รายงานสรุปผลการทดสอบแผนกู้คืนระบบคอมพิวเตอร์เพื่อรองรับสถานการณ์ฉุกเฉิน (Disaster Recovery Plan)

ของกรมปศุสัตว์

ปี พ.ศ. 2569

ของ

ระบบการเชื่อมโยงข้อมูล National Single Windows (NSW) ระยะที่ 5

ระบบทะเบียนเกษตรกรผู้เลี้ยงสัตว์ ระยะที่ 2

และระบบบริการอิเล็กทรอนิกส์ด้านอาหารสัตว์และวัตถุอันตรายด้านการปศุสัตว์ e-Feed

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สารบัญ

หน้า

ระบบการเชื่อมโยงข้อมูล National Single Windows (NSW) ระยะที่ 5

หัวข้อในการทดสอบแผนกู้คืน : ระบบ NSW5 ไม่สามารถส่งข้อมูลใบอนุญาตต่าง ๆ ไปยังกรมศุลกากรได้

การวิเคราะห์ความเสี่ยง

ระดับโอกาสในการเกิดเหตุการณ์ (Likelihood) : ระดับ3 (ปานกลาง มีโอกาสเกิดบางครั้ง)

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood)		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
4	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	มีโอกาสเกิดบางครั้ง
2	ต่ำ	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
1	ต่ำมาก	มีโอกาสเกิดในกรณียกเว้น

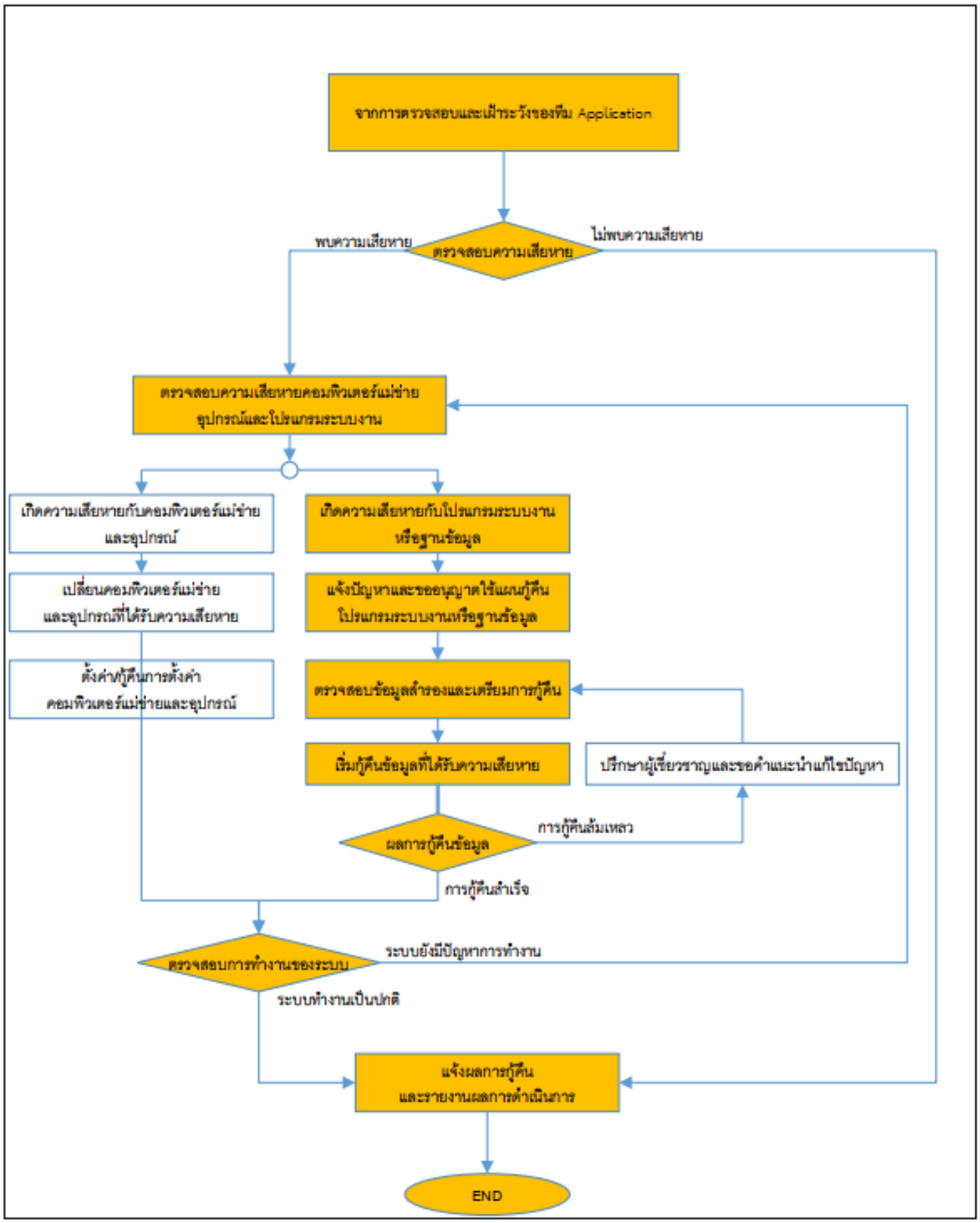
ระดับของผลกระทบ (Impact): ระดับ 4 (เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายต่อความปลอดภัยของข้อมูลต่างๆ บางส่วน)

ระดับความรุนแรงของผลกระทบ (Impact)		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	สูงมาก	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
4	สูง	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายต่อความปลอดภัยของข้อมูลต่างๆ บางส่วน
3	ปานกลาง	ระบบ IT มีปัญหาและมีความเสียหายไม่มาก
2	ต่ำ	ระบบ IT มีปัญหาและมีความเสียเพียงเล็กน้อยและสามารถแก้ไขได้
1	ต่ำมาก	ระบบ IT มีปัญหาซึ่งไม่เกิดผลกระทบต่อข้อมูลต่า ง ๆ

ระดับผลกระทบ : ระดับ 2

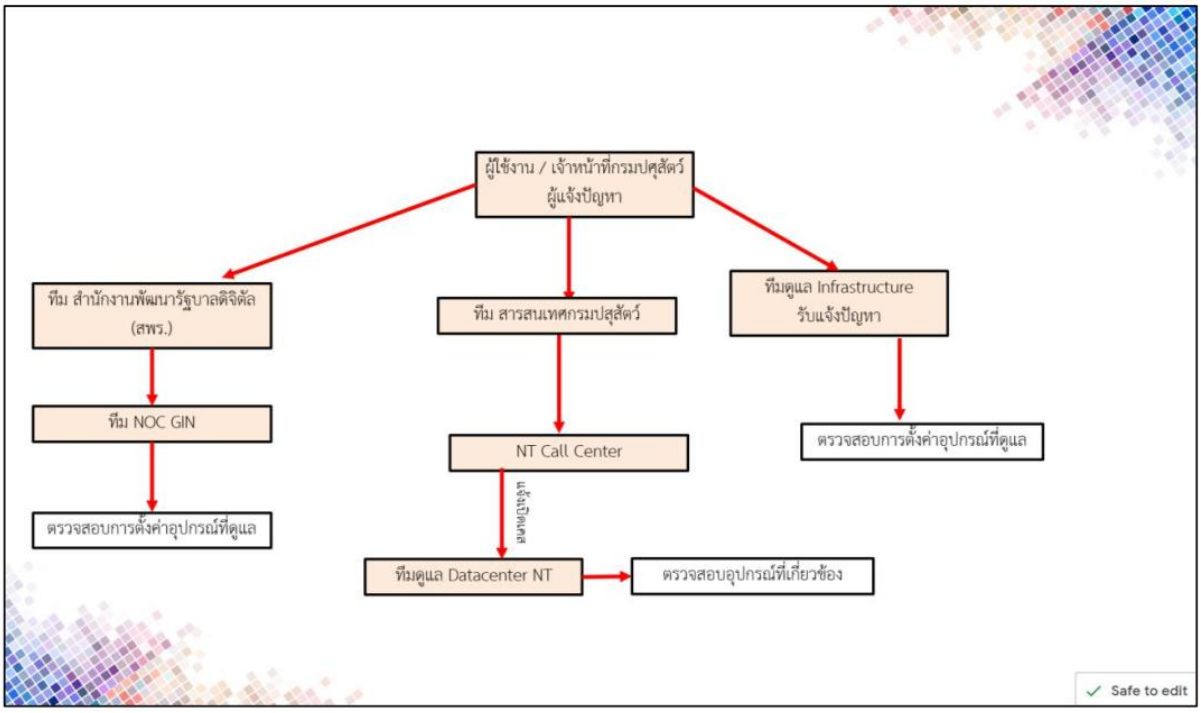
ภัยพิบัติและสถานการณ์ฉุกเฉิน	**โอกาสที่จะเกิด**	**ระดับผลกระทบ**	**คะแนนรวม**	**ระดับ**
เครือข่ายขัดข้อง	4	4	16	1
บุกรุกระบบคอมพิวเตอร์	4	4	16	1
ระบบ NSW5 ไม่สามารถส่งข้อมูลใบอนุญาตต่างๆ ไปยังกรมศุลกากร ได้	3	4	12	2
จราจล การชุมนุม/เหตุการณ์ความไม่สงบ	2	3	6	3
ไฟฟ้าดับ/ไฟฟ้าขัดข้อง	1	4	4	4
เพลิงไหม้	1	4	4	4
อุทกภัย	1	3	3	5
แผ่นดินไหว	1	3	3	5

ภาพรวมแผนผังการกู้คืนระบบกรณีเกิดสถานการณ์ฉุกเฉิน



กิจกรรมของแผน	กระบวนการสำคัญที่ต้องดำเนินการ
1. จากการตรวจสอบและเฝ้าระวังของทีม Applicationพบว่า ระบบ NSW Gateway ไม่สามารถเข้าใช้งานได้	ทีม Application ทำการตรวจสอบพบว่ามีเหตุผิดปกติ ทำการเก็บข้อมูลเกี่ยวกับปัญหา
2. ตรวจสอบความเสียหาย	ตรวจสอบรายละเอียดตามที่ได้ทำการตรวจสอบและเฝ้าระวังของทีม Application
3. ตรวจสอบความเสียหาย คอมพิวเตอร์แม่ข่าย อุปกรณ์และระบบงาน	ตรวจสอบหาต้นเหตุความผิดปกติ
4. เกิดความเสียหายกับคอมพิวเตอร์แม่ข่ายและอุปกรณ์	ตรวจพบสาเหตุความผิดปกติเกิดจากคอมพิวเตอร์แม่ข่าย หรือ อุปกรณ์ เสียหาย
5. เปลี่ยนคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่ได้รับความเสียหาย	เปลี่ยนคอมพิวเตอร์แม่ข่ายและอุปกรณ์ที่ได้รับความเสียหาย สลับสายจากอุปกรณ์ที่เสียหายมายัง อุปกรณ์ทดแทน
6. ตั้งค่า/กู้คืนการตั้งค่า คอมพิวเตอร์แม่ข่ายและอุปกรณ์	ตั้งค่าต่างๆของระบบปฏิบัติการ หรือคืนค่าคอนฟิกให้กับอุปกรณ์
7. เกิดความเสียหายของโปรแกรมระบบงาน หรือ ฐานข้อมูล	ตรวจพบต้นตอความผิดปกติเกิดจากโปรแกรมระบบงาน หรือ ระบบจัดการฐานข้อมูล
8. แจ้งปัญหาและขออนุญาตการใช้แผนกู้คืน โปรแกรมระบบงาน หรือฐานข้อมูล	แจ้งรายละเอียดปัญหาที่เกิดขึ้น และขออนุญาต ใช้แผนกู้คืนโปรแกรมระบบงานหรือฐานข้อมูล
9. ตรวจสอบข้อมูลสำรองและเตรียมการกู้คืน	ทำการตรวจสอบไฟล์ข้อมูลที่สำรองไว้และเตรียมความพร้อมสำหรับการกู้คืน
10. เริ่มกู้คืนข้อมูลที่ได้รับความเสียหาย	เริ่มดำเนินการกู้คืนข้อมูล
11. ผลการกู้คืนข้อมูล	ตรวจสอบผลการกู้คืนข้อมูล
12. ปรึกษาผู้เชี่ยวชาญและขอคำแนะนำแก้ไขปัญหา	หากการกู้คืนข้อมูลเกิดปัญหา และไม่สามารถแก้ไขได้ ให้ติดต่อขอคำแนะนำจากผู้เชี่ยวชาญ

ภาพแผนผังการกู้คืนกรณีระบบ NSW5 ไม่สามารถส่งข้อมูลใบอนุญาตต่าง ๆ ไปยังกรมศุลกากรได้



กิจกรรมของแผน	กระบวนการสำคัญที่ต้องดำเนินการ
1. จากการตรวจสอบและเฝ้าระวังของทีม Application พบว่า ระบบ NSW ไม่สามารถส่งข้อมูลไปยังกรมศุลกากรได้	ทีม Application ทำการตรวจสอบพบว่ามีเหตุผิดปกติ ทำการเก็บข้อมูลเกี่ยวกับปัญหา
2. ตรวจสอบความเสียหาย	ตรวจสอบรายละเอียดตามที่ได้ทำการตรวจสอบและเฝ้าระวังของทีม Application
3. เกิดความเสียหายของโปรแกรมระบบงาน หรือ ฐานข้อมูล	ตรวจพบต้นตอความผิดปกติเกิดจากโปรแกรมระบบงาน หรือ ระบบจัดการฐานข้อมูล
4. แจ้งปัญหาและขออนุญาตการใช้แผนกู้คืน โปรแกรมระบบงาน หรือฐานข้อมูล	แจ้งรายละเอียดปัญหาที่เกิดขึ้น และขออนุญาต ใช้แผนกู้คืนโปรแกรมระบบงานหรือฐานข้อมูล
5. ตรวจสอบข้อมูลสำรองและเตรียมการกู้คืน	ทำการตรวจสอบไฟล์ข้อมูลที่สำรองไว้ และเตรียมความพร้อมสำหรับการกู้คืน
6. เริ่มกู้คืนข้อมูลที่ได้รับความเสียหาย	เริ่มดำเนินการกู้คืนข้อมูล
7. ตรวจสอบการทำงานของระบบ	หลังจากการกู้คืนข้อมูลของโปรแกรมระบบงานหรือเครื่องคอมพิวเตอร์แม่ข่ายสำเร็จ ให้ทำการตรวจสอบการใช้งานอีกครั้ง

กิจกรรมของแผน	กระบวนการสำคัญที่ต้องดำเนินการ
8. แจ้งผลการกู้คืนและรายงานผลการดำเนินการ	เมื่อโปรแกรมระบบงานหรือเครื่องคอมพิวเตอร์แม่ข่าย สามารถใช้งานได้ปกติให้ทำการแจ้งผลการกู้คืนแก่เจ้าหน้าที่กรมปศุสัตว์และผู้ใช้งาน และรายงานผลการดำเนินการ

สรุปผลการทดสอบแผนกู้คืน

แผนทดสอบการกู้คืน ระบบการเชื่อมโยงข้อมูล National Single Windows (NSW) ระยะที่ 5 ปีงบประมาณ พ.ศ. 2569 เป นการจำลองสถานการณ์ Switch Broadband GIN IP 10.120.177.73 และ Gateway GIN IP 10.120.177.254 พบว่าไม่สามารถ เชื่อมต่อได้ส่งผลให้การส่งข้อมูลไปยังกรมศุลกากรไม่สำเร็จ

ทำการตรวจสอบทั้งด้าน Application กับ Hardware พบว่าไม่พบความผิดปกติ โดยตรวจสอบเพิ่มเติมพบว่าเป นปัญหา ที่ Switch Board brand เรื่องการ Config และทำการแก้ไข Config ใหม่

ผลการกู้คืนและทดสอบ: ใบอนุญาตสามารถส่งข้อมูลไปหา NSW กรมศุลกากรได้ปกติ

ระยะเวลาการดำเนินการ

หัวข้อ	ระยะเวลาประมาณการ	ระยะเวลาในการดำเนินการจริง
ระบบ NSW5 ไม่สามารถส่งข้อมูลใบอนุญาตต่างๆ ไปยัง กรมศุลกากรได้	7 ชั่วโมง 15 นาที	4 ชั่วโมง 50 นาที

แนวทางการบำรุงรักษา

- ตรวจสอบการสำรองข้อมูลโปรแกรมระบบงาน ของโครงการเป นประจำ
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายเป นประจำ
- สำรองข้อมูลแบบรายวันและรายเดือน และจัดเก็บไว้อย่างน้อย 7 วันย้อนหลัง

ข้อแนะนำการตรวจสอบเบื้องต้น

- หากไม่สามารถเข้าใช้งานผ่านเว็บไซต์ได้ เบื้องต้นต้องตรวจสอบระบบการป้องกันเครือข่าย (Firewall) และ ระบบเครือข่าย (Network)
- หากสามารถเข้าใช้งานผ่านเว็บไซต์ได้เป นบางครั้ง ต้องตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย

ระบบทะเบียนเกษตรกรผู้เลี้ยงสัตว์ ระยะที่ 2

หัวข้อในการทดสอบแผนกู้คืน : บัญชีVPN รั่วไหลและบัญชีUser รั่วไหล

การวิเคราะห์ความเสี่ยง

ระดับโอกาสในการเกิดเหตุการณ์(Likelihood): ระดับ 3 (มีโอกาสในการเกิดบางครั้ง)

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood)		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
4	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อย ๆ
3	ปานกลาง	มีโอกาสเกิดบางครั้ง
2	ต่ำ	อาจมีโอกาสเกิดแต่นาน ๆ ครั้ง
1	ต่ำมาก	มีโอกาสเกิดในกรณียกเว้น

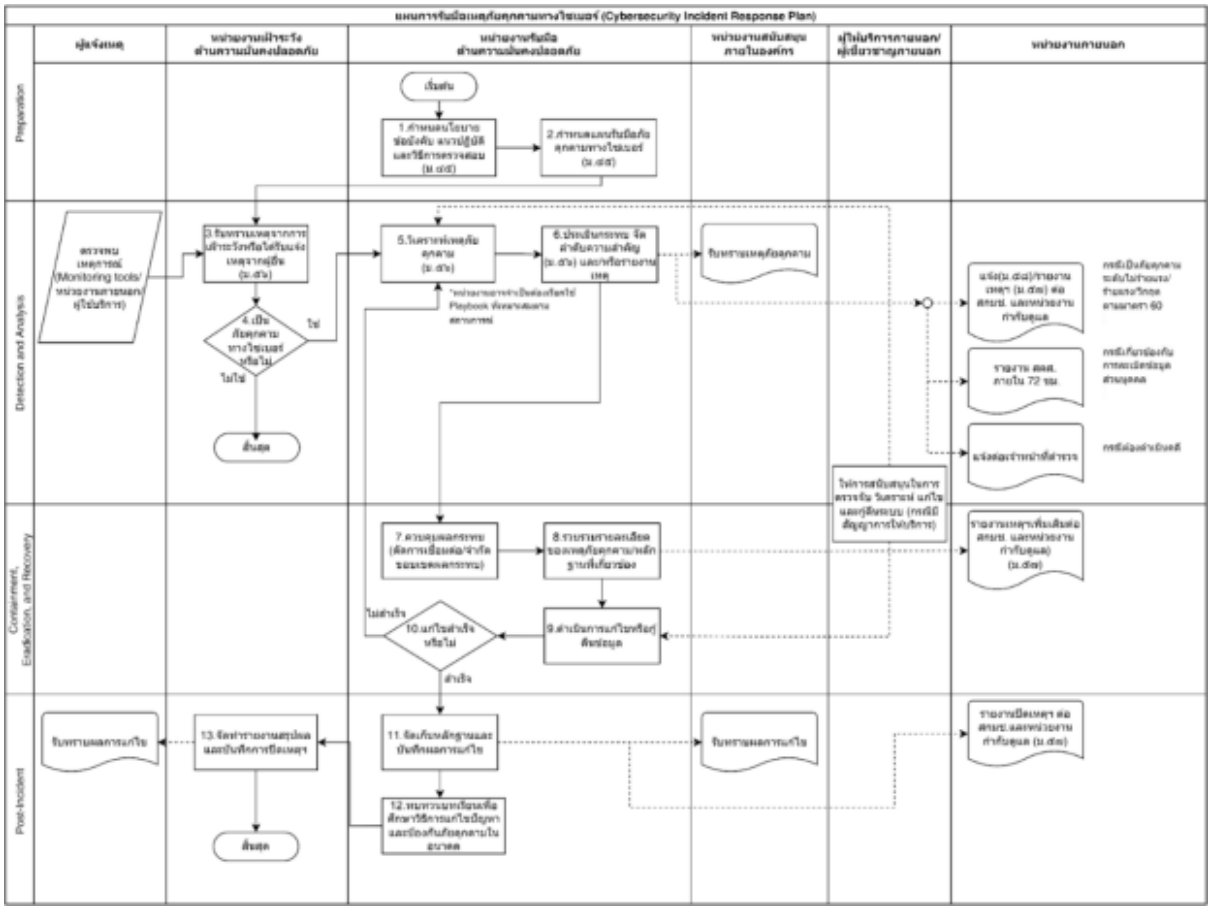
ระดับของผลกระทบ (Impact): ระดับ 5 เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลต่างๆ

ระดับความรุนแรงของผลกระทบ (Impact)		
ระดับ	**ระดับผลกระทบ**	**คำอธิบาย**
5	สูงมาก	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลต่าง ๆ
4	สูง	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายต่อความปลอดภัยของ ข้อมูลต่าง ๆ บางส่วน
3	ปานกลาง	ระบบ IT มีปัญหา และมีความเสียหายไม่มาก
2	ต่ำ	ระบบ IT มีปัญหา และมีความเสียหายเพียงเล็กน้อย และสามารถแก้ไขได้
1	ต่ำมาก	ระบบ IT มีปัญหา ซึ่งไม่เกิดผลกระทบต่อข้อมูลต่าง ๆ

ระดับผลกระทบ: ระดับ 1

ภัยพิบัติและสถานการณ์ฉุกเฉิน	โอกาสที่จะเกิด	ระดับผลกระทบ	คะแนนรวม	ระดับ
เครือข่ายขัดข้อง	3	5	15	1
ภัยคุกคามทางระบบคอมพิวเตอร์	3	5	15	1
เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็นระบบฐานข้อมูลเกิดความเสียหาย	3	5	15	1
จลาจล การชุมนุม/เหตุการณ์ความไม่สงบ	3	4	12	3
ไฟฟ้าดับ/ไฟฟ้าขัดข้อง	3	2	6	4
เพลิงไหม้	1	4	4	5
อุทกภัย	1	4	4	5
แผ่นดินไหว	1	4	4	5

ภาพรวมแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

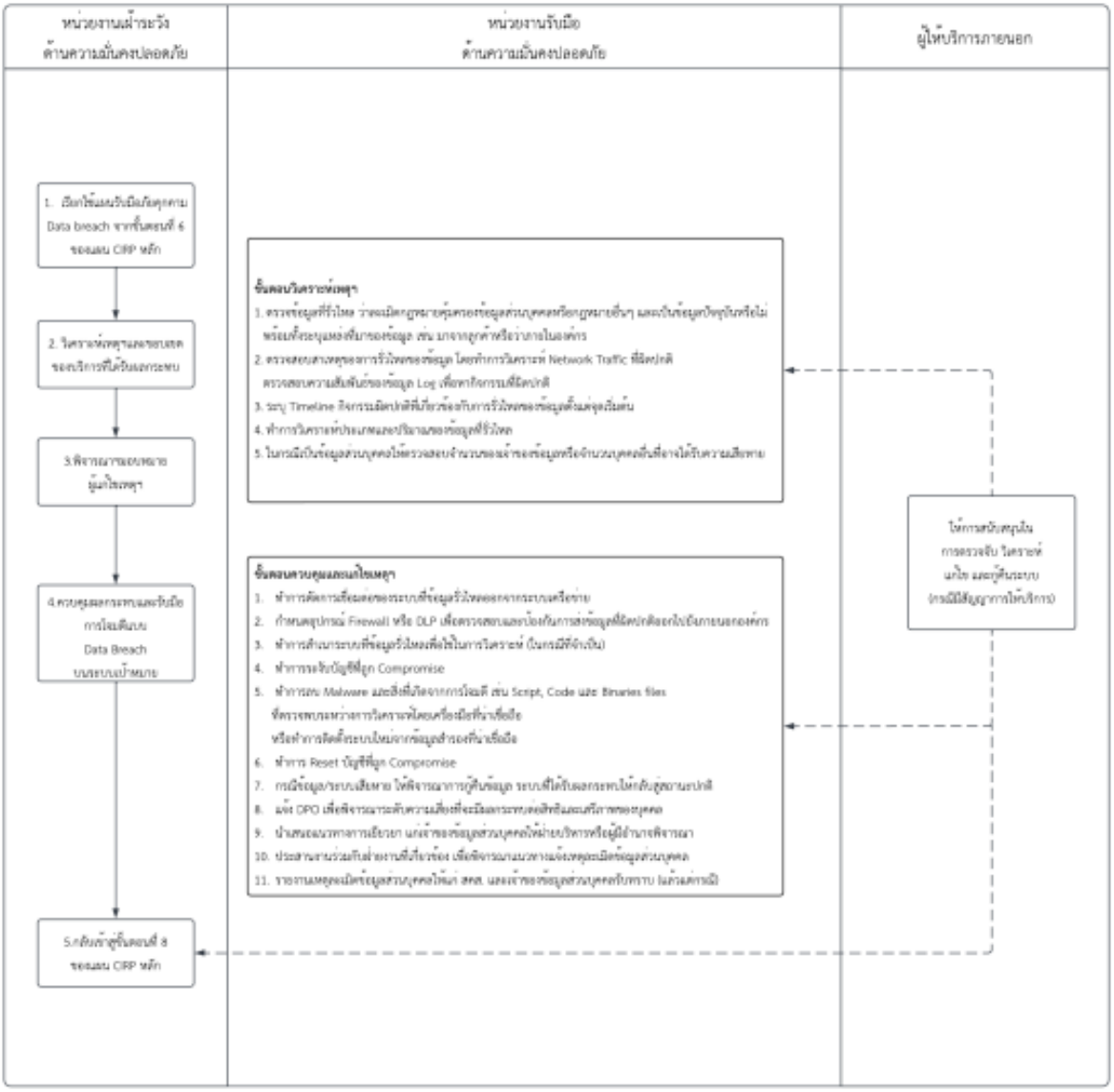


กิจกรรมของแผน	กระบวนการสำคัญที่ต้องดำเนินการ
ขั้นตอนการเตรียมการ (preparation)	
1. กำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบ	หน่วยงานรับมือด้านความมั่นคงปลอดภัย ร่วมกับผู้บริหารของหน่วยงาน กำหนดนโยบาย ข้อบังคับ แนวปฏิบัติและวิธีการตรวจสอบด้านความมั่นคงปลอดภัย โดยสอดคล้องตามประมวลแนวทาง ปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามมาตรา 13 วรรคหนึ่ง (4))
2. กำหนดแผนรับมือภัยคุกคามทางไซเบอร์	หน่วยงานรับมือด้านความมั่นคงปลอดภัย กำหนดแผนรับมือภัยคุกคามทางไซเบอร์โดยระบุ ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน กำหนดขั้นตอนและวิธีการในการรับมือกับ เหตุการณ์ภัยคุกคามทางไซเบอร์กำหนดผู้รับผิดชอบในแต่ละขั้นตอน และกำหนดให้มีการทดสอบ แผนรับมือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์(detection and analysis)	
3. รับทราบเหตุจากการเฝ้าระวังหรือได้รับแจ้งเหตุจากผู้อื่น	หน่วยงานรับมือด้านความมั่นคงปลอดภัย ได้รับทราบเหตุจากการเฝ้าระวัง (Monitoring tools) หรือได้รับแจ้งเหตุจากผู้อื่นที่ตรวจพบเหตุการณ์เช่น หน่วยงานภายนอก หรือ ผู้ใช้บริการ
4. ตรวจสอบว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาเหตุการณ์ว่าเป็นภัยคุกคามทางไซเบอร์ หรือไม่
5. ขั้นตอนวิเคราะห์เหตุภัยคุกคาม	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาประเภทของภัยคุกคาม หมวดหมู่ของภัยคุกคาม รายละเอียดแหล่งที่มาหรือต้นเหตุของภัยคุกคาม ข้อมูล จำนวนระบบ บริการ หรือ สินทรัพย์ที่ได้รับผลกระทบ
6. ประเมินผลกระทบ จัดลำดับความสำคัญ และ/หรือรายงานเหตุ	1. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ดำเนินการประเมินผลกระทบและจัดลำดับ ความสำคัญของเหตุภัยคุกคาม รวมถึงเลือกแนวทางในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ หมายเหตุ: หน่วยงานอาจจำเป็นต้องเรียกใช้ Playbook ที่เหมาะสมตามสถานการณ์

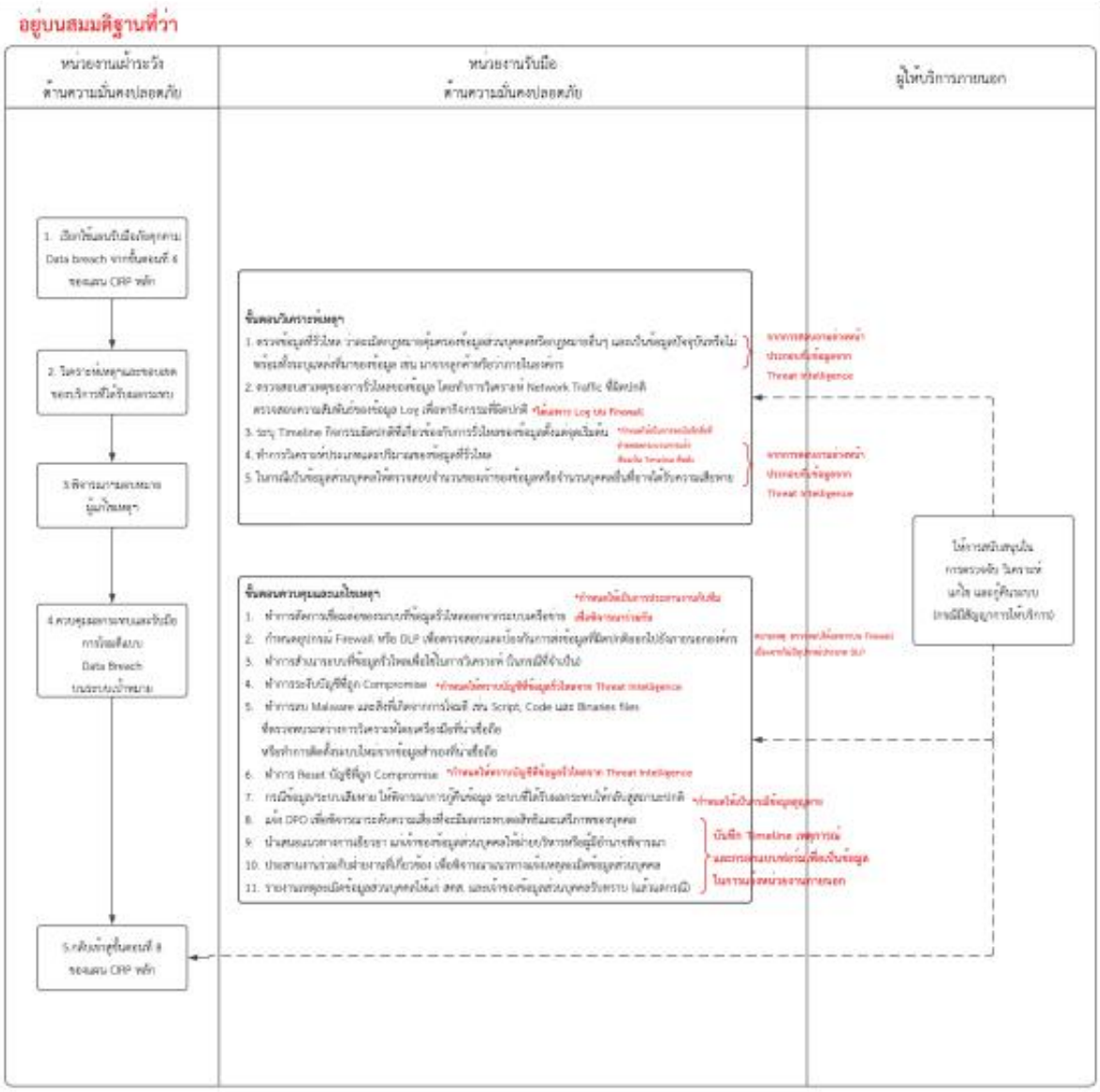
กิจกรรมของแผน	กระบวนการสำคัญที่ต้องดำเนินการ
	2. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงาน ต่าง ๆ • กรณีเป็นภัยคุกคามระดับไม่ร้ายแรง/ร้ายแรง/วิกฤต ตามมาตรา 60 หน่วยงานต้อง แจ้งเหตุภัยคุกคาม (มาตรา 58) (แบบฟอร์ม ก.1 หรือมีข้อมูลเทียบเท่า) และ/หรือ รายงานเหตุภัยคุกคาม (มาตรา 57) (แบบฟอร์ม ก.2) ต่อ สกมช. และหน่วยงานกำกับ ดูแล • กรณีเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล หน่วยงานอาจต้องแจ้งไปยัง สคส. • กรณีมีความจำเป็นต้องดำเนินคดีเนื่องจากเหตุนั้นเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง หน่วยงานอาจต้อง แจ้งไปยังเจ้าหน้าที่ตำรวจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication and recovery)	
7. ควบคุมผลกระทบ (ตัดการเชื่อมต่อ/จำกัดขอบเขตผลกระทบ)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ควรจำกัดขอบเขต (Containment) ผลกระทบของ เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทำการกำจัดสาเหตุ (Eradicate the incident) กำจัด หรือลบมัลแวร์และสาเหตุภัยคุกคามอื่น ๆ
8. รวบรวมรายละเอียดของเหตุภัยคุกคาม/หลักฐานที่เกี่ยวข้อง	1. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย บันทึกเหตุการณ์และดำเนินการจัดเก็บรักษา หลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มา ของบันทึกการ ยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน 2. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุการณ์เพิ่มเติมต่อ สกมช. และหน่วยงานกำกับดูแล (ม.57) (แบบฟอร์ม ก.2)
9. ดำเนินการแก้ไขหรือกู้คืนข้อมูล	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เรียกใช้งานกระบวนการกู้คืน (Recovery Process)
10. แก้ไขสำเร็จหรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาว่าระบบที่ได้รับผลกระทบจากภัยคุกคาม กลับสู่สถานะพร้อมใช้งานแล้วหรือไม่ หากยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ ตามปกติให้ดำเนินการต่อที่ขั้นตอนที่

	11 หากยังไม่สามารถแก้ไขได้ให้ดำเนินการขั้นตอนที่ 5 ซ้ำ เพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์อีกครั้ง
ขั้นตอนการดำเนินการภายหลังการแก้ไขปัญหาภัยคุกคามทางไซเบอร์(Post-Incident Activity)	
11. จัดเก็บหลักฐานและบันทึกผลการแก้ไข	1. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี 2. บันทึกผลการแก้ไขเหตุภัยคุกคามและวิธีการแก้ไขเพื่อจัดเก็บเป็นบทเรียน 3. รายงานปิดเหตุการณ์ต่อ สกมช. และหน่วยงานกำกับดูแล (ม.57) (แบบฟอร์ม ก.2)
12. ทบทวนบทเรียนเพื่อศึกษาวิธีการแก้ไขปัญหาและป้องกันภัยคุกคามในอนาคต	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว และกำหนดแนวทางในการป้องกันการเกิดเหตุซ้ำหรือป้องกันภัยคุกคามอื่นๆ ที่มีลักษณะคล้ายคลึงกันในอนาคต
13. จัดทำรายงานสรุปผลและบันทึกการปิดเหตุฯ	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดทำรายงานสรุปผลและบันทึกการปิดเหตุการณ์ รวมถึงแจ้งผลการแก้ไขไปยังผู้เกี่ยวข้องให้รับทราบ

ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook)



ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook) ในทางปฏิบัติ



กำหนดให้เหตุการณ์Data breach อยู่บนสมมติฐานที่ว่า

ขั้นตอนวิเคราะห์เหตุฯ

1. กำหนดให้ได้รับแจ้งรายชื่อของบัญชีผู้ใช้งานที่มีการรั่วไหลออกจากระบบแบบไม่มีการปิดกั้นข้อมูล (censored) เพื่อให้ สามารถนำบัญชีผู้ใช้งานที่รั่วไหลไปตรวจสอบและค้นหาในฐานข้อมูลได้ว่ามีพฤติกรรมผิดปกติหรือไม่ เนื่องจากในบางครั้ง ข้อมูลที่ทาง สกมช. แจ้งมาจะเป็นข้อมูลที่มีการเปิดเผยชื่อบัญชีผู้ใช้งานที่รั่วไหล แต่ในบางครั้งจะไม่มีการเปิดเผยชื่อผู้ใช้งาน หรือเป็นการเปิดเผยแค่ตัวอักษรแรก ทำให้ไม่สามารถค้นหาแบบเจาะจงได้ทำได้เพียงแค่ตรวจสอบระบบเครือข่ายว่ามีการ เชื่อมต่อที่ผิดปกติหรืออาจมีมัลแวร์หรือไม่
2. Log ที่นำมาวิเคราะห์เป็นของอุปกรณ์ป้องกันเครือข่าย (Firewall) เท่านั้นเนื่องจากในโครงการนี้ยังไม่ได้มีการติดตั้ง Agent ลงบนเครื่องคอมพิวเตอร์แม่ข่ายเพื่อเก็บ Log บนเครื่องคอมพิวเตอร์แม่ข่าย
3. กำหนดให้การตรวจสอบชนิดและปริมาณข้อมูลที่รั่วไหล เป็นการสอบถามปริมาณข้อมูลในระบบล่วงหน้าจากทีมผู้พัฒนาระบบเพื่อความรวดเร็วในการตรวจสอบเมื่อเกิดเหตุการณ์จริง

4. กำหนดให้การระบุTimeline กิจกรรมผิดปกติที่เกี่ยวข้องกับการรั่วไหลของข้อมูลตั้งแต่จุดเริ่มต้นเป็นการจดบันทึกสิ่งที่ทำ ตลอดกระบวนการแล้วเรียบเรียงเป็น Timeline ทีหลัง

ขั้นตอนการควบคุมและแก้ไขเหตุฯ

1. กำหนดเปลี่ยนจากการตัดการเชื่อมต่อของระบบที่ข้อมูลรั่วไหลออกจากระบบเครือข่ายเป็นการประสานงานร่วมกับทีม เพื่อพิจารณาร่วมกันว่าเหมาะสมที่จะตัดการเชื่อมต่อเลยหรือไม่ เนื่องจากระบบทะเบียนเกษตรเป็นระบบที่มีผู้ใช้งาน ตลอดเวลาและมีผลกระทบทางธุรกิจสูงหากทำการตัดการเชื่อมต่อทันที
2. กำหนดให้เป็นการตรวจสอบ Log บนอุปกรณ์ป้องกันเครือข่าย (Firewall) เนื่องจากในโครงการนี้ไม่มีอุปกรณ์ประเภท Data loss prevention (DLP)
3. กำหนดให้ทราบบัญชีที่ข้อมูลรั่วไหลจาก Threat Intelligenceเนื่องจากหากมีการปิดกั้น (censored)ชื่อบัญชีอาจไม่สามารถ ระบุได้ว่าเป็นบัญชีใดที่รั่วไหล หากไม่ได้มีการทำระบบเพื่อรองรับสถานการณ์นี้โดยเฉพาะเช่น ความสามารถในการดูการเข้าสู่ ระบบครั้งล่าสุดของผู้ใช้งานว่าตรงกับความเป็นจริงหรือไม่
4. กำหนดให้เป็นกรณีผู้ไม่หวังดีเข้ามาทำให้ข้อมูลในระบบสูญหายแต่ยังไม่ทำให้เครื่องคอมพิวเตอร์แม่ข่ายเสียหาย
5. กำหนดให้ข้อ 8 ถึง11 เป็นการบันทึกTimeline เหตุการณ์และกรอกแบบฟอร์มเพื่อเป็นข้อมูลในการแจ้งหน่วยงานภายนอกแทน

สรุปผลการทดสอบแผนกู้คืน

แผนทดสอบการกู้คืน ระบบทะเบียนเกษตรกรผู้เลี้ยงสัตว์ระยะที่ 2 เป็นการจำลองสถานการณ์บัญชีVPN รั่วไหล และบัญชีผู้ใช้งานรั่วไหล ส่งผลให้ผู้ไม่หวังดีสามารถเข้าสู่ภายในเครือข่ายและค้นหาฐานข้อมูลด้วยการสแกนพอร์ต โดยมีจุดประสงค์เพื่อต้องการจะนำข้อมูลออก อีกทั้งผู้ไม่หวังดียังมีการเข้าสู่ระบบเว็บไซต์เพื่อต้องการเก็บข้อมูลไปใช้ วางแผนการโจมตีต่อ

ผลการกู้คืนและทดสอบ: หลังจากได้รับแจ้งเหตุสามารถระงับบัญชีVPN ที่มีความผิดปกติและตรวจสอบบันทึกจราจรทางคอมพิวเตอร์และประสานไปยังทีมแอปพลิเคชันเพื่อให้ทำการรีเซ็ตบัญชีผู้ใช้งานเว็บไซต์ทำให้ ผู้ไม่หวังดีไม่สามารถเข้าถึงได้และทำการตรวจสอบฐานข้อมูลบัญชีผู้ใช้งาน ผลการตรวจสอบพบว่าไม่พบข้อมูลของ ชื่อผู้ใช้งานดังกล่าวในฐานข้อมูล จึงดำเนินการกู้คืนข้อมูลและตรวจสอบ ผลการตรวจสอบพบว่า ปรากฏข้อมูลของ ชื่อผู้ใช้งานดังกล่าวในฐานข้อมูลครบถ้วน ถูกต้องตรงตามข้อมูลเดิม ทั้งข้อมูลสิทธิ์การใช้งานและพื้นที่รับผิดชอบ

หัวข้อ	ระยะเวลาประมาณการ	ระยะเวลาในการดำเนินการจริง
บัญชีVPN และบัญชีผู้ใช้งานรั่วไหล	24 ชั่วโมง	22 ชั่วโมง 16 นาที

แนวทางการบำรุงรักษา

- ทำการตรวจสอบการเชื่อมต่อที่ผิดปกติเป็นประจำ

- หากเป็นไปได้แนะนำการพิจารณาติดตั้ง Agent เพื่อตรวจสอบกระบวนการทำงาน (process) ที่ผิดปกติบนเครื่องคอมพิวเตอร์แม่ข่าย แต่อาจต้องพิจารณาผลกระทบกับระบบงานในด้านการใช้ทรัพยากร

ข้อแนะนำการตรวจสอบเบื้องต้น

- ในระบบเครือข่ายสามารถตรวจสอบพฤติกรรมของการเข้าใช้งาน VPN ที่ผิดปกติเช่นจำนวนครั้งในการพยายาม เข้าสู่ระบบและ การเข้าสู่ระบบนอกเวลางาน

- สามารถตรวจสอบปริมาณในการรับส่งข้อมูล หากมีปริมาณสูงกว่าปกติอาจเป็นการสำรองข้อมูลหรือเป็นการ ถ่ายโอนข้อมูลออก

- สามารถตรวจสอบความพยายามในการเชื่อมต่อเข้ามายังฐานข้อมูล หากสูงเกินไปอาจแสดงถึงความผิดปกติ

ในส่วนการกู้คืนกรณีข้อมูลสูญหาย

สภาพปัญหา	ข้อมูลของชื่อผู้ใช้งาน a9401-02 สูญหายจากฐานข้อมูล ทำให้ไม่สามารถเข้าใช้งานระบบ ได้
วิธีการแก้ไข	กู้คืนฐานข้อมูล (Restore Database) บน Microsoft SQL Server จากไฟล์ข้อมูลสำรอง แบบเต็ม (Full Backup) และตรวจสอบยืนยันความถูกต้องของข้อมูล
ผลการดำเนินการ	ข้อมูลได้รับการกู้คืนครบถ้วน และผู้ใช้งานสามารถเข้าใช้งานระบบได้ตามปกติ

ข้อเสนอแนะและมาตรการป้องกัน

(1) กำหนดให้มีการสำรองข้อมูล (Backup) ฐานข้อมูลอย่างสม่ำเสมอตามรอบระยะเวลาที่กำหนด และจัดเก็บข้อมูลสำรองไว้แยกจากเครื่องแม่ข่ายหลัก

(2) จำกัดและควบคุมสิทธิ์การเข้าถึงฐานข้อมูล ให้เฉพาะเจ้าหน้าที่ผู้ได้รับมอบหมายเท่านั้น

(3) จัดเก็บบันทึกการใช้งานระบบ (Log) เพื่อใช้ตรวจสอบย้อนหลังเมื่อเกิดเหตุการณ์ผิดปกติ

ระบบบริการอิเล็กทรอนิกส์ด้านอาหารสัตว์และวัตถุอันตรายด้านการปศุสัตว์ e-Feed

หัวข้อในการทดสอบแผนกู้คืน: บัญชีผู้ใช้งานรั่วไหล

ระดับโอกาสในการเกิดเหตุการณ์ (Likelihood): ระดับ 3 (มีโอกาสในการเกิดบางครั้ง)

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood)		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
4	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	มีโอกาสเกิดบางครั้ง
2	ต่ำ	อาจมีโอกาสเกิดแต่นาน ๆ ครั้ง
1	ต่ำมาก	มีโอกาสเกิดในกรณียกเว้น

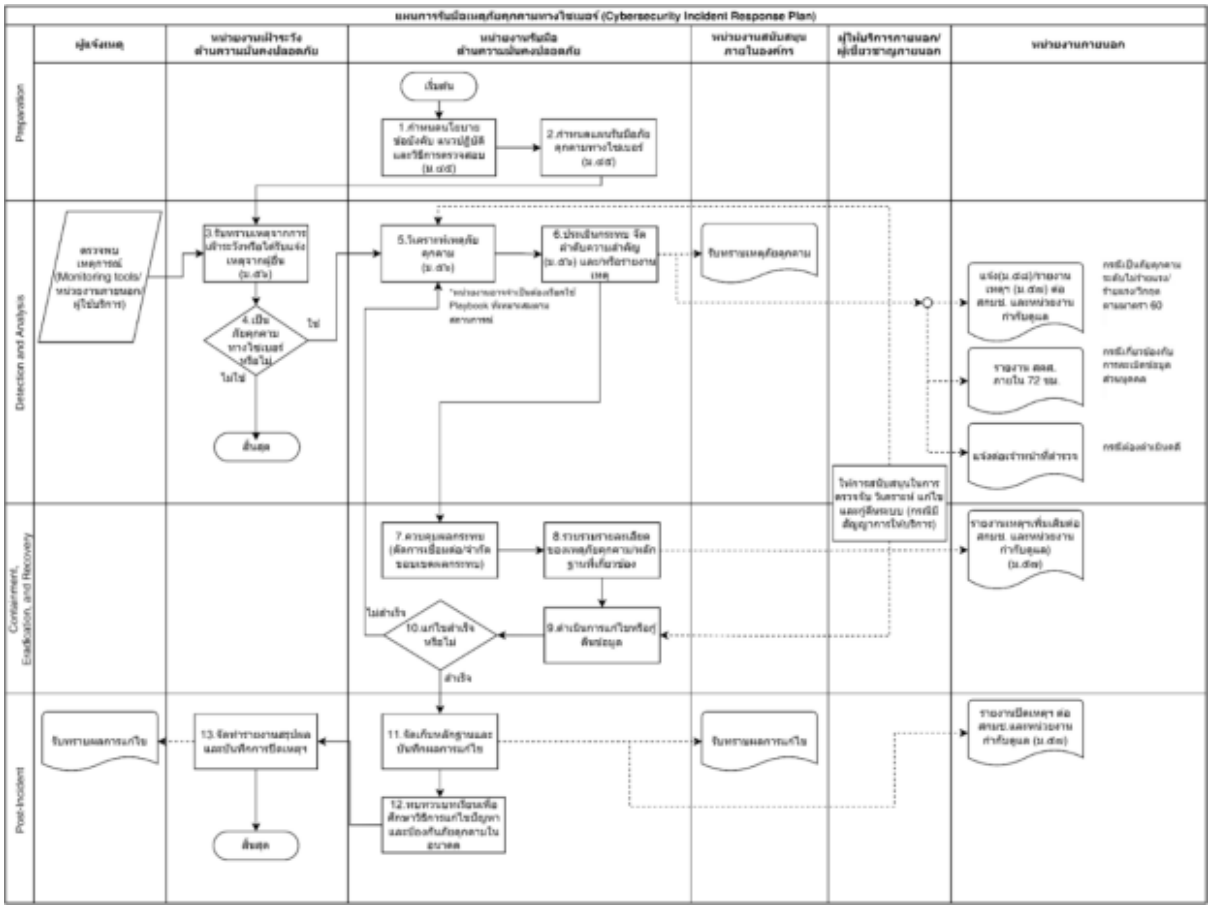
ระดับของผลกระทบ (Impact): ระดับ 5 เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลต่างๆ

ระดับความรุนแรงของผลกระทบ (Impact)		
ระดับ	**ระดับผลกระทบ**	**คำอธิบาย**
5	สูงมาก	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดความเสียหายต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายต่อความปลอดภัยของ ข้อมูลต่าง ๆ บางส่วน
3	ปานกลาง	ระบบ IT มีปัญหา และมีความเสียหายไม่มาก
2	ต่ำ	ระบบ IT มีปัญหา และมีความเสียหายเพียงเล็กน้อย และสามารถแก้ไขได้
1	ต่ำมาก	ระบบ IT มีปัญหา ซึ่งไม่เกิดผลกระทบต่อข้อมูลต่าง ๆ

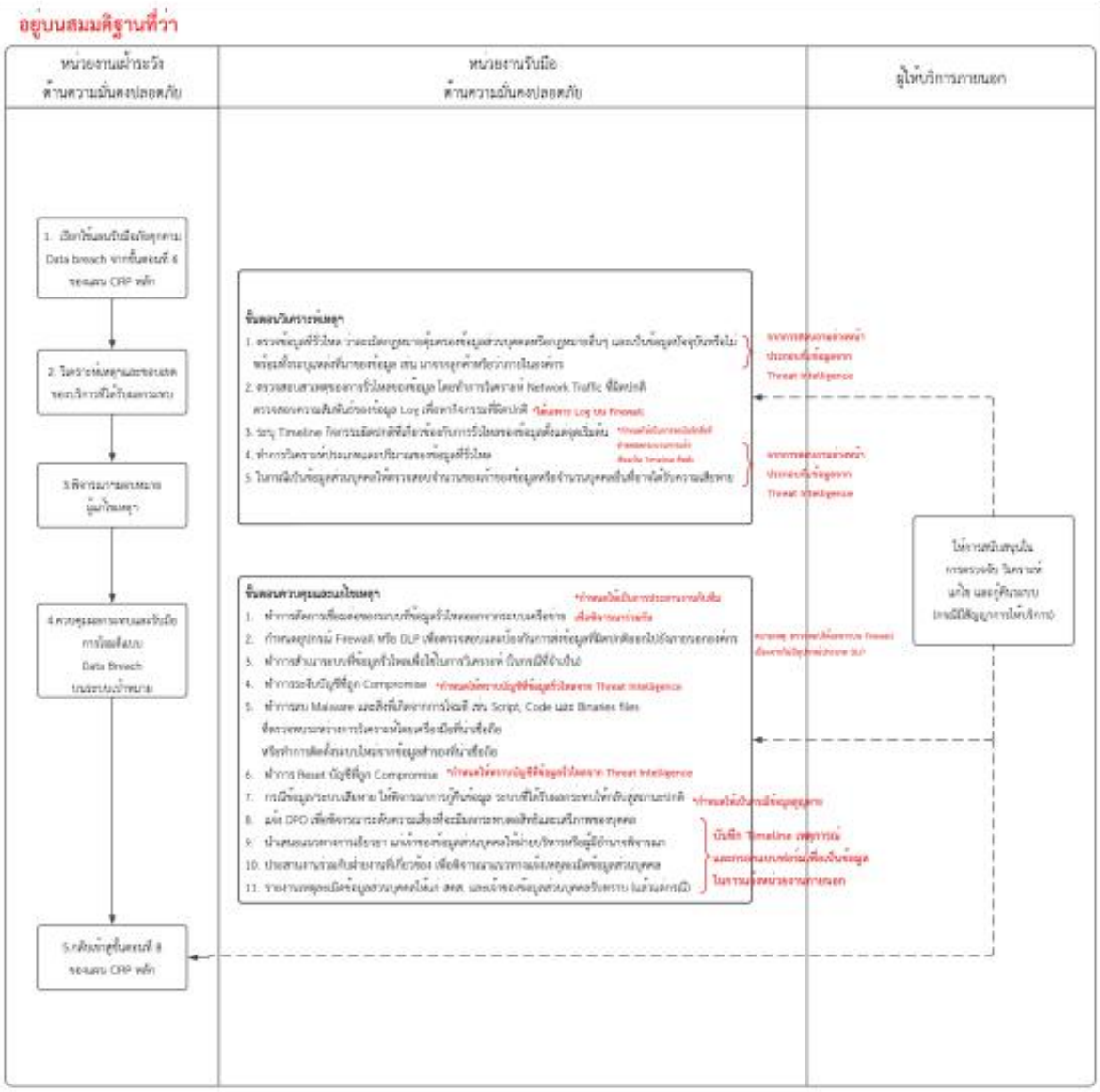
ระดับผลกระทบ: ระดับ 1

ภัยพิบัติและสถานการณ์ฉุกเฉิน	โอกาสที่จะเกิด	ระดับผลกระทบ	คะแนนรวม	ระดับ
เครือข่ายขัดข้อง	3	5	15	1
ภัยคุกคามทางระบบคอมพิวเตอร์	3	5	15	1
เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็นระบบ ฐานข้อมูลเกิดความเสียหาย	3	5	15	1
จลาจล การชุมนุม/เหตุการณ์ความไม่สงบ	3	4	12	3
ไฟฟ้าดับ/ไฟฟ้าขัดข้อง	3	2	6	4
เพลิงไหม้	1	4	4	5
อุทกภัย	1	4	4	5
แผ่นดินไหว	1	4	4	5

ภาพรวมแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)



ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook) ในทางปฏิบัติ



สรุปผลการทดสอบแผนกู้คืน

แผนทดสอบการกู้คืน ระบบเชื่อมโยงข้อมูลระบบ National Single Window (NSW) ระยะ 3 เป็นการจำลอง สถานการณ์บัญชีผู้ใช้งานระบบรั่วไหลและบัญชี VPN รั่วไหลส่งผลให้ผู้ไม่หวังดีสามารถเข้าสู่ภายในเครือข่ายและติดตั้ง มัลแวร์โดยมีจุดประสงค์เพื่อต้องการจะคงอยู่ในระบบและนำข้อมูลออกไปภายนอก

ผลการกู้คืนและทดสอบ: หลังจากได้รับแจ้งเหตุ สามารถระงับบัญชี VPN ที่มีความผิดปกติและตรวจสอบบันทึก จราจรทางคอมพิวเตอร์และประสานไปยังทีมแอปพลิเคชันเพื่อให้ทำการรีเซ็ตบัญชีผู้ใช้งานเว็บไซต์ทำให้ผู้ไม่หวังดี ไม่สามารถเข้าถึงได้

หัวข้อ	**ระยะเวลาประมาณการ**	**ระยะเวลาในการดำเนินการจริง**
บัญชีผู้ใช้งานระบบรั่วไหลและเครื่องออกรายงานติดมัลแวร์	21 ชั่วโมง 31 นาที	23 ชั่วโมง 46 นาที

แนวทางการบำรุงรักษา

- ทำการตรวจสอบการเชื่อมต่อที่ผิดปกติเป็นประจำ

- ทำการสแกนไวรัสอย่างสม่ำเสมอ

ข้อแนะนำการตรวจสอบเบื้องต้น

- ในระบบเครือข่ายสามารถตรวจสอบพฤติกรรมของการเข้าใช้งาน VPN ที่ผิดปกติเช่น จำนวนครั้งในการพยายามเข้าสู่ระบบและ การเข้าสู่ระบบนอกเวลางาน

- สามารถตรวจสอบปริมาณในการรับส่งข้อมูล หากมีปริมาณสูงกว่าปกติอาจเป็นการสำรองข้อมูลหรือเป็นการถ่ายโอนข้อมูลออก

- สามารถตรวจสอบความพยายามในการเชื่อมต่อเข้ามายังฐานข้อมูล หากสูงเกินไปอาจแสดงถึงความผิดปกติ

ในส่วนการกู้คืนกรณีข้อมูลสูญหาย

สภาพปัญหา	เครื่องออกรายงานไม่สามารถใช้งานได้
วิธีการแก้ไข	กู้คืนเครื่องคอมพิวเตอร์แม่ข่ายเสมือนจากข้อมูลสำรองและทำการตั้งค่าเครื่องออกรายงานให้กลับมาใช้งานได้
ผลการดำเนินการ	เครื่องออกรายงานสามารถใช้งานได้ตามปกติ

ข้อเสนอแนะและมาตรการป้องกัน

(1) กำหนดให้มีการสำรองข้อมูล (Backup) ฐานข้อมูลอย่างสม่ำเสมอตามรอบระยะเวลาที่กำหนด และจัดเก็บข้อมูลสำรองไว้แยกจากเครื่องแม่ข่ายหลัก

(2) จำกัดพอร์ตที่สามารถเข้าถึงจากภายนอกเท่าที่จำเป็นต่อการใช้งาน

(3) จัดเก็บบันทึกการใช้งานระบบ (Log) เพื่อใช้ตรวจสอบย้อนหลังเมื่อเกิดเหตุการณ์ผิดปกติ