IT RISK MANAGEMENT 2026

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ประจำปี 2569

งานเทคโนโลยีสารสนเทศ ศูนย์สุขภาพจิตที่ 4

สารบัญ

บทที่ 1
บทนำและบริบทองค์กร
(Introduction and Organizational Context)

1.1 ความเป็นมาและความสำคัญ (Background and Significance)

ศูนย์สุขภาพจิตที่ 4 ตระหนักถึงบทบาทของเทคโนโลยีดิจิทัลในการขับเคลื่อนภารกิจด้านสุขภาพจิตให้มีประสิทธิภาพ โปร่งใส และตอบสนองต่อความต้องการของผู้รับบริการและผู้มีส่วนได้ส่วนเสียได้อย่างเหมาะสม ทั้งในมิติการบริหารจัดการข้อมูล การให้บริการเชิงระบบ การติดตามเฝ้าระวัง และการสื่อสารองค์ความรู้แก่ประชาชน

เพื่อให้การใช้เทคโนโลยีสารสนเทศเป็นไปอย่างมีธรรมาภิบาล สามารถบริหารจัดการความไม่แน่นอนและเหตุการณ์ที่อาจก่อให้เกิดผลกระทบต่อภารกิจหลักได้อย่างเป็นระบบ ศูนย์สุขภาพจิตที่ 4 จึงจัดทำ “แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2569” ขึ้น เพื่อใช้เป็นกรอบแนวทางการระบุ วิเคราะห์ ประเมิน และกำหนดมาตรการจัดการความเสี่ยง ตลอดจนการติดตามประเมินผลอย่างต่อเนื่อง อันจะช่วยลดโอกาสเกิดเหตุการณ์ไม่พึงประสงค์และลดความรุนแรงของผลกระทบที่อาจเกิดขึ้นกับระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล และข้อมูลสำคัญของหน่วยงาน

แผนฉบับนี้มุ่งเน้นการดำเนินงานให้สอดคล้องกับหลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance) และแนวทางการบริหารความเสี่ยงที่เหมาะสม เพื่อสนับสนุนการดำเนินภารกิจของหน่วยงานให้มีความต่อเนื่อง มีเสถียรภาพ และเกิดความยั่งยืนในระยะยาว

1.2 บริบทองค์กร (Organizational Context)

ศูนย์สุขภาพจิตที่ 4 มีบทบาทสำคัญในการขับเคลื่อนงานสุขภาพจิตเชิงระบบของพื้นที่รับผิดชอบผ่านการใช้ระบบสารสนเทศและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนการบริหารจัดการ การรายงานข้อมูล และการให้บริการที่มีคุณภาพ โดยบริบทที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ สามารถสรุปได้ดังนี้

1.2.1 พันธกิจด้านดิจิทัล (Digital Mission)

หน่วยงานมุ่งเน้นการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการเฝ้าระวังและติดตามสถานการณ์สุขภาพจิต การจัดเก็บและรายงานข้อมูลอย่างเป็นระบบ รวมถึงการสื่อสารและเผยแพร่ความรอบรู้ด้านสุขภาพจิตแก่ประชาชนและเครือข่ายทั้งในและนอกระบบสาธารณสุข เพื่อให้การดำเนินงานมีความทันสมัย เข้าถึงได้ และตอบสนองต่อสถานการณ์ได้อย่างทันท่วงที

1.2.2 สภาพแวดล้อมภายใน (Internal Environment)

หน่วยงานมีการใช้ระบบฐานข้อมูลกลางและระบบบริหารงานภายใน ซึ่งต้องรองรับการเข้าถึงจากบุคลากรหลายส่วนงานและหลายระดับสิทธิ์การใช้งาน จึงจำเป็นต้องมีการกำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม ครอบคลุมการกำหนดสิทธิ์ผู้ใช้งาน การจัดการบัญชีผู้ใช้ การสำรองข้อมูล การจัดเก็บข้อมูลจราจรคอมพิวเตอร์และบันทึกเหตุการณ์ (Log Files) และการดูแลความพร้อมใช้งานของระบบอย่างต่อเนื่อง

1.2.3 สภาพแวดล้อมภายนอก (External Environment)

ภายใต้บริบทที่ประชาชนและผู้รับบริการให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ประกอบกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มสูงขึ้น ทั้งในรูปแบบการโจมตีระบบ การหลอกลวงทางอิเล็กทรอนิกส์ และมัลแวร์ หน่วยงานจึงมีความจำเป็นต้องยกระดับมาตรการป้องกันและการเฝ้าระวังให้ทันต่อสถานการณ์ รวมถึงพัฒนากระบวนการตอบสนองเหตุการณ์และการฟื้นฟูระบบให้มีประสิทธิภาพ

1.3 วัตถุประสงค์ (Objectives)

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2569 มีวัตถุประสงค์เพื่อ

1.3.1 ระบุ วิเคราะห์ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบต่อภารกิจหลักของศูนย์สุขภาพจิตที่ 4

1.3.2 กำหนดมาตรการควบคุมและแนวทางจัดการความเสี่ยงให้มีประสิทธิผล และทำให้ความเสี่ยงอยู่ในระดับที่หน่วยงานยอมรับได้ (Risk Appetite)

1.3.3 เสริมสร้างความตระหนักรู้และวัฒนธรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรทุกระดับ เพื่อให้เกิดการปฏิบัติอย่างต่อเนื่องและเป็นมาตรฐานเดียวกัน

1.3.4 สร้างความเชื่อมั่นแก่ผู้รับบริการและผู้มีส่วนได้ส่วนเสียว่า หน่วยงานมีมาตรการด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลที่เหมาะสม สามารถสนับสนุนการดำเนินงานได้อย่างต่อเนื่องและน่าเชื่อถือ

1.4 ขอบเขตการดำเนินงาน (Scope)

แผนบริหารความเสี่ยงฉบับนี้ครอบคลุมทรัพยากรด้านเทคโนโลยีสารสนเทศที่อยู่ภายใต้การกำกับดูแลของศูนย์สุขภาพจิตที่ 4 โดยแบ่งเป็น 3 ด้านหลัก ดังนี้

1.4.1 ด้านซอฟต์แวร์และข้อมูล (Software and Data)

ครอบคลุมเว็บไซต์องค์กร ระบบฐานข้อมูลด้านสุขภาพจิต ระบบสารสนเทศเพื่อการรายงาน/เฝ้าระวัง และซอฟต์แวร์ประยุกต์ที่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน รวมถึงข้อมูลสำคัญที่จัดเก็บและประมวลผลในระบบดังกล่าว

1.4.2 ด้านโครงสร้างพื้นฐานและเครือข่าย (Infrastructure and Network)

ครอบคลุมระบบเครือข่ายภายใน (LAN/WiFi) อุปกรณ์เครือข่ายและอุปกรณ์เชื่อมต่อ ตลอดจนองค์ประกอบที่เกี่ยวข้องกับความพร้อมใช้งานของระบบ เช่น ระบบสำรองไฟ การสำรองข้อมูล และการรักษาความปลอดภัยของอุปกรณ์

1.4.3 ด้านบุคลากรและการใช้งาน (People and Usage)

ครอบคลุมพฤติกรรมและแนวปฏิบัติของเจ้าหน้าที่ภายในหน่วยงานในการใช้งานระบบและอุปกรณ์เทคโนโลยีสารสนเทศ เช่น การกำหนดรหัสผ่าน การใช้อีเมลและอินเทอร์เน็ต การจัดการไฟล์ข้อมูล การกำหนดสิทธิ์การเข้าถึงระบบ และการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

1.5 นิยามศัพท์เฉพาะ (Definitions)

เพื่อให้การดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปในทิศทางเดียวกัน หน่วยงานกำหนดนิยามศัพท์เฉพาะที่ใช้ในเอกสารฉบับนี้ ดังต่อไปนี้

1.5.1 ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือสถานการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงาน โดยพิจารณาจาก “โอกาสเกิด” และ “ผลกระทบ”

1.5.2 การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการระบุ วิเคราะห์ ประเมิน จัดการ ติดตาม และทบทวนความเสี่ยงอย่างเป็นระบบ เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

1.5.3 โอกาสเกิด (Likelihood) หมายถึง ความถี่หรือความน่าจะเป็นที่เหตุการณ์ความเสี่ยงจะเกิดขึ้นในช่วงเวลาที่กำหนด

1.5.4 ผลกระทบ (Impact) หมายถึง ระดับความรุนแรงของผลเสียหายที่เกิดกับภารกิจ การให้บริการ ข้อมูล ทรัพย์สิน หรือชื่อเสียงของหน่วยงาน หากเหตุการณ์ความเสี่ยงเกิดขึ้น

1.5.5 มาตรการควบคุม (Control) หมายถึง มาตรการ กระบวนการ หรือแนวปฏิบัติที่จัดให้มีเพื่อป้องกัน ลด หรือควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

1.5.6 เจ้าของความเสี่ยง (Risk Owner) หมายถึง ผู้รับผิดชอบหลักในการกำกับดูแล ติดตาม และดำเนินมาตรการจัดการความเสี่ยงในประเด็นที่ได้รับมอบหมาย

1.5.7 ความเสี่ยงคงเหลือ (Residual Risk) หมายถึง ระดับความเสี่ยงที่ยังคงอยู่หลังจากได้ดำเนินมาตรการควบคุมแล้ว

1.5.8 ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite/Tolerance) หมายถึง ระดับความเสี่ยงที่หน่วยงานยินยอมให้คงอยู่ได้ โดยพิจารณาตามเกณฑ์ที่กำหนด เพื่อไม่ให้กระทบต่อภารกิจหลักและความเชื่อมั่นของผู้รับบริการ

1.5.9 ความมั่นคงปลอดภัยสารสนเทศ (Information Security) หมายถึง การคุ้มครองข้อมูลและระบบสารสนเทศให้มีความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) อย่างเหมาะสม รวมถึงการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

บทที่ 2
หลักเกณฑ์และกระบวนการบริหารจัดการความเสี่ยง
(Risk Management Criteria and Process)

เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์สุขภาพจิตที่ 4 เป็นไปอย่างเป็นระบบ มีมาตรฐานเดียวกัน สามารถเปรียบเทียบผลการประเมินในแต่ละรอบการติดตามได้อย่างถูกต้อง และเอื้อต่อการตัดสินใจเชิงบริหาร หน่วยงานจึงกำหนด “หลักเกณฑ์การประเมินความเสี่ยง” และ “กระบวนการดำเนินงาน” ตามแนวทางการบริหารความเสี่ยงที่เหมาะสมกับบริบทของหน่วยงาน ดังรายละเอียดต่อไปนี้

2.1 กระบวนการบริหารความเสี่ยง (Risk Management Process)

ศูนย์สุขภาพจิตที่ 4 กำหนดกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ครอบคลุม 5 ขั้นตอนหลัก เพื่อให้เกิดการดำเนินงานอย่างต่อเนื่องและตรวจสอบได้ ดังนี้

ภาพที่ 1 แสดงกระบวนการบริหารความเสี่ยง

2.1.1 การระบุปัจจัยเสี่ยง (Event Identification)

ดำเนินการรวบรวมและวิเคราะห์เหตุการณ์/ปัจจัยที่อาจก่อให้เกิดความเสี่ยงต่อการบรรลุเป้าหมายและภารกิจของหน่วยงาน โดยพิจารณาจากแหล่งที่มาความเสี่ยงทั้งภายในและภายนอก เช่น ระบบสารสนเทศ โครงสร้างพื้นฐาน บุคลากร กระบวนการทำงาน และผู้ให้บริการภายนอก รวมถึงบทเรียนจากเหตุการณ์ที่ผ่านมา

2.1.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

วิเคราะห์ระดับความเสี่ยงโดยพิจารณา“โอกาสเกิด (Likelihood)”และ“ผลกระทบ (Impact)” ตามเกณฑ์ที่กำหนด เพื่อให้สามารถจัดลำดับความสำคัญของความเสี่ยงได้อย่างเหมาะสมและสอดคล้องกับสภาพจริงของหน่วยงาน

2.1.3 การจัดการความเสี่ยง (Risk Response / Risk Treatment)

กำหนดมาตรการควบคุมและแผนการจัดการความเสี่ยง โดยเลือกกลยุทธ์ที่เหมาะสม เช่น การลด/ควบคุม การโอนย้าย การหลีกเลี่ยง หรือการยอมรับความเสี่ยง พร้อมกำหนดผู้รับผิดชอบ ระยะเวลาดำเนินการ และผลลัพธ์ที่คาดหวัง เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

2.1.4 การติดตามและรายงานผล (Monitoring and Reporting)

ติดตามความก้าวหน้าการดำเนินมาตรการ รวมถึงประเมินประสิทธิผลของการควบคุมความเสี่ยงอย่างต่อเนื่อง โดยจัดทำรายงานสถานะความเสี่ยง (Risk Status Report) เสนอผู้บริหารตามรอบระยะเวลาที่กำหนด และปรับมาตรการเมื่อพบความเสี่ยงมีแนวโน้มเพิ่มสูงขึ้นหรือเกิดเหตุการณ์ผิดปกติ

2.1.5 การทบทวนความเสี่ยง (Risk Review)

ทบทวนความเหมาะสมของทะเบียนความเสี่ยง เกณฑ์ประเมิน และมาตรการควบคุมตามวงรอบเวลา (อย่างน้อยปีละ 1 ครั้ง หรือเมื่อเกิดการเปลี่ยนแปลงสำคัญ) เพื่อให้แผนบริหารความเสี่ยงมีความทันสมัย สอดคล้องกับบริบท และรองรับสถานการณ์ที่เปลี่ยนแปลงได้อย่างมีประสิทธิภาพ

2.2 เกณฑ์การประเมินความเสี่ยง (Risk Assessment Criteria)

การประเมินความเสี่ยงของหน่วยงานใช้เกณฑ์ผสมผสานทั้งเชิงคุณภาพและเชิงปริมาณ โดยกำหนดระดับคะแนน “โอกาสเกิด” และ “ผลกระทบ” เป็น 5 ระดับ เพื่อให้การประเมินมีมาตรฐานเดียวกันและสามารถเทียบเคียงกันได้ในทุกประเด็นความเสี่ยง

2.2.1 เกณฑ์โอกาสที่จะเกิดความเสี่ยง (Likelihood Score)

ระดับ	โอกาสที่จะเกิด	คำอธิบายเกณฑ์เชิงความถี่
5	สูงมาก	มีเหตุการณ์เกิดขึ้นมากกว่า 5 ครั้งต่อปี
4	สูง	มีเหตุการณ์เกิดขึ้นประมาณ 4 ครั้งต่อปี
3	ปานกลาง	มีเหตุการณ์เกิดขึ้นประมาณ 3 ครั้งต่อปี
2	น้อย	มีเหตุการณ์เกิดขึ้นประมาณ 2 ครั้งต่อปี
1	น้อยมาก	มีเหตุการณ์เกิดขึ้นไม่เกิน 1 ครั้งต่อปี หรือไม่เคยเกิด

2.2.2 เกณฑ์ผลกระทบของความเสี่ยง (Impact Score)

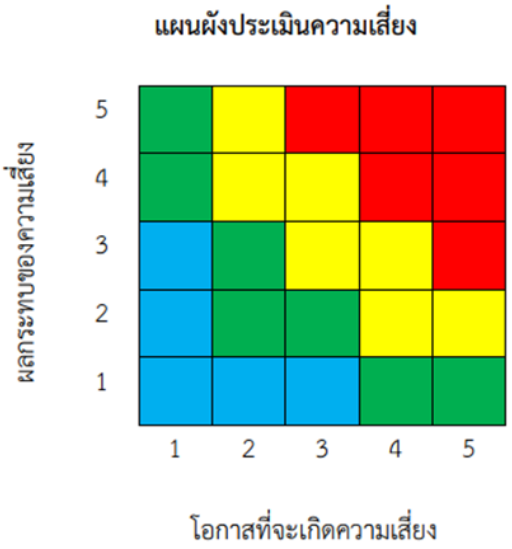
ระดับ	ความรุนแรง	คำอธิบายความเสียหาย (ด้านการดำเนินงาน/การเงิน)
5	สูงมาก	ระบบสำคัญหยุดทำงานทั้งหมด / เกิดเหตุข้อมูลรั่วไหลร้ายแรง / ความเสียหายมากกว่า 10 ล้านบาท
4	สูง	ระบบสำคัญขัดข้องบางส่วน / ข้อมูลผิดพลาดกระทบการตัดสินใจ / ความเสียหาย 500,000 – 10,000,000 บาท
3	ปานกลาง	ระบบขัดข้องแต่ยังมีระบบ/วิธีสำรองให้บริการได้บางส่วน / ความเสียหายมากกว่า 250,000 – 500,000 บาท
2	น้อย	เกิดเหตุขัดข้องเล็กน้อย แก้ไขได้ภายในระยะเวลาอันสั้น / ความเสียหาย 100,000 – 250,000 บาท
1	น้อยมาก	เหตุขัดข้องไม่มีนัยสำคัญ หรือกระทบจำกัดวง / ความเสียหายไม่เกิน 100,000 บาท

2.3 การประเมินระดับความเสี่ยง (Risk Matrix)

เพื่อให้การจัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์สุขภาพจิตที่ 4 เป็นไปอย่างเป็นมาตรฐาน สื่อสารได้ชัดเจน และใช้ประกอบการตัดสินใจเชิงบริหารได้อย่างเหมาะสม หน่วยงานกำหนดให้การประเมิน “ระดับความเสี่ยง” คำนวณจากคะแนนความเสี่ยง (Risk Score) ตามสูตรดังนี้

คะแนนความเสี่ยง (Risk Score) = โอกาสเกิด (L) × ผลกระทบ (I)

โดยกำหนดค่า L และ I ตามเกณฑ์ระดับคะแนน 5 ระดับในหัวข้อ 2.2 ทั้งนี้ เมื่อคำนวณคะแนนความเสี่ยงแล้ว หน่วยงานใช้ แผนผังประเมินความเสี่ยง (Risk Matrix 5×5) เพื่อแปลผลระดับความเสี่ยงตามช่วงคะแนนและสีมาตรฐาน ดังแสดงในภาพที่ 2



ภาพที่ 2 แผนผังประเมินความเสี่ยง (Risk Matrix 5×5)

ภาพที่ 2 แสดงความสัมพันธ์ระหว่าง “โอกาสที่จะเกิดความเสี่ยง (Likelihood)” และ “ผลกระทบของความเสี่ยง (Impact)” เพื่อใช้คำนวณและจำแนกระดับความเสี่ยงตามสีและช่วงคะแนนมาตรฐานของหน่วยงาน โดยกำหนดระดับความเสี่ยงเป็น 4 ระดับ ได้แก่ สีแดง (15–25) สีเหลือง (8–14) สีเขียว (4–7) และสีฟ้า (1–3)

2.3.1 การแปลผลระดับความเสี่ยงตามช่วงคะแนน (Risk Level Interpretation)

เพื่อให้การบริหารความเสี่ยงมีความชัดเจนและสอดคล้องกับระดับความเสี่ยงที่หน่วยงานยอมรับได้ (Risk Appetite) หน่วยงานกำหนดการแปลผลและแนวทางการดำเนินการตามช่วงคะแนน ดังนี้

(1) 15–25 คะแนน (สีแดง): ระดับความเสี่ยงสูง (High Risk)

- ความเสี่ยงอยู่ในระดับที่มีนัยสำคัญและอาจส่งผลกระทบต่อภารกิจหลักของหน่วยงาน
- ต้องกำหนดมาตรการจัดการ/แผนลดความเสี่ยงโดยเร่งด่วน ระบุผู้รับผิดชอบและกรอบเวลาอย่างชัดเจน
- รายงานผู้บริหารเพื่อพิจารณากำกับติดตามอย่างใกล้ชิด และทบทวนคะแนนความเสี่ยงซ้ำหลังดำเนินมาตรการ

(2) 8–14 คะแนน (สีเหลือง): ระดับความเสี่ยงค่อนข้างสูง (Moderately High Risk)

- ต้องจัดทำแผนจัดการความเสี่ยง (Risk Treatment Plan) และดำเนินมาตรการควบคุมเพิ่มเติมตามความเหมาะสม

- ติดตามความก้าวหน้าเป็นระยะ และรายงานผลตามรอบการติดตามที่กำหนดจนกว่าคะแนนความเสี่ยงจะลดลง

(3) 4–7 คะแนน (สีเขียว): ระดับความเสี่ยงค่อนข้างต่ำ (Moderately Low Risk)

- ให้ดำเนินมาตรการควบคุมพื้นฐาน/มาตรการเฝ้าระวัง เพื่อป้องกันไม่ให้ความเสี่ยงเพิ่มสูงขึ้น

- ติดตามสถานะตามรอบปกติ และทบทวนเมื่อมีการเปลี่ยนแปลงของระบบหรือกระบวนงานที่เกี่ยวข้อง

(4) 1–3 คะแนน (สีฟ้า): ระดับความเสี่ยงต่ำ (Low Risk)

- เป็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้

- ไม่จำเป็นต้องจัดทำแผนเพิ่มเติม แต่ให้คงมาตรการพื้นฐานและติดตามตามรอบการกำกับปกติ เพื่อให้มั่นใจว่าสถานการณ์ไม่เปลี่ยนแปลงไปในทิศทางที่เพิ่มความเสี่ยง

2.3.2 แนวปฏิบัติเพิ่มเติม (Operational Notes)

(1) กรณีความเสี่ยงที่เกี่ยวข้องกับ ข้อมูลส่วนบุคคล/ข้อมูลอ่อนไหว หรือมีผลกระทบต่อความเชื่อมั่นของผู้รับบริการ ให้พิจารณายกระดับการกำกับติดตามและรายงานผู้บริหารตามความเหมาะสม แม้คะแนนเชิงตัวเลขอยู่ในระดับปานกลาง

(2) เมื่อดำเนินมาตรการแล้ว ให้ประเมิน ความเสี่ยงคงเหลือ (Residual Risk) และบันทึกผลในทะเบียนความเสี่ยง (Risk Register) เพื่อใช้ในการติดตามและทบทวนตามวงรอบ

2.4 กลยุทธ์การตอบสนองความเสี่ยง (Risk Response Strategies)

ศูนย์สุขภาพจิตที่ 4 กำหนดแนวทางการตอบสนองความเสี่ยง 4 รูปแบบหลัก เพื่อให้หน่วยงานเลือกใช้ให้เหมาะสมกับลักษณะความเสี่ยง ต้นทุน และผลลัพธ์ที่คาดหวัง ดังนี้

2.4.1 การลด/ควบคุม (Treat / Mitigate)

ปรับปรุงระบบ กระบวนงาน หรือมาตรการควบคุม เพื่อ “ลดโอกาสเกิด” และ/หรือ “ลดผลกระทบ” ให้อยู่ในระดับที่ยอมรับได้

2.4.2 การยอมรับ (Take / Accept)

ยอมรับความเสี่ยงคงเหลือในกรณีที่ความเสี่ยงอยู่ในระดับต่ำหรือปานกลาง หรือกรณีที่ต้นทุนการควบคุมเพิ่มเติมไม่คุ้มค่าเมื่อเทียบกับผลประโยชน์ ทั้งนี้ต้องมีเหตุผลและผู้มีอำนาจอนุมัติชัดเจน

2.4.3 การโอนย้าย/แบ่งปัน (Transfer / Share)

โอนย้ายภาระหรือแบ่งปันความรับผิดชอบไปยังหน่วยงาน/ผู้ให้บริการภายนอก เช่น การจัดจ้างบริการบำรุงรักษา (MA) การใช้บริการ Cloud/Managed Service ภายใต้ข้อตกลงระดับการให้บริการ (SLA) หรือการทำประกันภัยที่เกี่ยวข้อง

2.4.4 การหลีกเลี่ยง (Terminate / Avoid)

ยกเลิกหรือปรับเปลี่ยนกิจกรรม/โครงการที่ก่อให้เกิดความเสี่ยงสูงเกินกว่าระดับที่หน่วยงานยอมรับได้ หรือไม่สามารถจัดการให้ลดลงได้ภายในกรอบทรัพยากรและข้อจำกัดที่มีอยู่

บทที่ 3
การระบุและการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT Risk Identification and Assessment)

ศูนย์สุขภาพจิตที่ 4 ได้ดำเนินการระบุและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยอาศัยกระบวนการตามที่กำหนดไว้ในบทที่ 2 ครอบคลุมการระบุปัจจัยเสี่ยง การวิเคราะห์โอกาสเกิด (Likelihood: L) และผลกระทบ (Impact: I) การคำนวณคะแนนความเสี่ยง (Risk Score = L×I) และการจัดระดับความเสี่ยงตามแผนผังประเมินความเสี่ยง (Risk Matrix) ทั้งนี้ กระบวนการดังกล่าวได้ดำเนินการโดยการระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานและผู้มีส่วนเกี่ยวข้อง (เช่น ผู้ดูแลระบบ เจ้าของระบบ/กระบวนงาน และผู้แทนส่วนงาน) ประกอบกับการพิจารณาข้อมูลเหตุการณ์ที่ผ่านมา เพื่อให้การประเมินมีความสอดคล้องกับบริบทและสภาพจริงของหน่วยงาน

เพื่อให้การนำเสนอมีความชัดเจนและครอบคลุม หน่วยงานได้จำแนกความเสี่ยงตามมิติของทรัพยากรและภัยคุกคามด้านเทคโนโลยีสารสนเทศ โดยเชื่อมโยงกับแนวคิดการจัดหมวดหมู่ความเสี่ยงในภาพรวมตามกรอบ COSO เพื่อสนับสนุนการกำกับติดตามและการกำหนดมาตรการจัดการความเสี่ยงได้อย่างเป็นระบบ

3.1 ผลการระบุปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Identification Results)

จากการพิจารณาบริบทการดำเนินงานและทรัพยากรสารสนเทศของศูนย์สุขภาพจิตที่ 4 หน่วยงานได้จำแนกประเด็นความเสี่ยงออกเป็น 5 มิติหลัก เพื่อให้ครอบคลุมองค์ประกอบด้านดิจิทัลทั้งหมด ดังนี้

3.1.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Risks)

เกี่ยวข้องกับความพร้อมของสถานที่ตั้งและสภาพแวดล้อมของห้องเครื่องแม่ข่าย (Server Room) เช่น อุณหภูมิ ความชื้น การระบายอากาศ ความปลอดภัยของพื้นที่ รวมถึงความเสี่ยงจากภัยธรรมชาติและอุบัติเหตุที่อาจกระทบต่อทรัพย์สินและความต่อเนื่องของระบบสารสนเทศ

3.1.2 ความเสี่ยงด้านอุปกรณ์และโครงสร้างพื้นฐาน (Hardware and Infrastructure Risks)

เกี่ยวข้องกับความขัดข้อง เสื่อมสภาพหรือการชำรุดของอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่ายและระบบสนับสนุน (เช่น ระบบไฟฟ้า) ซึ่งอาจส่งผลต่อความพร้อมใช้งานของระบบและบริการของหน่วยงาน

3.1.3 ความเสี่ยงด้านซอฟต์แวร์และข้อมูล (Software and Data Risks)

เกี่ยวข้องกับความถูกต้องครบถ้วนและความสมบูรณ์ของระบบฐานข้อมูล การสำรองและกู้คืนข้อมูล การจัดการเวอร์ชันของซอฟต์แวร์ รวมถึงความเสี่ยงด้านการละเมิดลิขสิทธิ์ซอฟต์แวร์ ซึ่งอาจนำไปสู่ผลกระทบด้านกฎหมาย ค่าใช้จ่าย และความน่าเชื่อถือของหน่วยงาน

3.1.4 ความเสี่ยงด้านบุคลากรและการเข้าถึง (People and Access Control Risks)

เกี่ยวข้องกับความรู้ความเข้าใจของผู้ใช้งานด้านการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย พฤติกรรมการใช้งาน การบริหารจัดการบัญชีผู้ใช้/รหัสผ่าน และการเข้าถึงข้อมูลตามสิทธิ์ (Access Control) ซึ่งหากไม่เหมาะสมอาจก่อให้เกิดการเข้าถึงข้อมูลโดยมิชอบหรือการรั่วไหลของข้อมูลสำคัญ

3.1.5 ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Threats)

เกี่ยวข้องกับการโจมตีจากผู้ไม่ประสงค์ดี เช่น มัลแวร์/ไวรัส การบุกรุกระบบ การโจมตีแบบหลอกลวงทางอิเล็กทรอนิกส์ และความเสี่ยงจากช่องโหว่ของระบบ ซึ่งอาจกระทบต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบ

3.2 ผลการวิเคราะห์และประเมินระดับความเสี่ยง (Risk Register – Inherent Risk Assessment)

หน่วยงานได้จัดทำทะเบียนความเสี่ยง (Risk Register) โดยประเมินค่าคะแนนความเสี่ยงจากโอกาสเกิด (L) และ ผลกระทบ (I) ตามเกณฑ์ในบทที่ 2 และคำนวณคะแนนความเสี่ยง (L×I) เพื่อจัดลำดับความสำคัญสำหรับการกำหนดมาตรการจัดการความเสี่ยงต่อไป ทั้งนี้ เพื่อความชัดเจนในการกำกับติดตามหน่วยงานกำหนดให้รหัสความเสี่ยง (Risk Code) เป็นรหัสอ้างอิงกลางในการรายงานและติดตามผล

เพื่อให้เกิดความชัดเจนทั้งในมิติการอ้างอิงและการตัดสินใจเชิงบริหาร หน่วยงานจัดทำผลการประเมินใน 2 รูปแบบ ได้แก่ (1) ทะเบียนความเสี่ยง (ตารางที่ 1) จัดเรียงตามรหัสความเสี่ยงเพื่อความสะดวกในการติดตามและรายงานผลอย่างต่อเนื่อง และ (2) ตารางสรุปลำดับความสำคัญของความเสี่ยง (ตารางที่ 2) จัดเรียงตามคะแนนความเสี่ยงจากสูงไปต่ำ เพื่อใช้ประกอบการกำหนดมาตรการจัดการความเสี่ยงและจัดสรรทรัพยากรอย่างเหมาะสม

ตารางที่ 1 ทะเบียนความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Register: Inherent Risk)

ลำดับ	ประเด็นความเสี่ยง	รหัส	L	I	คะแนน (L×I)	ระดับความเสี่ยง
1	ผู้ใช้งานขาดความรู้ในการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย	R01	5	4	20	สูงมาก
2	การเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ/เกินสิทธิ์ที่ได้รับอนุญาต	R02	5	5	25	สูงมาก
3	คอมพิวเตอร์/เครื่องแม่ข่ายขัดข้องหรือชำรุด	R03	3	5	15	สูงมาก
4	การถูกบุกรุกจากไวรัสหรือโปรแกรมประสงค์ร้าย (Malware)	R04	3	5	15	สูงมาก
5	อุณหภูมิและความชื้นห้องเครื่องแม่ข่าย (Server Room) ไม่เหมาะสม	R05	4	3	12	สูง
6	ระบบกระแสไฟฟ้าขัดข้อง/ไฟตก-ไฟดับกระทบระบบสารสนเทศ	R06	4	4	16	สูงมาก
7	การเชื่อมต่ออุปกรณ์ภายนอกที่ไม่ได้รับอนุญาต (เช่น USB/อุปกรณ์ส่วนตัว)	R07	5	2	10	สูง
8	ความเสียหายหรือสูญหายของฐานข้อมูลสำคัญ	R08	2	5	10	สูง
9	การติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง	R09	4	4	16	สูงมาก
10	ระบบเครือข่ายอินเทอร์เน็ตขัดข้อง	R10	2	4	8	สูง
11	ความเสียหายจากภัยธรรมชาติและอุบัติเหตุ	R11	1	5	5	ปานกลาง
12	สถานการณ์ความไม่สงบทางการเมือง/บ้านเมืองกระทบการดำเนินงาน	R12	1	4	4	ปานกลาง
13	การโจรกรรมอุปกรณ์คอมพิวเตอร์/ทรัพย์สินด้าน IT	R13	1	5	5	ปานกลาง

ตารางที่ 2 สรุปลำดับความสำคัญของความเสี่ยง (Priority Ranking) (Priority IT Risks Summary)

ลำดับความสำคัญ	ประเด็นความเสี่ยง	รหัส	L	I	คะแนน (LxI)	ระดับความเสี่ยง
1	การเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ/เกินสิทธิ์ที่ได้รับอนุญาต	R02	5	5	25	สูงมาก
2	ผู้ใช้งานขาดความรู้ในการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย	R01	5	4	20	สูงมาก
3	การติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง	R09	4	4	16	สูงมาก
4	ระบบกระแสไฟฟ้าขัดข้อง/ไฟตก-ไฟดับกระทบระบบสารสนเทศ	R06	4	4	16	สูงมาก
5	คอมพิวเตอร์/เครื่องแม่ข่ายขัดข้องหรือชำรุด	R03	3	5	15	สูงมาก
6	การถูกบุกรุกจากไวรัสหรือโปรแกรมประสงค์ร้าย (Malware)	R04	3	5	15	สูงมาก
7	อุณหภูมิและความชื้นห้องเครื่องแม่ข่าย (Server Room) ไม่เหมาะสม	R05	4	3	12	สูง
8	ความเสียหายหรือสูญหายของฐานข้อมูลสำคัญ	R08	2	5	10	สูง
9	การเชื่อมต่ออุปกรณ์ภายนอกที่ไม่ได้รับอนุญาต (เช่น USB/อุปกรณ์ส่วนตัว)	R07	5	2	10	สูง
10	ระบบเครือข่ายอินเทอร์เน็ตขัดข้อง	R10	2	4	8	สูง

ตารางที่ 3 ทะเบียนความเสี่ยงด้านเทคโนโลยีสารสนเทศและแนวทางจัดการ (IT Risk Register with Controls and Treatment Plan)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
(R01) ผู้ใช้งานขาดความรู้ในการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย	ความเสี่ยงด้านบุคลากรและการเข้าถึง	1. ขาดการอบรม/ทบทวนความรู้ด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง 2. แนวปฏิบัติด้านการใช้งานอีเมล/อินเทอร์เน็ต/ไฟล์งานยังไม่เป็นมาตรฐานเดียวกัน 3. มีพฤติกรรมเสี่ยง เช่น เปิดไฟล์แนบหรือคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือและใช้รหัสผ่านไม่รัดกุม	1. เพิ่มความเสี่ยงต่อการถูกโจมตีด้วยการหลอกลวงทางอิเล็กทรอนิกส์ (Phishing) และการติดโปรแกรมประสงค์ร้าย (Malware) 2. อาจก่อให้เกิดเหตุข้อมูลรั่วไหลหรือข้อมูลเสียหาย 3. กระทบต่อความต่อเนื่องในการให้บริการและความเชื่อมั่นของผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย	20	1. มีการสื่อสารข้อกำชับด้านการใช้งานเป็นครั้งคราว 2. มีเจ้าหน้าที่ IT ให้คำแนะนำและช่วยแก้ไขเมื่อเกิดเหตุ 3. มีการใช้งานโปรแกรมป้องกันไวรัสพื้นฐานในเครื่องผู้ใช้บางส่วน	Treat: 1. จัดทำแผนสร้างความตระหนักรู้ (Awareness Plan) อย่างน้อยปีละ 1 ครั้ง ครอบคลุมอีเมล ฟิชชิ่ง รหัสผ่าน และการจัดการข้อมูล 2. จัดทำคู่มือ/ประกาศแนวปฏิบัติที่เป็นมาตรฐานเดียวกัน
(R02) การเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ/เกินสิทธิ์ที่ได้รับอนุญาต	ความเสี่ยงด้านบุคลากรและการเข้าถึง	1. สิทธิ์การเข้าถึงข้อมูลไม่สอดคล้องกับบทบาทหน้าที่ 2. การใช้บัญชีผู้ใช้ร่วมกัน/การไม่แยกบัญชีรายบุคคล 3. รหัสผ่านไม่รัดกุมหรือมีการเปิดเผยรหัสผ่าน 4. การบันทึก/ตรวจสอบ Log ยังไม่ครอบคลุม	1. เกิดเหตุข้อมูลส่วนบุคคลรั่วไหลหรือถูกเปิดเผยโดยมิชอบ ไม่ปฏิบัติตาม PDPA 2. กระทบความน่าเชื่อถือและภาพลักษณ์ของหน่วยงาน 3. กระทบต่อความถูกต้องของข้อมูลและการตัดสินใจเชิงบริหาร	25	1. กำหนดสิทธิ์การใช้งานระบบในระดับหนึ่ง 2. มีการบันทึกการใช้งาน (Log) ในบางระบบ 3. มีผู้ดูแลระบบรับผิดชอบการจัดการบัญชีผู้ใช้	Treat: 1. กำหนดสิทธิ์ตามบทบาท (RBAC) 2. บังคับใช้บัญชีรายบุคคล 3. ใช้การยืนยันตัวตนหลายปัจจัย (MFA) สำหรับผู้ดูแลระบบ 4. จัดให้มีการตรวจสอบ Log ตามรอบ และกำหนดกระบวนการอนุมัติสิทธิ์อย่างเป็นทางการ

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
(R03) คอมพิวเตอร์/เครื่องแม่ข่ายขัดข้องหรือชำรุด	ความเสี่ยงด้านอุปกรณ์และโครงสร้างพื้นฐาน	1. อุปกรณ์เสื่อมสภาพตามอายุการใช้งาน 2. ขาดแผนบำรุงรักษาเชิงป้องกัน 3. ไม่มีอะไหล่/เครื่องสำรองสำหรับระบบสำคัญ 4. การเฝ้าระวังสุขภาพระบบและการแจ้งเตือนยังไม่เป็นระบบ	1. ระบบสารสนเทศหยุดให้บริการ ส่งผลให้การปฏิบัติงานล่าช้า 2. เสี่ยงต่อข้อมูลเสียหายจากการหยุดทำงานฉับพลัน 3. เพิ่มค่าใช้จ่ายในการซ่อม/จัดซื้อทดแทน และกระทบต่อความต่อเนื่องของภารกิจ	15	1. ดำเนินการซ่อมแซมเมื่อเกิดเหตุ 2. มีการสำรองข้อมูล 3. มีการดูแลอุปกรณ์ตามทรัพยากรที่มี	Treat/Transfer: 1. จัดทำแผนบำรุงรักษาเชิงป้องกันและบันทึกการตรวจสอบ 2. จัดทำบัญชีครุภัณฑ์ IT และแผนทดแทนตามอายุใช้งาน 3. จัดหาอะไหล่/เครื่องสำรองสำหรับระบบสำคัญ
(R04) การถูกบุกรุกจากไวรัสหรือโปรแกรมประสงค์ร้าย (Malware)	ความเสี่ยงด้านภัยคุกคามทางไซเบอร์	1. การอัปเดตแพตช์ระบบปฏิบัติการ/ซอฟต์แวร์ไม่สม่ำเสมอ 2. มาตรการป้องกันแบบหลายชั้นยังไม่เพียงพอ 3. พฤติกรรมผู้ใช้เสี่ยงต่อการเปิดไฟล์/ลิงก์ไม่ปลอดภัย 4. การแยกส่วนเครือข่าย/การจำกัดสิทธิ์ยังไม่ชัดเจน	1. ระบบอาจหยุดชะงักหรือข้อมูลถูกทำลาย/ถูกเข้ารหัส (เช่น Ransomware) 2. เสี่ยงต่อข้อมูลรั่วไหลและกระทบความเชื่อมั่น 3. ส่งผลต่อความต่อเนื่องในการให้บริการและภารกิจหลักของหน่วยงาน	15	1. มีโปรแกรมป้องกันไวรัสพื้นฐาน 2. มีการอัปเดตบางช่วงเวลา 3. มีการแก้ไขเมื่อเกิดเหตุเป็นรายกรณี	Treat: 1. จัดทำนโยบายการอัปเดตแพตช์และกำกับให้ปฏิบัติตาม 2. ยกระดับมาตรการป้องกันมัลแวร์ 3. จำกัดสิทธิ์ผู้ใช้และแยกสิทธิ์ผู้ดูแลระบบ 4. จัดทำแผนตอบสนองเหตุการณ์และซ้อมตามความเหมาะสม 5. สำรองข้อมูลแบบแยกชุดและทดสอบกู้คืน

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
(R05) อุณหภูมิและความชื้นห้องเครื่องแม่ข่าย (Server Room) ไม่เหมาะสม	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	1. ไม่มีอุปกรณ์วัด/ระบบแจ้งเตือนอุณหภูมิและความชื้น 2. ระบบปรับอากาศทำงานไม่ต่อเนื่องหรือไม่เพียงพอ 3. การระบายอากาศ/การจัดวางอุปกรณ์ไม่เหมาะสม	1. อุปกรณ์เสื่อมสภาพเร็วและเกิดความขัดข้องบ่อย 2. เสี่ยงต่อการหยุดให้บริการของระบบสำคัญ 3. เพิ่มค่าใช้จ่ายในการซ่อมบำรุงและกระทบต่อความต่อเนื่องของงาน	12	1. ตรวจสอบตามการสังเกตและดูแลตามประสบการณ์ 2. เปิดใช้งานเครื่องปรับอากาศตามช่วงเวลา	Treat: 1. ติดตั้งเครื่องวัดอุณหภูมิ/ความชื้นพร้อมระบบแจ้งเตือน 2. กำหนดเกณฑ์ควบคุมและบันทึกผลการตรวจสอบเป็นรายเดือน 3. ปรับปรุงระบบระบายอากาศและการจัดวางอุปกรณ์ให้เหมาะสม
(R06) ระบบกระแสไฟฟ้าขัดข้อง/ไฟตก-ไฟดับกระทบระบบสารสนเทศ	ความเสี่ยงด้านอุปกรณ์และโครงสร้างพื้นฐาน	1. ไฟฟ้าดับ/ไฟตกจากภายนอก 2. UPS ไม่เพียงพอหรือเสื่อมสภาพ 3. ขาดการทดสอบระบบสำรองและขั้นตอนปฏิบัติเมื่อเกิดเหตุ	1. ระบบหยุดชะงักฉับพลันส่งผลต่อการให้บริการ 2. เสี่ยงต่อความเสียหายของอุปกรณ์และข้อมูล 3. เพิ่มค่าใช้จ่ายในการซ่อม/ทดแทนและกระทบต่อภารกิจหลัก	16	1) มี UPS บางส่วนสำหรับอุปกรณ์บางรายการ 2) มีแนวปฏิบัติการปิดระบบเมื่อเกิดเหตุเป็นบางกรณี	Treat/Transfer: 1. ตรวจสอบและบำรุงรักษา UPS อย่างสม่ำเสมอและเพิ่มให้ครอบคลุมอุปกรณ์สำคัญ 2. จัดทำขั้นตอนรับมือไฟฟ้าขัดข้อง 3. ปรับปรุงมาตรฐานความปลอดภัยของระบบไฟฟ้าในพื้นที่
(R07) การเชื่อมต่ออุปกรณ์ภายนอกที่ไม่ได้รับอนุญาต	ความเสี่ยงด้านบุคลากรและการเข้าถึง	1. ไม่มีนโยบายควบคุมอุปกรณ์ภายนอกที่ชัดเจน 2. ไม่ควบคุมพอร์ต/สิทธิ์การใช้งาน 3. ความจำเป็นในการใช้งานอุปกรณ์ส่วนตัวของบุคลากร	1. เพิ่มความเสี่ยงต่อการติดมัลแวร์/การแพร่กระจายไวรัส 2. เสี่ยงต่อข้อมูลรั่วไหล 3. กระทบต่อความมั่นคงปลอดภัยของระบบและข้อมูล	10	1. มีการกำชับการใช้งาน 2. จำกัดการเชื่อมต่อในบางเครื่อง/บางพื้นที่	Treat: 1) จัดทำนโยบายการใช้อุปกรณ์ภายนอกและประกาศใช้ 2) จำกัด/ปิดการใช้งานพอร์ตตามระดับความจำเป็น 3) อนุญาตเฉพาะอุปกรณ์ที่ลงทะเบียนและผ่านการตรวจสอบ

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
(R08) ความเสียหายหรือสูญหายของฐานข้อมูลสำคัญ	ความเสี่ยงด้านซอฟต์แวร์และข้อมูล	1. การสำรองข้อมูลไม่ครบถ้วนหรือไม่เป็นไปตามรอบ 2. ไม่ทดสอบการกู้คืนข้อมูล 3. จัดเก็บข้อมูลสำรองไว้ที่เดียว 4. ไม่มีการกำหนดกรอบความต่อเนื่อง	1. สูญเสียข้อมูลสำคัญกระทบการรายงานและการตัดสินใจ 2. ระบบหยุดชะงักและฟื้นฟูใช้เวลานาน 3. ส่งผลต่อคุณภาพบริการและความเชื่อมั่น	10	1. มีการสำรองข้อมูลบางส่วน/บางระบบ 2. ดำเนินการกู้คืนเมื่อมีเหตุเป็นรายกรณี	Treat: 1. กำหนดนโยบายการสำรองข้อมูล 2. แยกชุดสำรองและจัดเก็บนอกสถานที่ตามความเหมาะสม 3. ทดสอบการกู้คืนอย่างน้อยปีละ 1 ครั้งและจัดทำรายงานผล
(R09) การติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง	ความเสี่ยงด้านซอฟต์แวร์และข้อมูล	1. ไม่จำกัดสิทธิ์การติดตั้งโปรแกรมอย่างเป็นระบบ 2. ไม่มีบัญชีรายการซอฟต์แวร์ 3. การจัดซื้อ/จัดหาไม่ทันต่อความต้องการใช้งาน 4. ผู้ใช้งานนำซอฟต์แวร์จากภายนอกมาติดตั้ง	1. เสี่ยงต่อการถูกดำเนินคดี/ค่าเสียหายตามกฎหมายลิขสิทธิ์ 2. เพิ่มช่องโหว่และความเสี่ยงมัลแวร์จากซอฟต์แวร์ที่ไม่ปลอดภัย 3. กระทบต่อความน่าเชื่อถือของหน่วยงาน	16	1. มีการกำชับเป็นครั้งคราว 2. ผู้ดูแลระบบช่วยติดตั้งบางกรณี	Treat: 1. จำกัดสิทธิ์ติดตั้ง และกำหนดขั้นตอนขออนุมัติการติดตั้ง 2. จัดทำบัญชีรายการซอฟต์แวร์และตรวจสอบรายไตรมาส 3. วางแผนจัดหาซอฟต์แวร์ที่ถูกต้องตามกฎหมาย
(R010) ระบบเครือข่ายอินเทอร์เน็ตขัดข้อง	ความเสี่ยงด้านอุปกรณ์และโครงสร้างพื้นฐาน	1. พึ่งพาผู้ให้บริการรายเดียว 2. ไม่มีช่องทางสำรอง 3. อุปกรณ์เครือข่ายอาจเสื่อมหรือกำลังรองรับไม่เพียงพอ	1. ไม่สามารถเข้าถึงระบบ/ส่งข้อมูลได้ตามเวลาที่กำหนด 2. กระทบการสื่อสารและการรายงานข้อมูล 3. ส่งผลต่อความต่อเนื่องของการให้บริการ	8	1. แจ้งผู้ให้บริการเมื่อเกิดเหตุขัดข้อง 2. แก้ไขเฉพาะหน้าเมื่อเกิดปัญหา	Treat/Transfer: 1. จัดทำอินเทอร์เน็ตสำรองหรือช่องทางสำรองตามความเหมาะสม 2. ติดตั้งระบบเฝ้าระวัง/แจ้งเตือนเครือข่าย 3. จัดทำแนวทางสลับเส้นทางเมื่อเกิดเหตุขัดข้อง

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
(R011) ความเสียหายจากภัยธรรมชาติและอุบัติเหตุ	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	1. ความเสี่ยงจากเหตุฉุกเฉินในพื้นที่ 2. การประเมินความเสี่ยงสถานที่และมาตรการป้องกันยังไม่เป็นระบบ 3. การสำรองทรัพยากรนอกสถานที่ยังไม่เพียงพอ	1. ทรัพย์สินและอุปกรณ์เสียหาย 2. ระบบหยุดชะงักระยะยาวและฟื้นฟูล่าช้า 3. กระทบต่อภารกิจหลักและความเชื่อมั่น	5	มาตรการความปลอดภัยพื้นฐานของอาคาร/สถานที่	Treat/Transfer: 1. จัดทำแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ 2. วางแผนจัดหาและติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง 3. สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
(R012) สถานการณ์ความไม่สงบทางการเมือง/บ้านเมือง กระทบการดำเนินงาน	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	1. การเดินทางและการเข้าปฏิบัติงานมีข้อจำกัด 2. โครงสร้างพื้นฐานภายนอกอาจถูกรบกวน 3. ช่องทางการสื่อสารบางส่วนอาจไม่เสถียร	1. งานบริการ/การประสานงานล่าช้า 2. การรายงานข้อมูลไม่เป็นไปตามกรอบเวลา 3. กระทบต่อความต่อเนื่องในการปฏิบัติงานบางภารกิจ	4	การประสานงานตามสถานการณ์เป็นกรณี ๆ	Accept/Treat: 1. จัดทำแนวทางการปฏิบัติงานสำรอง/ทำงานทางไกลตามความเหมาะสม 2. เตรียมช่องทางสื่อสารสำรอง
(R13) การโจรกรรมอุปกรณ์คอมพิวเตอร์/ทรัพย์สินด้าน IT	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	1. การควบคุมการเข้า–ออกบางพื้นที่ยังไม่เข้มงวด 2. อุปกรณ์พกพาไม่มีการล็อก/เข้ารหัส 3. การตรวจนับครุภัณฑ์ไม่เป็นวงรอบที่ชัดเจน	1. สูญเสียทรัพย์สินและค่าใช้จ่ายทดแทน 2. เสี่ยงข้อมูลรั่วไหลหากมีข้อมูลอยู่ในอุปกรณ์ 3. กระทบต่อการปฏิบัติงานและความเชื่อมั่น	5	1. ติดตั้งระบบรักษาความปลอดภัย 2. จัดเก็บอุปกรณ์ไว้ในที่มิดชิด 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมพื้นที่	Treat: 1. เพิ่มมาตรการควบคุมการเข้า–ออกพื้นที่สำคัญ 2. กำหนดให้เข้ารหัสอุปกรณ์พกพา 4. จัดทำขั้นตอนแจ้งเหตุ/สอบสวนและการบริหารความเสียหาย

3.3 สรุปภาพรวมผลการประเมิน (Summary of Assessment Results)

จากผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศจำนวน 13 รายการ พบว่า ความเสี่ยงระดับสูงมาก (สีแดง) จำนวน 6 รายการ ได้แก่ R02, R01, R09, R06, R03 และ R04 และความเสี่ยงระดับ สูง (สีเหลือง) จำนวน 4 รายการ ได้แก่ R05, R07, R08 และ R10 ซึ่งเป็นกลุ่มความเสี่ยงที่มีนัยสำคัญต่อการดำเนินภารกิจหลัก ความต่อเนื่องของระบบสารสนเทศ และความเชื่อมั่นของผู้รับบริการ จึงจำเป็นต้องกำหนดมาตรการจัดการความเสี่ยง (Risk Treatment) อย่างเป็นระบบในบทที่ 4 โดยระบุผู้รับผิดชอบ ระยะเวลา หลักฐาน และตัวชี้วัดให้ชัดเจน

ขณะเดียวกัน ความเสี่ยงระดับ ปานกลาง (สีเขียว) จำนวน 3 รายการ ได้แก่ R11, R13 และ R12 ให้ดำเนินมาตรการเฝ้าระวังและเตรียมความพร้อมตามมาตรการปกติ พร้อมทบทวนเมื่อมีการเปลี่ยนแปลงของบริบทการดำเนินงาน ทรัพยากร หรือเกิดเหตุการณ์สำคัญที่อาจทำให้ระดับความเสี่ยงเพิ่มสูงขึ้น

ทั้งนี้ ความเสี่ยงที่มีคะแนนสูงสุด คือ R02 การเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ (คะแนน 25) ซึ่งมีผลกระทบโดยตรงต่อความมั่นคงปลอดภัยของสารสนเทศ ภาพลักษณ์และความน่าเชื่อถือของหน่วยงาน รวมถึงความเสี่ยงด้านการไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) จึงควรกำหนดเป็นความเสี่ยงลำดับเร่งด่วนสูงสุดในการดำเนินมาตรการควบคุมและติดตามผลอย่างใกล้ชิด

เพื่อให้การนำผลการประเมินไปใช้ประโยชน์ได้อย่างเป็นรูปธรรม หน่วยงานได้จัดทำ ทะเบียนความเสี่ยงเชิงรายละเอียด (ตารางที่ 3) โดยระบุ ปัจจัยเสี่ยง ผลกระทบ ระดับความเสี่ยง แนวทางควบคุม และวิธีจัดการความเสี่ยง เป็นกรอบข้อมูลตั้งต้นสำหรับการจัดทำแผนปฏิบัติการในบทที่ 4 และการติดตามผลในรอบปีงบประมาณ

3.4 ข้อเสนอเชิงบริหารเพื่อการกำหนดทิศทาง (Management Implications and Recommendations)

เพื่อให้การจัดทำแผนปฏิบัติการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีทิศทางชัดเจน สอดคล้องกับระดับความเสี่ยง และสามารถบริหารทรัพยากรได้อย่างคุ้มค่า หน่วยงานเสนอแนวทางเชิงบริหารสำหรับการกำหนด “กลุ่มมาตรการหลัก” ดังนี้

3.4.1 กลุ่มมาตรการด้านการควบคุมการเข้าถึงและการคุ้มครองข้อมูลส่วนบุคคล (Access Control and PDPA Compliance)

ให้กำหนดเป็นประเด็นเร่งด่วนลำดับแรก โดยมุ่งเน้นการยกระดับการกำหนดสิทธิ์ตามบทบาทหน้าที่ การทบทวนสิทธิ์ตามรอบ การบันทึกและตรวจสอบการใช้งาน (Log) และการยืนยันตัวตนที่เหมาะสมสำหรับระบบสำคัญ ทั้งนี้ เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบและลดความเสี่ยงต่อการไม่ปฏิบัติตาม PDPA (เชื่อมโยงความเสี่ยง R02 และ R01)

3.4.2 กลุ่มมาตรการด้านความมั่นคงปลอดภัยไซเบอร์และการป้องกันโปรแกรมประสงค์ร้าย (Cybersecurity and Malware Protection)

ให้ยกระดับมาตรการเชิงเทคนิคและการบริหารจัดการร่วมกัน ได้แก่ การบริหารจัดการแพตช์ การป้องกันมัลแวร์ การเฝ้าระวังเหตุผิดปกติ และแนวทางตอบสนองเหตุการณ์ เพื่อให้สามารถลดโอกาสเกิดเหตุและจำกัดผลกระทบได้ทันท่วงที (เชื่อมโยงความเสี่ยง R04 และเชื่อมกับ R01)

3.4.3 กลุ่มมาตรการด้านความต่อเนื่องของระบบและความพร้อมใช้งาน (Service Continuity and Availability)

ให้กำหนดมาตรการด้านโครงสร้างพื้นฐานและความต่อเนื่อง ได้แก่ การจัดการไฟฟ้าสำรอง การบำรุงรักษาเชิงป้องกัน การจัดการอุปกรณ์สำรอง/สัญญาบำรุงรักษา และการกำหนดแนวทางฟื้นฟูเมื่อเกิดเหตุขัดข้อง เพื่อให้ระบบสามารถรองรับการให้บริการและลดผลกระทบจากการหยุดชะงัก (เชื่อมโยงความเสี่ยง R06, R03 และ R10)

3.4.4 กลุ่มมาตรการด้านธรรมาภิบาลซอฟต์แวร์และการปฏิบัติตามกฎหมายลิขสิทธิ์ (Software Governance and Legal Compliance)

ให้จัดทำระบบควบคุมการติดตั้งซอฟต์แวร์และบัญชีรายการซอฟต์แวร์ รวมถึงขั้นตอนการจัดหาและการตรวจสอบตามรอบ เพื่อป้องกันความเสี่ยงด้านกฎหมาย ความปลอดภัย และภาพลักษณ์องค์กร (เชื่อมโยงความเสี่ยง R09)

3.4.5 แนวทางการติดตามผลและการประเมินความเสี่ยงคงเหลือ (Monitoring and Residual Risk)

เพื่อให้แผนบริหารความเสี่ยงถูกนำไปใช้จริง หน่วยงานควรกำหนดให้มาตรการจัดการความเสี่ยงในบทที่ 4 ต้องมี “หลักฐานและตัวชี้วัด” ที่ตรวจสอบได้ และให้ประเมินคะแนนความเสี่ยงซ้ำหลังดำเนินมาตรการ (Residual Risk) ตามวงรอบที่กำหนด เพื่อใช้ประกอบการรายงานผู้บริหารและปรับปรุงมาตรการอย่างต่อเนื่อง ทั้งนี้ ให้ใช้ข้อมูลจาก ตารางที่ 3 เป็นฐานสำหรับการติดตามและการประเมินผลเชิงประจักษ์

บทที่ 4
แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
(IT Risk Management Plan)

4.1 หลักการและแนวทางการดำเนินงานของแผน (Plan Principles and Approach)

จากผลการระบุ วิเคราะห์ และประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศในบทที่ 3 ศูนย์สุขภาพจิตที่ 4 ได้จัดทำ แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อใช้เป็นกรอบแนวทางหลักในการควบคุมและจัดการความเสี่ยงให้เหมาะสมกับบริบทของหน่วยงาน โดยมีเป้าหมายสำคัญ คือ (1) ลดโอกาสเกิดเหตุการณ์ (Likelihood) (2) ลดผลกระทบ (Impact) (3) รักษาความต่อเนื่องของภารกิจและระบบสารสนเทศ และ (4) สร้างความเชื่อมั่นต่อผู้รับบริการและผู้มีส่วนได้ส่วนเสีย ภายใต้หลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance) และกฎหมาย/ข้อกำหนดที่เกี่ยวข้อง โดยเฉพาะการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

การกำหนดมาตรการและกิจกรรมในแผนนี้ยึดตามกลยุทธ์การตอบสนองความเสี่ยง 4 แนวทาง ได้แก่ (1) การควบคุม/ลดความเสี่ยง (Treat) (2) การถ่ายโอน/แบ่งปันความเสี่ยง (Transfer) (3) การยอมรับความเสี่ยง (Accept) และ (4) การหลีกเลี่ยงความเสี่ยง (Avoid) ทั้งนี้ หน่วยงานกำหนดให้ความเสี่ยงระดับสูงมาก (สีแดง) และ สูง (สีเหลือง) ต้องมีมาตรการที่ชัดเจน ตรวจสอบได้ และกำหนดผู้รับผิดชอบ พร้อมหลักฐานเชิงประจักษ์ในการติดตามผลตามรอบ

4.2 แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Plan)

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ครอบคลุมความเสี่ยงทุกระดับ โดยระบุรายการความเสี่ยง มาตรการควบคุม วิธีจัดการ ผู้รับผิดชอบ และการติดตามผลอย่างเป็นระบบ

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบหลัก นางสาวนันทภัค ชูเมือง
หน่วยงาน ศูนย์สุขภาพจิตที่ 4

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของศูนย์สุขภาพจิตที่ 4 บรรลุเป้าประสงค์ของการบริหารจัดการความเสี่ยง

ความเสี่ยง/ กิจกรรม	แผนจัดการความเสี่ยง	ระยะเวลา	ระยะเวลา												ผู้รับผิดชอบ
			2568			2569									
			10	11	12	1	2	3	4	5	6	7	8	9	
(R01) ผู้ใช้งานขาดความรู้ในการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย	1. จัดทำและเผยแพร่แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	1 ครั้ง/ปี	↔												งานเทคโนโลยีสารสนเทศ
	2. ดำเนินการอบรมพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	1 ครั้ง/ปี				↔									งานเทคโนโลยีสารสนเทศ
	2. กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยติดตามผลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	≥1 ครั้ง/ปี	←											→	งานเทคโนโลยีสารสนเทศ
(R02) การเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ/เกินสิทธิ์ที่ได้รับอนุญาต	1. จัดทำ/ทบทวนและประกาศใช้นโยบายควบคุมการเข้าถึงข้อมูลและแนวปฏิบัติด้าน PDPA/ความมั่นคงปลอดภัยสารสนเทศ	1 ครั้ง/ปี	↔												งานเทคโนโลยีสารสนเทศ
	2. ปรับสิทธิ์ตามบทบาทหน้าที่ (RBAC) และหลัก “สิทธิ์เท่าที่จำเป็น (Least Privilege)”	≥1 ครั้ง/ปี	←											→	งานเทคโนโลยีสารสนเทศ
	3. ทบทวนสิทธิ์ผู้ใช้งาน (Access Review) รายไตรมาส และตรวจสอบ Log ตามรอบ	≥4 ครั้ง/ปี	←											→	งานเทคโนโลยีสารสนเทศ

ความเสี่ยง/ กิจกรรม	แผนจัดการความเสี่ยง	ระยะเวลา	ระยะเวลา												ผู้รับผิดชอบ
			2568			2569									
			10	11	12	1	2	3	4	5	6	7	8	9	
(R03) เครื่องคอมพิวเตอร์/เครื่องแม่ข่าย ขัดข้องหรือชำรุด	1. แต่งตั้งเจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ส่วนบุคคล	1 ครั้ง/ปี	↔												งานอำนวยการ
	2. ตรวจสอบอุปกรณ์คอมพิวเตอร์ที่อยู่ในความรับผิดชอบ ตามแผนการบำรุงเครื่องคอมพิวเตอร์	≥1 ครั้ง/ปี	←	—	—	—	—	—	—	—	—	—	—	→	เจ้าหน้าที่ประจำเครื่อง
	3. สำรองข้อมูลสำคัญตามภารกิจหลัก ไว้ใน Data Bank ของหน่วยงาน หรือ External Hard disk ส่วนบุคคล	≥1 ครั้ง/ปี	←	—	—	—	—	—	—	—	—	—	—	→	เจ้าหน้าที่ประจำเครื่อง
(R04) การถูกบุกรุกจากไวรัสหรือโปรแกรมประสงค์ร้าp (Malware)	1. ติดตั้งโปรแกรมป้องกันไวรัสและทำการอัพเดทอย่างสม่ำเสมอ	≥1 ครั้ง/เดือน	←	—	—	—	—	—	—	—	—	—	—	→	งานเทคโนโลยีสารสนเทศ
	2. กำหนดรอบสแกน/ตรวจสอบเหตุผิดปกติและตรวจสอบ Log ตามรอบ	≥1 ครั้ง/เดือน	←	—	—	—	—	—	—	—	—	—	—	→	งานเทคโนโลยีสารสนเทศ
(R05) อุณหภูมิและความชื้นห้องเครื่องแม่ข่าย (Server Room) ไม่เหมาะสม	1. แต่งตั้งเจ้าหน้าที่ดูแลห้อง Server	1 ครั้ง/ปี	↔												งานอำนวยการ
	2. เจ้าหน้าที่ประจำห้อง server ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ	≥1 ครั้ง/เดือน	←	—	—	—	—	—	—	—	—	—	—	→	งานเทคโนโลยีสารสนเทศ
	3. ติดตั้งเครื่องวัดอุณหภูมิ/ความชื้นพร้อมการแจ้งเตือน	1 ครั้ง/ปี				↔									/ งานอาคารสถานที่
	4. ปรับปรุงการระบายอากาศ/การจัดวางอุปกรณ์	1 ครั้ง/ปี	↔												/ งานอาคารสถานที่

ความเสี่ยง/ กิจกรรม	แผนจัดการความเสี่ยง	ระยะเวลา	ระยะเวลา												ผู้รับผิดชอบ
			2568			2569									
			10	11	12	1	2	3	4	5	6	7	8	9	
(R06) ระบบกระแสไฟฟ้าขัดข้อง/ ไฟตก-ไฟดับ กระทบระบบสารสนเทศ	1. วางแผนการจัดหาและติดตั้ง UPS	1 ครั้ง/ปี				↔	↔								งานเทคโนโลยีสารสนเทศ
	2. ติดตั้งเครื่องสำรองไฟและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ	1 ครั้ง/ปี				↔	↔								งานเทคโนโลยีสารสนเทศ
(R07) การเชื่อมต่ออุปกรณ์ภายนอกที่ไม่ได้รับอนุญาต	1. จำกัด/ควบคุมพอร์ตและสิทธิ์ตามบทบาท/ความจำเป็น	≥1 ครั้ง/เดือน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	งานเทคโนโลยีสารสนเทศ
(R08) ความเสียหายหรือสูญหายของฐานข้อมูลสำคัญ	1. กำหนดนโยบายสำรองข้อมูล (รอบ/ชุด/ระยะเวลาเก็บ) ให้ชัดเจน	≥1 ครั้ง/ปี	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	งานเทคโนโลยีสารสนเทศ
	2. แยกชุดสำรองและจัดเก็บนอกสถานที่ตามความเหมาะสม	≥1 ครั้ง/ปี	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	งานเทคโนโลยีสารสนเทศ
(R09) การติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้อง	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น	1 ครั้ง/ปี			↔										งานเทคโนโลยีสารสนเทศ
(R010) ระบบเครือข่ายอินเตอร์เน็ตขัดข้อง	1. ตรวจสอบระบบเครือข่ายสื่อสารหลักจากผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISP) เพื่อแก้ไขปัญหาที่เกิดขึ้น	≥1 ครั้ง/เดือน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	งานเทคโนโลยีสารสนเทศ
	2. ตรวจสอบการทำงานของอุปกรณ์เครือข่ายหากพบปัญหาให้ดำเนินการแก้ไขอย่างรวดเร็ว	≥1 ครั้ง/เดือน	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	งานเทคโนโลยีสารสนเทศ

ความเสี่ยง/ กิจกรรม	แผนจัดการความเสี่ยง	ระยะเวลา	ระยะเวลา												ผู้รับผิดชอบ
			2568			2569									
			10	11	12	1	2	3	4	5	6	7	8	9	
(R011) ความเสียหาย จากภัยธรรมชาติและอุบัติเหตุ (R012) สถานการณ์ความไม่สงบทาง การเมือง / บ้านเมือง กระทบการดำเนินงาน	1. จัดทำแผนป้องกันและแก้ไขปัญหาจาก สถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบ เทคโนโลยีสารสนเทศ (IT Contingency Plan)	1 ครั้ง/ปี	↔												งานเทคโนโลยี สารสนเทศ
	2. วางแผนจัดหาและ ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ ระบบดับเพลิง	1 ครั้ง/ปี	↔												งานอำนวยการ
	3. สำรองข้อมูลระบบและฐานข้อมูล เก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	≥1 ครั้ง/เดือน	←	—	—	—	—	—	—	—	—	—	—	→	งานเทคโนโลยี สารสนเทศ
(R13) การถูกโจรกรรมอุปกรณ์ คอมพิวเตอร์ และอุปกรณ์ต่อพ่วง	1. ติดตั้งระบบรักษาความปลอดภัย ในการควบคุมการเข้า – ออก ห้อง Server	1 ครั้ง/ปี	↔												งานเทคโนโลยี สารสนเทศ
	2. ตรวจสอบจัดเก็บเครื่องคอมพิวเตอร์ที่สามารถ เคลื่อนย้ายได้สะดวก ไว้ในที่มิดชิด	≥1 ครั้ง/สัปดาห์	←	—	—	—	—	—	—	—	—	—	—	→	งานเทคโนโลยี สารสนเทศ
	3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมพื้นที่	1 ครั้ง/ปี	↔												งานอำนวยการ

4.3 เป้าหมายความเสี่ยงคงเหลือที่ยอมรับได้ (Residual Risk Target)

หน่วยงานกำหนดเป้าหมายให้ความเสี่ยงคงเหลือหลังดำเนินมาตรการ (Residual Risk) อยู่ในระดับที่ยอมรับได้ โดยกำหนดให้ คะแนนความเสี่ยงคงเหลือไม่เกิน 9 คะแนน ซึ่งถือเป็นระดับความเสี่ยงที่สามารถควบคุมและกำกับติดตามได้ภายใต้ทรัพยากรของหน่วยงาน ทั้งนี้ สำหรับความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลหรือระบบสำคัญ (เช่น ความเสี่ยงด้านการเข้าถึงข้อมูลโดยมิชอบ) ให้พิจารณากำหนดมาตรการที่เข้มงวดและมีการติดตามถี่ขึ้นตามความเหมาะสม

4.4 รอบการติดตาม รายงานผล และหลักฐานเชิงประจักษ์ (Monitoring, Reporting, and Evidence)

เพื่อให้แผนสามารถตรวจสอบและประเมินผลได้ หน่วยงานกำหนดรอบการติดตามและการรายงานดังนี้

(1) รายเดือน: ติดตามมาตรการเชิงเทคนิคและความพร้อมใช้งานของระบบที่มีผลต่อความต่อเนื่อง (เช่น ระบบสำรองไฟ การสำรองข้อมูล สถานะอุปกรณ์สำคัญตามความเหมาะสม) พร้อมจัดเก็บหลักฐานผลการตรวจสอบ

(2) รายไตรมาส: ทบทวนสิทธิ์การเข้าถึงข้อมูล (Access Review) ตรวจสอบรายการซอฟต์แวร์/ลิขสิทธิ์ และสรุปผลการดำเนินมาตรการความเสี่ยงระดับสูงมากและสูง เสนอผู้บริหารเพื่อพิจารณากำกับติดตาม

(3) รายปี: สรุปผลการดำเนินงานภาพรวมของแผน วิเคราะห์แนวโน้มความเสี่ยง (Trend) และข้อเสนอเพื่อปรับปรุงมาตรการในปีงบประมาณถัดไป

หลักฐานที่ต้องจัดเก็บประกอบการติดตาม ได้แก่ นโยบาย/แนวปฏิบัติที่ประกาศใช้ รายงานการตรวจสอบตามรอบ บันทึกการอบรม/สื่อสาร รายงานการทบทวนสิทธิ์ รายงานการตรวจซอฟต์แวร์/ลิขสิทธิ์ รายงานเหตุการณ์ผิดปกติ (Incident Report) และเอกสารสนับสนุนอื่นตามมาตรการในตารางแผน

4.5 การยกระดับการรายงานเมื่อเกิดเหตุการณ์สำคัญ (Escalation and Incident Handling)

ในกรณีเกิดเหตุการณ์ที่เข้าข่ายความเสี่ยงระดับสูงมาก (สีแดง) หรือเหตุการณ์ที่มีแนวโน้มกระทบข้อมูลส่วนบุคคล/ระบบสำคัญ ให้หน่วยงานดำเนินการรายงานผู้บริหารโดยทันที และจัดทำรายงานเหตุการณ์ (Incident Report) โดยระบุอย่างน้อย ได้แก่ สาเหตุเบื้องต้น ขอบเขตผลกระทบ มาตรการควบคุมชั่วคราว (Containment) มาตรการแก้ไข (Corrective Actions) และมาตรการป้องกันการเกิดซ้ำ (Preventive Actions) พร้อมจัดเก็บหลักฐานประกอบเพื่อการตรวจสอบ

4.6 การทบทวนและปรับปรุงแผน (Plan Review and Continuous Improvement)

หน่วยงานกำหนดให้มีการทบทวนความเหมาะสมของแผนและมาตรการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อเกิดเหตุการณ์สำคัญ/มีการเปลี่ยนแปลงบริบท เช่น การเปลี่ยนแปลงระบบงาน โครงสร้างพื้นฐาน งบประมาณ กฎหมาย/ข้อกำหนด หรือพบแนวโน้มภัยคุกคามที่เพิ่มสูงขึ้น โดยให้ใช้ผลการติดตามและหลักฐานเชิงประจักษ์ตามข้อ 4.4 เป็นข้อมูลประกอบการปรับปรุง เพื่อให้แผนมีความทันสมัยและสามารถใช้ได้จริงอย่างต่อเนื่อง

บทที่ 5
บทสรุปและข้อเสนอแนะ
(Conclusion and Recommendations)

5.1 บทสรุปการดำเนินงาน (Executive Summary)

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของศูนย์สุขภาพจิตที่ 4 ประจำปีงบประมาณ พ.ศ. 2569 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการกำกับดูแลและยกระดับความมั่นคงปลอดภัยของระบบสารสนเทศให้สอดคล้องกับหลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance) ตลอดจนรองรับการดำเนินงานด้านสุขภาพจิตที่ต้องอาศัยข้อมูลและระบบดิจิทัลเป็นกลไกสำคัญ โดยมุ่งเน้นการลดโอกาสเกิดเหตุการณ์ ลดผลกระทบ และรักษาความต่อเนื่องของการปฏิบัติงาน (Service Continuity) รวมถึงการคุ้มครองข้อมูลที่มีความอ่อนไหวและข้อมูลส่วนบุคคลตามข้อกำหนดที่เกี่ยวข้อง

ผลการระบุและประเมินความเสี่ยงรวมทั้งสิ้น 13 ประเด็น พบว่า ความเสี่ยงระดับ สูงมาก (สีแดง) จำนวน 6 รายการ ได้แก่ R02, R01, R09, R06, R03 และ R04 ซึ่งเป็นกลุ่มความเสี่ยงที่มีนัยสำคัญต่อความมั่นคงปลอดภัยของข้อมูล การปฏิบัติตามกฎหมาย และความเชื่อมั่นของผู้รับบริการ ขณะเดียวกันความเสี่ยงระดับ สูง (สีเหลือง) จำนวน 4 รายการ และระดับ ปานกลาง (สีเขียว) จำนวน 3 รายการ ได้กำหนดมาตรการควบคุมและแนวทางดำเนินการในระดับที่เหมาะสมกับทรัพยากรของหน่วยงาน พร้อมกำหนดรอบการติดตามเพื่อให้สามารถประเมินสถานะความเสี่ยงได้อย่างต่อเนื่อง

ทั้งนี้ หน่วยงานได้จัดทำ ตารางทะเบียนความเสี่ยง (ตารางที่ 3) และแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อใช้เป็นเครื่องมือหลักในการกำกับติดตาม โดยมาตรการสำคัญครอบคลุมการควบคุมเชิงป้องกัน (Preventive Controls) การควบคุมเชิงตรวจจับ (Detective Controls) และการควบคุมเชิงแก้ไข (Corrective Controls) โดยกำหนดเป้าหมายให้ คะแนนความเสี่ยงคงเหลือ (Residual Risk) ไม่เกิน 9 คะแนน ตามที่ระบุในบทที่ 4 เพื่อให้หน่วยงานสามารถบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และสนับสนุนภารกิจบริการด้านสุขภาพจิตให้ดำเนินไปอย่างต่อเนื่อง มีเสถียรภาพ และปลอดภัย

5.2 ปัจจัยความสำเร็จ (Key Success Factors)

เพื่อให้การดำเนินการตามแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเกิดผลสัมฤทธิ์อย่างเป็นรูปธรรมและตรวจสอบได้ หน่วยงานควรให้ความสำคัญต่อปัจจัยสนับสนุนหลัก ดังนี้

5.2.1 การสนับสนุนจากผู้บริหาร (Management Support)

ผู้บริหารต้องกำกับทิศทาง อนุมัตินโยบาย กำหนดความคาดหวังต่อการปฏิบัติตามมาตรการ และสนับสนุนทรัพยากร/งบประมาณที่จำเป็น โดยเฉพาะมาตรการที่มีผลต่อความเสี่ยงระดับสูงมากและสูง รวมถึงการมอบหมายผู้รับผิดชอบที่ชัดเจนและมีอำนาจดำเนินการ

5.2.2 ความตระหนักรู้และวินัยการปฏิบัติของบุคลากร (Staff Awareness and Compliance)

บุคลากรทุกระดับต้องมีความรู้ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามแนวปฏิบัติของหน่วยงานอย่างสม่ำเสมอ เนื่องจากความเสี่ยงจำนวนหนึ่งมีปัจจัยจากพฤติกรรมการใช้งาน (Human Factor) ซึ่งส่งผลต่อความถี่ของเหตุการณ์และความรุนแรงของผลกระทบโดยตรง

5.2.3 ระบบการติดตามประเมินผลและการรายงานอย่างต่อเนื่อง (Continuous Monitoring and Reporting)

ต้องดำเนินการตรวจสอบตามรอบที่กำหนดในบทที่ 4 พร้อมจัดเก็บหลักฐานเชิงประจักษ์ (Evidence) เพื่อประเมินความคืบหน้าและประสิทธิผลของมาตรการ รวมถึงสามารถยกระดับรายงานเมื่อพบเหตุผิดปกติหรือความเสี่ยงมีแนวโน้มเพิ่มสูงขึ้นได้อย่างทันท่วงที

5.2.4 ความพร้อมด้านกระบวนการและมาตรฐานงาน (Process Readiness and Standardization)

ต้องจัดให้มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกัน เช่น การกำหนดสิทธิ์เข้าถึงข้อมูล การสำรองข้อมูล การจัดการซอฟต์แวร์ และการตอบสนองเหตุการณ์ เพื่อให้การดำเนินงานมีความสม่ำเสมอ ลดความคลาดเคลื่อน และตรวจสอบย้อนกลับได้

5.3 ข้อเสนอแนะเพื่อการพัฒนา (Recommendations)

เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีความยั่งยืน สามารถยกระดับมาตรการให้เท่าทันภัยคุกคาม และรองรับการเปลี่ยนแปลงของระบบงานในอนาคต หน่วยงานควรพิจารณาดำเนินการเพิ่มเติมดังต่อไปนี้

5.3.1 การทบทวนและยกระดับนโยบาย/แนวปฏิบัติให้เป็นระบบ (Policy and Procedure Enhancement)

ให้ทบทวนและปรับปรุงนโยบาย/แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและ PDPA อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย/ระบบงาน พร้อมกำหนดแบบฟอร์มและขั้นตอนมาตรฐาน เช่น ขั้นตอนการขอ/อนุมัติสิทธิ์ การตรวจสอบบันทึกการใช้งาน และการจัดการเหตุการณ์ เพื่อเพิ่มความชัดเจนในการปฏิบัติและการตรวจสอบ

5.3.2 การยกระดับสมรรถนะบุคลากรด้านความมั่นคงปลอดภัย (Capability Building)

ให้จัดอบรมเชิงปฏิบัติการด้าน Cyber Security และการคุ้มครองข้อมูลส่วนบุคคล โดยเน้นทักษะที่เกี่ยวข้องกับงานจริง เช่น การระวังฟิชชิ่ง การจัดการรหัสผ่าน การจัดการไฟล์/ข้อมูลอ่อนไหว และการแจ้งเหตุการณ์ รวมถึงมีการประเมินผลหลังอบรมเพื่อใช้ปรับปรุงอย่างต่อเนื่อง

5.3.3 การพัฒนาเครื่องมือสนับสนุนการเฝ้าระวังและการสำรองข้อมูล (Technology Enablement)

ให้พิจารณายกระดับเครื่องมือที่สนับสนุนมาตรการสำคัญตามทรัพยากรและความเหมาะสม เช่น เครื่องมือเฝ้าระวัง/แจ้งเตือนเหตุผิดปกติ ระบบบริหารจัดการแพตช์ และแนวทางสำรองข้อมูลที่เพิ่มความมั่นคงปลอดภัย (รวมถึงการจัดเก็บสำรองแยกชุด/นอกสถานที่) ทั้งนี้ หากจะใช้ Cloud Storage ให้กำหนดหลักเกณฑ์ด้านความมั่นคงปลอดภัย การกำหนดสิทธิ์ และการประเมินผู้ให้บริการอย่างรอบคอบก่อนนำมาใช้

5.3.4 การบูรณาการการบริหารความเสี่ยงด้าน IT กับความเสี่ยงองค์กร (Integration with Enterprise Risk Management: ERM)

ให้เชื่อมโยงผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศกับการบริหารความเสี่ยงภาพรวมของหน่วยงาน เพื่อให้ผู้บริหารเห็นภาพรวมความเสี่ยงที่ส่งผลต่อภารกิจหลักและสามารถจัดลำดับความสำคัญของทรัพยากรได้อย่างเหมาะสม รวมทั้งใช้ข้อมูลแนวโน้ม (Trend) จากการติดตามผลประกอบการตัดสินใจเชิงนโยบาย

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศฉบับนี้จัดทำขึ้นเพื่อเป็น “เครื่องมือบริหารจัดการเชิงระบบ” เป็นกรอบการดำเนินงานที่ช่วยคุ้มครองทรัพยากรด้านเทคโนโลยีสารสนเทศและข้อมูลสำคัญของหน่วยงาน รวมถึงเสริมสร้างความเชื่อมั่นของประชาชนต่อการให้บริการภาครัฐในยุคดิจิทัล ศูนย์สุขภาพจิตที่ 4 จึงมุ่งมั่นที่จะดำเนินมาตรการตามแผนอย่างต่อเนื่อง ทบทวนและปรับปรุงให้ทันต่อบริบทและภัยคุกคามที่เปลี่ยนแปลง เพื่อยกระดับสู่การเป็นองค์กรดิจิทัลที่น่าเชื่อถือ (Trusted Digital Organization) และสนับสนุนภารกิจด้านสุขภาพจิตของประเทศอย่างมั่นคงและยั่งยืนต่อไป

ผู้เสนอแผน

(นางสาวนันทภัค ชูเมือง)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

ผู้อนุมัติแผน

(นางสาวรัชวัลย์ บุญโฉม)
ผู้อำนวยการศูนย์สุขภาพจิตที่ 4