข้อมูลและระบบ (Data & System Protection Measures)

โรงพยาบาล.....

สถานที่ : Data Center / ห้อง Server

วันที่ประกาศใช้ :

1. วัตถุประสงค์

เพื่อป้องกันความเสียหายของข้อมูลและลดความเสี่ยงจากการหยุดชะงักของระบบสารสนเทศที่สำคัญของหน่วยงาน โดยกำหนดมาตรการและระบบสำรองที่เหมาะสมกับความเสี่ยง

2. ระบบและมาตรการที่ใช้

หน่วยงานมีการติดตั้งและใช้งานระบบป้องกันความเสียหายของข้อมูลและระบบ ดังนี้

1. ระบบไฟฟ้าสำรอง (UPS)

- ติดตั้ง UPS สำหรับ Server HIS และอุปกรณ์สำคัญ
- รองรับไฟฟ้าสำรองได้ประมาณ 20–30 นาที
- มีการทดสอบการทำงานภายใต้โหลดจริง

2. ระบบ RAID

- Server HIS ใช้ RAID 5
- Server เอกสารใช้ RAID 1 (Mirror)
- NAS สำรองใช้ RAID 10

เพื่อป้องกันข้อมูลสูญหายจากความเสียหายของ Disk

3. Redundant Power Supply

- Server สำคัญติดตั้ง Power Supply แบบซ้ำซ้อน
- ทดสอบการสลับแหล่งจ่ายไฟ (Main → Backup)

4. Redundant Server / Failover

- มี Server สำรองสำหรับระบบสำคัญ
- ทดสอบการทำงานกรณี Server หลักขัดข้อง

3. การตรวจสอบและบำรุงรักษา

- ตรวจสอบ UPS, RAID และระบบสำรองอย่างสม่ำเสมอ
- มีการทดสอบเชิงสถานการณ์ (Simulation / Failover Test)
- บันทึกผลการตรวจสอบและผลการทดสอบเป็นหลักฐาน

4. ผู้รับผิดชอบ

- System Administrator
- IT Support
- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

ผู้อำนวยการโรงพยาบาล

เอกสารที่ 2

บันทึกการตรวจสอบและบำรุงรักษาระบบสำรอง

(UPS, RAID, Redundant Power Supply และ Redundant Server)

วันที่ ตรวจสอบ	ระบบที่ตรวจสอบ	รายละเอียดการ ตรวจสอบ	สถานะ	ผลการทดสอบ	ผู้ตรวจสอบ
10 มี.ค. 25xx	UPS Server HIS	ตรวจสอบไฟฟ้าสำรอง และแบตเตอรี่	ปกติ	สำรองไฟได้ 22 นาที	IT Support
15 มี.ค. 25xx	RAID 5 (HIS)	ตรวจสอบสถานะ RAID ผ่านซอฟต์แวร์	ปกติ	Healthy ไม่มี Disk เสีย	System Admin
20 มี.ค. 25xx	Redundant Power Supply	ทดสอบสลับ แหล่งจ่ายไฟ	สำเร็จ	ระบบไม่ดับ แจ้ง เตือน Active	ช่างเทคนิค
25 มี.ค. 25xx	Redundant Server	ทดสอบ Failover	สำเร็จ	Server สำรอง ทำงานใน 2 นาที	หัวหน้า IT

แบบฟอร์มตรวจสอบระบบป้องกันความเสียหายของข้อมูล

ระบบ	มาตรการที่ใช้	ผลการตรวจสอบล่าสุด	หมายเหตุ
Server HIS	UPS / RAID 5 / Dual PSU	ผ่าน	ทดสอบ มี.ค. 25xx
Server เอกสาร	RAID 1	ผ่าน	Rebuild สำเร็จ
NAS สำรอง	RAID 10	ผ่าน	ใช้งานปกติ

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ✓ มี UPS + ผลทดสอบจริง
- ✓ มี RAID หลายรูปแบบตามความเหมาะสม
- ✓ มี Redundant Power / Server
- ✓ มีบันทึกการตรวจสอบหลายรอบ
- ✓ มีภาพแสดงว่าระบบ “ใช้งานได้จริง ไม่ใช่แค่มีอุปกรณ์”

อ้างอิงเกณฑ์ หมวดที่ 5 ข้อ CS.5.5

“มีระบบเฝ้าระวัง และรักษาความมั่นคงปลอดภัยทางกายภาพ Data Center ของหน่วยงาน”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.5.5

หน่วยงานมีระบบเฝ้าระวังและรักษาความมั่นคงปลอดภัยทางกายภาพของ Data Center อย่างเหมาะสม โดยมีการติดตั้งกล้องวงจรปิด ระบบตรวจจับการบุกรุก ระบบควบคุมการเข้า-ออก และมีเจ้าหน้าที่ดูแลพื้นที่ พร้อมทั้งมีการตรวจสอบและบำรุงรักษาระบบอย่างสม่ำเสมอ และจัดเก็บบันทึกเป็นหลักฐาน

2 ตัวอย่าง

เอกสารที่ 1

นโยบายและมาตรการรักษาความปลอดภัยทางกายภาพห้อง Data Center

โรงพยาบาล

สถานที่ : ห้อง Data Center / ห้อง Server

วันที่ประกาศใช้ :

1. วัตถุประสงค์

เพื่อกำหนดมาตรการในการเฝ้าระวังและรักษาความมั่นคงปลอดภัยทางกายภาพของห้อง Data Center ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม การก่อวินาศกรรม และเหตุการณ์ที่อาจกระทบต่อระบบสารสนเทศของหน่วยงาน

2. ขอบเขต

ครอบคลุมพื้นที่

- ห้อง Data Center
- ห้อง Server
- จุดเข้า-ออก และพื้นที่ควบคุมระบบสำคัญ

3. ระบบเฝ้าระวังและความปลอดภัยที่ติดตั้ง

ระบบ	รายละเอียด
กล้องวงจรปิด (CCTV)	ติดตั้งอย่างน้อย 2 จุด (ภายใน-ภายนอกห้อง) บันทึกภาพย้อนหลัง ≥ 30 วัน
Motion / Intrusion Sensor	ตรวจจับการเคลื่อนไหวผิดปกติ พร้อมสัญญาณเตือน
ระบบควบคุมการเข้า-ออก	ใช้สมุดลงชื่อ / ระบบสแกนบัตร
เจ้าหน้าที่รักษาความปลอดภัย	ดูแลพื้นที่ในช่วงนอกเวลาราชการ
ระบบแจ้งเตือน	แจ้งเตือนเหตุผิดปกติไปยังผู้รับผิดชอบ

4. การควบคุมการเข้า-ออก

- อนุญาตเฉพาะบุคลากรที่ได้รับมอบหมาย
- ผู้มาติดต่อภายนอกต้องมีผู้ควบคุมดูแลตลอดเวลา
- มีบันทึกการเข้า-ออกทุกครั้ง

5. การตรวจสอบและบำรุงรักษา

- ตรวจสอบระบบ CCTV และ Sensor อย่างน้อยเดือนละ 1 ครั้ง
- ตรวจสอบการบันทึกภาพและระบบแจ้งเตือน
- จัดทำบันทึกผลการตรวจสอบเป็นเอกสารหลักฐาน

ลงชื่อ

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ

ผู้อำนวยการโรงพยาบาล

เอกสารที่ 2

รายงานการตรวจสอบระบบเฝ้าระวังความปลอดภัย Data Center

วันที่ตรวจสอบ	ระบบที่ตรวจสอบ	รายละเอียด	สถานะ	ผู้ตรวจสอบ
5 มี.ค. 25xx	CCTV	ตรวจสอบภาพ/การบันทึกย้อนหลัง	ปกติ	IT Support
5 มี.ค. 25xx	Motion Sensor	ทดสอบการตรวจจับและแจ้งเตือน	ปกติ	IT Support
6 มี.ค. 25xx	ระบบเข้า-ออก	ตรวจสอบสมุดลงชื่อ	ปกติ	หัวหน้า IT

แบบฟอร์มตรวจสอบระบบเฝ้าระวังและความปลอดภัยทางกายภาพ

รายการตรวจสอบ	มี / ไม่มี	ผลการตรวจสอบ	หมายเหตุ
กล้องวงจรปิด (CCTV)	มี	ใช้งานปกติ	บันทึก ≥ 30 วัน
Motion / Intrusion Sensor	มี	แจ้งเตือนปกติ	ทดสอบแล้ว
ระบบควบคุมการเข้า-ออก	มี	ลงชื่อครบถ้วน	ตรวจสอบรายเดือน
เจ้าหน้าที่รักษาความปลอดภัย	มี	ปฏิบัติงานตามแผน	เฉพาะนอกเวลาราชการ

ผู้ตรวจสอบ

วันที่

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มี CCTV + Sensor อย่างน้อย 1-2 ระบบ
- ☒ ครอบคลุมพื้นที่สำคัญ
- ☒ มี Log / บันทึกตรวจสอบ
- ☒ มีนโยบายเป็นลายลักษณ์อักษร
- ☒ มีภาพแสดงว่าระบบ “ใช้งานจริง”

อ้างอิงเกณฑ์ หมวดที่ 6 ข้อ CS.6.1

“จัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) อย่างน้อยปีละ 1 ครั้ง โดยมีผู้ตรวจสอบภายใน หรือ ภายนอกที่มีความรู้ความสามารถ และจัดทำรายงานผลต่อผู้บริหารที่เกี่ยวข้อง”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.6.1

หน่วยงานมีการจัดทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และดำเนินการตรวจสอบอย่างน้อยปีละ 1 ครั้ง พร้อมรายงานผลต่อผู้บริหาร

2 เอกสารที่ 1

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ Cybersecurity Audit Plan

โรงพยาบาล :

ปีงบประมาณ : 25xx

ผู้อนุมัติ : ผู้อำนวยการหน่วยงาน / CIO

วันที่อนุมัติ : / /

1. วัตถุประสงค์

1. เพื่อตรวจสอบระดับความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ
2. เพื่อประเมินความเสี่ยง ช่องโหว่ และจุดที่ต้องปรับปรุง
3. เพื่อรายงานผลการตรวจสอบต่อผู้บริหารและใช้เป็นข้อมูลในการปรับปรุงระบบ

2. ขอบเขตการตรวจสอบ (Audit Scope)

- นโยบายและแนวปฏิบัติด้าน Cybersecurity
- การควบคุมสิทธิ์การเข้าถึง (Access Control)
- ระบบเครือข่าย / Firewall / Antivirus
- การสำรองและกู้คืนข้อมูล (Backup & Recovery)
- การจัดเก็บและตรวจสอบ Log
- ความรู้ความเข้าใจของบุคลากรด้าน PDPA และ Cybersecurity

3. รูปแบบและผู้ตรวจสอบ

☒ ผู้ตรวจสอบภายใน (ฝ่าย IT / คณะกรรมการ Audit)

☐ ผู้ตรวจสอบภายนอก (ถ้ามี)

4. ความถี่ในการตรวจสอบ

- ดำเนินการตรวจสอบ อย่างน้อยปีละ 1 ครั้ง

เอกสารที่ 2

ตารางแผนการตรวจสอบ (Audit Schedule)

ลำดับ	กิจกรรม	รายละเอียด	ระยะเวลา	ผู้รับผิดชอบ
1	แต่งตั้งทีมตรวจสอบ	กำหนดคณะกรรมการ Audit และขอบเขต	มิ.ย. 25xx	CIO
2	Opening Meeting	ชี้แจงวัตถุประสงค์และแนวทาง	มิ.ย. 25xx	Audit Team
3	ตรวจสอบเอกสาร	Policy, Procedure, Log, Training	มิ.ย. 25xx	Auditor
4	ตรวจสอบระบบ IT	Server, Network, Firewall, Backup	มิ.ย. 25xx	Auditor + IT
5	สัมภาษณ์บุคลากร	ความเข้าใจ PDPA / Cyber	มิ.ย. 25xx	Auditor
6	สรุปผลและจัดทำรายงาน	Audit Findings & Risk	มิ.ย. 25xx	หัวหน้าทีม Audit
7	นำเสนอผู้บริหาร	รายงานผลอย่างเป็นทางการ	มิ.ย. 25xx	CIO / ผอ.

เอกสารที่ 3

แบบฟอร์มบันทึกผลการตรวจสอบ Cybersecurity Audit Result Form

หัวข้อที่ตรวจสอบ	ผลการตรวจ	ระดับความเสี่ยง	ข้อเสนอแนะ
นโยบาย Cybersecurity	มีและใช้งาน	ต่ำ	ทบทวนประจำปี
การควบคุมสิทธิ์ผู้ใช้	ใช้งานจริง	กลาง	เพิ่มการทบทวนสิทธิ์ทุก 6 เดือน
ระบบ Backup	มี แต่ยังไม่ทดสอบกู้คืน	กลาง	เพิ่ม Recovery Drill
Antivirus / Patch	ใช้งานบางระบบ	กลาง	ขยายให้ครอบคลุมทั้งหมด

เอกสารที่ 4

รายงานสรุปผลการตรวจสอบ Cybersecurity Audit Report (Summary)

ผลการประเมินโดยรวม :

☒ ผ่านในระดับยอมรับได้ ☐ ต้องปรับปรุงเร่งด่วน

ประเด็นที่ต้องปรับปรุง

1. เพิ่มการทดสอบกู้คืนข้อมูล
2. ปรับปรุงกระบวนการ Patch Management
3. จัดอบรม Cybersecurity Awareness เพิ่ม

รายงานผลต่อผู้บริหารเมื่อวันที่ :

Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

-  Cybersecurity Audit Plan
-  ตาราง Audit Schedule
-  Audit Result / Audit Report
-  หลักฐานการรายงานผู้บริหาร

อ้างอิงเกณฑ์ หมวดที่ 6 ข้อ CS.6.2

“จัดให้มีแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) และแจ้งผู้เกี่ยวข้องรับทราบ”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.6.2

หน่วยงานจัดให้มีแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) และแจ้งผู้เกี่ยวข้องรับทราบ โดยดำเนินการจัดทำแผน Incident Response Plan เป็นลายลักษณ์อักษร กำหนดผู้รับผิดชอบ หน่วยงานที่เกี่ยวข้อง และช่องทางติดต่อ และแจ้งบุคลากรที่เกี่ยวข้องรับทราบแผน

2 เอกสารที่ 1

แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

หน่วยงาน :

ฉบับที่ : 1.0

วันที่ประกาศใช้ : / /

ผู้อนุมัติ : ผู้อำนวยการ / CIO

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการตรวจจับ แจ้งเตือน วิเคราะห์ และตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างเป็นระบบ ลดผลกระทบต่อข้อมูล ระบบบริการ และความเชื่อมั่นของหน่วยงาน

2. ขอบเขตของแผน (Scope)

ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ

- ระบบสารสนเทศ : HIS, LIS, ฐานข้อมูลผู้ป่วย
- ระบบเครือข่าย : Internet, Firewall, Switch
- อุปกรณ์ IT : Server, PC, Laptop, USB, External HDD
- ช่องทางการสื่อสาร : Email, Web, Social Media

3. ช่องทางแจ้งเหตุและผู้รับแจ้ง

- โทรศัพท์ (Hotline IT) : 09x-xxx-xxxx
- Email : itincident@hospital.go.th
- แบบฟอร์มแจ้งเหตุ : IR-01 (ผ่านระบบ Intranet)
- ผู้รับแจ้งหลัก : หัวหน้าฝ่าย IT / ผู้ประสานงาน IRP

4. ขั้นตอนการตอบสนองเหตุการณ์ (Incident Response Lifecycle)

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ
ตรวจจับ (Detection)	ระบบแจ้งเตือน หรือผู้ใช้งานรายงานเหตุผิดปกติ	Firewall / Antivirus / Helpdesk
วิเคราะห์ (Analysis)	ตรวจสอบ Log, IP, ลักษณะภัย และความรุนแรง	IT Security / DPO
แจ้งเหตุ (Notification)	แจ้งหัวหน้า IT ผู้บริหาร และผู้เกี่ยวข้อง	แบบฟอร์ม IR-01
ควบคุมเหตุ (Containment)	แยกระบบที่ได้รับผลกระทบ ปิดช่องโหว่	System Admin
กู้คืน (Recovery)	Restore ข้อมูลจาก Backup / Patch ระบบ	IT Support
รายงานเหตุ (Reporting)	สรุปเหตุการณ์ ผลกระทบ และแนวทางแก้ไข	เจ้าหน้าที่ IT
ทบทวนแผน (Review)	วิเคราะห์บทเรียนและปรับปรุงแผน IRP	ทีม Cybersecurity

5. รายชื่อผู้เกี่ยวข้องในแผน (Contact List)

บทบาท	ตำแหน่ง	ช่องทางติดต่อ
Incident Manager	CIO / หัวหน้า IT	โทร. 0xx-xxx-xxxx
System Admin	เจ้าหน้าที่ IT	โทร. 0xx-xxx-xxxx
DPO	เจ้าหน้าที่คุ้มครองข้อมูล	โทร. 0xx-xxx-xxxx
ผู้บริหาร	ผอ.หน่วยงาน	โทร. 0xx-xxx-xxxx

6. การแจ้งและรับทราบแผน

- แจ้งแผน IRP ผ่าน Email ภายในหน่วยงาน
- จัดเก็บแผนบน Intranet / ห้อง IT
- ชี้แจงแผนให้บุคลากรที่เกี่ยวข้องรับทราบ
- ให้ผู้รับผิดชอบลงนามรับทราบแผน

เอกสารที่ 2

แบบฟอร์มแจ้งเหตุภัยคุกคามทางไซเบอร์ (IR-01)

รายการ	รายละเอียด
ผู้แจ้งเหตุ	
วันที่ / เวลา	
ประเภทเหตุการณ์	☐ Malware ☐ Phishing ☐ Ransomware ☐ อื่น ๆ
ระบบที่เกี่ยวข้อง	☐ HIS ☐ LIS ☐ Network ☐ Email
รายละเอียดเหตุการณ์	
การดำเนินการเบื้องต้น	
ผู้รับแจ้ง	

เอกสารที่ 3

บันทึกเหตุการณ์ภัยคุกคาม (Incident Record)

วันที่	ประเภทเหตุ	ระบบที่ได้รับผลกระทบ	การดำเนินการ	ผู้รับผิดชอบ
10 มี.ค. 25xx	Malware	Server HIS	แยกระบบ + Restore	System Admin
22 เม.ย. 25xx	Phishing	Email บุคลากร	Reset Password	IT Support

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ Incident Response Plan (IRP)
- ☒ แบบฟอร์ม IR-01
- ☒ บันทึกเหตุการณ์ (Incident Record)
- ☒ หลักฐานการแจ้งรับทราบแผน

อ้างอิงเกณฑ์ หมวดที่ 6 ข้อ CS.6.3

“มีการฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ”

1 ตัวอย่าง “คำตอบลงในแบบประเมิน”

ข้อ CS.6.3

หน่วยงานมีการฝึกซ้อมและทบทวนแผนรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ 1 ครั้ง มีการบันทึกผล วิเคราะห์บทเรียน และนำไปปรับปรุงแผน พร้อมรายงานเสนอผู้บริหาร

2 เอกสารที่ 1

แผนการฝึกซ้อมแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Exercise Plan)

โรงพยาบาล

ปีงบประมาณ : 25xx

ผู้รับผิดชอบ : หัวหน้าฝ่าย IT / DPO

1. วัตถุประสงค์

1. เพื่อทดสอบความพร้อมของบุคลากรตาม Incident Response Plan
2. เพื่อประเมินขั้นตอนการแจ้งเหตุ วิเคราะห์ และตอบสนอง
3. เพื่อปรับปรุงแผน IRP ให้เหมาะสมกับสถานการณ์จริง

2. รูปแบบการฝึกซ้อม

- ☒ Tabletop Exercise
- ☐ Simulation
- ☐ Incident Drill ร่วมหน่วยงานภายนอก

3. ความถี่

- ☒ อย่างน้อยปีละ 1 ครั้ง
- ☐ เมื่อมีการเปลี่ยนแปลงระบบสำคัญ

เอกสารที่ 2

แบบฟอร์มบันทึกการฝึกซ้อม Incident Response Plan

รายการ	รายละเอียด
วันที่ฝึกซ้อม	15 พฤษภาคม 25xx
เวลา	09.00 – 12.00 น.
สถานที่	ห้องประชุม IT
สถานการณ์จำลอง	ข้อมูลवेชระเบียนรั่วไหลจาก Email Phishing
รูปแบบ	Tabletop Exercise
ผู้เข้าร่วม	IT, DPO, เวชระเบียน, ผู้บริหาร
ผู้ควบคุมการฝึก	หัวหน้าฝ่าย IT

เอกสารที่ 3

แบบฟอร์มประเมินผลการฝึกซ้อม (IRP Exercise Evaluation)

ประเด็นประเมิน	ผลการประเมิน
ความเข้าใจขั้นตอน IRP	☒ ดี ☐ ปานกลาง ☐ ต้องปรับปรุง
การแจ้งเหตุ	☒ ถูกต้อง ☐ ลำช้า
ระยะเวลาแจ้งเหตุ	35 นาที
การประสานงาน	☒ เหมาะสม ☐ ต้องปรับปรุง
ปัญหาที่พบ	บุคลากรบางส่วนไม่ทราบช่องทางแจ้งเหตุ
ข้อเสนอแนะ	เพิ่มป้าย QR แจ้งเหตุ + อบรมเสริม

เอกสารที่ 4

บันทึกการทบทวนและปรับปรุงแผน IRP

(Plan Review & Improvement Log)

วันที่	ประเด็นที่พบ	การปรับปรุง	ผู้รับผิดชอบ
20 พ.ค. 25xx	แจ้งเหตุล่าช้า	เพิ่ม QR แจ้งเหตุหน้าแผนก	IT
20 พ.ค. 25xx	บุคลากรใหม่ไม่เข้าใจ IRP	เพิ่ม IRP ในปฐมนิเทศ	HR + IT

เอกสารที่ 5

รายงานสรุปผลการฝึกซ้อมเสนอผู้บริหาร

สรุปผลโดยรวม :

- หน่วยงานสามารถปฏิบัติตาม Incident Response Plan ได้
- พบจุดที่ต้องปรับปรุงด้านการสื่อสาร
- มีการกำหนดแนวทางแก้ไขและปรับปรุงแผนแล้ว

ผู้รับรองรายงาน :

หัวหน้าฝ่าย IT / ผู้อำนวยการโรงพยาบาล

ลงชื่อ..... วันที่.....

3 Checklist ตรวจสอบก่อนส่ง (สำคัญมาก)

- ☒ มีการฝึกซ้อม Incident Response Plan อย่างน้อยปีละ 1 ครั้ง
- ☒ มีการบันทึกผลการฝึกซ้อม
- ☒ มีการทบทวนและปรับปรุงแผน
- ☒ มีรายงานเสนอผู้บริหาร

เอกสารประกอบ

- แผนการฝึกซ้อม IRP
- บันทึกการฝึกซ้อม
- รายงานผลการฝึกซ้อม
- บันทึกการปรับปรุงแผน



กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support



มาตรฐานระบบบริการสุขภาพ ด้าน 9 การรักษาความมั่นคง ปลอดภัยไซเบอร์ (Cyber Security)

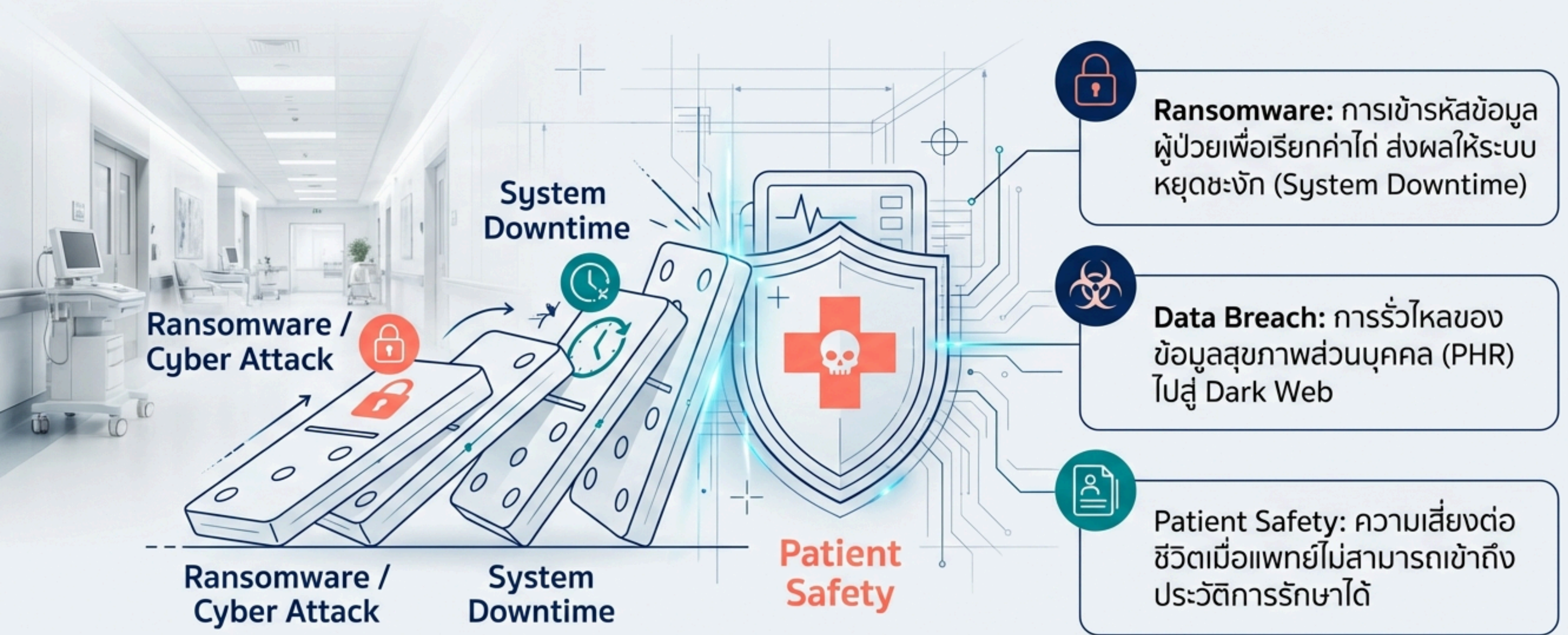
กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมสนับสนุนบริการสุขภาพ

การรักษาความมั่นคงปลอดภัยไซเบอร์ Cyber Security

มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อระบบสารสนเทศ เพื่อให้ระบบบริการที่สำคัญของหน่วยงานภาคส่วนต่างๆ ดำรงไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้



สถานพยาบาลคือโครงสร้างพื้นฐานสำคัญ (CII) ที่ตกเป็นเป้าหมายการโจมตี



Objective: เพื่อลดความเสี่ยงจากระบบหยุดชะงัก และสร้างความเชื่อมั่นให้กับประชาชน

วัตถุประสงค์

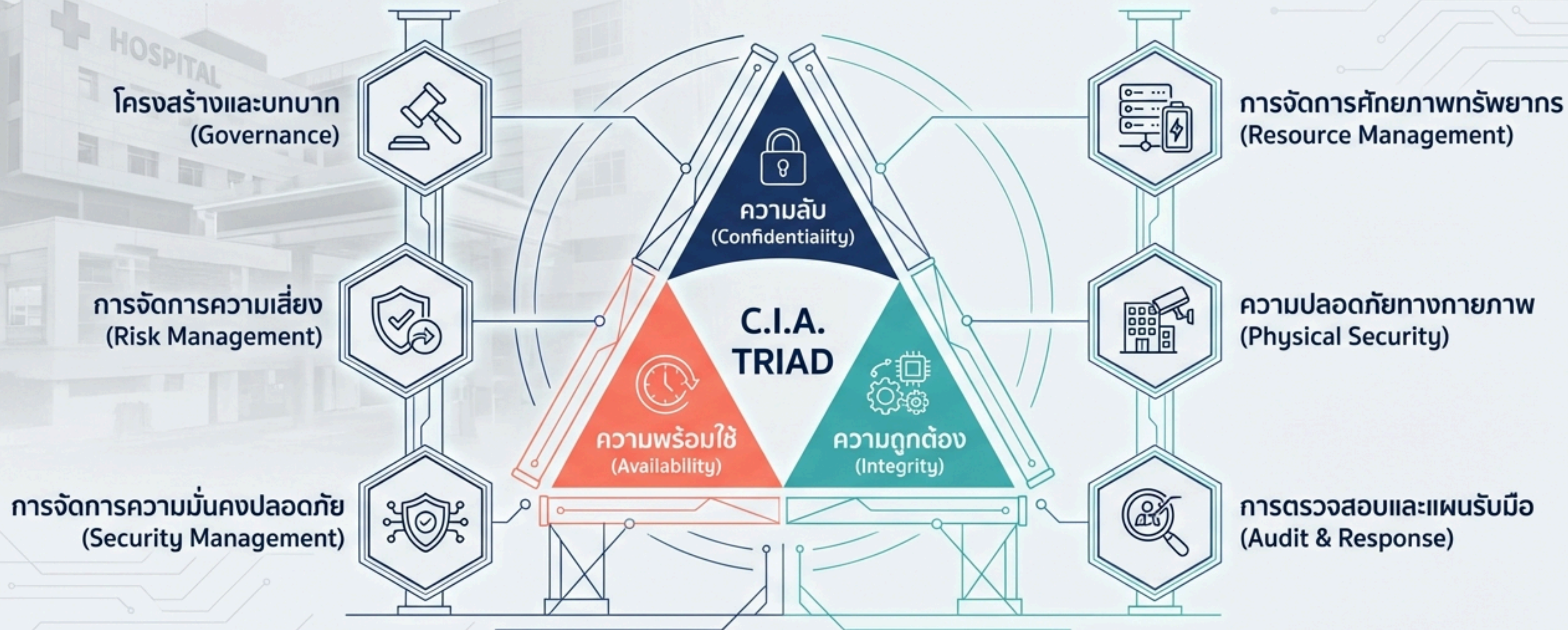
เพื่อยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ให้มีประสิทธิภาพยิ่งขึ้น พร้อมทั้งมีมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบเครือข่ายของสถานพยาบาล หน่วยงานสาธารณสุข และฐานข้อมูลสุขภาพ

เพื่อลดความเสี่ยงจากระบบหยุดชะงัก (System Downtime) ที่อาจส่งผลต่อการรักษาผู้ป่วย

เพื่อสร้างความน่าเชื่อถือ ความมั่นใจให้แก่ประชาชน ในการใช้บริการสถานพยาบาล



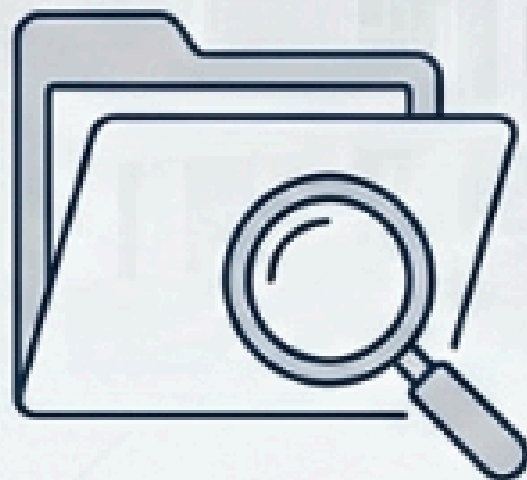
กรอบมาตรฐาน 6 หมวด เพื่อปกป้องความลับ ความถูกต้อง และความพร้อมใช้



วิธีการให้คะแนน คะแนนเต็ม 100 คะแนน

0

ไม่พบหลักฐานการดำเนินการ
(No Evidence)



0.5

มีหลักฐานบางส่วน แต่ไม่ครบถ้วน
หรือยังไม่มี การลงนามอนุมัติ
(Partial/Unsigned)



1

มีหลักฐานครบถ้วนสมบูรณ์
และได้รับการอนุมัติจากผู้บริหาร
(Evidence + Approved)



เกณฑ์แบ่งระดับผลการ ประเมิน 3 ระดับ

0-59 คะแนน

พื้นฐาน

มีด้านใดด้านหนึ่งจาก 9 ด้าน
คะแนนต่ำกว่า 60

60-84 คะแนน

พัฒนา

85-100 คะแนน

คุณภาพ

ทั้ง 9 ด้าน คะแนน
85 ขึ้นไป

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

- CS.1.1 มีการจัดโครงสร้างการดูแลระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ พร้อมกำหนดอำนาจหน้าที่ และความรับผิดชอบ
- CS.1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของสถานพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
- CS.1.3 มีนโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล
- CS.1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม
- CS.1.5 มีการกำหนดมาตรการ/นโยบาย/แนวปฏิบัติด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกฎหมายและกฎระเบียบที่เกี่ยวข้อง เช่น พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2565 กฎหมายและกฎระเบียบที่เกี่ยวข้องอื่น

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.1.1 มีการจัดโครงสร้างการดูแลระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหาร และฝ่ายเทคโนโลยีสารสนเทศ พร้อมกำหนดอำนาจหน้าที่ และความรับผิดชอบ

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มีคำสั่งแต่งตั้งผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ ในการดูแลระบบสารสนเทศของโรงพยาบาล และไม่มีการกำหนดอำนาจหน้าที่ และความรับผิดชอบ
0.5	มีคำสั่งแต่งตั้งผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ ในการดูแลระบบสารสนเทศของโรงพยาบาล แต่ไม่มีการกำหนดอำนาจหน้าที่ และความรับผิดชอบ เป็นลายลักษณ์อักษร
1	มีคำสั่งแต่งตั้งผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ ในการดูแลระบบสารสนเทศของโรงพยาบาล และกำหนดอำนาจหน้าที่ และความรับผิดชอบ และ แสดงเอกสารคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร

เอกสารประกอบ/เอกสารตัวอย่าง

1. เอกสารคำสั่งแต่งตั้งผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ ในการดูแลระบบสารสนเทศของโรงพยาบาล และกำหนดอำนาจหน้าที่ และความรับผิดชอบเป็นลายลักษณ์อักษร
เอกสารคำสั่งแต่งตั้งผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่า ทั้งนี้ หน่วยงานอาจมีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศอยู่ที่หน่วยงานตนเองหรือที่หน่วยงานระดับสูงขึ้นไปก็ได้ เช่น ในกรณีที่เป็นโรงพยาบาลทั่วไป (รพท.) โรงพยาบาลขนาดกลาง (โรงพยาบาลชุมชน) และขนาดเล็ก (โรงพยาบาลส่งเสริมสุขภาพตำบล) อาจมีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงานอยู่ที่สำนักงานเขตสุขภาพ หรือสำนักงานสาธารณสุขจังหวัด (สสจ.) หรือหน่วยงานระดับกรมฯ ที่เป็นต้นสังกัด เป็นต้น

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของสถานพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและ
การใช้งานเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศ ที่เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
0.5	มีบางส่วน ในการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ บางหัวข้อ
1	มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ครบทุกหัวข้อ อันประกอบด้วย (ก) การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (ข) การบริหารความเสี่ยงและ (ค) นโยบายและแนวปฏิบัติ

เอกสารประกอบ/เอกสารตัวอย่าง

1.แผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศ เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ครบทุกหัวข้อ อันประกอบด้วย (ก) การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (ข) การบริหารความเสี่ยงและ (ค) นโยบายและแนวปฏิบัติ ลงนามโดยผู้บริหารของหน่วยงาน

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.1.3 มีนโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี นโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล
0.5	มีนโยบาย หรือ แผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล
1	มีนโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล

เอกสารประกอบ/เอกสารตัวอย่าง

1.นโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล ประกอบด้วย เช่น เรื่องการจัดการสิทธิ์การเข้าถึง (Access Control) , เรื่องการจัดการสินทรัพย์และข้อมูล, มาตรการจัดเก็บข้อมูลผู้ป่วยและ PII ตาม PDPA , การบริหารความเสี่ยง (Risk Management) , การสำรองข้อมูลและการกู้คืน (Backup & Recovery) เป็นต้น

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.1.3 มินโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล

ตัวอย่างเนื้อหานโยบายหลัก (Core Policies)

หมวดย่อย	รายละเอียด
Access Control	ควบคุมการเข้าถึงระบบและข้อมูล (รหัสผ่าน, 2FA, Role-Based)
Backup & Recovery	กำหนดรอบสำรองข้อมูล, แผนกู้คืน, ทดสอบแผน
Malware & Patch	ป้องกันไวรัส, อัปเดตซอฟต์แวร์, Patch OS
Incident Response	มีแผน IRP, การแจ้งเหตุ, ช่องทางติดต่อฉุกเฉิน
Awareness	จัดฝึกอบรม, ประเมินผลความรู้พนักงาน
Privacy & PDPA	ปกป้องข้อมูลส่วนบุคคล, แจ้งเหตุรั่วไหล
Asset Inventory	บริหารจัดการทะเบียนทรัพย์สิน

ตัวอย่างแผนการดำเนินงาน (Implementation Plan)

ลำดับ	กิจกรรมหลัก	ระยะเวลา	ผู้รับผิดชอบ
1	จัดตั้งคณะกรรมการรักษาความมั่นคงไซเบอร์		ผอ./ฝ่าย IT
2	สำรวจระบบ + จัดทำ Asset Inventory		IT Officer
3	อบรม Awareness ทุกแผนก		HR/IT
4	ทบทวนนโยบาย + ทดสอบแผนรับมือ		CISO
5	ตรวจสอบความปลอดภัย + Audit		External Auditor

เอกสารประกอบ/เอกสารตัวอย่าง

1.นโยบายและแผนงานว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถานพยาบาล ประกอบด้วย เช่น เรื่องการจัดการสิทธิ์การเข้าถึง (Access Control) , เรื่องการจัดการสินทรัพย์และข้อมูล, มาตรการจัดเก็บข้อมูลผู้ป่วยและ PII ตาม PDPA , การบริหารความเสี่ยง (Risk Management) , การสำรองข้อมูลและการกู้คืน (Backup & Recovery) เป็นต้น

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การแสดงโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม
0.5	มี การแสดงโครงสร้างหรือการจัดอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม แต่ไม่มีการกำหนดบทบาท หน้าที่ อย่างชัดเจน
1	มี การแสดง โครงสร้าง และ อัตรากำลัง ของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม และมีการกำหนดบทบาท หน้าที่ อย่างชัดเจน

เอกสารประกอบ/เอกสารตัวอย่าง

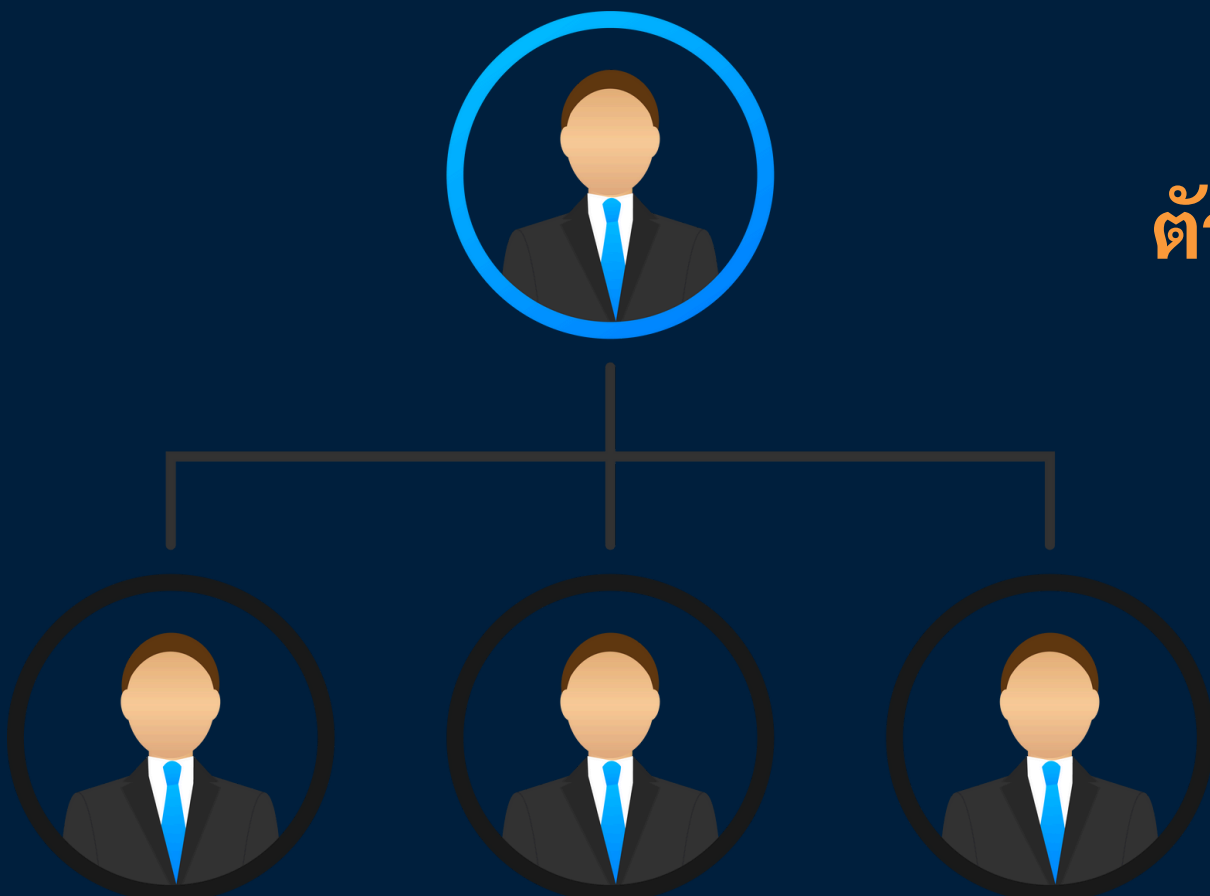
1.ผังโครงสร้างองค์กร (Organizational Chart) ที่มีการระบุตำแหน่งผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ เช่น มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO)

2.เอกสารที่แสดงถึงบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของสถานพยาบาลที่เหมาะสม

ตัวอย่างโครงสร้างพื้นฐานของฝ่ายเทคโนโลยีสารสนเทศในสถานพยาบาล



ตัวอย่างการระบุอัตรากำลัง + บทบาทหน้าที่ (Roles & Responsibilities)

ตำแหน่ง	จำนวน	บทบาทหน้าที่
CIO / หัวหน้า IT	1	วางแผน ICT, กำกับนโยบายไซเบอร์,
System Admin	1	ดูแล Server, Backup, Patch
Network Engineer	1	ดูแลเครือข่าย, Firewall, VPN, WiFi
Helpdesk / Support	1	แก้ไขปัญหาเครื่องลูกข่าย, สนับสนุนผู้ใช้งาน
DPO	1	ดูแลด้าน PDPA, ตรวจสอบการใช้ข้อมูล
เจ้าหน้าที่ประจำเวร (เวชระเปียน/อื่น ๆ)	-	อาจมีผู้ปฏิบัติงานทำหน้าที่ IT พิเศษใน

เอกสารประกอบ/เอกสารตัวอย่าง

- 1.ผังโครงสร้างองค์กร (Organizational Chart) ที่มีการระบุตำแหน่งผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ เช่น มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือมีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO)
- 2.เอกสารที่แสดงถึงบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

หมวดที่ 1 โครงสร้างและบทบาท การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.1.5 มีการกำหนดมาตรการ/นโยบาย/แนวปฏิบัติด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกฎหมาย และกฎระเบียบที่เกี่ยวข้อง เช่น พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กฎหมายและกฎระเบียบที่เกี่ยวข้องอื่น

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การกำหนดมาตรการหรือนโยบายหรือแนวปฏิบัติด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกฎหมาย และกฎระเบียบที่เกี่ยวข้อง เช่น พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2565 กฎหมายและกฎระเบียบที่เกี่ยวข้องอื่น
0.5	มี การกำหนดมาตรการหรือนโยบายหรือแนวปฏิบัติด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกฎหมาย และกฎระเบียบที่เกี่ยวข้อง เช่น พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2565 กฎหมายและกฎระเบียบที่เกี่ยวข้องอื่น แต่ยังไม่มีประกาศการบังคับใช้อย่างเป็นทางการ
1	มี การกำหนดมาตรการหรือนโยบายหรือแนวปฏิบัติด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกฎหมาย และกฎระเบียบที่เกี่ยวข้อง เช่น พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กฎหมายและกฎระเบียบที่เกี่ยวข้องอื่น และประกาศใช้อย่างเป็นทางการ

เอกสารประกอบ/เอกสารตัวอย่าง

1.นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

2.นโยบายหรือแนวปฏิบัติคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เนื้อหา เช่น: หลักการเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล , การขอความยินยอมจากเจ้าของข้อมูลสิทธิของเจ้าของข้อมูล (เช่น สิทธิขอเข้าถึง แก้ไข หรือเพิกถอนข้อมูล) ,การรักษาความมั่นคงปลอดภัยของข้อมูล

แนวทางการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

3.แนวปฏิบัติในการบริหารจัดการข้อมูล (Data Governance Guidelines) เนื้อหา เช่น :การจำแนกประเภทข้อมูล (Sensitive, Confidential, Public) การจัดเก็บข้อมูลและการทำลายข้อมูลอย่างปลอดภัย การสำรองข้อมูล และกู้คืนข้อมูล

4.นโยบายหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายและระบบสารสนเทศ (Network & System Security Policy) เนื้อหา เช่น : มาตรการเช่น ด้าน Firewall, Intrusion Detection & Prevention System (IDPS) แนวปฏิบัติในการเข้ารหัสข้อมูล (Encryption) การควบคุมและตรวจสอบระบบเครือข่าย

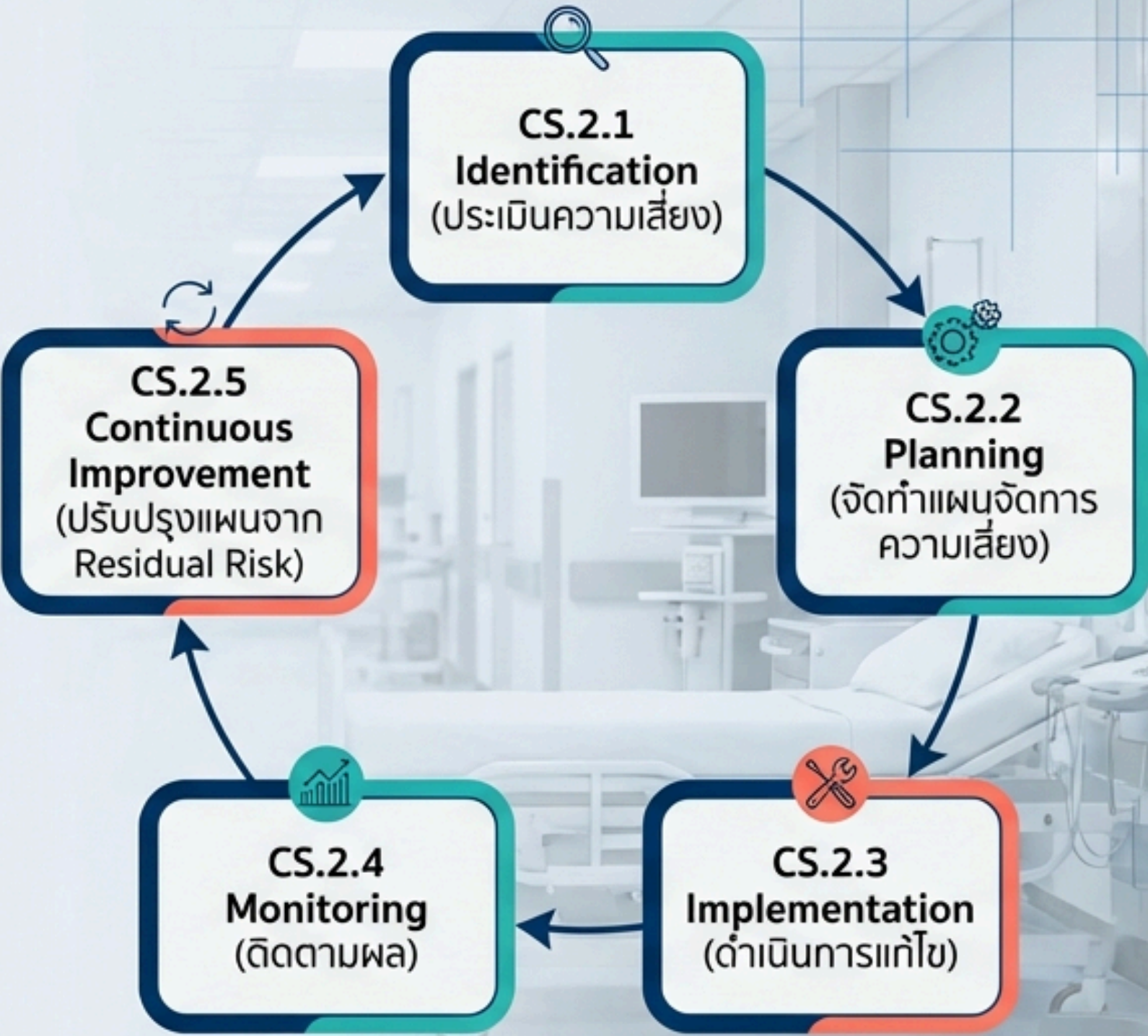
หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

- CS.2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน
- CS.2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการหรือกระบวนการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน
- CS.2.3 การดำเนินการตามแผนจัดการความเสี่ยง
- CS.2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงานเสนอต่อผู้บริหาร
- CS.2.5 มีการนำผลการประเมินหรือความเสี่ยงที่ยังคงเหลืออยู่ มาปรับปรุงแผนการจัดการความเสี่ยงอย่างต่อเนื่อง

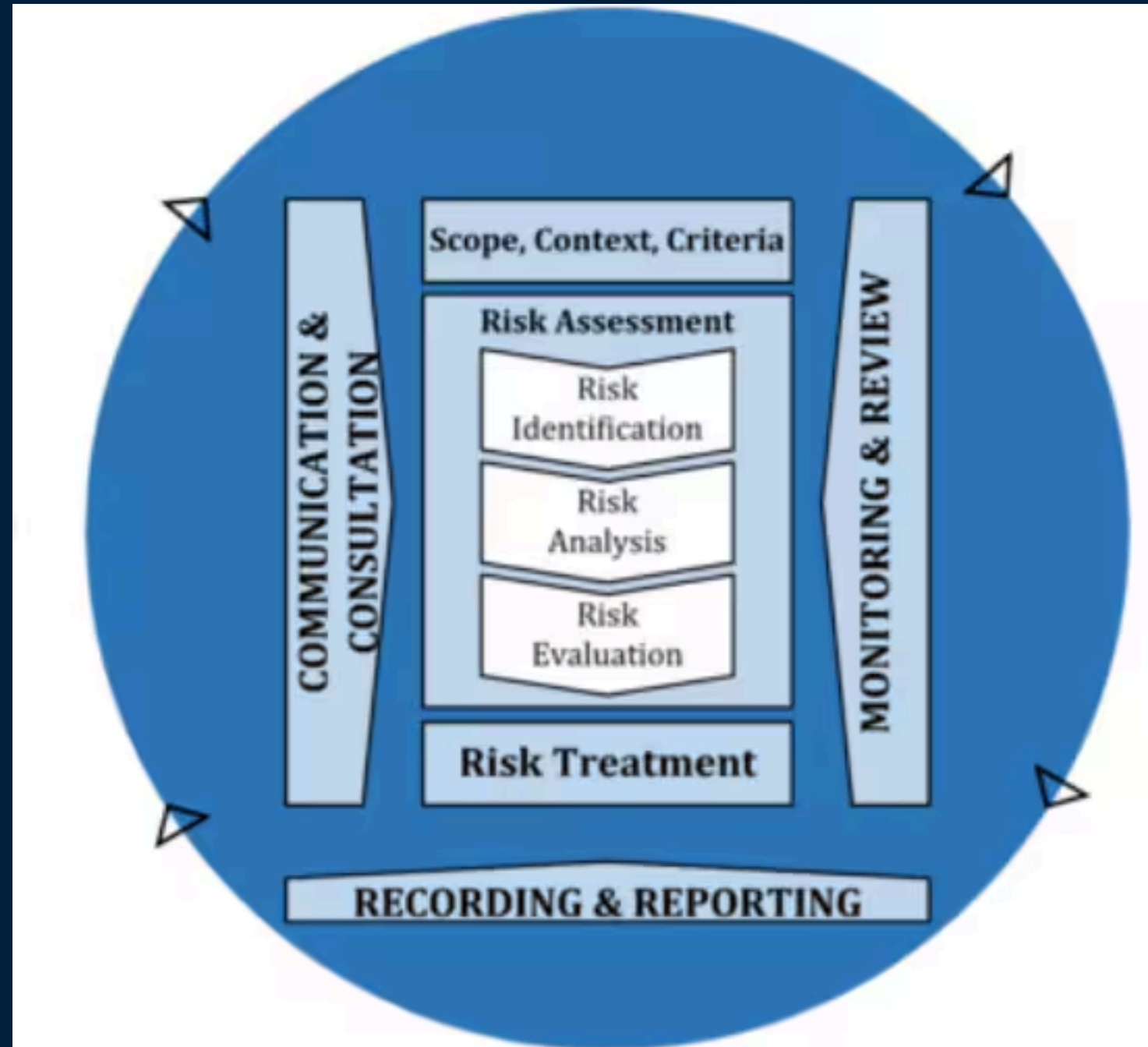
หมวดที่ 2: การจัดการความเสี่ยง (Risk Management)

CS.2.1: Risk Assessment

		Severity				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood	Very Unlikely	Low	Low Med	Medium	Med Hi	High
	Unlikely	Low	Low Med	Medium	Med Hi	High
	Possible	Low	Low Med	Medium	Med Hi	High
	Likely	Low	Low Med	Medium	Med Hi	High
	Very Likely	Low	Low Med	Medium	High	High

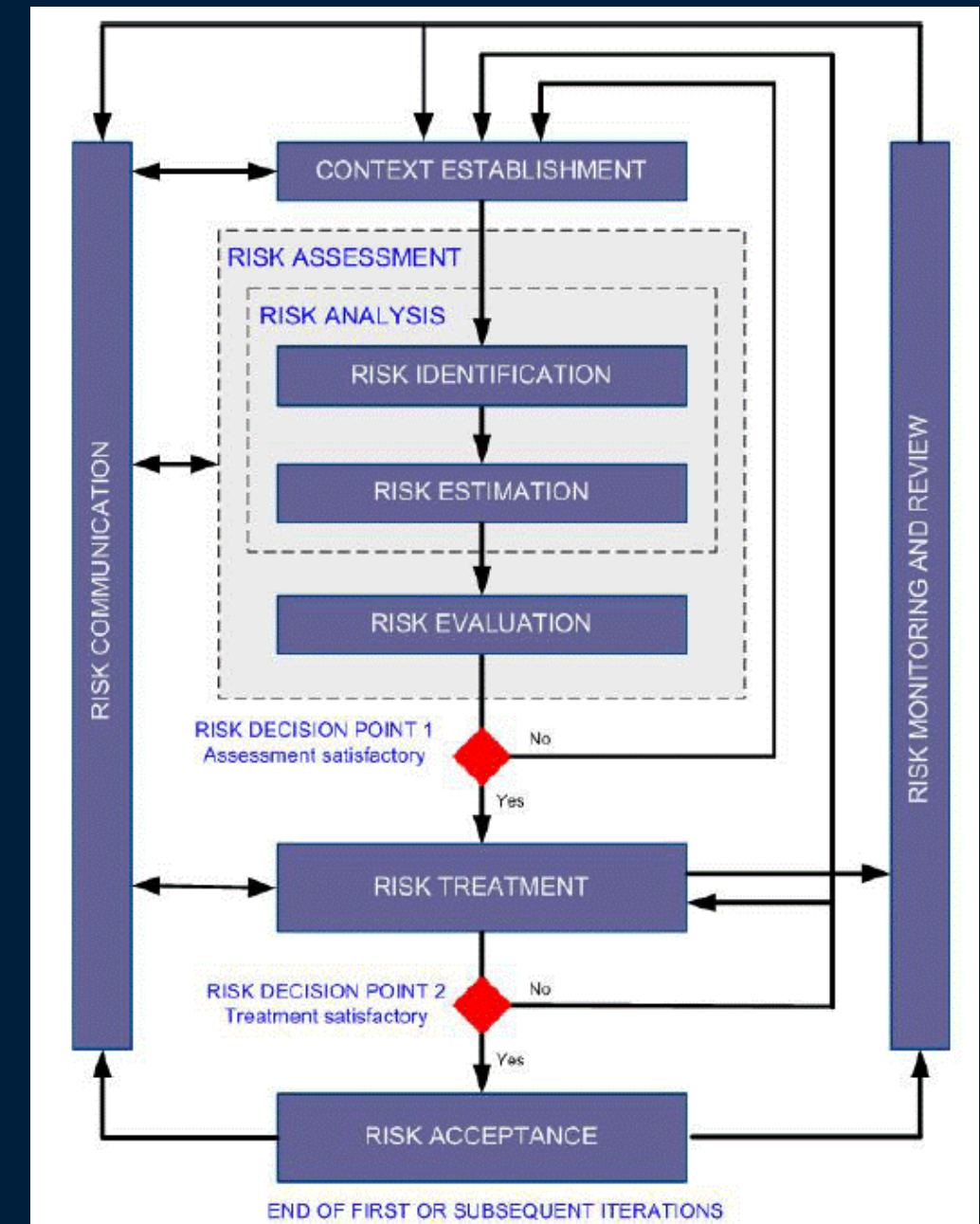


หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ



Source: ISO 31000:2018 –Risk Management Guidelines

การกำหนดบริบท
การระบุความเสี่ยง
การวิเคราะห์ความเสี่ยง
การประเมินความเสี่ยง
การจัดการความเสี่ยง
สื่อสารกับทุกฝ่ายที่เกี่ยวข้อง
ติดตามความเสี่ยงที่ยังหลงเหลือ



Source: ISO/IEC 27005:2018 –Information Security Risk Management

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี กระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน
0.5	มี การประเมินความเสี่ยง แต่ไม่ครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน
1	มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. กรอบแนวทางการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
 - 2. รายงานการประเมินและวิเคราะห์ความเสี่ยง (Risk Assessment Report) ประกอบด้วย ตารางวิเคราะห์ความเสี่ยง (Risk Register) เอกสารการประชุมคณะทำงานด้านความเสี่ยง

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน

ตัวอย่างโครงสร้าง “กระบวนการประเมินความเสี่ยง” (IT Risk Assessment Process)

ขั้นตอน	รายละเอียด	เอกสารประกอบ
1. รวบรวมทรัพย์สินสารสนเทศ (IT Asset Inventory)	ครอบคลุม Hardware, Software, Network, Data, People	- ทะเบียนทรัพย์สินสารสนเทศ
2. วิเคราะห์ภัยคุกคามและช่องโหว่ (Threats & Vulnerabilities)	เช่น Malware, การเข้าถึงไม่ได้รับอนุญาต, ความล้มเหลวของระบบ	- ตารางวิเคราะห์ภัย
3. ประเมินโอกาส & ผลกระทบ (Likelihood & Impact)	ใช้ตาราง Matrix (เช่น 1-5) → คำนวณระดับความเสี่ยง	- Risk Matrix
4. จัดลำดับความเสี่ยง (Risk Ranking)	แยก High / Medium / Low → เตรียมแผนจัดการ	- Risk Register
5. มีการประชุมร่วมทุกฝ่าย	ผู้บริหาร, IT, เจ้าหน้าที่หน่วยงาน	- บันทึกประชุม, ลายเซ็นเข้าร่วม
6. รายงานผลการประเมิน	ส่งให้ผู้บริหารรับทราบและอนุมัติ	- Risk Assessment Report

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย โดยครอบคลุมทรัพย์สินสารสนเทศ (Information Asset Inventory) ที่อยู่ภายใต้ขอบเขตการให้บริการสาธารณสุขของหน่วยงาน

ตัวอย่างตาราง Risk Assessment Matrix

Risk assessment matrix

Likelihood	Severity				
	Negligible	Minor	Moderate	Significant	Severe
	Very Likely	Low Med	Medium	Med Hi	High
	Likely	Low	Low Med	Medium	Med Hi
	Possible	Low	Low Med	Medium	Med Hi
	Unlikely	Low	Low Med	Medium	Med Hi
	Very Unlikely	Low	Low	Low Med	Medium

Risk Matrix Example

Likelihood X Severity = Risk Level

ทรัพย์สิน	ความเสี่ยง	โอกาส (1-5)	ผลกระทบ (1-5)	ความเสี่ยงรวม	ระดับความเสี่ยง
HIS Server	ไฟฟ้าดับไม่มีสำรอง	4	5	20	สูง (High)
Internet Router	ถูกแฮกผ่านช่องโหว่	3	4	12	ปานกลาง
เวชระเบียน	บุคคลเข้าโดยไม่อนุญาต	2	5	10	ปานกลาง
Antivirus SW	ลิขสิทธิ์หมดอายุ	3	2	6	ต่ำ

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการหรือกระบวนการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี แผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร
0.5	มี แผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร การกำหนดกลยุทธ์โครงการ หรือ ระยะเวลาดำเนินการ ผู้รับผิดชอบ แต่ไม่ได้รับการอนุมัติจากผู้บริหาร
1	มี แผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลา ดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน และได้รับการอนุมัติจากผู้บริหาร

เอกสารประกอบ/เอกสารตัวอย่าง
1.แผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ มาตรการลดความเสี่ยงและแนวทางควบคุม ระยะเวลาดำเนินการ ผู้รับผิดชอบ และได้รับการอนุมัติจากผู้บริหาร

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการหรือกระบวนการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน

ส่วนประกอบของเอกสาร
บทนำ – อธิบายวัตถุประสงค์ของแผน (เช่น ลดผลกระทบต่อ HIS, ป้องกัน Downtime)
สาระสำคัญของความเสี่ยงที่พบ – นำมาจาก Risk Assessment
แนวทางจัดการความเสี่ยง (Risk Treatment Strategy)

ตัวอย่างตารางแผนจัดการความเสี่ยง

ลำดับ	ความเสี่ยงที่ประเมิน	กลยุทธ์ / วิธีลดความเสี่ยง	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	สถานะ
1	Server HIS ไม่มี UPS	จัดซื้อ + ติดตั้ง UPS 2,000 VA	1 พ.ค. พ.ศ.2568	ฝ่าย IT	เสร็จแล้ว
2	ไม่มี Firewall ภายนอก	เสนอขออนุมัติซื้อ FortiGate 40F	1 พ.ค. พ.ศ.2568	หัวหน้า IT	ดำเนินการ
3	เจ้าหน้าที่ไม่มีความรู้ด้าน PDPA	อบรมความรู้พื้นฐาน + แบบประเมินหลังเรียน	1 พ.ค. พ.ศ.2568	HR + DPO	วางแผนแล้ว
4	ข้อมูลไม่ได้ Backup อัตโนมัติ	ติดตั้งระบบ Auto Backup + ทดสอบกู้คืน	1 พ.ค. พ.ศ.2568	System Admin	ยังไม่เริ่ม

ใช้หลักการ Risk Treatment Options เช่น:
ลดความเสี่ยง (Mitigation)
ยอมรับความเสี่ยง (Acceptance)
โอนความเสี่ยง (Transfer เช่น ซื้อประกัน)
หลีกเลี่ยง (Avoidance เช่น ยกเลิกระบบที่ไม่ปลอดภัย)

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.3 การดำเนินการตามแผนจัดการความเสี่ยง

หมายถึงการแสดงว่า แผนจัดการความเสี่ยงที่จัดทำไว้ใน CS.2.2 ได้ถูกนำไปปฏิบัติจริง ครบถ้วน พร้อมหลักฐานที่สามารถตรวจสอบได้

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การดำเนินการตามแผนจัดการความเสี่ยงตาม ข้อ 2.2
0.5	มี การดำเนินการตามแผนจัดการความเสี่ยง ตามข้อ 2.2 แต่ไม่ครบถ้วน
1	มี การดำเนินการตามแผนจัดการความเสี่ยง ตามข้อ 2.2 ครบถ้วน

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1.รายงานการดำเนินการตามแผนบริหารความเสี่ยง (Risk Mitigation Implementation Report)
 - รายงานความคืบหน้าการดำเนินมาตรการลดความเสี่ยง ผลการดำเนินการจริงที่เปรียบเทียบกับแผนที่วางไว้
 - หลักฐานประกอบ:
 - รายงานผลการดำเนินมาตรการควบคุมความเสี่ยง
 - เอกสารหรือหลักฐานที่แสดงถึงการดำเนินการจริง (เช่น Log การตั้งค่าความปลอดภัย, Screenshot ระบบ)

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.3 การดำเนินการตามแผนจัดการความเสี่ยง

“รายงานการดำเนินการตามแผนจัดการความเสี่ยง”
(ชื่อเต็ม: Risk Mitigation Implementation Report)

- 1. บทนำ
สรุปแผนที่ถูกอนุมัติจาก CS.2.2
ระยะเวลาดำเนินการ
ผู้รับผิดชอบหลัก
- 2. ตารางแสดงผลการดำเนินงาน
- 3. ภาพหลักฐานแนบ (แนบไฟล์)
- 4. ข้อเสนอแนะ / ปัญหาที่พบ

ตัวอย่างตารางแสดงผลการดำเนินงาน

ลำดับ	ความเสี่ยงที่ระบุ	แนวทางจัดการ	ผลการดำเนินงาน	หลักฐานประกอบ	สถานะ
1	ขาดระบบสำรองไฟ Server	ติดตั้ง UPS 2,000 VA	ติดตั้งแล้ว 100% วันที่ 10 พ.ค. 68	รูปถ่าย + Memo ส่งมอบ	✅ เสร็จสิ้น
2	ไม่มี Firewall	จัดซื้อ + ติดตั้ง FortiGate 40F	สัญญาซื้อขายลงนามแล้ว, รอส่งของ	ใบสั่งซื้อ + TOR	🔄 ดำเนินการ
3	เจ้าหน้าที่ไม่เข้าใจ PDPA	อบรม + ทำแบบทดสอบ	อบรมแล้ว 30 คน, ผ่านเกณฑ์ 95%	รายชื่อ + รูปอบรม + แบบทดสอบ	✅ เสร็จสิ้น
4	ไม่มี Auto Backup	วางระบบ Backup อัตโนมัติ	กำลังตั้งค่าทดสอบกู้คืน	Log Screen + Manual	🔧 กำลังดำเนินการ

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน
จัดทำเป็นรายงานเสนอต่อผู้บริหาร

ถือเป็นขั้นตอน “Check” ในวงจร PDCA ที่แสดงว่าองค์กร ไม่เพียงแต่วางแผนและดำเนินการ แต่ยังตรวจสอบผลลัพธ์และรายงานต่อผู้บริหารอย่างเป็นระบบ

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน
0.5	มี การติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และ วิเคราะห์ผลการประเมิน แต่ ไม่มี การจัดทำเป็นรายงานที่ลงนามโดยผู้บริหาร
1	มี การติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และ วิเคราะห์ผลการประเมิน มี การจัดทำเป็นรายงานลงนามโดยผู้บริหาร

เอกสารประกอบ/เอกสารตัวอย่าง
1.รายงานผลการติดตามการดำเนินงานตามมาตรการควบคุมความเสี่ยง

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงานเสนอต่อผู้บริหาร

ตัวอย่าง “รายงานการติดตามและประเมินผลแผนจัดการความเสี่ยง”

- 1. สรุปภาพรวม
สรุปว่าดำเนินการตามแผนความเสี่ยงที่จัดทำไว้แล้วกี่เปอร์เซ็นต์ มีกิจกรรมที่เสร็จสิ้น, อยู่ระหว่างดำเนินการ, หยุดชะงัก พบความเสี่ยงใหม่เพิ่มหรือไม่
- 2. ตารางประเมินผล (พร้อมวิเคราะห์)
- 3. กราฟประกอบ (ถ้ามี)
- 4. สรุปข้อเสนอแนะต่อผู้บริหาร
 - ต้องมี “รายงานเป็นลายลักษณ์อักษร” ที่สรุปผล + วิเคราะห์
 - ลงนามหรือเสนอผู้บริหารรับทราบ (อย่างน้อย 1 รอบต่อปี)
 - เชื่อมโยงกับผลจาก CS.2.3 อย่างเป็นระบบ

ลำดับ	ความเสี่ยง	แนวทางที่วางไว้	ผลลัพธ์จริง	ประเมินผล (ดี/ปานกลาง/ควรปรับ)	หมายเหตุ
1	ระบบไม่มี Firewall	ติดตั้ง FortiGate 40F	ติดตั้งแล้ว, ป้องกันได้ 3 เหตุการณ์	✅ ดี	ทดสอบแล้ว
2	ไม่มีการอบรม PDPA	อบรมบุคลากร 30 คน	อบรมแล้ว แต่ 20% ยังไม่ผ่านแบบทดสอบ	⚠️ ควรปรับ	รอบถัดไปเน้นภาคปฏิบัติ
3	ไม่มี Auto Backup	วางระบบ Backup + ทดสอบ DR	สำรองแล้ว แต่ DR ใช้เวลานานเกิน 3 ชม.	⚠️ ปานกลาง	ทบทวนขั้นตอนกู้คืน

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.5 มีการนำผลการประเมินหรือความเสี่ยงที่ยังคงเหลืออยู่ มาปรับปรุงแผนการจัดการความเสี่ยงอย่างต่อเนื่อง

ถือเป็นขั้นตอน “Act” ในวงจร PDCA ซึ่งเน้น การปรับปรุงแผน จากบทเรียนที่ได้ เพื่อให้แผนมีความทันสมัยและสอดคล้องกับสถานการณ์จริง

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับปรุงแผนการจัดการความเสี่ยง
0.5	มี ผลการประเมินการดำเนินการจัดการความเสี่ยง แต่ ไม่ได้ปรับปรุง แผนการจัดการความเสี่ยง เสนอผู้บริหารอนุมัติ
1	มี ผลการประเมินการดำเนินการจัดการความเสี่ยง และปรับปรุงแผนการจัดการความเสี่ยงเสนอผู้บริหารลงนาม

เอกสารประกอบ/เอกสารตัวอย่าง
1.รายงานการทบทวนและปรับปรุงแผนความเสี่ยง (Risk Review & Improvement Report)

หมวดที่ 2 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

CS.2.5 มีการนำผลการประเมินหรือความเสี่ยงที่ยังคงเหลืออยู่ มาปรับปรุงแผนการจัดการความเสี่ยงอย่างต่อเนื่อง

- 1. วิเคราะห์ “ความเสี่ยงที่ยังคงอยู่” (Residual Risk)
หลังจากมีการดำเนินการตามแผน (CS.2.3) และประเมินผล (CS.2.4)
ระบุว่า “ยังมีอะไรที่ไม่ครอบคลุม, ไม่สำเร็จ, หรือเกิดความเสี่ยงใหม่”
- 2. จัดทำ “แผนปรับปรุงใหม่” (Improved Risk Plan)
- 3. จัดทำ “รายงานทบทวนและปรับปรุง” (Risk Review & Improvement Report)

เนื้อหาเอกสารควรมี:

- สรุปผลความเสี่ยงที่ยังคงอยู่
- เหตุผลที่ยังไม่สามารถจัดการได้
- แนวทางปรับแผนใหม่
- การอนุมัติโดยผู้บริหาร (พร้อมลายเซ็น)
- แนบตารางเปรียบเทียบ แผนเดิม vs แผนปรับปรุง

ลำดับ	ความเสี่ยงเดิม	ผลลัพธ์จริง	ความเสี่ยงที่ยังคงอยู่	สาเหตุ	แนวทางเพิ่มเติม	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
1	Server ไม่มี UPS	ติดตั้งแล้ว	ไม่มี UPS สำรองห้อง Server 2	งบไม่พอ	ขออนุมัติงบ Q4 เพิ่มเติม	1 พ.ค. 2568	IT Manager
2	ข้อมูลไม่ Backup	Backup อัตโนมัติแล้ว	DR ยังใช้เวลาเกิน 3 ชม.	วิธีทดสอบไม่เหมาะสม	ทบทวนแผน DR → ใช้ Cloud DR	1 ต.ค. 2568	System Admin
3	ไม่มี Awareness ด้าน PDPA	อบรมรอบเดียว	บุคลากรใหม่ยังไม่เข้าใจ	ขาดแผนอบรมต่อเนื่อง	สร้าง e-learning PDPA + Quiz	ก.ย.-พ.ย. 2568	HR + IT

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.1 มีการจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific information security policy) มีหัวข้ออย่างน้อยต่อไปนี้

- 1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)
- 2) การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งานและการจัดทำแผนเตรียมความพร้อมรับมือภัยคุกคาม
- 3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

CS.3.2 มีนโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคล (PII) ป้องกันความลับผู้ป่วย มีให้รู้ไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

CS.3.3 มีการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) อย่างสม่ำเสมอ

CS.3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติสร้างความรู้ความเข้าใจ ให้บุคลากรทุกคนได้รับทราบ และ ถือปฏิบัติ

CS.3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด และนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติ อย่างต่อเนื่อง

หมวดที่ 3: การจัดการความมั่นคงปลอดภัย (Security Management)



Policy & Rules

CS.3.1: แนวปฏิบัติเฉพาะเรื่อง (Access Control, Password Policy)



Awareness & Culture

CS.3.3: การสร้างความตระหนักรู้ (Awareness Training) - Phishing, Social Engineering

CS.3.4: การสื่อสารนโยบาย (Communication)

CS.3.5: การตรวจสอบความเข้าใจ (Compliance Check / Phishing Simulation)

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.1 มีการจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific information security policy) มีหัวข้ออย่างน้อยต่อไปนี้

- 1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)
- 2)การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งานและการจัดทำแผนเตรียมความพร้อมรับมือภัยคุกคาม
- 3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
0.5	มี แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (มีหัวข้อไม่ครบถ้วน) ลงนามโดยผู้บริหาร
1	มี แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (มีหัวข้อครบถ้วน) ระเบียบปฏิบัติ ลงนามโดยผู้บริหาร

เอกสารประกอบ/เอกสารตัวอย่าง

1.แนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific information security policy) มีหัวข้ออย่างน้อยต่อไปนี้

- 1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)
- 2) การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งานและการจัดทำแผนเตรียมความพร้อมรับมือภัยคุกคาม
- 3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.2 มีนโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคล (PII) ป้องกันความลับผู้ปวยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี นโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว
0.5	มี นโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคล (PII) ป้องกันความลับผู้ปวยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้านแต่ ไม่มี แจ้งต่อเจ้าหน้าที่ภายในหน่วยงานรับทราบ ถือปฏิบัติ
1	มี นโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคล (PII) ป้องกันความลับผู้ปวยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน และแจ้งต่อเจ้าหน้าที่ภายในหน่วยงานรับทราบ ถือปฏิบัติ

เอกสารประกอบ/เอกสารตัวอย่าง
1.นโยบายและระเบียบปฏิบัติหรือมาตรการที่รักษาความเป็นส่วนตัว ปกป้องข้อมูลส่วนบุคคล (PII) ป้องกันความลับผู้ปวยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน ที่ได้รับการลงนามจากผู้บริหาร และมีการแจ้งต่อเจ้าหน้าที่ภายในหน่วยงานเพื่อรับทราบและถือปฏิบัติ

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.3 มีการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) อย่างสม่ำเสมอ

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี แผนงานการสร้างความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
0.5	มีหน่วยงานของท่านมีแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) บางส่วนตามรายละเอียดข้อ (ก) - (ง)
1	หน่วยงานของท่านมีแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ครบถ้วนตามรายละเอียดข้อ (ก) - (ง)

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. แผนงานในการสร้างตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
 - 2. คู่มือปฏิบัติงานของบุคลากรทุกประเภท
 - 3. รายการกิจกรรมและกำหนดการจัดกิจกรรมที่เกี่ยวข้องในแผนงาน

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.3 มีการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) อย่างสม่ำเสมอ

รายละเอียดแผนงานการสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

- (ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท เช่น
- 1. พนักงานใหม่ (New Employees)
 - 2. ผู้ใช้และระดับบริหาร (User and Management)
 - 3. เจ้าหน้าที่สนับสนุนงานด้านโครงสร้างพื้นฐาน

สำคัญทางสารสนเทศ

(ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงาน

(ค) การสร้างความตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับ

การใช้งานและการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ง) การสื่อสารอย่างสม่ำเสมอและทันทั่วที่ครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคาม ทางไซเบอร์ผลกระทบ และการบรรเทาผลกระทบ

หมวด	รายละเอียด	ตัวอย่าง
(ก) กลุ่มเป้าหมายที่ได้รับความรู้	- พนักงานใหม่ (Orientation) - ผู้ใช้ทั่วไปและผู้บริหาร - เจ้าหน้าที่โครงสร้างพื้นฐาน (IT/ระบบ)	- เอกสารอบรม - แบบฝึกหัด/Quiz
(ข) การเผยแพร่ความรับผิดชอบของแต่ละกลุ่ม	- ผอ.รับผิดชอบนโยบาย - IT ปฏิบัติการเทคนิค - บุคลากรทั่วไปต้องไม่คลิกลิงก์แปลก ๆ	- โปสเตอร์บทบาทหน้าที่ - Infographic
(ค) สร้างความรู้เรื่องกฎหมาย กฎ ระเบียบ แนวปฏิบัติ	- PDPA, พ.ร.บ.ไซเบอร์, นโยบาย รพ.- วิธีป้องกันข้อมูลรั่วไหล / Social Engineering	- วิดีโอความยาว 5 นาที - Line Group แชร์ข่าวภัยคุกคามทางไซเบอร์
(ง) สื่อสารอย่างสม่ำเสมอและทันเวลา	- จัดอบรมประจำปี / รอบไตรมาส - สื่อแจ้งเตือน Phishing Simulation - ป้ายประกาศ / LINE Broadcast	- ตารางกิจกรรม - Screenshot การแจ้งเตือน

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.3 มีการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) อย่างสม่ำเสมอ

ตัวอย่างแผนกิจกรรม Cybersecurity Awareness ประจำปี

เดือน	กิจกรรม	รายละเอียด	ผู้รับผิดชอบ
ม.ค.	ประกาศนโยบายความมั่นคงปลอดภัยไซเบอร์	แจ้งนโยบายอย่างเป็นทางการทุกแผนก ผ่าน email / LINE	ผอ. + ฝ่าย IT
ก.พ.	อบรมพนักงานใหม่	Cybersecurity เบื้องต้น + ข้อตกลงการใช้งานระบบ	HR + IT
มี.ค.	ทำแบบประเมินความรู้ไซเบอร์ (Online Quiz)	ส่งลิงก์แบบทดสอบสั้น 10 ข้อ พร้อมเฉลย	IT
เม.ย.	แจก Infographic: “5 เทคนิคเลี่ยง Phishing”	ติดโปสเตอร์ + แชร์ผ่านกลุ่ม LINE	IT + สื่อสารองค์กร
พ.ค.	ฝึกซ้อม Tabletop: ข้อมูลรั่วไหลจำลอง	ซักซ้อมขั้นตอน IRP กับเจ้าหน้าที่แผนกต่าง ๆ	IT + ทีม DPO
มิ.ย.	อบรม Social Media & ความลับผู้ป่วย	เน้นพฤติกรรมเสี่ยง เช่น โพสต์ภาพคนไข้/จอ HIS	PR + HR
ก.ค.	แจ้งเตือนภัยไซเบอร์จริง (Incident Alert)	แชร์เหตุการณ์จริงในวงการแพทย์/รพ. พร้อมวิธีป้องกัน	IT
ส.ค.	แจก Cyber Hygiene Checklist	เอกสาร 1 หน้าให้บุคลากรเช็กตัวเอง	IT
ก.ย.	อบรมผู้บริหาร: Cyber & PDPA	กฎหมาย, ความรับผิดชอบ, การจัดสรรทรัพยากร	CIO
ต.ค.	Phishing Simulation (จำลองการโจมตี)	ส่ง Email จำลอง → วิเคราะห์พฤติกรรม	IT Security Team
พ.ย.	ประกวดโปสเตอร์/คลิป TikTok ด้านไซเบอร์	ส่งเสริมการมีส่วนร่วม + Awareness จากภายใน	ฝ่ายคุณภาพ
ธ.ค.	สรุปผลกิจกรรม/ประเมินผลรับรู้	วิเคราะห์ผลกิจกรรมตลอดปี เสนอต่อผู้บริหาร	IT + HR

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติ สร้างความรู้ความเข้าใจ ให้บุคลากรทุกคนได้รับทราบ และ ถือนโยบายปฏิบัติ

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ
0.5	มี การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ แต่ไม่ครบถ้วน (ข้อ 1.3, 3.1 - ข้อ 3.2)
1	มี หลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ (ข้อ 1.3, 3.1 - ข้อ 3.2) อย่างครบถ้วน

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. ประกาศภายใน (Internal Announcement) ที่ออกโดยผู้บริหารหรือฝ่ายเทคโนโลยีสารสนเทศ
 - 2. หนังสือเวียน (Circular Letter) ที่ส่งไปยังบุคลากรทุกฝ่ายเพื่อแจ้งนโยบายและระเบียบปฏิบัติ

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด และนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติอย่างต่อเนื่อง

เน้นที่ การประเมิน Compliance ของบุคลากร ไม่ใช่แค่แจ้งนโยบายอย่างเดียว แต่ต้อง ตรวจสอบ-ติดตามผล-ปรับปรุง

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป
0.5	มี การตรวจสอบอย่างเป็นระบบว่าบุคลากรได้รับทราบ เข้าใจ และยอมรับระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ผ่านการทดสอบความรู้ แบบประเมิน หรือข้อตกลงการปฏิบัติตาม (Compliance Agreement) แต่ไม่มีการประเมินผลการปฏิบัติตามอย่างเป็นระบบ หรือไม่มีหลักฐานชัดเจนเกี่ยวกับการนำผลการประเมินมาปรับปรุงระเบียบปฏิบัติ
1	มีการตรวจสอบอย่างเป็นระบบว่าบุคลากรได้รับทราบ เข้าใจ และยอมรับระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ผ่านการทดสอบความรู้ แบบประเมิน หรือข้อตกลงการปฏิบัติตาม (Compliance Agreement) และมีการติดตามผลการปฏิบัติอย่างต่อเนื่อง และนำผลการประเมินมาปรับปรุงกระบวนการบังคับใช้ระเบียบปฏิบัติอย่างเป็นระบบ

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. แบบทดสอบหรือแบบประเมินผล เพื่อวัดความเข้าใจและการถือปฏิบัติตามแนวปฏิบัติของบุคลากร
 - 2. รายงานผลการตรวจสอบ แบบทดสอบความรู้ เอกสารยืนยันการปฏิบัติตามของบุคลากร และหลักฐานการนำผลการประเมินมาปรับปรุง

หมวดที่ 3 การจัดการความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์

CS.3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด และนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติอย่างต่อเนื่อง

เน้นที่ การประเมิน Compliance ของบุคลากร ไม่ใช่แค่แจ้งนโยบายอย่างเดียว แต่ต้อง ตรวจสอบ-ติดตามผล-ปรับปรุง

ตัวอย่างโครงสร้างการดำเนินงาน

ขั้นตอน	รายละเอียด	เอกสารประกอบ
1. แจ้งนโยบายอย่างเป็นทางการ	แจ้งให้บุคลากรทุกคนรับทราบผ่าน Email / LINE / ประชุม	ประกาศภายใน, เอกสารลงนามรับทราบ
2. ตรวจสอบว่า “เข้าใจ-ยอมรับ”	ทำแบบประเมินความเข้าใจ หรือให้ลงนามข้อตกลง (Compliance Agreement)	แบบประเมินออนไลน์, แบบลงนาม
3. ประเมินการปฏิบัติตามจริง (Compliance Monitoring)	ตรวจ log, สุ่มตรวจพฤติกรรมการใช้งาน, ตรวจสอบความเสี่ยงจากพนักงาน	รายงาน audit log, แบบประเมิน supervisor
4. วิเคราะห์ผลการประเมิน	สรุปว่ามีช่องโหว่/ปัญหาอะไร เช่น เข้าใจผิด, ไม่ทำตาม	รายงานประเมินผล, สถิติการฝ่าฝืน
5. ปรับปรุงระเบียบ/แนวปฏิบัติ	ปรับข้อความในนโยบาย, เพิ่มรอบอบรม, แก่กระบวนการให้เข้มข้น	นโยบายเวอร์ชันใหม่, บันทึกการประชุมปรับแผน

หมวดที่ 4 การจัดการศักยภาพของทรัพยากร ในระบบเทคโนโลยีสารสนเทศ

- CS.4.1 มีการจัดทำทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ (Critical services) ของหน่วยงาน
- CS.4.2 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, People
- CS.4.3 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากร ด้าน Hardware, Software, Network
- CS.4.4 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ที่จำเป็น (Functional Competency) ของบุคลากรด้าน IT ทุกคน และประเมินสมรรถนะตามบทบาทหน้าที่ และจัดทำแผนเพิ่มสมรรถนะรายบุคคล
- CS.4.5 มีการนำผลการวิเคราะห์ สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People มาปรับปรุงจัดทำแผนเพิ่มศักยภาพ อย่างต่อเนื่อง

หมวดที่ 4: การจัดการทรัพยากร (Resource Management)



หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.1 มีการจัดทำทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ (Critical services) ของหน่วยงาน

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี มีการจัดทำทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ (Critical services) ของหน่วยงาน
0.5	มี มีการจัดทำทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ (Critical services) ของหน่วยงาน แต่ระบุรายละเอียดไม่ครบถ้วนหรือไม่ครอบคลุมทุกทรัพย์สินที่เกี่ยวข้องกับบริการที่สำคัญ
1	มี การจัดทำทะเบียนทรัพย์สินด้านสารสนเทศที่ครอบคลุมทุกทรัพย์สินที่เกี่ยวข้องกับบริการที่สำคัญ ของหน่วยงาน มีการระบุรายละเอียด เช่น ประเภททรัพย์สิน เจ้าของทรัพย์สิน (Asset Owner) ความสำคัญ ความเสี่ยง และมีการปรับปรุงข้อมูลอย่างสม่ำเสมอ

เอกสารประกอบ/เอกสารตัวอย่าง

- ทะเบียนทรัพย์สินด้านสารสนเทศที่ครอบคลุมทุกทรัพย์สินที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน มีการระบุรายละเอียด เช่น ประเภททรัพย์สิน เจ้าของทรัพย์สิน (Asset Owner) ความสำคัญ ความเสี่ยง

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.1 มีการจัดทำทะเบียนทรัพย์สินด้านสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ (Critical services) ของหน่วยงาน

การจัดทำ ทะเบียนทรัพย์สินด้านสารสนเทศ (IT Asset Inventory) ที่เกี่ยวข้องกับบริการสำคัญของหน่วยงาน เป็นหัวใจหลักของข้อ CS.4.1 ซึ่งต้อง:

ครอบคลุม 4 ประเภทหลักของทรัพย์สิน

Hardware – เช่น Server, PC, Switch, UPS

Software – เช่น HIS, Antivirus, Database

Network – เช่น Router, Firewall, Load Balancer

People/Data/Docs – เช่น บัญชีผู้ใช้, เอกสารนโยบาย

ตัวอย่างโครงสร้าง “ทะเบียนทรัพย์สินด้านสารสนเทศ”

ลำดับ	ประเภททรัพย์สิน	รายการ	เจ้าของทรัพย์สิน (Asset Owner)	ความสำคัญ (Critical/Non)	ความเสี่ยง (High/Med/Low)	สถานะ	หมายเหตุ
1	Hardware	Server HIS #1	หัวหน้า IT	Critical	High	ใช้งานอยู่	อายุใช้งาน > 7 ปี
2	Software	ระบบ HIS (เวอร์ชัน 5.0)	หัวหน้า IT	Critical	Medium	ใช้งานอยู่	ไม่มีสัญญาบำรุง
3	Network	Firewall FortiGate	ผู้ดูแลระบบ	Critical	High	ใช้งานอยู่	ต้อง Renew license
4	Document	นโยบาย Data Backup	CISO	Critical	Low	ล่าสุด 2566	ยังไม่อัปเดตนโยบาย

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.2 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People

เป้าหมายคือการประเมินว่าทรัพยากรเทคโนโลยีสารสนเทศที่มีในปัจจุบัน เพียงพอและเหมาะสมหรือไม่ เมื่อเทียบกับภารกิจบริการสุขภาพ และกำหนด “ช่องว่าง” ที่ต้องพัฒนา

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี ผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People
0.5	มี ผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน แต่ไม่ครบทุกด้าน
1	มี ผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People ครบทุกด้าน

เอกสารประกอบ/เอกสารตัวอย่าง

- 1.สรุปผลการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.2 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People

ตัวอย่างหัวข้อ“รายงานการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis”

1. วิเคราะห์สถานการณ์ปัจจุบัน (Current State Analysis)

ด้านทรัพยากร	รายการที่มีอยู่	สถานะ / ความสามารถ	ความเสี่ยง / ข้อจำกัด
Hardware	Server HIS อายุ 7 ปี	ทำงานได้แต่ไม่รองรับ HIS รุ่นใหม่	ความเสี่ยงสูงจากการหยุดทำงาน
Software	Antivirus = AVG Free	ไม่มีระบบอัปเดตอัตโนมัติ / ไม่มีการแจ้งเตือนภัย	ไม่ผ่านเกณฑ์ PDPA
Network	ไม่มีระบบ IDS/IPS	Firewall ธรรมดา, ไม่มีระบบตรวจจับภัย	เสี่ยงต่อการถูกโจมตีโดยไม่รู้ตัว
People	IT 1 คน, ไม่มีใบรับรองไซเบอร์	ไม่มีแผนพัฒนา/อบรม	ไม่สามารถรองรับเหตุการณ์ Incident จริง

2. ตาราง Gap Analysis

ด้าน	สถานะปัจจุบัน	ความต้องการ/เป้าหมาย	Gap (ช่องว่าง)
Hardware	Server รุ่นเก่า (RAM 4GB)	ต้องการ Server รองรับ HIS Web	ความจุและความเร็วไม่พอ
Software	ไม่มี Patch Management	ต้องมีระบบอัปเดตอัตโนมัติ	เสี่ยงต่อ Zero-day
Network	ไม่มีระบบแยก VLAN ระหว่างบุคลากร/คนไข้	ต้องมี Network Isolation	เสี่ยงข้อมูลรั่วข้ามระบบ
People	IT ไม่มีการอบรมด้าน PDPA/Cyber	ต้องมีใบรับรอง / อบรมทุกปี	ขาดความรู้ + Compliance

ร่วมวิเคราะห์กับหลายฝ่าย เช่น ฝ่ายบริหาร, IT, ผู้ใช้งาน

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.3 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากร ด้าน Hardware, Software, Network

จัดทำ แผนอย่างเป็นทางการ ที่มีเป้าหมายชัดเจน ครอบคลุม การพัฒนา/ทดแทน/เพิ่มเติม ระบบสารสนเทศให้เหมาะสมกับความเสี่ยงและภารกิจ

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network
0.5	มี การจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network แต่ขาดด้านใดด้านหนึ่ง
1	มี การจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network ครบทุกด้าน

เอกสารประกอบ/เอกสารตัวอย่าง

1.แผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน HARDWARE, SOFTWARE,NETWORK

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.3 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากร ด้าน Hardware, Software, Network

ตัวอย่างตารางแผนจัดการศักยภาพ

ด้าน	รายการ	แนวทางพัฒนา	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ	หมายเหตุ
Hardware	Server HIS	จัดซื้อ/ติดตั้ง Dell R650	มิ.ย.-ก.ค. 68	หัวหน้า IT	ผ่านงบแล้ว
Software	Antivirus	ติดตั้ง Bitdefender GravityZone	มิ.ย.-ก.ค. 68	IT Support	รอใบเสนอราคา
Network	Firewall	ซื้อ FortiGate + แยก VLAN	ส.ค.-ก.ย. 68	System Admin	ขออนุมัติกรรมการ

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.4 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ที่จำเป็น (Functional Competency) ของบุคลากรด้าน IT ทุกคน และประเมินสมรรถนะตามบทบาทหน้าที่ และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคน ผลการประเมินสมรรถนะตามบทบาทหน้าที่ และแผนการเพิ่มสมรรถนะรายบุคคล
0.5	มี การกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคน หรือ ผลการประเมินสมรรถนะตามบทบาทหน้าที่ หรือ แผนการเพิ่มสมรรถนะรายบุคคล
1	มี การกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคนและ ผลการประเมินสมรรถนะตามบทบาทหน้าที่ และ มีแผนการเพิ่มสมรรถนะรายบุคคล

เอกสารประกอบ/เอกสารตัวอย่าง

1. เอกสารแสดงกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคน
2. ผลการประเมินสมรรถนะตามบทบาทหน้าที่
3. แผนการเพิ่มสมรรถนะรายบุคคล

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.5 มีการนำผลการวิเคราะห์ สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People มาปรับปรุงจัดทำแผนเพิ่มศักยภาพ อย่างต่อเนื่อง

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การวิเคราะห์สถานการณ์ปัจจุบันหรือการทำ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People หรือไม่มีการดำเนินการปรับปรุงแผนเพิ่มศักยภาพตามผลการวิเคราะห์
0.5	มี การวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้านบางส่วน (เช่น เพียงทรัพยากรด้าน Hardware หรือ Software) แต่ไม่มีแผนการปรับปรุงที่ชัดเจน หรือแผนที่มีอยู่ไม่ครอบคลุมทุกด้านหรือไม่มีการดำเนินการปรับปรุงอย่างต่อเนื่อง
1	มี การวิเคราะห์สถานการณ์ปัจจุบันและทำ Gap Analysis ครอบคลุมทรัพยากรทุกด้าน ได้แก่ Hardware, Software, Network และ People และมีแผนการปรับปรุงที่ชัดเจน ซึ่งมีการติดตามผลและปรับปรุงแผนอย่างต่อเนื่อง เพื่อเพิ่มศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.5 มีการนำผลการวิเคราะห์ สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People มาปรับปรุงจัดทำแผนเพิ่มศักยภาพ อย่างต่อเนื่อง

เอกสารประกอบ/เอกสารตัวอย่าง

- 1. รายงานการวิเคราะห์สถานการณ์ปัจจุบัน (Current State Analysis Report) : เอกสารที่แสดงถึงการวิเคราะห์ทรัพยากรด้านต่าง ๆ เช่น Hardware, Software, Network, และ People ในสถานการณ์ปัจจุบัน ข้อมูลที่ระบุถึงความสามารถของทรัพยากรที่มีอยู่และข้อจำกัดต่าง ๆ
- 2. รายงานการทำ Gap Analysis : การเปรียบเทียบสถานการณ์ปัจจุบันกับความต้องการหรือเป้าหมายที่คาดหวัง ระบุช่องว่าง (Gaps) ที่พบในทรัพยากรแต่ละประเภท เช่น ความไม่พอเพียงของฮาร์ดแวร์ ซอฟต์แวร์ที่ล้าสมัย หรือช่องว่างในทักษะของบุคลากร

ด้านทรัพยากร	รายการที่วิเคราะห์	ความสามารถที่มี	ข้อจำกัด / ความเสี่ยง
Hardware	Server, Storage, PC, Printer, UPS	- มี Server 2 ชุด (1 main + 1 backup) - มี UPS รองรับ 30 นาที	- Server อายุใช้งานเกิน 7 ปี - UPS ไม่ครอบคลุมระบบทั้งหมด
Software	HIS, LIS, Antivirus, Backup SW	- ใช้ HIS ที่พัฒนาในประเทศ - มี Antivirus + ระบบสำรองข้อมูล	- ไม่ได้อัปเดตระบบปฏิบัติการ (OS) - ไม่มีระบบอัปเดตอัตโนมัติ
Network	Router, Firewall, Internet, WiFi	- มี Firewall แยกระดับ - WiFi แยก Guest กับ Staff	- Network redundancy ไม่เพียงพอ - ไม่มีระบบตรวจจับภัย (IDS/IPS)
People	IT Officer, Support, Admin	- มี IT Officer 1 คน - มี Admin ฝ่ายเวชระเบียนช่วยบ้าง	- ขาดบุคลากรเฉพาะด้าน Cybersecurity - ไม่มีแผนพัฒนาสมรรถนะรายบุคคล

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.5 มีการนำผลการวิเคราะห์ สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People มาปรับปรุงจัดทำแผนเพิ่มศักยภาพ อย่างต่อเนื่อง

เอกสารประกอบ/เอกสารตัวอย่าง

3. แผนเพิ่มศักยภาพ (Capacity Improvement Plan) : แผนการที่แสดงถึงการปรับปรุงหรือพัฒนาทรัพยากรที่มีอยู่ เช่น การอัปเกรดฮาร์ดแวร์ ซอฟต์แวร์ หรือการฝึกอบรมบุคลากร เป็นต้น รวมถึง การระบุขั้นตอนการดำเนินการ, ระยะเวลาที่ต้องการ, และผู้รับผิดชอบในการดำเนินการ

หมวดทรัพยากร	รายการที่ต้องพัฒนา	เป้าหมาย	ขั้นตอนดำเนินการ	ระยะเวลา	ผู้รับผิดชอบ
Hardware	Server หลัก (Main Server) อายุเกิน 7 ปี	อัปเกรดเป็น Server ใหม่ที่รองรับระบบ HIS	1. จัดหางบ2. จัดซื้อและติดตั้ง3. ย้ายระบบและทดสอบ	Q1-Q2	หัวหน้าฝ่าย IT
Software	ระบบ Antivirus & Patch Management	ติดตั้งระบบอัปเดตอัตโนมัติทั่วทั้งองค์กร	1. คัดเลือกซอฟต์แวร์2. ติดตั้ง3. ทดสอบ & อบรมการใช้งาน	Q2	เจ้าหน้าที่ IT
Network	ไม่มีระบบตรวจจับภัย (IDS/IPS)	ติดตั้งระบบ Intrusion Detection	1. วิเคราะห์ความต้องการ2. จัดซื้อและติดตั้ง3. ทดสอบและเก็บ log	Q3	IT + ผู้รับเหมา
People	ขาดความรู้ด้าน Cybersecurity	เพิ่มสมรรถนะบุคลากรด้าน IT Security	1. กำหนด Competency 2. ส่งอบรมหลักสูตร CompTIA Security+/ISO27001 3. ประเมินหลังอบรม	Q2-Q4	HR + IT
Policy	ไม่มีแผนการซ้อมรับภัยคุกคามไซเบอร์	จัดทำแผน IRP และฝึกซ้อมปีละ 1 ครั้ง	1. ร่างแผน IRP2. ฝึกซ้อม Table-top Exercise3. สรุปผลและปรับปรุง	Q3-Q4	CISO / ผู้บริหาร

หมวดที่ 4 การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

CS.4.5 มีการนำผลการวิเคราะห์ สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network และ People มาปรับปรุงจัดทำแผนเพิ่มศักยภาพ อย่างต่อเนื่อง

เอกสารประกอบ/เอกสารตัวอย่าง

- 4. เอกสารการติดตามและประเมินผล (Monitoring and Evaluation Documentation) : รายงานการติดตามผลการดำเนินการตามแผนที่จัดทำขึ้น หรือ การประเมินความสำเร็จของการปรับปรุงศักยภาพทรัพยากร และการปรับแผนเมื่อมีการเปลี่ยนแปลงสถานการณ์
- 5. รายงานการประชุมหรือการนำเสนอแผน (Meeting Notes or Presentation Files) : บันทึกการประชุมที่แสดงถึงการหารือเกี่ยวกับผลการวิเคราะห์ Gap และการจัดทำแผนการปรับปรุง รวมถึง เอกสารการนำเสนอแผนในที่ประชุม เพื่อให้ผู้เกี่ยวข้องได้รับข้อมูลและความคิดเห็น

ตัวอย่าง สรุปผลการดำเนินงานรายการกิจกรรม

หมวดทรัพยากร	กิจกรรมตามแผน	เป้าหมาย	ผลการดำเนินจริง	ความก้าวหน้า	ปัญหา / อุปสรรค
Hardware	จัดซื้อ Server ใหม่	เสร็จไตรมาส 2	ดำเนินการแล้ว 100%	สำเร็จ	-
Software	อัปเดต Patch HIS	100% Server	เสร็จแล้ว 80%	ดำเนินการ	ขาด License Key
Network	ติดตั้ง IDS/IPS	เริ่ม Q3	ยังไม่เริ่ม	ล่าช้า	งบประมาณล่าช้า
People	อบรม Cybersecurity	เจ้าหน้าที่ 4 คน	อบรมแล้ว 3 คน	รอดำเนินการ	1 คนติดเวร
Policy	ทบทวน IRP	เสร็จไตรมาส 2	ทบทวนแล้วแต่ยังไม่อนุมัติ	รอดำเนินการ	ผู้บริหารไม่อยู่เซ็น

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

- CS.5.1 กำหนดมาตรการการรักษาความปลอดภัยทางกายภาพ การทบทวนสิทธิ์บุคลากรที่ได้รับอนุญาตให้เข้าถึง Data Center และการกำหนด หน้าที่ความรับผิดชอบในการดูแล Data Center ของหน่วยงาน
- CS.5.2 การกำหนดรอบการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูล รวมถึงป้องกันสื่อบันทึกการสำรองข้อมูลจากความเสียหาย และการสูญหาย และการเข้าถึงโดยไม่ได้รับอนุญาต
- CS.5.3 มีระบบป้องกันอัคคีภัย เช่น ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงหรือระบบดับเพลิงอัตโนมัติ ให้เหมาะสมกับความเสี่ยง
- CS.5.4 มีมาตรการหรือระบบป้องกันความเสียหายของข้อมูล และระบบ เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server ให้เหมาะสมกับความเสี่ยง
- CS.5.5 มีระบบเฝ้าระวัง และรักษาความมั่นคงปลอดภัยทางกายภาพ Data Center ของหน่วยงาน

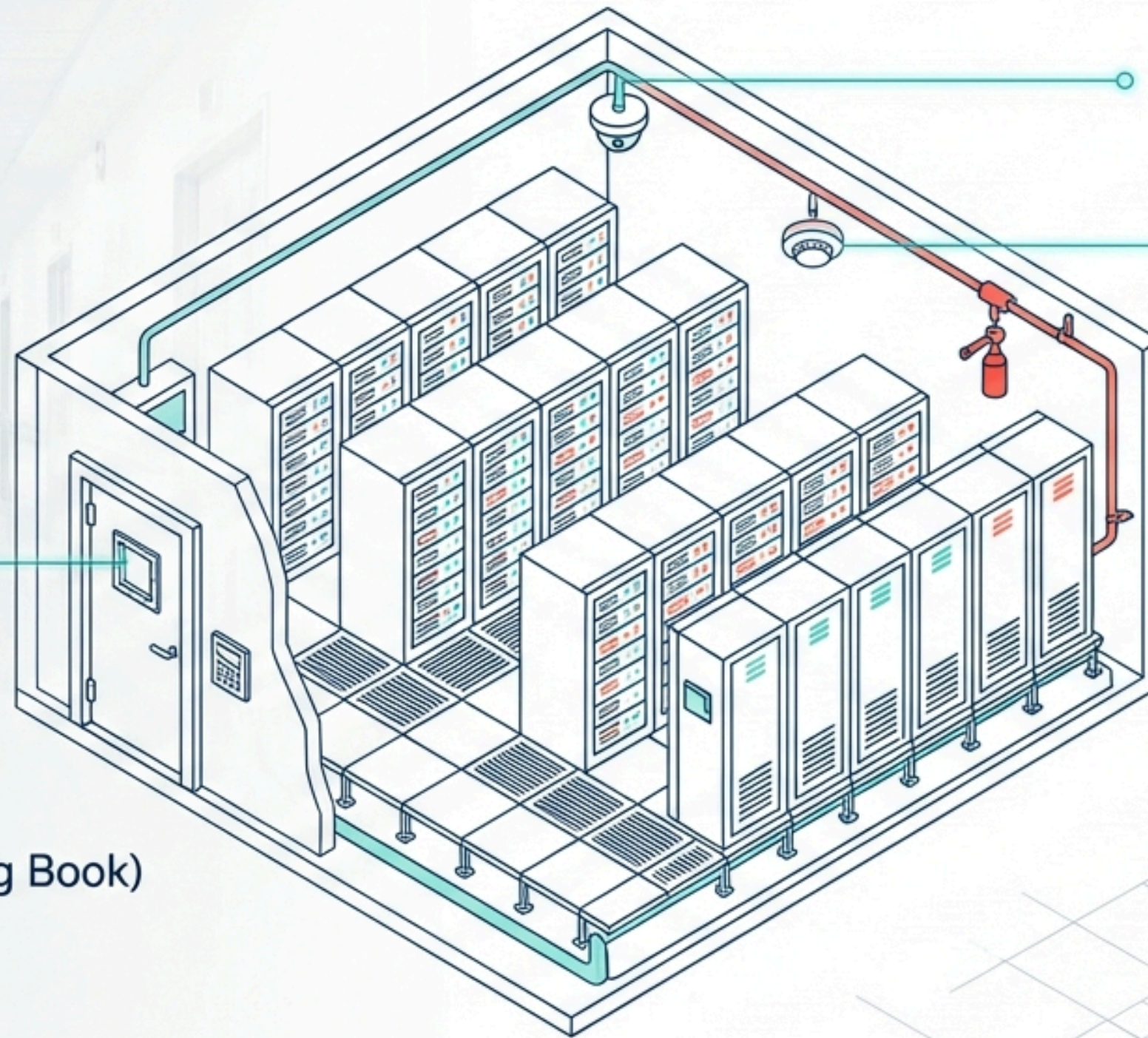


หมวดที่ 5 (ส่วนที่ 1): ความปลอดภัยทางกายภาพ (Data Center Security)

CS.5.1 Access Control
(ควบคุมการเข้า-ออก / Log Book)

CS.5.5 Surveillance (CCTV)

CS.5.3 Fire Protection
(ระบบป้องกันอัคคีภัย)

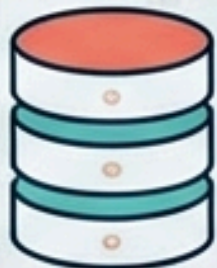


หมวดที่ 5 (ส่วนที่ 2): ความพร้อมใช้และการสำรองข้อมูล (Resilience & Backup) System Continuity

CS.5.4 Redundancy



UPS
(ระบบสำรองไฟอัตโนมัติ)



RAID
(ระบบจัดเก็บข้อมูลแบบกลุ่ม)



HA (High Availability -
ระบบทำงานทดแทน)

CS.5.2 Backup & Recovery



Backup Schedule
(ตารางการสำรองข้อมูล)



Recovery Test
(ทดสอบกู้คืนข้อมูล - ปีละ 1 ครั้ง)



Media Protection
(การป้องกันสื่อบันทึกข้อมูล)

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.1 กำหนดมาตรการการรักษาความปลอดภัยทางกายภาพ การทบทวนสิทธิ์บุคลากรที่ได้รับอนุญาตให้เข้าถึง Data Center และ
การกำหนดหน้าที่ความรับผิดชอบในการดูแล Data Center ของหน่วยงาน

มีมาตรการครอบคลุม 3 ส่วนหลัก ได้แก่ 🚪 การป้องกันภายนอก, 🔍 การทบทวนสิทธิ์ และ 👤 การระบุผู้รับผิดชอบ

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การกำหนดมาตรการการรักษาความปลอดภัยทางกายภาพ หรือไม่มีเอกสารที่แสดงถึงมาตรการรักษาความปลอดภัย เช่น ไม่มีการควบคุมการเข้าถึงพื้นที่ หรือไม่มีกำหนดหน้าที่และความรับผิดชอบในการดูแล Data Center
0.5	มีการกำหนดมาตรการบางประการ เช่น การควบคุมการเข้าถึงพื้นที่ Data Center แต่ยังไม่ครอบคลุมทุกด้าน หรือไม่มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ หรือไม่มีกำหนดหน้าที่ความรับผิดชอบในการดูแล Data Center อย่างชัดเจน
1	มีการกำหนดมาตรการการรักษาความปลอดภัยทางกายภาพที่ครอบคลุมและชัดเจน เช่น การควบคุมการเข้าถึงพื้นที่ Data Center อย่างเข้มงวด การทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ และกำหนดหน้าที่ความรับผิดชอบในการดูแล Data Center โดยมีกระบวนการที่ชัดเจนและเอกสารการดำเนินการที่สามารถตรวจสอบได้

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. เอกสารที่แสดงถึงมาตรการในการรักษาความปลอดภัยภายใน Data Center โดยครอบคลุมทั้งการควบคุมการเข้าถึงพื้นที่ การจัดการการเข้าถึงจากบุคคลภายนอก และการป้องกันการบุกรุก
 - 2. รายงานการทบทวนสิทธิ์การเข้าถึง (Access Rights Review Report)
 - 3. นโยบายที่กำหนดการควบคุมการเข้าถึงพื้นที่ Data Center รวมถึงข้อกำหนดเกี่ยวกับการใช้บัตรประจำตัว, การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) หรือระบบอื่น ๆ ที่ใช้ในการควบคุมการเข้าถึง
 - 4. เอกสารที่ระบุหน้าที่และความรับผิดชอบของบุคลากรในการดูแลรักษาความปลอดภัยของ Data Center เช่น ผู้รับผิดชอบในการควบคุมการเข้าถึง หรือผู้ที่รับผิดชอบในการตรวจสอบระบบความปลอดภัยภายใน Data Center

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.1 กำหนดมาตรการการรักษาความปลอดภัยทางกายภาพ การทบทวนสิทธิ์บุคลากรที่ได้รับอนุญาตให้เข้าถึง Data Center และ
การกำหนดหน้าที่ความรับผิดชอบในการดูแล Data Center ของหน่วยงาน

ตัวอย่าง โครงสร้างเอกสาร "มาตรการรักษาความปลอดภัยทางกายภาพ Data Center"

มาตรการรักษาความปลอดภัยทางกายภาพ (Physical Security Measures)

- การเข้าออกพื้นที่ Data Center ต้องใช้บัตรอนุญาตพิเศษ (Access Card) หรือแนวทางอื่นๆ
- ติดตั้งระบบล็อกอัตโนมัติ + กล้องวงจรปิด (CCTV) บันทึกภาพย้อนหลังได้อย่างน้อย 30 วัน
- ห้ามบุคคลภายนอก (รวมถึง outsource) เข้าโดยไม่มีผู้ควบคุม
- มีการจดบันทึก log การเข้า-ออก (Manual หรือ Digital Log)

การทบทวนสิทธิ์เข้าถึง Data Center (Access Rights Review)

- ทบทวนรายชื่อผู้มีสิทธิ์เข้า Data Center ทุก 6 เดือน
- ยกเลิกสิทธิ์ทันทีเมื่อพนักงานลาออก/พ้นหน้าที่
- ใช้แบบฟอร์มอนุมัติสิทธิ์จากผู้บริหาร/หัวหน้าหน่วย

การกำหนดหน้าที่ความรับผิดชอบ (Roles & Responsibility)

- ผู้ดูแลหลัก (Primary Operator): ดูแลการควบคุมสิทธิ์และการบำรุงรักษา
- ผู้ตรวจสอบ (Auditor): ตรวจสอบการเข้าออก, CCTV, อุปกรณ์สำรอง
- ผู้บริหารระบบ (IT Manager): รับผิดชอบบริหารความเสี่ยงและอนุมัติสิทธิ์
- จัดทำ ผังผู้รับผิดชอบ และ เอกสารคำสั่งแต่งตั้ง

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.2 การกำหนดรอบการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูล รวมถึงป้องกันสื่อบันทึกการสำรองข้อมูลจากความเสียหาย และการสูญหาย และการเข้าถึงโดยไม่ได้รับอนุญาต

เป้าหมายคือให้ ข้อมูลสำคัญของโรงพยาบาลสามารถกู้คืนได้อย่างปลอดภัยและต่อเนื่อง หากเกิดเหตุการณ์ฉุกฉุกเงินหรือภัยคุกคามทางไซเบอร์

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มีการกำหนดรอบการสำรองข้อมูล หรือไม่มีการทดสอบการกู้คืนข้อมูล หรือไม่มีการมาตรการในการป้องกันสื่อบันทึกการสำรองข้อมูลจากความเสียหาย การสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต
0.5	มี การกำหนดรอบการสำรองข้อมูล แต่ขาดการทดสอบการกู้คืนข้อมูล หรือขาดมาตรการในการป้องกันสื่อบันทึกจากการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
1	มี การกำหนดรอบการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอและครบถ้วน พร้อมทั้งมีมาตรการป้องกันสื่อบันทึกการสำรองข้อมูลจากความเสียหาย การสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาตอย่างเข้มงวด เช่น การเก็บรักษาในพื้นที่ที่ปลอดภัย การเข้ารหัสข้อมูล และการควบคุมการเข้าถึงข้อมูล

- เอกสารประกอบ/เอกสารตัวอย่าง
- แผนการสำรองข้อมูล (Backup Plan) : เอกสารที่แสดงถึงการกำหนดรอบการสำรองข้อมูล เช่น ความถี่ในการสำรองข้อมูล (รายวัน รายสัปดาห์ ฯลฯ) และประเภทของข้อมูลที่ต้องการสำรอง รายละเอียดขั้นตอนการสำรองข้อมูลที่ชัดเจน เช่น การใช้ระบบสำรองข้อมูลอัตโนมัติ หรือการกำหนดวิธีสำรองข้อมูลที่เหมาะสม
 - รายงานการทดสอบการกู้คืนข้อมูล (Data Recovery Testing Report) : เอกสารที่แสดงถึงการทดสอบการกู้คืนข้อมูล เช่น การทดสอบการกู้คืนข้อมูลจากแหล่งสำรองข้อมูลภายใต้สถานการณ์ต่าง ๆ รวมถึงการบันทึกผลการทดสอบ เช่น ระยะเวลาที่ใช้ในการกู้คืนข้อมูล หรือประสิทธิภาพของกระบวนการกู้คืน
 - นโยบายการป้องกันสื่อบันทึกข้อมูล (Data Backup Media Protection Policy) : นโยบายที่ระบุถึงมาตรการการป้องกันสื่อบันทึกข้อมูลจากการสูญหาย การเสียหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การเก็บสื่อบันทึกในที่ปลอดภัย การใช้การเข้ารหัสข้อมูลในขณะที่เก็บรักษา และการควบคุมการเข้าถึงสื่อบันทึก

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.2 การกำหนดรอบการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูล รวมถึงป้องกันสื่อบันทึกการสำรองข้อมูลจากความเสียหาย และการสูญหาย และการเข้าถึงโดยไม่ได้รับอนุญาต

เป้าหมายคือให้ ข้อมูลสำคัญของโรงพยาบาลสามารถกู้คืนได้อย่างปลอดภัยและต่อเนื่อง หากเกิดเหตุการณ์ฉุกเฉินหรือภัยคุกคามทางไซเบอร์

ตัวอย่างหัวข้อ "แผนการสำรองและกู้คืนข้อมูล" (Data Backup & Recovery Plan)

1. รอบ การสำรองข้อมูล (Backup Schedule)
- HIS, LIS, ระบบเวชระเบียน: สำรอง ทุกวัน (Daily Backup)
 - ระบบอื่น ๆ: อย่างน้อยสัปดาห์ละ 1 ครั้ง
 - เก็บไว้ 2 ชุด ได้แก่:
Onsite: ภายในโรงพยาบาล (Server สำรอง)
Offsite: ภายนอก เช่น Cloud / External Storage

2. การทดสอบการกู้คืนข้อมูล (Data Recovery Testing)
- ต้องมีการทดสอบกู้คืนข้อมูล (Recovery Drill) อย่างน้อยปีละ 1 ครั้ง
 - ใช้ข้อมูลจริงในสภาวะจำลอง (Disaster Simulation)
 - บันทึกผล เช่น: ระยะเวลา, ความสมบูรณ์ของข้อมูล, อุปสรรคที่พบ

ระบบ	ความถี่	วิธีการ	สถานที่เก็บ
HIS	รายวัน	Full + Incremental	Onsite Server + Cloud
LAB (LIS)	รายวัน	Scheduled Script	External NAS
เอกสารเวชระเบียน	รายสัปดาห์	Manual Scan	External HDD (ล็อกตู้)

วันที่ทดสอบ	ระบบ	ระยะเวลากู้คืน	ผลลัพธ์	ผู้ทำการทดสอบ
30 มิ.ย. พ.ศ.2568	HIS	2 ชม. 30 นาที	กู้คืน 100%	System Admin

3. มาตรการป้องกันสื่อสำรองข้อมูล
- จัดเก็บในที่ปลอดภัย เช่น ห้องล็อกเฉพาะ, ตู้เซฟ, NAS เฉพาะ
 - เข้ารหัสข้อมูล (Encryption) ทั้งขณะเก็บและส่งข้อมูล
 - ควบคุมการเข้าถึงสื่อบันทึก เช่น Flash Drive, External HDD
 - มีบันทึก/Log การเบิกใช้ / ตรวจสอบสภาพอุปกรณ์
 - สื่อที่เสื่อมสภาพ → มีแนวทางทำลาย (Secure Destruction)



หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.3 มีระบบป้องกันอัคคีภัย เช่น ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงหรือระบบดับเพลิงอัตโนมัติ
ให้เหมาะสมกับความเสี่ยง

การปกป้อง Data Center และอุปกรณ์สำคัญจากความเสียหายที่เกิดจากไฟไหม้ ทั้งเชิงป้องกัน แจ้งเตือน และตอบสนอง

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มีการติดตั้งระบบป้องกันอัคคีภัย หรือไม่มีเอกสารที่แสดงถึงการมีระบบป้องกันอัคคีภัยในพื้นที่ Data Center
0.5	มี การติดตั้งระบบป้องกันอัคคีภัยบางประเภท เช่น ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิง หรือระบบดับเพลิงอัตโนมัติ แต่ขาดการตรวจสอบและบำรุงรักษาอย่างสม่ำเสมอ
1	มี การติดตั้งระบบป้องกันอัคคีภัยที่ครบถ้วนและเหมาะสมกับความเสี่ยง เช่น ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิง หรือระบบดับเพลิงอัตโนมัติในพื้นที่ที่สำคัญ เช่น Data Center และมีการตรวจสอบและบำรุงรักษาอย่างสม่ำเสมอ

- เอกสารประกอบ/เอกสารตัวอย่าง
1. แผนการป้องกันอัคคีภัย (Fire Protection Plan) : เอกสารที่ระบุถึงมาตรการในการป้องกันอัคคีภัยภายในสถานที่สำคัญ เช่น Data Center หรือห้องเซิร์ฟเวอร์ ซึ่งรวมถึงระบบตรวจจับควัน ระบบดับเพลิง หรือเครื่องดับเพลิงอัตโนมัติ
 2. แผนการบำรุงรักษาระบบป้องกันอัคคีภัย (Fire Protection Maintenance Plan) : เอกสารที่แสดงถึงแผนการบำรุงรักษาและการตรวจสอบระบบป้องกันอัคคีภัย เช่น การตรวจสอบเครื่องดับเพลิง ระบบตรวจจับควัน หรือระบบดับเพลิงอัตโนมัติ และการเปลี่ยนอะไหล่เมื่อจำเป็น
 3. บันทึกการตรวจสอบระบบดับเพลิง (Fire System Inspection Logs) : บันทึกที่แสดงถึงการตรวจสอบและการทดสอบระบบดับเพลิงและอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบตรวจจับควัน, เครื่องดับเพลิง, หรือระบบดับเพลิงอัตโนมัติ โดยมีการบันทึกผลการตรวจสอบอย่างสม่ำเสมอ
 4. รูปถังดับเพลิง, Sensor, Alarm, ระบบดับเพลิงอัตโนมัติ

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.3 มีระบบป้องกันอัคคีภัย เช่น ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงหรือระบบดับเพลิงอัตโนมัติให้เหมาะสมกับความเสี่ยง

การปกป้อง Data Center และอุปกรณ์สำคัญจากความเสียหายที่เกิดจากไฟไหม้ ทั้งเชิงป้องกัน แจ้งเตือน และตอบสนอง

1.ตัวอย่างประเภทระบบอัคคีภัย

ระบบ	รายละเอียด	ความเหมาะสม
ระบบตรวจจับควัน (Smoke Detector)	ตรวจจับควันก่อนเกิดเพลิงไหม้	จำเป็นทุกพื้นที่ใน Data Center
ระบบสัญญาณเตือนภัย (Alarm System)	แจ้งเตือนทันทีเมื่อเกิดควัน/ไฟ	ต้องเชื่อมต่อกับหน่วยรักษาความปลอดภัย
เครื่องดับเพลิงเคมีแห้ง (Dry Chemical Fire Extinguisher)	วางมุมห้อง หรือจุดที่สามารถหยิบใช้ได้สะดวก	สำหรับบุคลากรใช้กรณีฉุกเฉิน
ระบบดับเพลิงอัตโนมัติ (Fire Suppression System)	เช่น ระบบก๊าซ FM-200 / CO ₂ / Nitrogen	เหมาะกับ Server Room ไม่มีน้ำ



- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. แผนการป้องกันอัคคีภัย (Fire Protection Plan) : เอกสารที่ระบุถึงมาตรการในการป้องกันอัคคีภัยภายในสถานที่สำคัญ เช่น Data Center หรือห้องเซิร์ฟเวอร์ ซึ่งรวมถึงระบบตรวจจับควัน ระบบดับเพลิง หรือเครื่องดับเพลิงอัตโนมัติ
 - 2. แผนการบำรุงรักษาระบบป้องกันอัคคีภัย (Fire Protection Maintenance Plan) : เอกสารที่แสดงถึงแผนการบำรุงรักษาและการตรวจสอบระบบป้องกันอัคคีภัย เช่น การตรวจสอบเครื่องดับเพลิง ระบบตรวจจับควัน หรือระบบดับเพลิงอัตโนมัติ และการเปลี่ยนอะไหล่เมื่อจำเป็น
 - 3. บันทึกการตรวจสอบระบบดับเพลิง (Fire System Inspection Logs) : บันทึกที่แสดงถึงการตรวจสอบและการทดสอบระบบดับเพลิงและอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบตรวจจับควัน, เครื่องดับเพลิง, หรือระบบดับเพลิงอัตโนมัติ โดยมีการบันทึกผลการตรวจสอบอย่างสม่ำเสมอ
 - 4. รูปถังดับเพลิง, Sensor, Alarm, ระบบดับเพลิงอัตโนมัติ

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.4 มีมาตรการหรือระบบป้องกันความเสียหายของข้อมูล และระบบ เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server ให้เหมาะสมกับความเสี่ยง

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี มาตรการหรือระบบป้องกันความเสียหายของข้อมูลหรือระบบ เช่น ระบบ UPS, RAID, หรือระบบสำรองอื่นๆ เพื่อป้องกันการสูญหายของข้อมูลหรือการหยุดชะงักของระบบ
0.5	มี มาตรการหรือระบบป้องกันความเสียหายของข้อมูล บางประเภท เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server แต่ยังไม่ครอบคลุมทุกระบบที่สำคัญ
1	มี มาตรการหรือระบบป้องกันความเสียหายของข้อมูล อย่างครบถ้วน เช่น ระบบไฟฟ้าสำรอง (UPS), ระบบ RAID, ระบบ Redundant Power Supply, และ Redundant Server ที่ครอบคลุมการป้องกันการสูญหายของข้อมูลและความเสี่ยงจากการหยุดทำงานของระบบ พร้อมทั้งมีการตรวจสอบและบำรุงรักษาอย่างสม่ำเสมอ

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.4 มีมาตรการหรือระบบป้องกันความเสียหายของข้อมูล และระบบ เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server ให้เหมาะสมกับความเสี่ยง

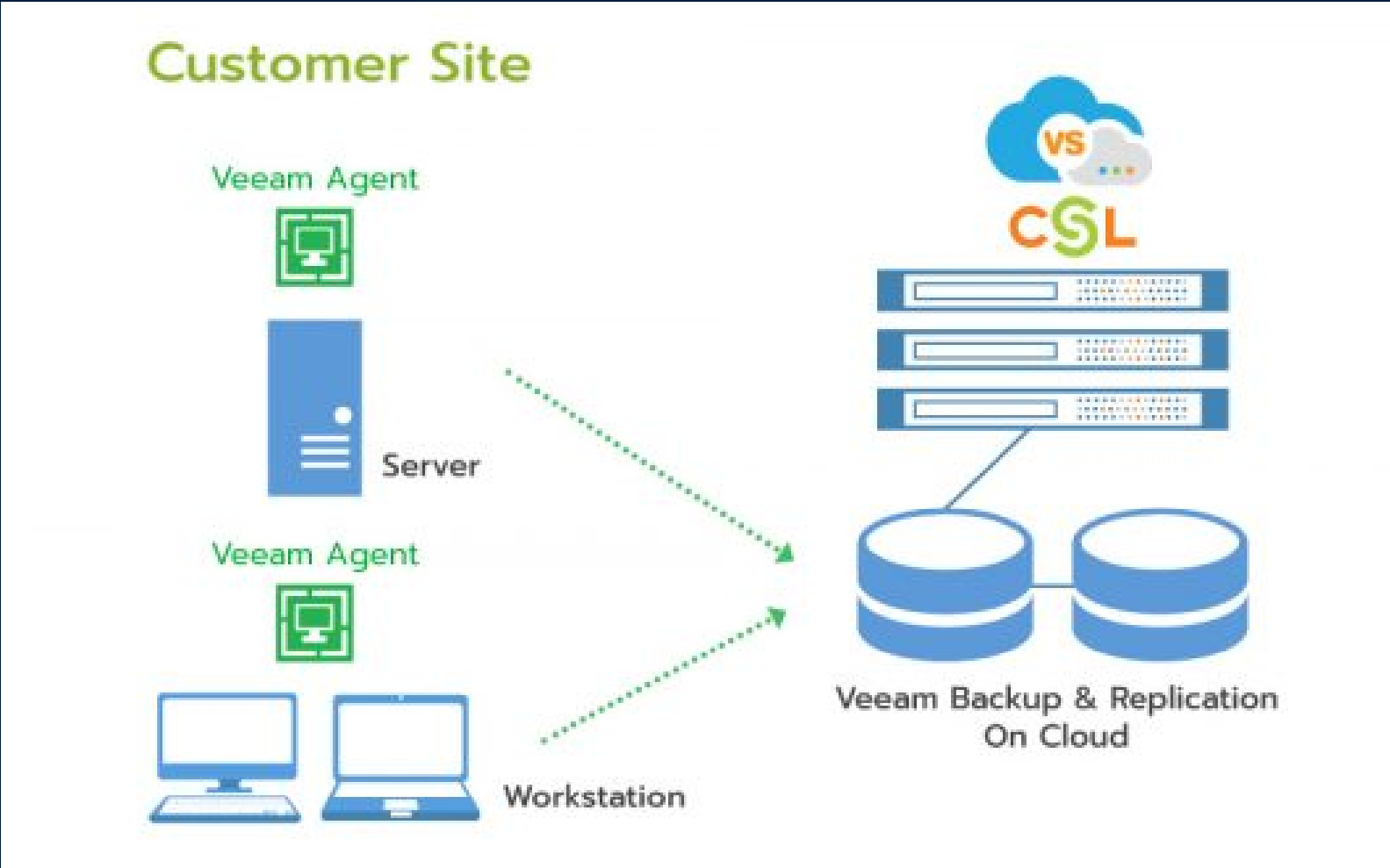
เอกสารประกอบ/เอกสารตัวอย่าง

1. แผนการสำรองไฟฟ้าสำรอง (UPS Plan) : เอกสารที่แสดงถึงการติดตั้งและการใช้ระบบ UPS (Uninterruptible Power Supply) เพื่อให้มีแหล่งพลังงานสำรองในกรณีเกิดการขัดข้องจากแหล่งไฟฟ้าหลัก เช่น การระบุประเภทของ UPS และความจุในการสำรองไฟฟ้า
2. แผนการใช้ระบบ RAID (RAID Implementation Plan) : แผนการที่แสดงถึงการใช้ระบบ RAID (Redundant Array of Independent Disks) เพื่อเพิ่มความปลอดภัยของข้อมูลในกรณีที่เกิดความเสียหายกับฮาร์ดดิสก์ โดยระบุประเภทของ RAID ที่ใช้งาน เช่น RAID 1, RAID 5 หรือ RAID 10
3. รายงานการตรวจสอบและการบำรุงรักษาระบบ RAID (RAID Maintenance and Inspection Report) : รายงานที่แสดงถึงการตรวจสอบและการบำรุงรักษาระบบ RAID รวมถึงการตรวจสอบสภาพของดิสก์และการทดสอบการกู้คืนข้อมูล
4. เอกสารที่แสดงการติดตั้งระบบ Redundant Power Supply ที่ช่วยให้มีแหล่งพลังงานสำรองในกรณีที่แหล่งพลังงานหลักขัดข้อง เช่น การติดตั้งแหล่งพลังงานสองชุดเพื่อให้สามารถสลับใช้ได้ทันที
5. แผนการติดตั้งและการใช้ระบบ Redundant Server (Redundant Server Plan) : เอกสารที่แสดงถึงการติดตั้งระบบ Redundant Server เพื่อให้การทำงานของเซิร์ฟเวอร์สำคัญไม่หยุดชะงัก เช่น การติดตั้งเซิร์ฟเวอร์สำรองที่สามารถทดแทนเมื่อเซิร์ฟเวอร์หลักมีปัญหา
6. บันทึกที่แสดงถึงการตรวจสอบและการบำรุงรักษาระบบทั้งหมด เช่น UPS, RAID, Redundant Power Supply, และ Redundant Server พร้อมกับผลการทดสอบการทำงานในแต่ละรอบ

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.4 มีมาตรการหรือระบบป้องกันความเสียหายของข้อมูล และระบบ เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server ให้เหมาะสมกับความเสี่ยง

ตัวอย่าง แผนผังการสำรองข้อมูล



แผนการใช้ระบบ RAID (RAID Implementation Plan)

รายการ	ระบบงาน	ประเภท RAID	จำนวน Disk	ความสามารถ	หมายเหตุ
1	Server HIS	RAID 5	4 ลูก (3+1 parity)	ทนต่อการเสียหาย 1 ลูกโดยไม่สูญเสียข้อมูล	รองรับ Hot-Swap
2	Server เอกสารเวชระเบียน	RAID 1 (Mirror)	2 ลูก (1 สำรอง)	ข้อมูลสำเนาทั้งแบบเรียลไทม์	ใช้ SSD
3	NAS สำรอง	RAID 10	4 ลูก (2+2)	เร็วและปลอดภัย (Speed + Redundancy)	ใช้จัดเก็บสำรองระยะกลาง

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.4 มีมาตรการหรือระบบป้องกันความเสียหายของข้อมูล และระบบ เช่น ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server ให้เหมาะสมกับความเสี่ยง

ตัวอย่าง บันทึกการตรวจสอบและบำรุงรักษาระบบสำรอง ที่รวมถึง UPS, RAID, Redundant Power Supply และ Redundant Server พร้อมผลการทดสอบในแต่ละรอบ

วันที่ตรวจสอบ	ระบบที่ตรวจสอบ	รายละเอียดการตรวจสอบ	สถานะ	ผลการทดสอบ	ผู้ตรวจสอบ
10 มี.ค. พ.ศ. 2568	UPS Server HIS	ตรวจสอบแรงดันไฟฟ้าสำรอง + แบตเตอรี่	ปกติ	สำรองไฟได้ 22 นาที	IT Support
15 มี.ค. พ.ศ. 2568	RAID 5 Storage (HIS)	เช็คสถานะ RAID ผ่านซอฟต์แวร์	ปกติ	Healthy – ไม่มี Disk เสีย	System Admin
20 มี.ค. พ.ศ. 2568	Redundant Power Supply	ทดสอบสลับแหล่งจ่ายไฟ (Main → Backup)	สำเร็จ	ระบบไม่ดับ, แจ้งเตือน Active	ช่างเทคนิค
25 มี.ค. พ.ศ. 2568	Redundant Server	จำลอง Server หลักลุ่ม, ทดสอบ Failover	สำเร็จ	Server สำรองทำงานภายใน 2 นาที	หัวหน้า IT
10 มี.ย. พ.ศ. 2568	UPS Server HIS	ทดสอบการสำรองไฟแบบเต็มโหลด	ผ่าน	สามารถรองรับโหลด 95% ได้ 20 นาที	IT Support
15 มี.ย. พ.ศ. 2568	RAID 1 (Mirror)	ถอด Disk 1 แล้วทดสอบ Rebuild	สำเร็จ	Rebuild ภายใน 1 ชม. ข้อมูลไม่สูญหาย	System Admin

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.5 มีระบบเฝ้าระวัง และรักษาความมั่นคงปลอดภัยทางกายภาพ Data Center ของหน่วยงาน

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี ระบบเฝ้าระวังหรือระบบรักษาความปลอดภัยทางกายภาพ เช่น ไม่มีการติดตั้งกล้องวงจรปิดหรือไม่มีเจ้าหน้าที่รักษาความปลอดภัย
0.5	มีระบบเฝ้าระวังบางประเภท เช่น กล้องวงจรปิดหรือสัญญาณเตือนผู้บุกรุก แต่ไม่มีการติดตั้งครบถ้วนในทุกพื้นที่ที่สำคัญ หรือไม่มีการตรวจสอบระบบอย่างสม่ำเสมอ
1	มี ระบบเฝ้าระวังที่ครบถ้วนและมีประสิทธิภาพ เช่น กล้องวงจรปิด หรือระบบสัญญาณเตือนผู้บุกรุก หรือ เจ้าหน้าที่รักษาความปลอดภัย หรือซอฟต์แวร์การบริหารจัดการความปลอดภัยทางกายภาพที่ครอบคลุมพื้นที่ทั้งหมดที่มีความสำคัญ และพร้อมการตรวจสอบบำรุงรักษาอย่างสม่ำเสมอ

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1.แผนการติดตั้งและการใช้ระบบเฝ้าระวัง (Surveillance System Installation Plan) : เอกสารที่แสดงถึงการติดตั้งระบบเฝ้าระวัง เช่น กล้องวงจรปิด, สัญญาณเตือนผู้บุกรุก, หรือซอฟต์แวร์ที่ใช้ในการบริหารจัดการระบบรักษาความปลอดภัย
 - 2.รายงานการติดตั้งกล้องวงจรปิด (CCTV Installation Report) : รายงานที่แสดงรายละเอียดการติดตั้งกล้องวงจรปิด เช่น จำนวนกล้อง, ตำแหน่งการติดตั้ง, การเชื่อมต่อกับระบบบริหารจัดการ และการตั้งค่า
 - 3.บันทึกการตรวจสอบระบบเฝ้าระวัง (Surveillance System Inspection Logs) : บันทึกที่แสดงการตรวจสอบและการบำรุงรักษาระบบเฝ้าระวัง เช่น การตรวจสอบกล้องวงจรปิด, สัญญาณเตือนภัย, และอุปกรณ์รักษาความปลอดภัยอื่น ๆ
 - 4.รายงานการทดสอบระบบเฝ้าระวัง (Surveillance System Testing Report) : รายงานที่แสดงผลการทดสอบระบบเฝ้าระวัง เช่น การทดสอบการทำงานของกล้องวงจรปิด, ระบบสัญญาณเตือนภัย, และซอฟต์แวร์ที่ใช้ในการจัดการความปลอดภัย

หมวดที่ 5 การรักษาความปลอดภัยทางกายภาพ และทางสภาพแวดล้อมของ DATA CENTER

CS.5.5 มีระบบเฝ้าระวัง และรักษาความมั่นคงปลอดภัยทางกายภาพ Data Center ของหน่วยงาน

1.นโยบายการรักษาความปลอดภัยห้อง Data Center อย่างเป็นลายลักษณ์อักษร

มาตรการรักษาความปลอดภัยทางกายภาพ Data Center
ระบบที่ควรมี (อย่างน้อย 1-2 ระบบขึ้นไป)



ระบบ	รายละเอียด	จุดประสงค์
 CCTV (กล้องวงจรปิด)	ติดตั้งอย่างน้อย 2 จุด (ภายใน-นอกห้อง) + บันทึกย้อนหลัง ≥ 30 วัน	เฝ้าระวังบุคคลที่เข้า-ออก
 Motion / Intrusion Sensor	ตรวจจับการเคลื่อนไหวผิดปกติ + ส่งเสียงเตือน/แจ้งผ่านระบบ	ป้องกันบุคคลไม่ได้รับอนุญาต
 เจ้าหน้าที่รักษาความปลอดภัย / เวกกลาง	ดูแลพื้นที่ห้อง Server ในช่วงเวลานอกเวลาทำการ	เพิ่มชั้นความปลอดภัย
 บันทึกการเข้า-ออก (Manual หรือ Digital Log)	มีสมุดเซ็นเข้าออก / ระบบสแกนบัตร	ย้อนตรวจสอบได้ว่าผู้ใดเข้าเมื่อใด
 อุปกรณ์ดับเพลิง + ระบบไฟฟ้าฉุกเฉิน	ครอบคลุมสถานการณ์ไฟไหม้/ไฟดับ	เพิ่มความมั่นคงปลอดภัยสถานที่

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.1 จัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) อย่างน้อยปีละ 1 ครั้ง
โดยมีผู้ตรวจสอบภายใน หรือ ภายนอกที่มีความรู้ความสามารถ และจัดทำรายงานผลต่อผู้บริหารที่เกี่ยวข้อง

CS.6.2 จัดให้มีแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) และแจ้งผู้เกี่ยวข้องรับทราบ

CS.6.3 มีการฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (INCIDENT RESPONSE PLAN) อย่างน้อยปีละ 1 ครั้ง
หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ



หมวดที่ 6: การตรวจสอบและแผนรับมือ (Audit & Incident Response)

The Check (การตรวจสอบ)



CS.6.1 Cybersecurity
Audit (ตรวจสอบประจำปี)

The Response (การรับมือ)



CS.6.2 Incident Response
Plan (IRP) - แผนรับมือที่เป็น
ลายลักษณ์อักษร

CS.6.3 Drills (การฝึกซ้อม
Tabletop Exercise)

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.1 จัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) อย่างน้อยปีละ 1 ครั้ง โดยมีผู้ตรวจสอบภายใน หรือ ภายนอกที่มีความรู้ความสามารถและจัดทำรายงานผลต่อผู้บริหารที่เกี่ยวข้อง

เป็นการประเมิน ความพร้อม ความปลอดภัย และจุดอ่อน ของระบบสารสนเทศในภาพรวม เพื่อใช้วางแผนพัฒนาและลดความเสี่ยง

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)
0.5	มี แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) แต่ขาดรายงานผลการดำเนินงานผลต่อผู้บริหารที่เกี่ยวข้อง
1	มี แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) อย่างน้อยปีละ 1 ครั้ง โดยมีผู้ตรวจสอบภายใน หรือ ภายนอกที่มีความรู้ความสามารถ และจัดทำรายงานผลต่อผู้บริหารที่เกี่ยวข้อง

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. เอกสารแผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) รายละเอียด เช่น รายละเอียดขอบเขตการตรวจสอบ (Audit Scope) รายชื่อผู้ตรวจสอบและคุณสมบัติของผู้ตรวจสอบ (Auditor Credentials) ตารางเวลาการตรวจสอบ (Audit Schedule) เป็นต้น
 - 2. รายงานผลการตรวจสอบ (Audit Report) รายละเอียด เช่น รายงานการประเมินความเสี่ยง (Risk Assessment Report) รายงานผลการตรวจสอบด้านเทคนิค (Penetration Test / Vulnerability Assessment Report) รายงานสรุปการตรวจสอบและข้อค้นพบ (Audit Findings Report) ข้อเสนอแนะและแผนแก้ไข (Recommendations & Remediation Plan) เป็นต้น

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.1 จัดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) อย่างน้อยปีละ 1 ครั้ง โดยมีผู้ตรวจสอบภายใน หรือ ภายนอกที่มีความรู้ความสามารถและจัดทำรายงานผลต่อผู้บริหารที่เกี่ยวข้อง

ตัวอย่าง แผนการตรวจสอบด้าน Cybersecurity (Cybersecurity Audit Plan)

ลำดับ	กิจกรรม	รายละเอียด	ช่วงเวลา	ผู้รับผิดชอบ
1	กำหนดทีมตรวจสอบและขอบเขต	แต่งตั้งคณะกรรมการ Audit หรือจ้าง Outsource และกำหนดสิ่งที่จะตรวจ เช่น Policy, Access Control, Backup	30 มิ.ย. ค.ศ. 2025	CIO / ผอ.รพ.
2	จัดประชุมเปิด Audit (Opening Meeting)	แจ้งเป้าหมาย ตรวจสอบข้อมูลพื้นฐาน และแบ่งงาน	30 มิ.ย. ค.ศ. 2025	Audit Team
3	เก็บรวบรวมเอกสารและตรวจสอบนโยบาย	ตรวจสอบนโยบายไซเบอร์, ระเบียบปฏิบัติ, Log, การอบรม	30 มิ.ย. ค.ศ. 2025	Auditor
4	ตรวจสอบระบบ IT และ Network	ตรวจสอบ Firewall, การตั้งค่าสิทธิ์, Antivirus, Backup	30 มิ.ย. ค.ศ. 2025	Auditor + IT Support
5	สัมภาษณ์บุคลากร	ประเมินความเข้าใจบุคลากรเกี่ยวกับ PDPA และภัยไซเบอร์	30 มิ.ย. ค.ศ. 2025	Auditor
6	สรุปผลตรวจสอบและจัดทำรายงาน	สรุปจุดแข็ง/จุดอ่อน/คำแนะนำ → ทำ Cybersecurity Audit Report	30 มิ.ย. ค.ศ. 2025	หัวหน้าทีม Audit
7	นำเสนอผลต่อผู้บริหาร	ประชุมเสนอรายงานผลและข้อเสนอแนะอย่างเป็นทางการ	30 มิ.ย. ค.ศ. 2025	CIO / ผอ.รพ.
8	จัดทำ Action Plan แก้ไขจุดอ่อน	แผนงานตอบสนองข้อเสนอแนะ เช่น ปรับนโยบาย, อบรมเพิ่ม	31 ก.ค. ค.ศ. 2025	ทีม IT + ผู้บริหาร

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.2 จัดให้มีแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) และแจ้งผู้เกี่ยวข้องรับทราบ

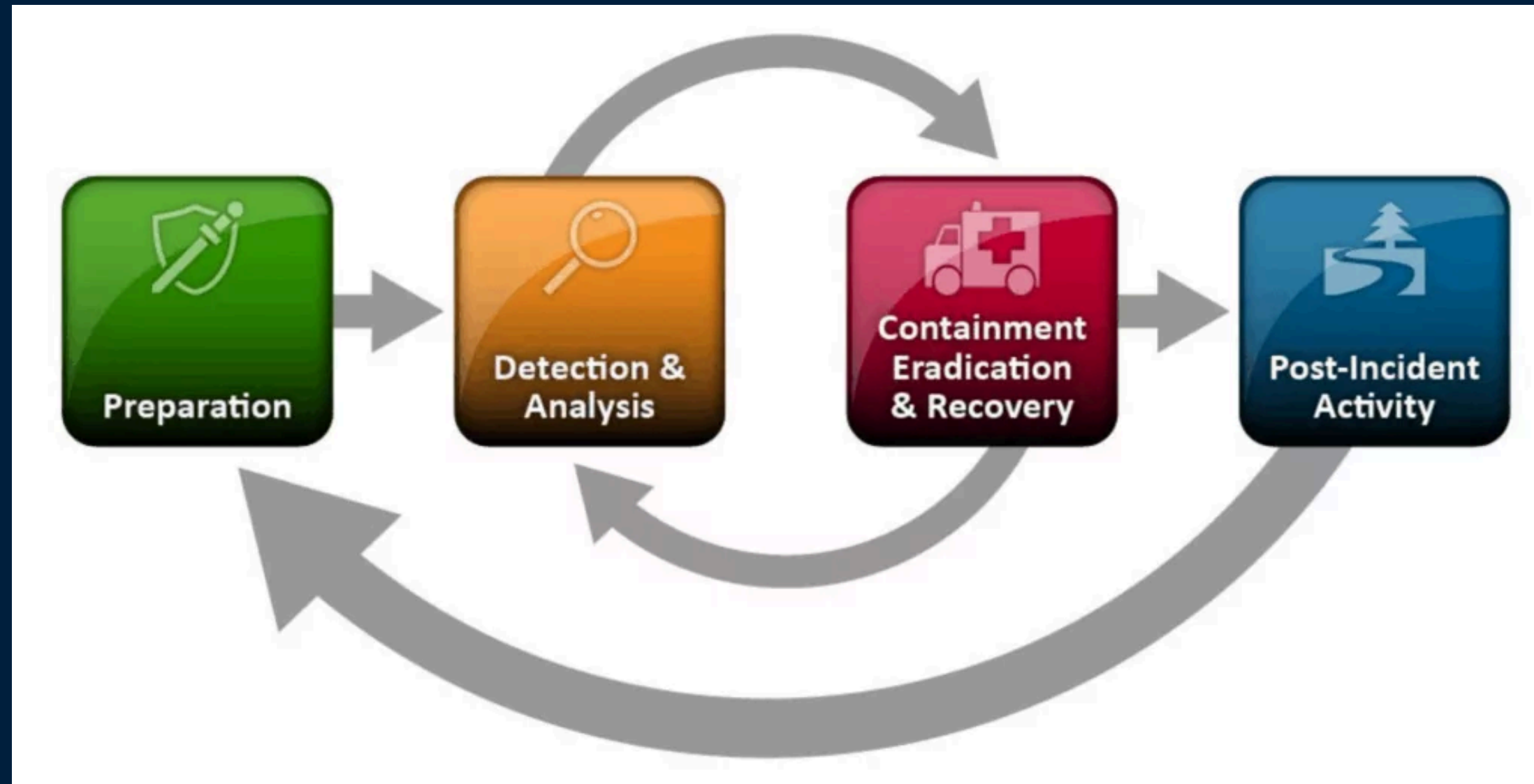
ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี แผนการรับมือ หรือแผนไม่ได้ถูกจัดทำเป็นเอกสาร
0.5	มี แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) โดยมีองค์ประกอบอย่างน้อยดังนี้ ช่องการติดต่อของผู้รับผิดชอบ หน่วยงานที่เกี่ยวข้อง และแจ้งผู้เกี่ยวข้องรับทราบ (มีอย่างใดอย่างหนึ่ง)
1	มี แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) โดยมีองค์ประกอบอย่างน้อยดังนี้ ช่องการติดต่อของผู้รับผิดชอบ หน่วยงานที่เกี่ยวข้อง และแจ้งผู้เกี่ยวข้องรับทราบ

เอกสารประกอบ/เอกสารตัวอย่าง

- 1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan - IRP) โดยมีองค์ประกอบอย่างน้อยดังนี้ ช่องการติดต่อของผู้รับผิดชอบ หน่วยงานที่เกี่ยวข้อง
- 2. หลักฐานการแจ้งหน่วยงานหรือเจ้าหน้าที่ที่เกี่ยวข้อง

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.2 จัดให้มีแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) และแจ้งผู้เกี่ยวข้องรับทราบ



วัตถุประสงค์:
เพื่อตรวจจับ แจ้งเตือน วิเคราะห์ และตอบสนองต่อ
เหตุการณ์ภัยคุกคามทางไซเบอร์อย่างรวดเร็ว
ลดผลกระทบต่อข้อมูลผู้ป่วย ระบบบริการ และความเชื่อ
มั่นของประชาชน
เป็นไปตาม พ.ร.บ.ไซเบอร์ และแนวทาง ISO/IEC 27035
เป็นต้น

1. ขอบเขตของแผน (Scope)
ครอบคลุมภัยคุกคามทางไซเบอร์ต่อ:
ระบบ HIS, LIS, ฐานข้อมูลผู้ป่วย
ระบบเครือข่าย (Internet, Firewall, Switch)
อุปกรณ์พกพา (Laptop, USB, External HDD)
ช่องทางการสื่อสาร (Email, Web, Social Media)

เจาะลึกแผนรับมือภัยคุกคาม (Incident Response Plan - IRP)



Call Tree



Commander
ผู้สั่งการ



Tech Lead
หัวหน้าทีมเทคนิค



PR
ประชาสัมพันธ์



Legal
ฝ่ายกฎหมาย



Management
ผู้บริหาร

- **Communication:** ช่องทางติดต่อฉุกเฉิน (Call Tree)
- **Roles:** ระบุหน้าที่ชัดเจน
- **Drill:** ตัวอย่างการซ้อม Tabletop Exercise (Ransomware)

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

1. ขอบเขตของแผน (Scope)
ครอบคลุมภัยคุกคามทางไซเบอร์ต่อ:
ระบบ HIS, LIS, ฐานข้อมูลผู้ป่วย
ระบบเครือข่าย (Internet, Firewall, Switch)
อุปกรณ์พกพา (Laptop, USB, External HDD)
ช่องทางการสื่อสาร (Email, Web, Social Media)

2. ขั้นตอนการตอบสนองเหตุการณ์ (Incident Response Lifecycle)

ขั้นตอน	รายละเอียด	เครื่องมือ/ผู้รับผิดชอบ
ตรวจจับ (Detection)	ระบบแจ้งเตือน, ผู้ใช้รายงานเหตุผิดปกติ	Firewall, Antivirus, Helpdesk
วิเคราะห์ (Analysis)	ตรวจสอบ Log, IP, ลักษณะภัย, ความรุนแรง	IT Security, DPO
แจ้งเหตุ (Notification)	แจ้งหัวหน้า IT, ผอ., DPO และผู้เกี่ยวข้อง	แบบฟอร์ม IR-01 / Email
ควบคุมเหตุ (Containment)	แยกเครื่อง/ระบบที่ถูกโจมตี, ปิดพอร์ต	System Admin
กู้คืน (Recovery)	ใช้ Backup / Restore / Patch ช่องโหว่	IT Support
รายงานเหตุการณ์ (Reporting)	สรุปเหตุการณ์, สาเหตุ, ผลกระทบ, แนวทางแก้ไข	เจ้าหน้าที่ IT
ปรับปรุงแผน (Review)	ทบทวนแผน IRP, แจ้งบทเรียนให้ทีมงาน	ทีมความมั่นคงไซเบอร์

3. ช่องทางแจ้งเหตุ และผู้รับแจ้งเหตุ
Hotline IT: 09x-xxx-xxxx
Email: itincident@hospital.go.th
แบบฟอร์มแจ้งเหตุ: IR-01 (มีในเว็บไซต์อินเทอร์เน็ต)
ผู้รับแจ้งหลัก: หัวหน้า IT / ผู้ประสาน IRP

4. รายชื่อผู้เกี่ยวข้องในแผน IRP (Contact List)

5. การแจ้งและรับทราบแผน
แจ้งแผนผ่าน:
✓ Email ภายใน
✓ ป้ายประกาศแผน IRP หน้าห้อง IT
✓ แนบในคู่มือพนักงานใหม่
ผู้รับผิดชอบทุกคน ลงชื่อรับทราบ แผนในแบบฟอร์ม IRP-Acceptance

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)
และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.3 มีการฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง
หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

เพื่อให้หน่วยงาน พร้อมตอบสนองเหตุการณ์ไซเบอร์จริง โดยไม่เกิดความสับสน และมีการปรับปรุงแผนให้ทันสมัย

ระดับคะแนน	แนวทางการประเมิน
0	ไม่มี การฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง
0.5	มี การฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง
1	มี การฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานเสนอต่อผู้บริหาร

- เอกสารประกอบ/เอกสารตัวอย่าง
- 1. รายงานการทดสอบแผนรับมือภัยคุกคาม (Incident Response Testing & Drills) เช่น รายงานการทดสอบแผน (Tabletop Exercise / Simulation Report) , หลักฐานการทบทวนแผน และการปรับปรุง (Plan Review & Improvement Log)
 - 2.แนวทางปรับปรุงเพื่อป้องกันเหตุการณ์ในอนาคต (Preventive Measures & Remediation Plan)

หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.3 มีการฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

ตัวอย่างรูปแบบการฝึกซ้อมที่แนะนำ

รูปแบบ	รายละเอียด	เหมาะกับ
✓ Tabletop Exercise (จำลองเหตุการณ์บนโต๊ะ)	อภิปรายและจำลองบทบาทกรณีภัยคุกคาม (เช่น Ransomware, ข้อมูลรั่ว)	โรงพยาบาลขนาดเล็ก-กลาง
✓ Simulation (สถานการณ์จำลองจริง)	ส่ง Email Phishing, ถอดสาย/ปิดระบบจำลอง	โรงพยาบาลที่มีระบบ IT ทีมพร้อม
✓ Incident Drill ร่วมกับหน่วยอื่น	ร่วมกับ สสจ., กสทช., กสท., บริษัท IT	หน่วยงาน CII หรือขนาดใหญ่



หมวดที่ 6 การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan) และแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

CS.6.3 มีการฝึกซ้อม และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

ตัวอย่างการฝึกซ้อม

ขั้นตอน	รายละเอียด
1. เตรียมสถานการณ์	เช่น ข้อมูลवेชระเบียนร้ວบน Facebook, Server ຄູກ Ransomware
2. ຣະບຸກລຸ່ມເປົ້າໝາຍ	IT, DPO, ຫຼັກໜ້າແຜນກ, ເຈົ້າໜ້າທີ່ເວກ
3. ຝຶກບທບາທຕາມແຜນ IRP	ແຈ້ງເຫຕຸ, ກັກກັນຣະບບ, ຣາຍງານ, ຟື້ນຟູ
4. ເກັບ Log ການຂ້ອມ	ເວລາແຈ້ງ, ເວລາແກ້ໄຂ, ປັນຫາທີ່ພບ
5. ທບທວນ + ປຸ້ງປຸ້ງແຜນ	ວິເຄາະຫໍ່ສິ່ງທີ່ໄດ້ເຮັດຮູ້, ແກ້ໄຂ IRP

ตัวอย่างสรุปรายงานการฝึกซ้อม (ย่อ)

สถานการณ์: การรั่วไหลของข้อมูลवेชระเบียนจากอีเมลผิดผู้รับ
วันที่ฝึก: 15 พ.ค. 2568
ผู้เกี่ยวข้อง: IT, DPO, ຫຼັກໜ້າເວชระเบียน, ພອ.
เวลาแจ้งเหตุ – ແກ້ໄຂ: 9.02 ນ. – 9.37 ນ. (ภายใน 35 นาที)
ข้อค้นพบ: ບຸກລາກຣບາກກນໄມ່ທຣາບຂ່ອງທາງແຈ້ງເຫຕຸ / ຂາດແບບ ຟອຣ໌ມ IR-01
แนวทางปรับปรุง: ເພີ່ມປ້າຍ QR ແຈ້ງເຫຕຸໜ້າແຜນກເວชระเบียน + ຈັດອບຣມເສຣີມໃນ Q3

ความปลอดภัยไซเบอร์ คือความปลอดภัยของผู้ป่วย

- Resilience: ระบบพร้อมใช้งาน
- Trust: ประชาชนเชื่อมั่น
- Compliance: สอดคล้องตามกฎหมาย

การรักษาความมั่นคงปลอดภัยไซเบอร์ไม่ใช่
‘ทางเลือก’ แต่เป็น ‘หน้าที่’ ของ
สถานพยาบาลยุคดิจิทัล

ช่องทางการติดต่อสอบถาม

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมสนับสนุนบริการสุขภาพ
โทร 021937000 ต่อ 18206



Line id :@191zmgwi

อ้างอิง

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

มาตรฐาน ISO/IEC 27001

มาตรฐาน ISO 31000:2018 –Risk Management Guidelines

มาตรฐาน ISO/IEC 27005:2018 –Information Security Risk Management



กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support



Thank You

For Your Attention

