CORRECTIVE ACTION PROCEDURE

(ISMS-PC-12)

แก้ไขครั้งที่ 2.2

กองทุนเพื่อความเสมอภาคทางการศึกษา

Equitable Education Fund

การควบคุมเอกสาร

ผู้เรียบเรียง/ผู้จัดทำ	ผู้ตรวจสอบ/ผู้ทบทวน	ผู้อนุมัติ
ธนศักดิ์ สุกรีวนัส (ธนศักดิ์ สุกรีวนัส)	ศุภชัย กาญจนโภคิน (ศุภชัย กาญจนโภคิน)	(สุชาดา จัตุรภุชพิทักษ์)
นักวิชาการ สำนักเทคโนโลยีสารสนเทศ	ผู้อำนวยการ สำนักเทคโนโลยีสารสนเทศ	ผู้ช่วยผู้จัดการ (ด้านระบบงาน)
วันที่ 14 ธ.ค. 2566	วันที่ 19 ธ.ค. 66	วันที่ 16 ม.ค. 67

ประวัติการปรับปรุงเอกสาร

ครั้งที่	วันที่อนุมัติ	ผู้จัดทำ	รายละเอียดการแก้ไข
1.0	23 ก.ย. 2562	รุ่งอนันต์ ศิรินิยมชัย	ประกาศใช้ครั้งแรก
2.0	05 ม.ค. 2564	เปรมฤดี กังวานวงศ์	ทบทวนเอกสารให้สอดคล้องกับโครงสร้าง ISMS และ Document Owner
2.1	27 ธ.ค. 2565	สุเทพ ทองแดง	ทบทวนเอกสารและปรับปรุง - ปรับชื่อจาก ศูนย์เทคโนโลยีสารสนเทศ เปลี่ยนเป็น สำนักเทคโนโลยีสารสนเทศ
2.2	16 ม.ค. 2567	ธนศักดิ์ สุกรีวนัส	ทบทวนเอกสาร

สารบัญ

หน้า

1. บทนำ

1.1 วัตถุประสงค์

- เพื่อกำหนดกระบวนการมาตรฐานในการควบคุม แก้ไข และป้องกันปัญหา ข้อบกพร่อง หรือสิ่งที่ไม่สอดคล้องตามข้อกำหนดในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร
- เพื่อเป็นแนวทางในการป้องกันปัญหาหรือสิ่งที่ไม่เป็นไปตามข้อกำหนดที่มีโอกาสเกิดขึ้นได้

1.2 ขอบเขตการใช้งาน

ครอบคลุมการแก้ไข/ป้องกันปัญหาหรือสิ่งที่ไม่เป็นไปตามข้อกำหนดในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1.3 คำจำกัดความ

ลำดับที่	คำ	ความหมาย
1	องค์กร	กองทุนเพื่อความเสมอภาคทางการศึกษา หรือ กสศ.
2	Information Security Management Representative (ISMR)	ตัวแทนฝ่ายบริหารระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ
3	Information Security Management Assistance (ISMA)	ผู้ช่วยตัวแทนฝ่ายบริหารระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ
4	Corrective Action	การดำเนินการแก้ไขข้อบกพร่องหรือสิ่งที่ไม่เป็นไปตามข้อกำหนดและป้องกันการเกิดข้อบกพร่องขึ้นซ้ำ

2. ขั้นตอนการปฏิบัติงาน

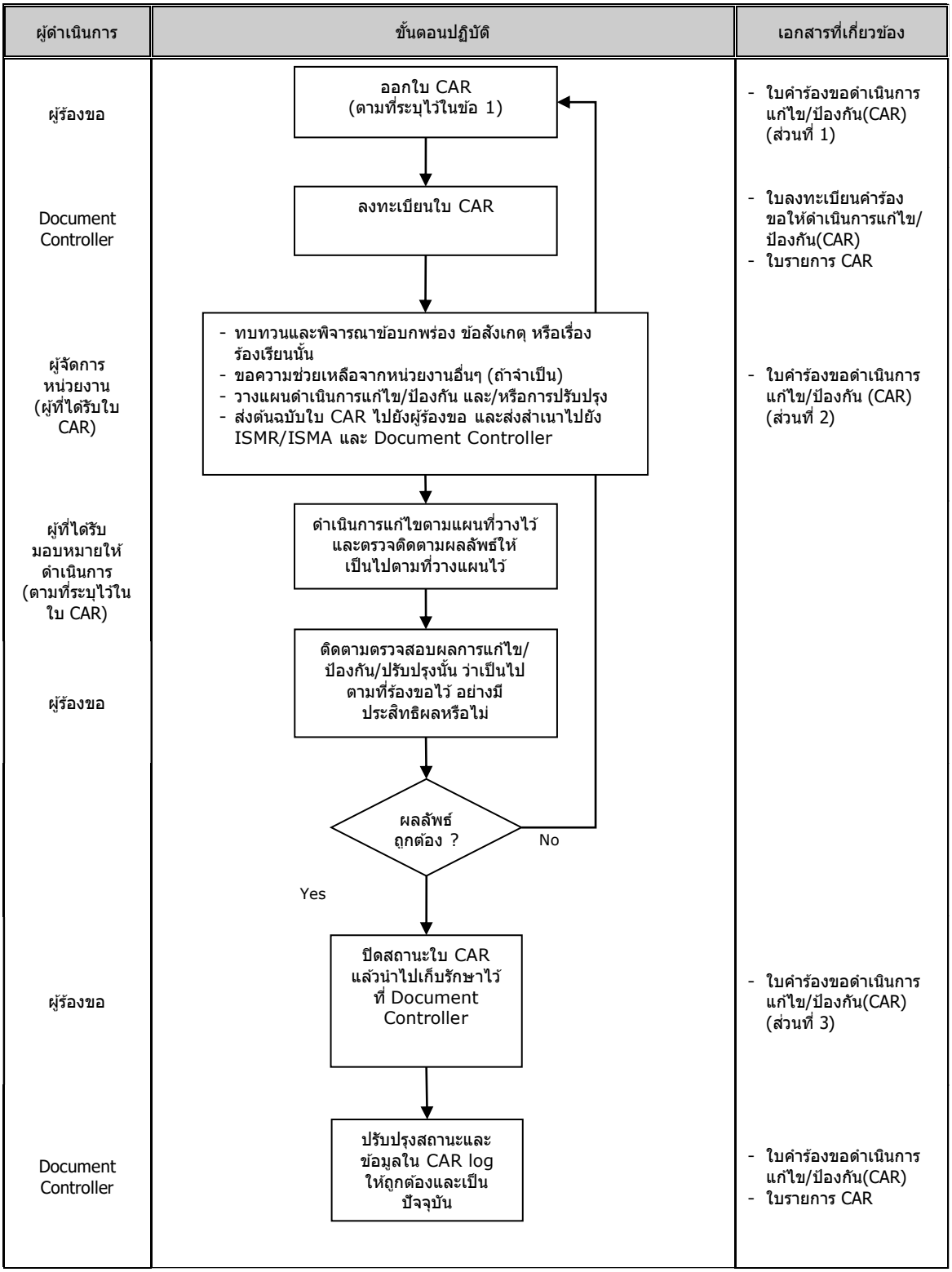
2.1 แหล่งที่มาของการดำเนินการแก้ไข/ป้องกัน

ใบคำร้องขอดำเนินการแก้ไข/ป้องกัน (CAR) ต้องถูกจัดทำขึ้นเมื่อ

- พบข้อบกพร่องหรือสิ่งที่ไม่เป็นไปตามข้อกำหนด
- มีแนวโน้มว่าจะเกิดข้อบกพร่องหรือสิ่งที่ไม่เป็นไปตามข้อกำหนดขึ้น
- พบประเด็นที่สามารถพัฒนาปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรให้ดียิ่งขึ้น
- ผู้ดำเนินการออกใบคำร้องขอดำเนินการแก้ไข/ป้องกัน (CAR) ให้อ้างอิงจากตารางต่อไปนี้

สถานการณ์	ผู้มีหน้าที่ออก CAR
การตรวจประเมินภายใน (Internal audits)	หัวหน้าทีมผู้ตรวจประเมิน/ผู้ตรวจประเมิน
การตรวจประเมินจากผู้ตรวจสอบภายนอกองค์กร (External audits)	ISMR/ISMA
ระหว่างการปฏิบัติงาน (During operations) (เช่น พบว่าไม่มีการตรวจติดตามการเก็บบันทึก ไม่ทำตามขั้นตอนปฏิบัติงานที่วางไว้ หรือไม่ปฏิบัติตามนโยบาย หรือ SLA)	พนักงานผู้พบเห็น
เรื่องร้องเรียนจากผู้ใช้งานหรือบุคคลที่สาม	เจ้าหน้าที่ผู้รับเรื่องร้องเรียนนั้น
เหตุละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น (หลังจากผ่านขั้นตอนการแก้ไขเรียบร้อยแล้ว)	ทีมงานผู้รับผิดชอบในการแก้ไขเหตุละเมิด หรือ ISMR/ISMA

2.2 ขั้นตอนการดำเนินการแก้ไข



หมายเหตุ :

- Document Controller ต้องเป็นผู้ติดตามใบคำร้องขอดำเนินการแก้ไข/ป้องกัน ทุกใบและปรับปรุงสถานะลงในใบรายการ ISMS-FM-11 Corrective Action Request (CAR) Log เพื่อรายงานความคืบหน้าให้ ISMR/ISMA ทราบทุกเดือน
- การดำเนินการป้องกัน ต้องมีความเหมาะสมกับผลกระทบที่อาจเกิดขึ้นจากข้อบกพร่องหรือสิ่งที่ไม่เป็นไปตามข้อกำหนด
- ในกรณีที่เป็นเรื่องร้องเรียนจากผู้ใช้งานหรือบุคคลภายนอก ต้องมีการรายงานสาเหตุและวิธีการแก้ไขปัญหาไปยังผู้ใช้งานหรือบุคคลภายนอกให้รับทราบด้วย
- กระบวนการแก้ไข Corrective Action มีระยะเวลาดำเนินการ ดังนี้

  1) Conformity ไม่ดำเนินการแก้ไข

  2) Non-Conformity: Major ดำเนินการแก้ไขให้แล้วเสร็จภายใน 20 วัน

  3) Non-Conformity: Minor ดำเนินการแก้ไขให้แล้วเสร็จภายใน 30 วัน

  4) Observation ดำเนินการแก้ไขให้แล้วเสร็จภายใน 90 วัน โดยพิจารณาปรับปรุงในข้อสังเกตที่เหมาะสมกับความคุ้มค่าและบริบทองค์กร ทั้งนี้การแก้ไขปัญหาในบางกรณีอาจต้องใช้ทรัพยากรเพิ่มเติมในการแก้ไขปัญหา ซึ่งส่งผลให้ระยะเวลาที่ใช้ในการแก้ไขปัญหาเกินจากที่กำหนด

2.3 การรายงานผลการดำเนินการแก้ไข

- ISMR/ISMA ต้องตรวจติดตามและทบทวนผลลัพธ์ของการดำเนินการแก้ไข/ป้องกัน เพื่อให้มั่นใจว่ามีประสิทธิภาพ ประสิทธิผล โดยเฉพาะใบคำขอดำเนินการแก้ไข/ป้องกัน ISMS-FM-10 Corrective Action Request (CAR) Form ที่ล่าช้าหรือถูกปฏิเสธจากผู้ร้องขอ
- ISMR/ISMA ต้องทำการสรุปผลลัพธ์ของการดำเนินการแก้ไข/ป้องกัน เพื่อนำเสนอในการประชุมทบทวนของฝ่ายบริหาร (Management Review Meeting)

3. เอกสารอ้างอิง

ลำดับที่	ชื่อเอกสาร	หมายเหตุ
1	ISMS-FM-10 Corrective Action Request (CAR) Form	
2	ISMS-FM-11 Corrective Action Request (CAR) Log	

4. กฎหมายที่เกี่ยวข้อง

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พ.ศ. 2560
2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
5. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553