

	คู่มือการปฏิบัติงาน	วันที่เริ่มใช้ 1 ต.ค. 69
	หน่วยงาน : สำนักยุทธศาสตร์และแผน	รวม 21 กระบวนการงาน
	กลุ่มงาน : 6. ศูนย์ข้อมูลและสารสนเทศ	รวม 7 กระบวนการงาน
	กระบวนการงาน : การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์และเครือข่ายคอมพิวเตอร์	ลำดับที่ 6.5/21

1. วัตถุประสงค์

1. เพื่อกำหนดแนวทางการบริหารจัดการสิทธิ์การใช้งานให้สอดคล้องกับบทบาทหน้าที่ ความจำเป็นในการปฏิบัติงาน และหลัก Least Privilege
2. เพื่อให้การให้บริการระบบเครือข่ายและการดูแลรักษาเครื่องคอมพิวเตอร์แม่ข่ายมีขั้นตอน มาตรฐาน และหลักฐานประกอบที่ตรวจสอบย้อนหลังได้
3. เพื่อกำหนดแนวทางการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ โดยประยุกต์ใช้ NIST Cybersecurity Framework 2.0 ในระดับ Function และเกณฑ์/แนวทางด้านเทคโนโลยีสารสนเทศที่หน่วยงานกำหนด
4. เพื่อสนับสนุนการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับคอมพิวเตอร์ ธุรกรรมอิเล็กทรอนิกส์ ข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยไซเบอร์ และอาชญากรรมทางเทคโนโลยี
5. เพื่อให้มีแบบฟอร์ม รายงาน บันทึก และหลักฐานประกอบการดำเนินงานที่พร้อมต่อการติดตาม ตรวจสอบ และปรับปรุงกระบวนการงาน

2. ขอบเขต

คู่มือฉบับนี้ครอบคลุมการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์และเครือข่ายคอมพิวเตอร์ของหน่วยงาน โดยแบ่งเป็น 4 กระบวนการหลัก ดังนี้

1. การบริหารจัดการสิทธิ์การใช้งาน ประกอบด้วย การเปิดสิทธิ์ ปรับปรุงสิทธิ์ ยกเลิกสิทธิ์ ระบุสิทธิ์ และการทบทวนสิทธิ์ตามสถานะบุคลากรหรือรอบที่หน่วยงานกำหนด
2. การให้บริการระบบเครือข่ายและการดูแลรักษาเครื่องคอมพิวเตอร์แม่ข่าย ประกอบด้วย การตรวจสอบสถานะระบบ การแก้ไขปัญหา การบำรุงรักษา การเปลี่ยนแปลงค่าคอนฟิก การติดตั้งแพตช์ และการสำรอง/กู้คืนข้อมูล
3. การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วย การจัดทำบัญชีระบบและทรัพย์สินสารสนเทศ การประเมินความเสี่ยง การเฝ้าระวัง การบันทึกเหตุการณ์ การตอบสนองต่อเหตุการณ์ และการปรับปรุงมาตรการควบคุม
4. การปฏิบัติตามกฎหมายที่เกี่ยวข้อง ประกอบด้วย การรวบรวมข้อกำหนด วิเคราะห์ผลกระทบ กำหนดหลักฐานที่ต้องจัดเก็บ และทบทวนความสอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

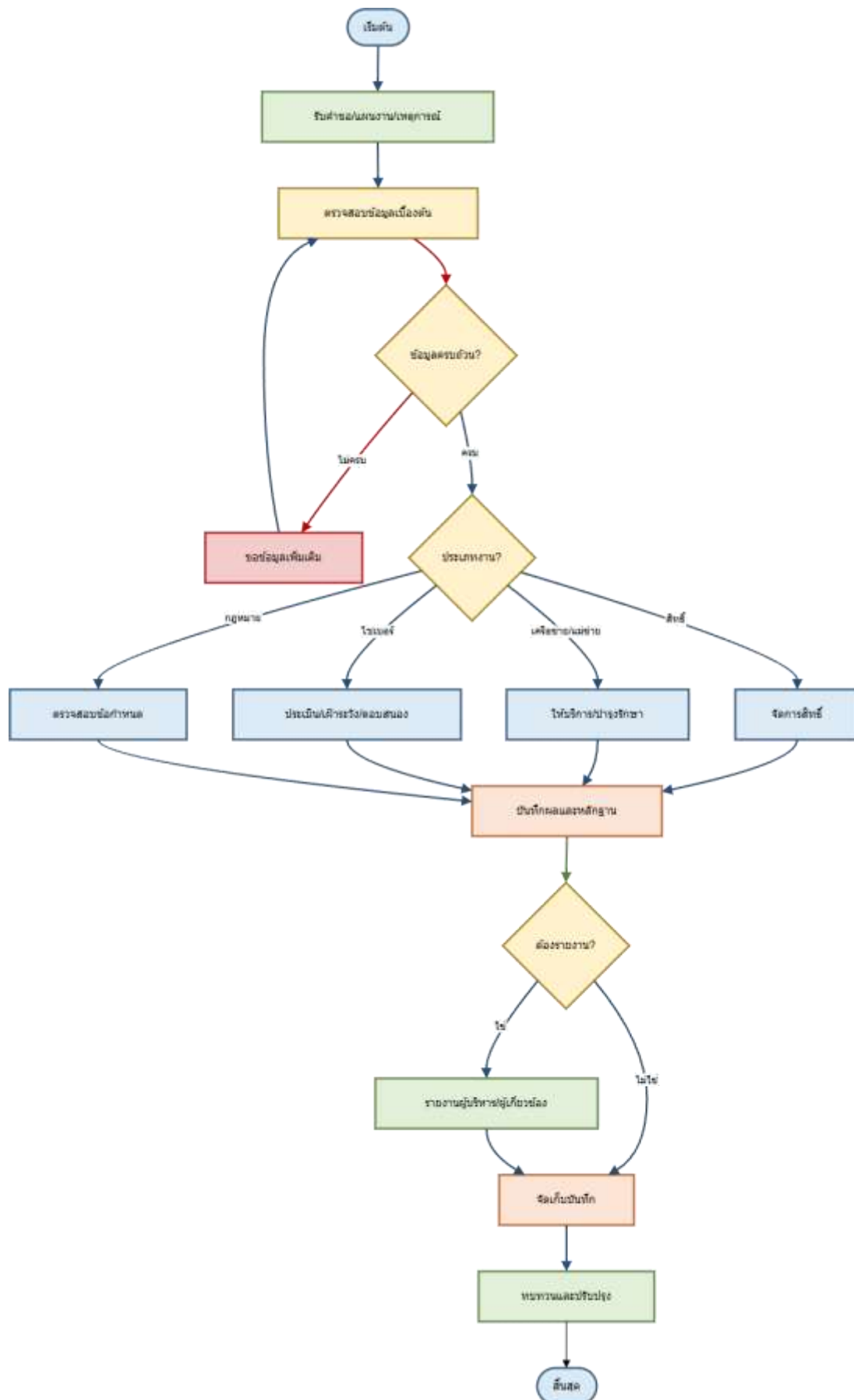
3. คำจำกัดความ

คำศัพท์	ความหมาย
สิทธิ์การใช้งาน	ระดับการเข้าถึงระบบ ข้อมูล อุปกรณ์ หรือบริการสารสนเทศที่กำหนดให้ผู้ใช้งานตามบทบาทหน้าที่
ผู้ใช้งาน	บุคลากรภายในหรือผู้เกี่ยวข้องที่ได้รับอนุญาตให้ใช้งานระบบของหน่วยงาน
ผู้ดูแลระบบ	บุคลากรหรือผู้ได้รับมอบหมายให้ดูแล ติดตั้ง กำหนดค่า ตรวจสอบ และแก้ไขปัญหาระบบ
เจ้าของระบบ	หน่วยงานหรือผู้รับผิดชอบหลักของระบบสารสนเทศและข้อมูลที่เกี่ยวข้อง
ระบบเครือข่าย	โครงสร้างพื้นฐานด้านการสื่อสารข้อมูล เช่น Switch, Router, Firewall, Wireless, VPN และบริการเครือข่ายที่เกี่ยวข้อง
เครื่องคอมพิวเตอร์แม่ข่าย	เครื่องแม่ข่ายจริงหรือเสมือนที่ให้บริการระบบสารสนเทศ ฐานข้อมูล เว็บไซต์ แอปพลิเคชัน หรือบริการภายในหน่วยงาน
Log	บันทึกเหตุการณ์ของระบบ อุปกรณ์ บัญชีผู้ใช้งาน หรือแอปพลิเคชัน เพื่อใช้ตรวจสอบย้อนหลัง
Backup	การสำรองข้อมูล ระบบ หรือค่าคอนฟิก เพื่อใช้กู้คืนเมื่อเกิดความผิดปกติ
Restore	การกู้คืนข้อมูล ระบบ หรือบริการจากข้อมูลสำรอง
Incident	เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์หรือเหตุการณ์ที่อาจส่งผลกระทบต่อระบบ ข้อมูล หรือการให้บริการ
Cybersecurity	การดำเนินการเพื่อป้องกัน ตรวจสอบ และกู้คืนจากภัยคุกคามทางไซเบอร์
NIST CSF 2.0	กรอบการบริหารจัดการความเสี่ยงด้านไซเบอร์ที่ประกอบด้วย Function หลัก ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover
ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้โดยตรงหรือโดยอ้อม ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
Least Privilege	หลักการให้สิทธิ์เท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น
Access Review	การทบทวนความจำเป็นและความถูกต้องของสิทธิ์การใช้งานเป็นระยะหรือเมื่อสถานะบุคลากรเปลี่ยนแปลง

4. หน้าที่ความรับผิดชอบ

ผู้เกี่ยวข้อง	หน้าที่ความรับผิดชอบ	เอกสาร/หลักฐานที่เกี่ยวข้อง
ผู้บริหาร	กำหนดนโยบาย สนับสนุนทรัพยากร รับทราบรายงานความเสี่ยง เหตุการณ์สำคัญ และผลการดำเนินงาน	นโยบาย คำสั่ง บันทึกอนุมัติ รายงานผู้บริหาร
หัวหน้าหน่วยงาน	รับรองความจำเป็นในการใช้สิทธิ์หรือบริการระบบของบุคลากรในสังกัด และประสานข้อมูลกับ HR/IT	บันทึกรับรองสิทธิ์ หนังสือแจ้ง HR/IT
HR	เป็นผู้เริ่มคำขอด้านบุคลากร เช่น เปิดสิทธิ์ ปรับปรุงสิทธิ์ ยกเลิกสิทธิ์ ย้ายงาน ลาออก และตรวจสอบสถานะบุคลากร	IT-FM-01 IT-FM-05 รายชื่อบุคลากร หนังสือแจ้งเปลี่ยนแปลงสถานะ
IT	ตรวจสอบข้อมูล พิจารณาสีทธิ์ด้านเทคนิค ดำเนินการในระบบ เฝ้าระวัง แก้ไขปัญหา จัดเก็บหลักฐาน และรายงานผล	Log แบบฟอร์ม IT-FM-01 ถึง IT-FM-06 รายงานบริการ รายงานเหตุการณ์
เจ้าของระบบ	กำหนดความต้องการทางธุรกิจของระบบ รับรองสิทธิ์การใช้งาน และให้ข้อมูลผลกระทบต่อระบบ	รายการระบบ หนังสือรับรองสิทธิ์ รายงานผลกระทบ
ผู้ใช้งาน	ใช้งานระบบตามสิทธิ์ที่ได้รับ รักษาความลับของบัญชีผู้ใช้งาน และแจ้งเหตุผิดปกติ	บันทึกแจ้งเหตุ แบบฟอร์มคำขอ
ผู้ให้บริการภายนอก	ปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย สัญญา SLA และข้อกำหนดด้านข้อมูลของหน่วยงาน	สัญญา SLA รายงานบริการ รายงานเหตุการณ์จากผู้ให้บริการ

5. แผนผังการปฏิบัติงาน (Work Flow)



6. ขั้นตอนการปฏิบัติงาน

การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์และเครือข่ายคอมพิวเตอร์

ลำดับ	ฝั่งกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารอ้างอิง
1	รับคำขอ/แผนงาน/ เหตุการณ์	รับเรื่องจาก HR ผู้ใช้งาน เจ้าของระบบ ผู้บริหาร หรือ ข้อกำหนดด้านกฎหมาย/มาตรฐานที่เกี่ยวข้อง	HR / IT / เจ้าของ ระบบ / ผู้ใช้งาน	IT-FM-01, IT-FM- 02, IT-FM-03
2	ตรวจสอบข้อมูล เบื้องต้น	ตรวจสอบความครบถ้วนของข้อมูล รายละเอียดระบบ ผู้ ขอรับบริการ เหตุการณ์ หรือเอกสารประกอบ	IT	แบบฟอร์มที่เกี่ยวข้อง
3	ขอข้อมูลเพิ่มเติม	กรณีข้อมูลไม่ครบถ้วน ให้แจ้งผู้เกี่ยวข้องเพื่อแก้ไขหรือ เพิ่มเติมข้อมูลก่อนดำเนินการ	IT / HR / ผู้ขอรับ บริการ	บันทึกการ ประสานงาน
4	จำแนกประเภท งาน	จำแนกงานเป็นการจัดการสิทธิ์ การให้บริการระบบ เครือข่าย/เครื่องแม่ข่าย การบริหารจัดการไซเบอร์ หรือ การปฏิบัติตามกฎหมาย	IT	คู่มือฉบับนี้
5	จัดการสิทธิ์	ดำเนินการตามกระบวนการบริหารจัดการสิทธิ์การใช้งาน	HR / IT / เจ้าของ ระบบ	IT-FM-01, IT-FM-05
6	ให้บริการ/ บำรุงรักษา	ดำเนินการให้บริการระบบเครือข่ายและดูแลรักษาเครื่อง คอมพิวเตอร์แม่ข่าย	IT	IT-FM-02
7	ประเมิน/เฝ้าระวัง/ ตอบสนอง	ดำเนินการประเมินความเสี่ยง เฝ้าระวัง ตรวจสอบจับ ตอบสนอง และกู้คืนจากเหตุการณ์ด้านไซเบอร์	IT / เจ้าของระบบ / ผู้บริหาร	IT-FM-03, IT-FM- 04, IT-FM-06
8	ตรวจสอบ ข้อกำหนด	ตรวจสอบกฎหมาย มาตรฐาน หรือข้อกำหนดที่เกี่ยวข้อง กับระบบ ข้อมูล และกระบวนการงาน	IT / ผู้รับผิดชอบ Compliance	Checklist กฎหมาย/ มาตรฐาน
9	บันทึกผลและ หลักฐาน	บันทึกผลการดำเนินการในแบบฟอร์ม รายงาน Log หรือ หลักฐานที่เกี่ยวข้อง	IT	IT-FM-01 ถึง IT-FM- 06
10	รายงานผู้บริหาร/ ผู้เกี่ยวข้อง	กรณีเป็นเหตุสำคัญ ความเสี่ยงสูง หรือประเด็นด้าน กฎหมาย ให้รายงานผู้บริหารหรือผู้เกี่ยวข้องรับทราบ	IT / ผู้บริหาร	รายงานผล/บันทึก ข้อความ
11	จัดเก็บบันทึก	จัดเก็บเอกสารและหลักฐานการดำเนินงานให้ตรวจสอบ ย้อนหลังได้	IT	เอกสารบันทึก/Log
12	ทบทวนและ ปรับปรุง	ทบทวนผลการดำเนินงาน ปัญหา อุปสรรค และปรับปรุง มาตรการควบคุมหรือขั้นตอนปฏิบัติงาน	IT / HR / เจ้าของ ระบบ	รายงานทบทวน/ ข้อเสนอแนะ

7. มาตรฐานงาน

1. การบริหารจัดการสิทธิ์การใช้งาน การกำหนด แก้ไข ระบุ หรือยกเลิกสิทธิ์การใช้งาน ต้องได้รับการ
อนุมัติจากผู้มีอำนาจ และเป็นไปตามบทบาทหน้าที่ (Role-Based Access Control) และหลัก Least
Privilege

2. การทบทวนสิทธิ์การใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานตามรอบที่หน่วยงานกำหนด หรือเมื่อมี
การเปลี่ยนแปลงสถานะบุคลากร

3. การให้บริการระบบเครือข่ายและเครื่องแม่ข่าย การติดตั้ง ปรับปรุง บำรุงรักษา และแก้ไขปัญหาหาระบบ
เครือข่ายหรือเครื่องแม่ข่าย ต้องมีการบันทึกผลการดำเนินงานและสามารถตรวจสอบย้อนหลังได้

4. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ด้านความมั่นคงปลอดภัยไซ
เบอร์ต้องได้รับการบันทึก วิเคราะห์ ตอบสนอง และรายงานตามระดับความรุนแรงของเหตุการณ์

5. การประเมินความเสี่ยงด้านไซเบอร์ ต้องมีการระบุ วิเคราะห์ ประเมิน และติดตามความเสี่ยงด้านไซ
เบอร์ตามแนวทางบริหารความเสี่ยงของหน่วยงาน

6. การสำรองและกู้คืนข้อมูล ระบบและข้อมูลสำคัญต้องได้รับการสำรองข้อมูล และมีการทดสอบการกู้คืน
ข้อมูลตามแผนที่กำหนด

7. การจัดเก็บหลักฐานและบันทึก เอกสาร บันทึก Log และหลักฐานที่เกี่ยวข้อง ต้องได้รับการจัดเก็บอย่างเหมาะสม และสามารถตรวจสอบย้อนหลังได้

8. การปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง การดำเนินงานต้องสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และมาตรฐานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง

9. การปรับปรุงอย่างต่อเนื่อง ต้องมีการทบทวนผลการดำเนินงาน ปัญหา อุปสรรค และแนวทางปรับปรุงกระบวนการอย่างต่อเนื่อง

8. ระบบติดตามและประเมินผล

ลำดับ	ประเด็นติดตามและประเมินผล	วิธีการติดตาม/ประเมินผล	ความถี่	ผู้รับผิดชอบ	เอกสาร/หลักฐาน
1	การบริหารจัดการสิทธิ์การใช้งาน	ตรวจสอบจำนวนคำขอเปิด ปรับปรุงระบบ และยกเลิกสิทธิ์ รวมถึงผลการดำเนินการตามคำขอ	รายเดือน / ตามคำขอ	IT / HR	หนังสือตอบกลับ
2	การทบทวนสิทธิ์การใช้งาน	ตรวจสอบผลการทบทวนสิทธิ์ของผู้ใช้งาน ผู้ดูแลระบบ และบัญชีสิทธิ์สูง	ตามรอบที่หน่วยงานกำหนด	HR / IT / เจ้าของระบบ	IT-FM-05, รายงานทบทวนสิทธิ์
3	การให้บริการระบบเครือข่ายและเครื่องแม่ข่าย	ติดตามสถานะการให้บริการ ปัญหาที่เกิดขึ้น การแก้ไข และระยะเวลาการดำเนินการ	รายเดือน / เมื่อเกิดเหตุ	IT	IT-FM-02, รายงานการให้บริการ
4	การสำรองและกู้คืนข้อมูล	ตรวจสอบผลการสำรองข้อมูล ความสำเร็จ/ไม่สำเร็จของการสำรองข้อมูล และผลการทดสอบกู้คืนข้อมูล	ตามรอบที่หน่วยงานกำหนด	IT / เจ้าของระบบ	IT-FM-06, Backup Log, Restore Report
5	การประเมินความเสี่ยงด้านไซเบอร์	ติดตามรายการความเสี่ยง ระดับความเสี่ยง มาตรการควบคุม และสถานะการดำเนินการลดความเสี่ยง	รายไตรมาส / ตามรอบที่กำหนด	IT / เจ้าของระบบ	IT-FM-04, Risk Register
6	การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	ติดตามจำนวนเหตุการณ์ ประเภทเหตุการณ์ ระดับความรุนแรง การตอบสนอง และบทเรียนหลังเหตุการณ์	เมื่อเกิดเหตุ / รายเดือน	IT / ผู้บริหาร	IT-FM-03, Incident Report, Log, Screenshot
7	การปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง	ตรวจสอบความครบถ้วนของหลักฐานที่เกี่ยวข้องกับกฎหมาย มาตรฐาน และข้อกำหนดด้านไซเบอร์	รายปี / เมื่อมีการเปลี่ยนแปลงข้อกำหนด	IT / ผู้รับผิดชอบ Compliance	Checklist กฎหมาย, รายงานทบทวน
8	การจัดเก็บหลักฐานและบันทึก	ตรวจสอบความครบถ้วนของแบบฟอร์ม Log รายงาน และเอกสารประกอบ เพื่อให้สามารถตรวจสอบย้อนหลังได้	รายไตรมาส / รายปี	IT	แบบฟอร์ม IT-FM-01 ถึง IT-FM-06, Log, รายงาน
9	การปรับปรุงกระบวนการงาน	ทบทวนปัญหา อุปสรรค ข้อเสนอแนะ และผลการดำเนินงาน เพื่อนำไปปรับปรุงคู่มือและแนวทางปฏิบัติ	รายปี / เมื่อมีเหตุสำคัญ	IT / ผู้บริหาร	รายงานสรุปผล, ข้อเสนอแนะ, บันทึกการประชุม

9. เอกสารอ้างอิง

- พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2565
- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566
- NIST Cybersecurity Framework 2.0

10. แบบฟอร์มที่ใช้

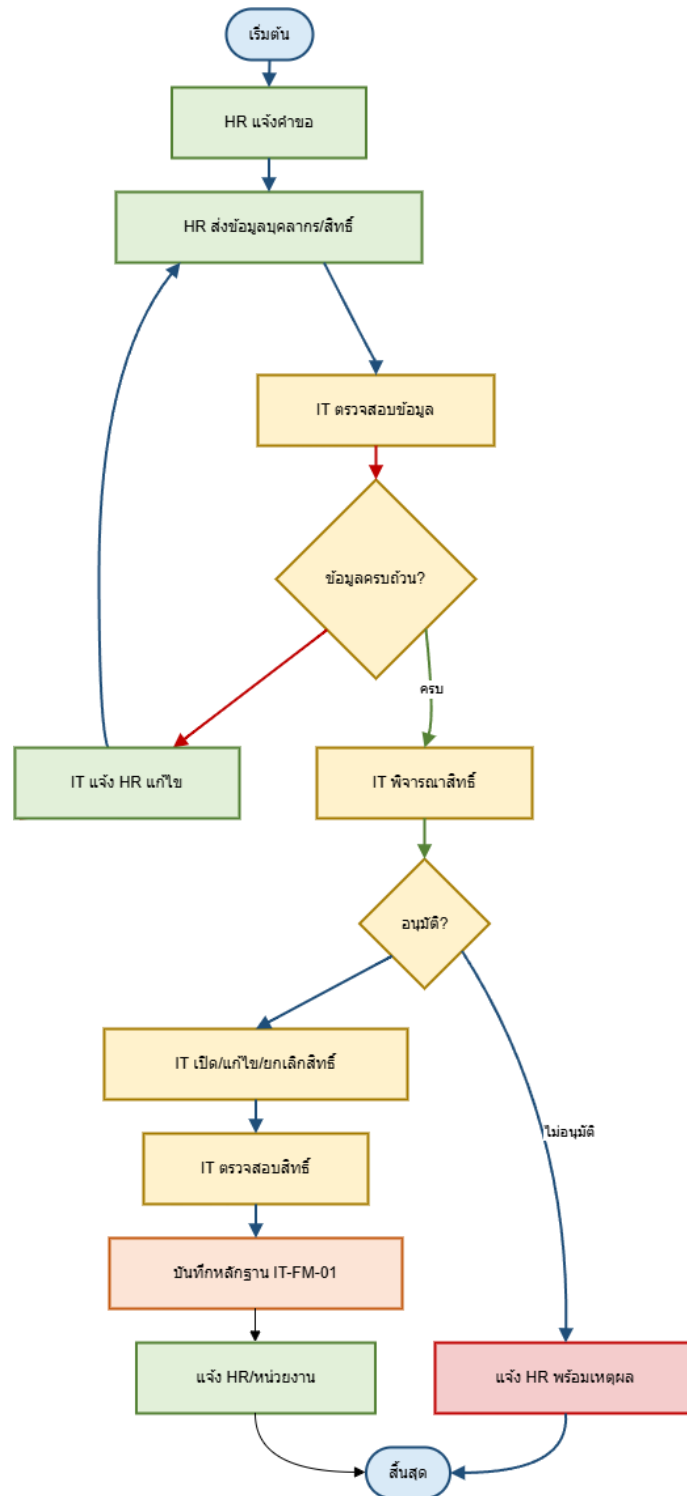
1. IT-FM-02 แบบฟอร์มบันทึกการให้บริการระบบเครือข่ายและเครื่องแม่ข่าย
2. IT-FM-03 แบบฟอร์มบันทึกเหตุการณ์ด้านไซเบอร์
3. IT-FM-04 แบบฟอร์มประเมินความเสี่ยงด้านไซเบอร์
4. IT-FM-05 แบบฟอร์มทบทวนสิทธิ์การใช้งาน
5. IT-FM-06 แบบฟอร์มรายงานผลการสำรองและกู้คืนข้อมูล

11. ภาคผนวก

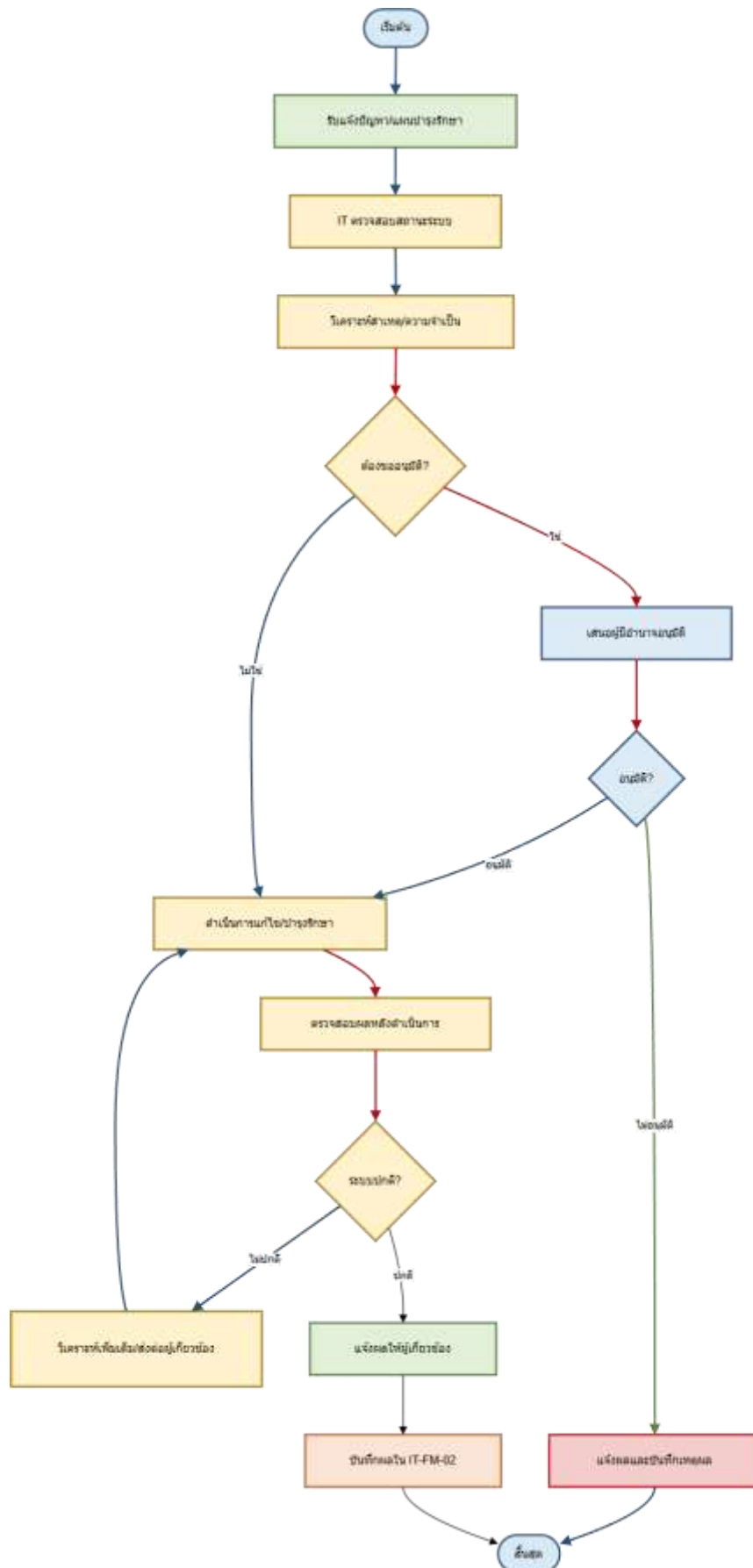
- ภาคผนวก ก แผนผัง Work Flow รายการกระบวนการ
- ภาคผนวก ข ตารางบทบาทและความรับผิดชอบ
- ภาคผนวก ค Checklist การตรวจสอบระบบเครือข่ายและเครื่องแม่ข่าย
- ภาคผนวก ง Checklist การปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง
- ภาคผนวก จ แบบฟอร์มที่ใช้

ภาคผนวก ก แผนผัง Work Flow รายการกระบวนการ

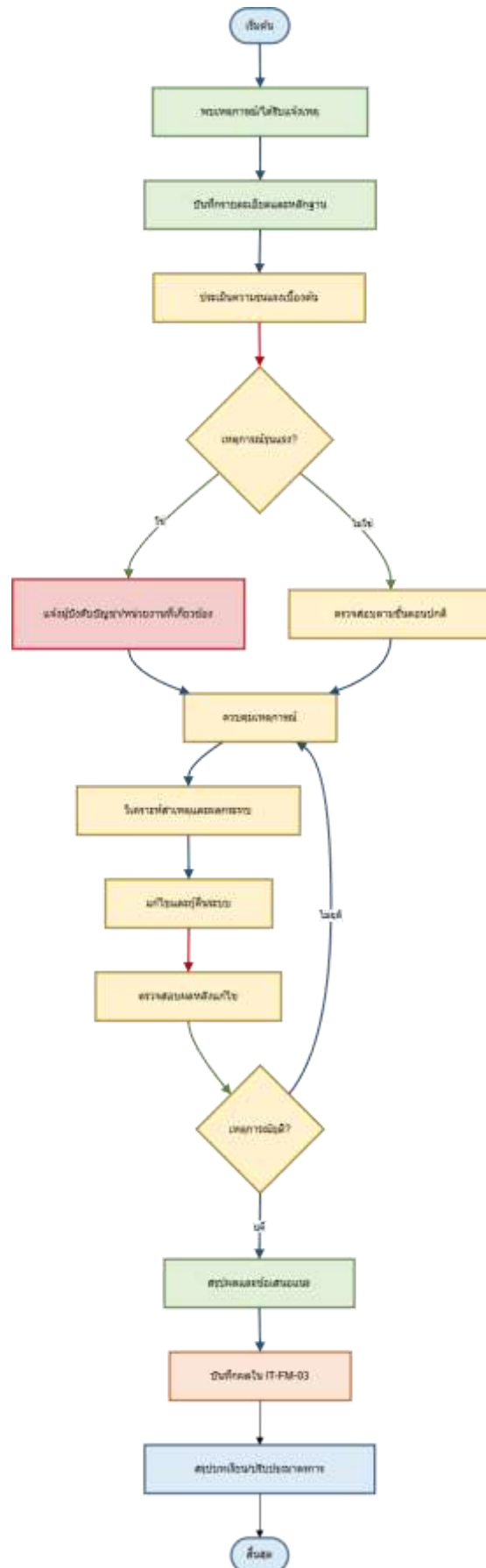
ก.1 การบริหารจัดการสิทธิ์การใช้งาน



ก.2 การให้บริการระบบเครือข่ายและการดูแลรักษาเครื่องแม่ข่าย



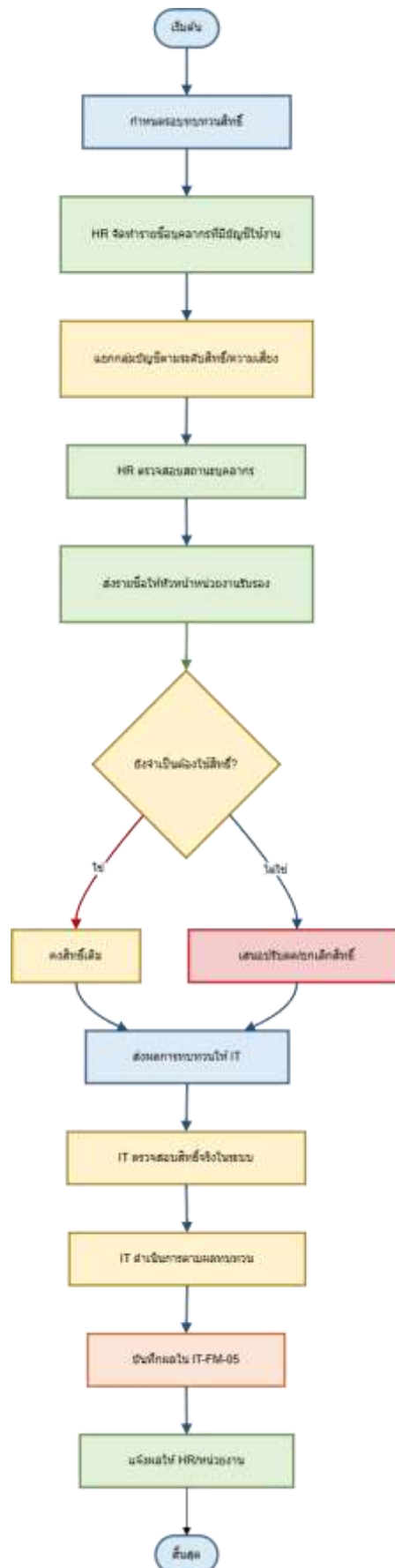
ก.3 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์



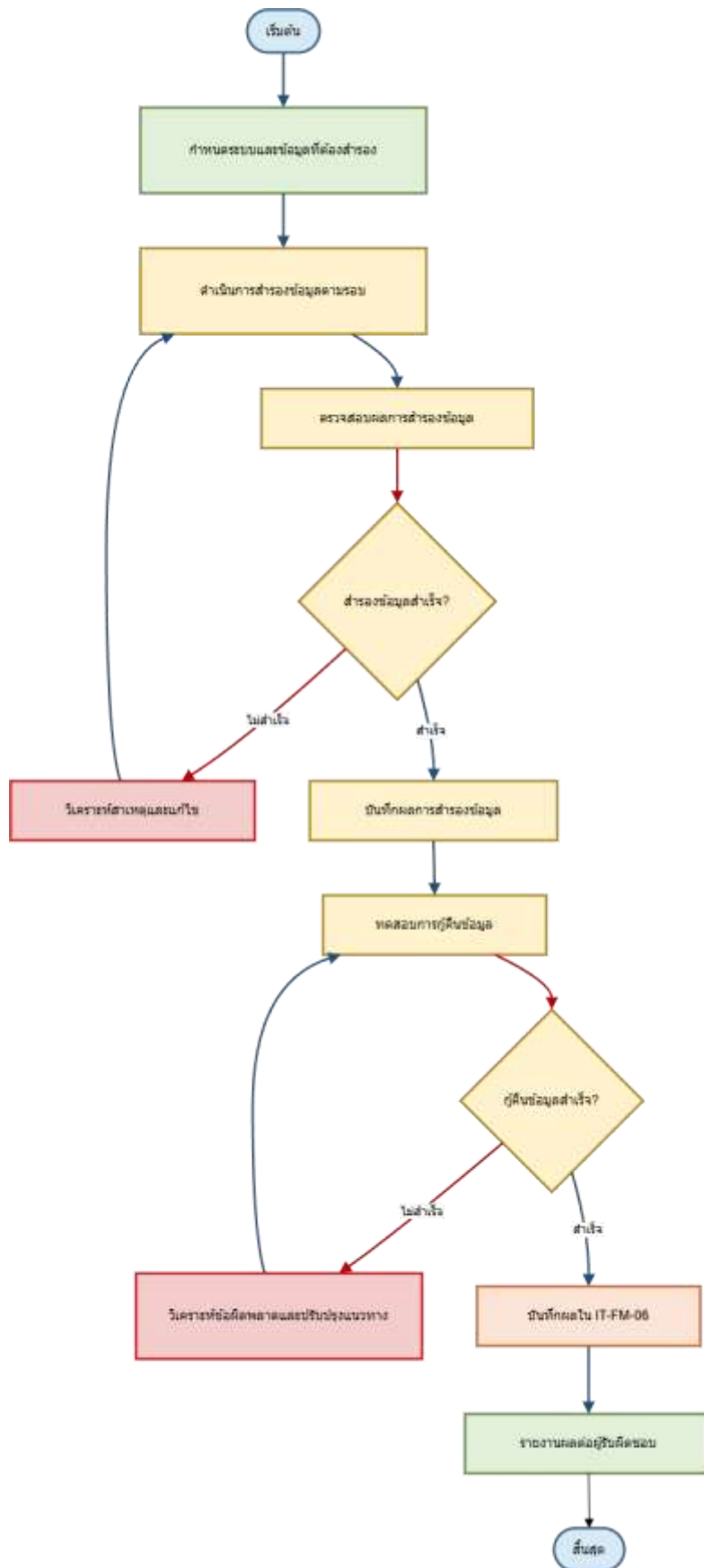
ก.4 การประเมินความเสี่ยงด้านไซเบอร์



ก.5 การทบทวนสิทธิการใช้งาน



ก.6 การสำรองและกู้คืนข้อมูล



ภาคผนวก ข ตารางบทบาทและความรับผิดชอบ

กิจกรรม	HR	IT	หัวหน้าหน่วยงาน	เจ้าของระบบ	ผู้บริหาร
เปิด/ปรับปรุง/ยกเลิกสิทธิ์	R	A/R	C	C	I
ทบทวนสิทธิ์	R	R	A/C	C	I
ให้บริการเครือข่าย/แม่ข่าย	I	A/R	C	C	I
บันทึกเหตุการณ์ไซเบอร์	I	A/R	I	C	I/A เมื่อรุนแรง
ประเมินความเสี่ยงไซเบอร์	I	R	C	A/R	I
สำรองและกู้คืนข้อมูล	I	A/R	I	C	I
ทบทวนกฎหมาย/มาตรฐาน	I	R	I	C	A/I

คำอธิบาย: R = Responsible, A = Accountable, C = Consulted, I = Informed

ภาคผนวก ค Checklist การตรวจสอบระบบเครือข่ายและเครื่องแม่ข่าย

ลำดับ	รายการตรวจสอบ	สถานะ	หลักฐาน/หมายเหตุ
1	ตรวจสอบสถานะการทำงานของเครื่องแม่ข่ายและบริการสำคัญ	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
2	ตรวจสอบ CPU, Memory, Disk และ Network Utilization	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
3	ตรวจสอบสถานะ Firewall, Switch, Router, Wireless Controller หรืออุปกรณ์ที่เกี่ยวข้อง	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
4	ตรวจสอบ Patch หรือ Security Update	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
5	ตรวจสอบ Antivirus/Endpoint Protection	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
6	ตรวจสอบ Log เหตุการณ์ผิดปกติ	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
7	ตรวจสอบบัญชีผู้ดูแลระบบและสิทธิ์พิเศษ	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
8	ตรวจสอบผลการสำรองข้อมูลล่าสุด	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
9	ตรวจสอบการตั้งค่าเวลา NTP	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	
10	ตรวจสอบเอกสารการเปลี่ยนแปลงค่าคอนฟิก	[] ผ่าน [] ไม่ผ่าน [] ไม่เกี่ยวข้อง	

ภาคผนวก ง Checklist การปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

ลำดับ	ประเด็นตรวจสอบ	กฎหมาย/มาตรฐานที่เกี่ยวข้อง	สถานะ	หลักฐาน	หมายเหตุ
1	มีการกำหนดผู้รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์	พ.ร.บ.ไซเบอร์ / NIST CSF 2.0	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		
2	มีการบริหารจัดการสิทธิ์ผู้ใช้งานและสิทธิ์ผู้ดูแลระบบ	NIST CSF 2.0 / แนวทางภายใน	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		
3	มีการบันทึกและตรวจสอบ Log ของระบบสำคัญ	พ.ร.บ.คอมพิวเตอร์ / NIST CSF 2.0	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		
4	มีมาตรการคุ้มครองข้อมูลส่วนบุคคลในระบบที่เกี่ยวข้อง	พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		
5	มีการสำรองข้อมูลและทดสอบการกู้คืน	NIST CSF 2.0 / แนวทาง BCP/DRP	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		
6	มีขั้นตอนตอบสนองเหตุการณ์ด้านไซเบอร์	NIST CSF 2.0 / แนวทาง Incident Response	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		
7	มีข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก	NIST CSF 2.0 / สัญญา/SLA	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		
8	มีการทบทวนความเสี่ยงด้านไซเบอร์เป็นระยะ	NIST CSF 2.0 / ISO 31000/ISO 27005 (อ้างอิงแนวคิด)	☐ มี ☐ ไม่มี ☐ ต้องตรวจสอบเพิ่มเติม		

ภาคผนวก จ แบบฟอร์มที่ใช้

รหัสแบบฟอร์ม	ชื่อแบบฟอร์ม	วัตถุประสงค์การใช้
IT-FM-02	แบบฟอร์มบันทึกการให้บริการระบบเครือข่ายและเครื่องแม่ข่าย	ใช้บันทึกการให้บริการ แก้ไขปัญหา และบำรุงรักษาระบบ
IT-FM-03	แบบฟอร์มบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	ใช้บันทึกเหตุการณ์ ความรุนแรง หลักฐาน และการตอบสนอง
IT-FM-04	แบบฟอร์มประเมินความเสี่ยงด้านไซเบอร์	ใช้ประเมินภัยคุกคาม ช่องโหว่ ผลกระทบ และมาตรการควบคุม
IT-FM-05	แบบฟอร์มทบทวนสิทธิ์การใช้งาน	ใช้ทบทวนความจำเป็นในการมีสิทธิ์ตามสถานะบุคลากรและระดับความเสี่ยง
IT-FM-06	แบบฟอร์มรายงานผลการสำรองและกู้คืนข้อมูล	ใช้รายงานผล Backup และการทดสอบ Restore