

ประกาศกรมส่งเสริมการเกษตร
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของกรมส่งเสริมการเกษตร พ.ศ. ๒๕๖๙

เพื่อให้การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมส่งเสริมการเกษตร เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นมาตรฐานในการดำเนินการรักษาความปลอดภัยไซเบอร์

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ประกอบกับมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรมส่งเสริมการเกษตรจึงออกประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า “ประกาศกรมส่งเสริมการเกษตร เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมส่งเสริมการเกษตร พ.ศ. ๒๕๖๙”

๒. การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมส่งเสริมการเกษตร พ.ศ. ๒๕๖๙ มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อความมั่นคงปลอดภัยไซเบอร์ สำหรับการใช้งานระบบเครือข่าย ข้อมูล และระบบดิจิทัลของกรมส่งเสริมการเกษตร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานของกรมส่งเสริมการเกษตร ได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติ ให้ผู้บริหาร ผู้ปฏิบัติการด้านเทคโนโลยี ผู้ปฏิบัติการด้านเฝ้าระวังและตอบสนองเหตุ ผู้ใช้งานทั่วไป และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมส่งเสริมการเกษตร ตระหนักถึงความสำคัญการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยจะต้องมีการทบทวนให้สอดคล้องกับสภาพแวดล้อมและกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๓. กรณีที่มีการแก้ไขเพิ่มเติมแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้ถือปฏิบัติตามที่ได้มีการแก้ไข หรือเพิ่มเติม นั้น

๔. ให้ใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมส่งเสริมการเกษตร พ.ศ. ๒๕๖๙ ตามแนบท้ายประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๘ เมษายน พ.ศ. ๒๕๖๙

(นางอัญชลี สุวจิตตานนท์)
อธิบดีกรมส่งเสริมการเกษตร

EST. 1967
DEPARTMENT OF AGRICULTURAL EXTENSION
กรมส่งเสริมการเกษตร

ประมวลแนวทางปฏิบัติ และกรอบมาตรฐาน ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ ของกรมส่งเสริมการเกษตร พ.ศ. 2569



:::::::::::::::

สารบัญ

1. ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 1

1.1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 3

1.2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 3

1.3 แผนการรับมือภัยคุกคามทางไซเบอร์ 3

2. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 4

2.1 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Identify) 6

2.2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) 8

2.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) 10

2.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) 12

2.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) 14

3. การจัดหา การพัฒนา และการบำรุงรักษาระบบดิจิทัล 16

3.1 การวิเคราะห์ ออกแบบการจัดหาและพัฒนา และการบำรุงรักษาระบบดิจิทัล 17

3.2 วิธีการประมวลผลในระบบดิจิทัล 18

3.3 มาตรฐานการเข้ารหัสข้อมูล 19

3.4 ระบบนิเวศและสภาพแวดล้อมสำหรับการพัฒนา บริการดิจิทัล การสนับสนุน และความมั่นคงปลอดภัยไซเบอร์ 20

4. แนวปฏิบัติด้านรักษาความมั่นคงปลอดภัยไซเบอร์ 21

4.1 กลุ่มกำกับดูแลและเจ้าของงาน (Governance / Owner) 22

4.2 กลุ่มปฏิบัติการเทคโนโลยี (Infrastructure) 26

4.3 กลุ่มเฝ้าระวังและตอบสนองเหตุ (SOC / IR) 34

4.4 กลุ่มพัฒนาและผู้รับจ้าง ผู้ขาย หรือผู้ให้บริการภายนอก (DevOpSec) 39

4.5 กลุ่มผู้ใช้งานทั่วไป (User) 45

อภิธานศัพท์ 50

คณะผู้จัดทำ 51

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมส่งเสริมการเกษตร

1. ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์



แผนการตรวจสอบ (Audit Plan)
ตรวจสอบปีละ 1 ครั้ง
(BIA & Critical Services)

การประเมินความเสี่ยง (Risk Assessment)
ระบุ วิเคราะห์ KRI
ปีละ 1 ครั้ง

แผนรับมือภัยคุกคามไซเบอร์ (Response Plan)
CIRP & สื่อสารบุคลากร
ทบทวนสม่ำเสมอ

2. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

Identify (ระบุ)
ทะเบียนทรัพย์สิน Penetration Test



Protect (ป้องกัน)
Access Control, Hardening
ตระหนักรู้

Detect (ตรวจจับ)
เฝ้าระวังเหตุผิดปกติ, วิเคราะห์ภัยคุกคาม

Respond (เผชิญเหตุ)
แผน CIRP, ซ้อมรับมือ (Exercise)

Recover (ฟื้นฟู)
แผน BCP,
กู้คืนระบบ (RTO/RPO)

3. การจัดหา การพัฒนา และการบำรุงรักษาระบบดิจิทัล



Design & Analysis
ระบุข้อกำหนดความปลอดภัย

Evaluation
ตรวจสอบความถูกต้องข้อมูล

Encryption
มาตรฐานสากล
(At rest & In transit)

Environment
แยกสภาพแวดล้อม
จัดการช่องโหว่

4. แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้บริหาร/เจ้าของข้อมูล (Governance)
กำหนดนโยบาย
อนุมัติ

ผู้ดูแลระบบ (Infrastructure)
เทคนิค, แก้ไข
ป้องกัน

ทีมเฝ้าระวัง (SOC/IR)
ตรวจจับ แจ้งเตือน
War Room

ผู้พัฒนา/คู่ค้า (DevOps/Vendor)
Secure SDLC
SLA Support

ผู้ใช้งานทั่วไป (User)
ปฏิบัติตามแนวทางฯ
ให้ความร่วมมือ



1. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Audit Plan)



ตรวจสอบอย่างน้อยปีละ 1 ครั้ง



ต้องจัดให้มีการตรวจสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจากภายนอกเป็นประจำทุกปี



เน้นบริการที่สำคัญและ BIA

การตรวจสอบต้องครอบคลุมการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เพื่อจัดลำดับความสำคัญในการป้องกันและฟื้นฟู



รายงานและติดตามผล



ต้องมีการตรวจสอบกระบวนการและผลการวิเคราะห์เพื่อลดโอกาสที่บริการสำคัญหยุดชะงัก

2. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)



ระบุและวิเคราะห์ KRI



ประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง โดยระบุภัยคุกคามและช่องโหว่ทั้งจากภายในและภายนอกผ่านตัวชี้วัดความเสี่ยงสำคัญ (KRI)

การประเมินค่าความเสี่ยง (Risk Evaluation)

วิเคราะห์โอกาสเกิดและผลกระทบเพื่อกำหนดระดับความเสี่ยงที่หน่วยงานยอมรับได้



การจัดการความเสี่ยง (Risk Management)



กำหนดแนวทางควบคุมและป้องกันโดยคำนึงถึงความคุ้มค่าเพื่อให้ความเสี่ยงที่เหลืออยู่ในระดับที่ยอมรับได้

3. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Threat Response Plan)



จัดตั้งทีมรับมือ CIRT



แต่งตั้งคณะกรรมการและทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Team: CIRT) ที่ได้รับบทบาทจาก CISO

จัดทำและทบทวนแผน CIRP

จัดทำแผนรับมือภัยคุกคาม (Cybersecurity Incident Response Plan: CIRP) และทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ



อบรมและซ้อมรับมือ (Exercise)



จัดอบรมสร้างความตระหนักรู้และสื่อสารแผนไปยังบุคลากรที่เกี่ยวข้อง รวมถึงการซ้อมรับมือเหตุการณ์เป็นประจำ

2. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมส่งเสริมการเกษตรมุ่งมั่นสร้างความเชื่อมั่นทางดิจิทัล ด้วยการนำกรอบมาตรฐาน NIST Cybersecurity Framework มาใช้ในการบริหารจัดการความเสี่ยงอย่างเป็นระบบ เพื่อให้ระบบดิจิทัล ของกรมส่งเสริมการเกษตร ข้อมูลสำคัญ รวมถึงระบบที่ใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ได้รับการปกป้องอย่างเหมาะสมและมั่นคง ปลอดภัย พร้อมรองรับทุกภารกิจของกรมส่งเสริมการเกษตรในยุคดิจิทัล โดยการดำเนินงานตามกรอบมาตรฐานดังกล่าวครอบคลุมวงจร การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ 5 ด้านหลัก ได้แก่





2.1 Identify การระบุทรัพย์สินและความเสี่ยง

- โครงสร้างพื้นฐานอุปกรณ์กายภาพ/ดิจิทัล
- เครื่องมือความมั่นคงปลอดภัย
- การเชื่อมโยง/ผู้ให้บริการภายนอก
- วิเคราะห์ภัยคุกคาม/ความเสี่ยง



2.2 Protect การป้องกันและลดความเสี่ยง

- มาตรการป้องกันกายภาพ/ดิจิทัล
- ออกแบบปลอดภัย (Secure Design)
- แผนลดความเสี่ยง
- สร้างความพร้อมบุคลากร



2.3 Detect การตรวจสอบและเฝ้าระวัง

- เฝ้าระวังกายภาพ/ดิจิทัล
- ตรวจจับภัยคุกคามเครือข่าย
- บูรณาการข้อมูล Helpdesk
- แจ้งเตือน/รายงานเหตุการณ์



2.4 Respond การเผชิญเหตุและควบคุมสถานการณ์

- ยืนยัน/จัดระดับเหตุการณ์
- ควบคุม/จำกัดผลกระทบ
- ประสานงาน/สื่อสาร
- บันทึก/ติดตามแก้ไข



2.5 Recover การฟื้นฟูและปรับปรุง

- ฟื้นฟูระบบสู่สภาวะปกติ
- สรุปบทเรียนจากเหตุการณ์
- ตรวจสอบความพร้อมก่อนบริการ

2.1 การระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Identify)



ทำความเข้าใจทรัพย์สินดิจิทัล ข้อมูล ระบบ บริการ และความเสี่ยงที่อาจส่งผลต่อภารกิจองค์กร เพื่อให้เห็นภาพรวมความเสี่ยงไซเบอร์อย่างเป็นระบบ โดยทุกอุปกรณ์ต้องมีการกำหนดรหัสทรัพย์สิน (Asset ID) ระบุเจ้าของทรัพย์สิน (Asset Owner) ระดับความสำคัญ และระดับความเสี่ยง เพื่อใช้ประกอบการประเมินความเสี่ยงและกำหนดมาตรการควบคุมที่เหมาะสม

2.1.1 โครงสร้างพื้นฐานกายภาพ (Physical Infrastructure)

จัดทำบัญชีรายการโครงสร้างพื้นฐานเชิงกายภาพที่สนับสนุนระบบดิจิทัลขององค์กรได้แก่ ศูนย์ข้อมูล อุปกรณ์แม่ข่าย อุปกรณ์ลูกข่าย ระบบเครือข่าย ระบบไฟฟ้า ระบบสำรองไฟ ระบบควบคุมความชื้นและอุณหภูมิ และอุปกรณ์สนับสนุนอื่นที่เกี่ยวข้อง รวมถึงโครงสร้างพื้นฐานที่ใช้รองรับการประมวลผล การจัดเก็บข้อมูล หรือการให้บริการระบบดิจิทัลและระบบที่ใช้ AI

2.1.2 โครงสร้างระบบดิจิทัล (Digital System)

จัดทำบัญชีรายการโครงสร้างระบบดิจิทัล ได้แก่ ระบบแม่ข่ายเสมือน ระบบปฏิบัติการ แอปพลิเคชัน ฐานข้อมูล ระบบเครือข่าย และสิทธิ์การเข้าถึง รวมถึงระบบ บริการ โมเดล หรือแพลตฟอร์ม AI ทั้งที่พัฒนาและให้บริการภายในองค์กร และที่ใช้บริการจากผู้ให้บริการภายนอก เพื่อให้สามารถบริหารจัดการและควบคุมความเสี่ยงได้อย่างเป็นระบบ

2.1.3 ระบบป้องกันและรับมือภัยคุกคามไซเบอร์ (Cybersecurity)

จัดทำบัญชีรายการระบบและเครื่องมือด้านความมั่นคงปลอดภัยไซเบอร์ที่ใช้ในการตรวจจับ ป้องกัน รับมือภัยคุกคาม และฟื้นฟูสภาพระบบดิจิทัลขององค์กร รวมถึงมาตรการและเครื่องมือที่ใช้ควบคุม เฝ้าระวัง รวมถึงลดความเสี่ยงจากการใช้ AI ให้สอดคล้องกับระดับความเสี่ยงที่ประเมินไว้

2.1.4 การเชื่อมโยงและการพึ่งพา (Interconnection & Dependency)

จัดทำการเชื่อมโยงและการพึ่งพาระหว่างโครงสร้างเชิงกายภาพ และระบบดิจิทัล การเคลื่อนไหว การแลกเปลี่ยนข้อมูล การเชื่อมต่อกับผู้ให้บริการและหน่วยงานภายนอก รวมถึงการพึ่งพาบริการ ระบบ หรือแพลตฟอร์ม AI จากภายนอก พร้อมระบุจุดเชื่อมต่อหรือองค์ประกอบที่มีความเสี่ยงเพื่อใช้ประเมินและจัดการความเสี่ยงเชิงระบบ

2.1.5 ภัยคุกคาม ช่องโหว่ และความเสี่ยง (Threats, Vulnerabilities and Risks)

รวบรวมและวิเคราะห์ภัยคุกคาม ช่องโหว่ และเหตุการณ์ความเสี่ยง โดยครอบคลุมโครงสร้างเชิงกายภาพ ระบบดิจิทัล บุคลากร กระบวนการทำงาน รวมถึงภัยคุกคามและความเสี่ยงที่เกิดจากการใช้ AI เช่น การรั่วไหลของข้อมูล การใช้งานที่ไม่เป็นไปตามนโยบาย หรือผลกระทบจากความผิดพลาดของระบบ AI

2.2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)



กำหนดและดำเนินมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน ลดโอกาสเกิดเหตุ และจำกัดผลกระทบจากความเสี่ยง โดยครอบคลุมความเสี่ยงที่เกี่ยวข้องกับระบบดิจิทัลและ AI

2.2.1 มาตรการป้องกันโครงสร้างพื้นฐานกายภาพ (Physical Protection)

กำหนดและดำเนินมาตรการควบคุมด้านกายภาพสำหรับศูนย์ข้อมูล อุปกรณ์แม่ข่าย อุปกรณ์ลูกข่าย ระบบเครือข่าย ระบบไฟฟ้า ระบบสำรองไฟ และระบบปรับอากาศ รวมถึงการควบคุมการเข้าถึง การเฝ้าระวัง และการบำรุงรักษาให้เหมาะสมกับระดับความสำคัญของทรัพย์สิน รวมถึงโครงสร้างพื้นฐานที่รองรับการประมวลผล การจัดเก็บข้อมูล หรือบริการ AI

2.2.2 มาตรการป้องกันโครงสร้างระบบดิจิทัล (Digital Protection)

กำหนดและดำเนินมาตรการควบคุมระบบดิจิทัล ได้แก่ การจัดการสิทธิ์การเข้าถึง การพิสูจน์ตัวตน การป้องกันมัลแวร์ การป้องกันเครือข่าย การปกป้องแอปพลิเคชันและฐานข้อมูล การควบคุมและป้องกันการนำข้อมูลขององค์กรไปใช้กับระบบหรือบริการ AI ที่ไม่ได้รับอนุญาต รวมถึงการใช้ระบบป้องกันและรับมือภัยคุกคามไซเบอร์ให้สอดคล้องกับความเสี่ยงที่ประเมินไว้

2.2.3 การจัดการความเสี่ยงและแผนลดความเสี่ยง (Risk Treatment)

จัดทำและดำเนินแผนจัดการความเสี่ยง โดยเลือกแนวทางการยอมรับ ลด โอน หรือหลีกเลี่ยงความเสี่ยง พร้อมกำหนดกิจกรรม มาตรการ งบประมาณ และผู้รับผิดชอบอย่างชัดเจน การกำหนดข้อจำกัดการใช้งาน AI ตามระดับความเสี่ยง

2.2.4 การบูรณาการความมั่นคงปลอดภัยในการออกแบบและจัดหา (Security Design & Procurement)

กำหนดให้การพัฒนา การปรับปรุงระบบ และการจัดหาครุภัณฑ์หรือบริการด้านดิจิทัลต้องคำนึงถึงความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบ (Security by Design) โดยครอบคลุมการออกแบบ การพัฒนา การจัดหา และการใช้งาน AI อย่างมั่นคงปลอดภัย และต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไว้ในเอกสาร TOR สัญญา และข้อตกลงกับผู้ให้บริการ

2.2.5 การสร้างความพร้อมของบุคลากรและกระบวนการ (People & Process Readiness)

กำหนดมาตรการด้านกระบวนการทำงาน หน้าที่ความรับผิดชอบ การฝึกอบรม และการสื่อสาร เพื่อให้บุคลากรที่เกี่ยวข้องสามารถปฏิบัติตามมาตรการป้องกันด้านไซเบอร์ได้อย่างถูกต้อง รวมถึงการสร้างความตระหนักรู้เกี่ยวกับความเสี่ยง ข้อจำกัด และแนวทางการใช้ AI อย่างเหมาะสมและปลอดภัย

2.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)



เฝ้าระวังตรวจจับและรับรู้เหตุการณ์หรือพฤติกรรมผิดปกติที่อาจเป็นภัยคุกคามต่อระบบดิจิทัล โครงสร้างพื้นฐาน และข้อมูลขององค์กรอย่างต่อเนื่อง เพื่อให้สามารถตรวจพบและตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที ครอบคลุมการตรวจจับเหตุการณ์หรือพฤติกรรมผิดปกติที่เกี่ยวข้องกับ AI รวมถึงการใช้งานที่อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์หรือการคุ้มครองข้อมูลส่วนบุคคล

2.3.1 การเฝ้าระวังโครงสร้างพื้นฐานกายภาพ

เฝ้าระวังสถานะของศูนย์ข้อมูล อุปกรณ์แม่ข่าย อุปกรณ์ลูกข่าย ระบบเครือข่าย ระบบไฟฟ้า ระบบสำรองไฟ และระบบควบคุมความชื้นและอุณหภูมิ รวมถึงโครงสร้างพื้นฐานที่สนับสนุนการให้บริการระบบดิจิทัลและระบบที่ใช้ AI เพื่อรับรู้ความผิดปกติที่อาจส่งผลต่อความพร้อมใช้งาน ความต่อเนื่องของบริการ และความมั่นคงปลอดภัยไซเบอร์ขององค์กร

2.3.2 การเฝ้าระวังระบบดิจิทัล

เฝ้าระวังระบบปฏิบัติการ แอปพลิเคชัน ฐานข้อมูล ระบบเครือข่าย และสิทธิ์การเข้าถึง โดยครอบคลุมการตรวจจับเหตุการณ์หรือพฤติกรรมผิดปกติที่เกี่ยวข้องกับ AI รวมถึงการใช้งานที่ไม่สอดคล้องกับนโยบายขององค์กรหรือมีความเสี่ยงต่อความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลเพื่อให้สามารถตรวจจับและรับรู้ความผิดปกติได้อย่างเหมาะสมและทันท่วงที

2.3.3 การตรวจจับภัยคุกคามจากเครือข่ายและระบบความมั่นคงปลอดภัย

ใช้ระบบเฝ้าระวังและตรวจจับภัยคุกคามด้านไซเบอร์ เช่น ระบบตรวจจับพฤติกรรมเครือข่าย ระบบวิเคราะห์บันทึกเหตุการณ์ และข้อมูลจากระบบป้องกันและควบคุมความมั่นคงปลอดภัยไซเบอร์ รวมถึงบันทึกและสัญญาณที่เกี่ยวข้องกับการเชื่อมต่อหรือการใช้งานบริการ AI เพื่อระบุเหตุการณ์หรือแนวโน้มภัยคุกคามที่อาจเกิดขึ้น

2.4.4 รวบรวมและวิเคราะห์ข้อมูลจากแพลตฟอร์ม Helpdesk

การแจ้งเหตุจากผู้ใช้งาน และเหตุผิดปกติที่ถูกรายงาน รวมถึงเหตุที่เกี่ยวข้องกับการใช้งานระบบหรือบริการ AI เพื่อใช้เป็นข้อมูลประกอบการตรวจจับ ยืนยัน และประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างครบถ้วน

2.3.5 การบันทึก แจ้งเตือน และรายงานเหตุการณ์

บันทึกเหตุการณ์และพฤติกรรมผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงเหตุการณ์ที่เกี่ยวข้องกับ AI แจ้งเตือนหน่วยงานที่เกี่ยวข้องตามระดับความรุนแรงและจัดทำรายงานสถานะการเฝ้าระวังและเหตุการณ์ด้านไซเบอร์อย่างสม่ำเสมอ เพื่อใช้ในการติดตาม วิเคราะห์แนวโน้มและปรับปรุงมาตรการควบคุมขององค์กรอย่างต่อเนื่อง

2.4 มาตรการเผชิญเหตุเมื่อตรวจพบภัยคุกคามทางไซเบอร์ (Respond)



ควบคุมจัดการลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบและทันต่อสถานการณ์ ครอบคลุมเหตุการณ์ที่เกิดจากหรือเกี่ยวข้องกับระบบ AI ตลอดวงจรการใช้งานของระบบเพื่อป้องกันการขยายผลกระทบ การละเมิดข้อมูล และความเสียหายต่อภารกิจขององค์กร

2.4.1 การรับแจ้งและยืนยันเหตุการณ์

รับแจ้งเหตุจากระบบเฝ้าระวัง ระบบตรวจจับภัยคุกคาม ระบบ Helpdesk ผู้ใช้งาน หรือแหล่งข้อมูลอื่นที่เกี่ยวข้อง พร้อมดำเนินการตรวจสอบ วิเคราะห์ และยืนยันเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงเหตุการณ์ที่เกี่ยวข้องกับการใช้ การให้บริการ หรือการทำงานผิดปกติของระบบ AI เพื่อประเมินลักษณะ ขอบเขต และผลกระทบเบื้องต้นของเหตุการณ์อย่างเหมาะสม

2.4.2 การจัดระดับและยกระดับเหตุการณ์

ประเมินระดับความรุนแรงและความสำคัญของเหตุการณ์ โดยพิจารณาผลกระทบต่อข้อมูล ระบบ บริการ ผู้ใช้งาน รวมถึงความน่าเชื่อถือของระบบ AI พร้อมกำหนดระดับเหตุการณ์ และยกระดับการตอบสนองตามแผนการรับมือภัยคุกคามทางไซเบอร์ของกรมส่งเสริมการเกษตร การพิจารณาแจ้งหน่วยงานที่เกี่ยวข้องตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้องในกรณีเหตุการณ์ที่มีผลกระทบสูงหรือเกี่ยวข้องกับข้อมูลส่วนบุคคล

2.4.3 การควบคุมและจำกัดผลกระทบ

ดำเนินการควบคุมเหตุการณ์เพื่อจำกัดผลกระทบและป้องกันการขยายความเสียหาย เช่น การกักกันระบบ การจำกัดสิทธิ์การเข้าถึง การแยกเครือข่าย การระงับการทำงานของโมเดลหรือบริการ AI ชั่วคราว หรือการหยุดการประมวลผลข้อมูลที่มีความเสี่ยง ทั้งนี้ ต้องคำนึงถึงความต่อเนื่องของภารกิจและความปลอดภัยของข้อมูลเป็นสำคัญ

2.4.4 การประสานงานและสื่อสาร

ประสานการดำเนินงานระหว่างหน่วยงานที่เกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ทีมความมั่นคงปลอดภัยไซเบอร์ ผู้พัฒนาหรือผู้ให้บริการระบบ AI และหน่วยงานสนับสนุนที่เกี่ยวข้อง พร้อมดำเนินการสื่อสารเหตุการณ์ตามแนวทางที่กำหนด โดยคำนึงถึงความถูกต้อง ความเหมาะสม และการคุ้มครองข้อมูลเพื่อสร้างความเข้าใจที่ตรงกันและลดผลกระทบจากการสื่อสารที่คลาดเคลื่อน

2.4.5 การบันทึกและติดตามการแก้ไขเหตุการณ์

บันทึกรายละเอียดเหตุการณ์ การวิเคราะห์ การตัดสินใจ และการดำเนินการแก้ไขอย่างครบถ้วนติดตามสถานะการแก้ไขจนเหตุการณ์ยุติ และนำบทเรียนที่ได้รับไปใช้ในการปรับปรุงมาตรการ กระบวนการ และแนวทางการใช้งานระบบ AI เพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์และลดความเสี่ยงในการเกิดเหตุซ้ำในอนาคต

2.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)



กำหนดแนวทางในการฟื้นฟูระบบ บริการ และข้อมูลที่ได้รับผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้กลับสู่สภาวะปกติอย่างปลอดภัย พร้อมทั้งนำบทเรียนที่ได้รับไปใช้ในการปรับปรุงมาตรการ กระบวนการ และแนวทางการใช้งาน ครอบคลุมการฟื้นฟูเหตุการณ์ที่เกิดจากหรือเกี่ยวข้องกับระบบ AI

2.5.1 การฟื้นฟูระบบและบริการ

ดำเนินการฟื้นฟูระบบ แอปพลิเคชัน ข้อมูล และโครงสร้างพื้นฐานที่ได้รับผลกระทบจากเหตุการณ์ตามลำดับความสำคัญที่กำหนดไว้ในแผนฟื้นฟูระบบและแผนกู้คืนระบบ (Disaster Recovery Plan / Business Continuity Plan) รวมถึงการฟื้นฟูระบบหรือโมเดล AI ชุดข้อมูลที่เกี่ยวข้อง เพื่อให้ระบบสามารถกลับมาให้บริการได้อย่างปลอดภัยและต่อเนื่อง

2.5.2 การตรวจสอบความพร้อมหลังการฟื้นฟู

ตรวจสอบความถูกต้อง ความครบถ้วน และความมั่นคงปลอดภัยของระบบ ข้อมูล และบริการดิจิทัลหลังการฟื้นฟู ก่อนเปิดให้บริการตามปกติ โดยต้องรวมถึงการตรวจสอบความถูกต้องของข้อมูลที่ถูกกู้คืน การตั้งค่าความปลอดภัยของระบบ และการทำงานของระบบ AI และผลลัพธ์ที่ได้เพื่อให้มั่นใจว่าไม่มีความเสี่ยงหลงเหลือจากเหตุการณ์เดิม

2.5.3 การสรุปบทเรียนจากเหตุการณ์

รวบรวม วิเคราะห์ และสรุปบทเรียนจากเหตุการณ์ที่เกิดขึ้นทั้งในด้านเทคนิค กระบวนการทำงาน การสื่อสาร และการประสานงานรวมถึงบทเรียนที่เกี่ยวข้องกับการออกแบบ การใช้งาน หรือการกำกับดูแลระบบ AI เพื่อระบุจุดอ่อน ช่องว่าง และโอกาสในการปรับปรุงการบริหารความเสี่ยงด้านไซเบอร์ขององค์กร

2.5.4 การปรับปรุงมาตรการ แผน และมาตรฐาน

นำบทเรียนที่ได้รับมาปรับปรุงนโยบาย มาตรการควบคุม แผนการรับมือภัยคุกคามทางไซเบอร์ แผนฟื้นฟูและแผนกู้คืนระบบ รวมถึงแนวทางปฏิบัติด้านการใช้ระบบ AI อย่างมั่นคงปลอดภัยให้สอดคล้องกับความเสี่ยงปัจจุบัน เทคโนโลยีที่เปลี่ยนแปลง และแนวปฏิบัติหรือมาตรฐานที่เกี่ยวข้อง

2.5.5 การรายงานและติดตามผลระยะยาว

จัดทำรายงานผลการฟื้นฟู การปรับปรุงมาตรการ และการจัดการเหตุการณ์เสนอต่อผู้บริหารและหน่วยงานที่เกี่ยวข้องตามลำดับ พร้อมทั้งติดตามผลการดำเนินงานอย่างต่อเนื่องเพื่อตรวจสอบประสิทธิผลของมาตรการที่ปรับปรุงแล้ว และยกระดับความมั่นคงปลอดภัยไซเบอร์และการใช้ระบบ AI ขององค์กรในระยะยาว

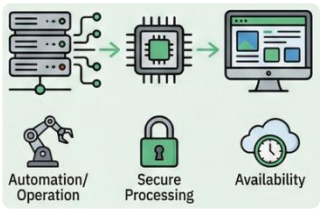
3. การจัดหา การพัฒนา และการบำรุงรักษาระบบดิจิทัล

แนวปฏิบัติในการวิเคราะห์ ออกแบบ พัฒนา ดำเนินงาน และบำรุงรักษาระบบดิจิทัลของกรมส่งเสริมการเกษตรให้มีความมั่นคงปลอดภัย สอดคล้องกับกฎหมาย มาตรฐาน และกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องตลอดวงจรชีวิตของระบบ ประกอบด้วย

3.1 การวิเคราะห์ ออกแบบการจัดหาและพัฒนาและการบำรุงรักษาระบบดิจิทัล (Analysis and Design for Digital System Acquisition, Development, and Maintenance)



3.2 วิธีการประมวลผลในระบบดิจิทัล (Digital Processing Methods and System Operation)



3.3 มาตรฐานการเข้ารหัสข้อมูล (Data Encryption and Protection Standards)



3.4 ระบบนิเวศและสภาพแวดล้อมสำหรับการพัฒนา บริการดิจิทัล การสนับสนุน และความมั่นคงปลอดภัยไซเบอร์ (Ecosystem and Environment for Digital Service Development, Support, and Cybersecurity)



3.1 การวิเคราะห์ ออกแบบ การจัดหาและพัฒนา และการบำรุงรักษาระบบดิจิทัล

การวิเคราะห์ ออกแบบ จัดหา พัฒนา และบำรุงรักษาระบบดิจิทัลของกรมส่งเสริมการเกษตร ต้องคำนึงถึงความมั่นคงปลอดภัยไซเบอร์ตลอดวงจรชีวิตของระบบ ตั้งแต่การกำหนดความต้องการ การประเมินความเสี่ยง การออกแบบและพัฒนาอย่างมั่นคงปลอดภัย ไปจนถึงการบำรุงรักษาและปรับปรุงระบบ เพื่อให้ระบบดิจิทัลมีความปลอดภัย เชื่อถือได้ และสอดคล้องกับนโยบายและข้อกำหนดที่เกี่ยวข้อง ดังนี้



3.1.1 ต้องระบุและจัดทำบัญชีรายการระบบดิจิทัล ทรัพย์สินสารสนเทศ ข้อมูล และองค์ประกอบที่เกี่ยวข้องกับระบบ รวมถึงระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ข้อจำกัด ข้อกำหนดกฎหมายและนโยบายที่เกี่ยวข้อง ก่อนการจัดหา พัฒนา หรือปรับปรุงระบบ

3.1.2 ต้องออกแบบและพัฒนาระบบโดยบูรณาการมาตรการด้านความมั่นคงปลอดภัยตั้งแต่ขั้นตอนเริ่มต้น (Secure by Design) รวมถึงกำหนดสิทธิ์การเข้าถึงตามบทบาทหน้าที่ การแยกสภาพแวดล้อม การพัฒนาและใช้งานจริง การป้องกันข้อมูลส่วนบุคคล ข้อมูลสำคัญ และการจัดทำเอกสารประกอบระบบให้ครบถ้วนและเป็นปัจจุบัน



3.1.3 ต้องจัดให้มีการตรวจสอบ ทดสอบ และประเมินความมั่นคงปลอดภัยของระบบระหว่างการพัฒนาและก่อนนำไปใช้งานจริง รวมถึงการตรวจสอบและแก้ไขช่องโหว่ และการติดตามความผิดปกติที่อาจเกิดขึ้นจากการออกแบบหรือการพัฒนา

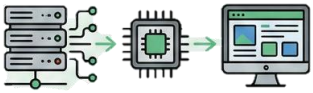
3.1.4 เมื่อพบข้อบกพร่องหรือเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบ หน่วยงานต้องดำเนินการแก้ไข ปรับปรุง หรือควบคุมผลกระทบโดยทันที พร้อมกำหนดผู้รับผิดชอบและขั้นตอนการดำเนินการอย่างชัดเจน

3.1.5 ต้องทบทวนผลกระทบจากเหตุการณ์หรือข้อบกพร่องที่เกิดขึ้น ปรับปรุงกระบวนการออกแบบ พัฒนา และบำรุงรักษาระบบ รวมถึงจัดทำมาตรการป้องกันไม่ให้เกิดเหตุซ้ำ และปรับปรุงเอกสารและแนวปฏิบัติที่เกี่ยวข้อง

3.2 วิธีการประมวลผลในระบบดิจิทัล

การควบคุมและกำกับดูแลกระบวนการประมวลผลข้อมูลในระบบดิจิทัล เพื่อให้การรับข้อมูล การประมวลผล และการแสดงผลลัพธ์มีความถูกต้องครบถ้วน และเชื่อถือได้ รวมถึงสามารถตรวจจับ จัดการ และแก้ไขความผิดพลาดหรือความผิดปกติที่อาจเกิดขึ้นระหว่างการดำเนินงานของระบบได้อย่างเหมาะสม ดังนี้

3.2.1 ต้องระบุประเภทข้อมูล กระบวนการประมวลผล จุดควบคุมที่สำคัญ ความเสี่ยงที่อาจเกิดขึ้นในแต่ละขั้นตอน ตั้งแต่การรับข้อมูล การประมวลผล ตลอดจนการแสดงผลลัพธ์



3.2.2 ระบบดิจิทัลต้องมีมาตรการควบคุมการประมวลผลที่เหมาะสม ได้แก่ การตรวจสอบความถูกต้องของข้อมูลนำเข้า การควบคุมกระบวนการประมวลผล และการรักษาความถูกต้องครบถ้วนของข้อมูล รวมถึงการกำหนดขั้นตอนปฏิบัติและความรับผิดชอบของผู้เกี่ยวข้อง

3.2.3 ระบบต้องสามารถตรวจจับความผิดพลาด ความผิดปกติ หรือความไม่สมบูรณ์ของข้อมูลในระหว่างการประมวลผล และต้องมีการแจ้งเตือนหรือบันทึกเหตุการณ์เพื่อให้สามารถตรวจสอบย้อนหลังได้

3.2.4 เมื่อพบข้อผิดพลาดในการประมวลผลหรือข้อมูลผลลัพธ์ ต้องดำเนินการแก้ไขตามขั้นตอนที่กำหนด พร้อมระบุผู้รับผิดชอบในการตรวจสอบและยืนยันความถูกต้องของข้อมูลก่อนนำไปใช้งาน

3.2.5 ต้องดำเนินการแก้ไขข้อมูลหรือกระบวนการที่ผิดพลาด ฟื้นฟูความถูกต้องของข้อมูล และทบทวนมาตรการควบคุมเพื่อป้องกันไม่ให้เกิดข้อผิดพลาดซ้ำในอนาคต

3.3 มาตรฐานการเข้ารหัสข้อมูล

การคุ้มครองข้อมูลของกรมส่งเสริมการเกษตรด้วยการเข้ารหัสข้อมูลอย่างเหมาะสมตามลำดับชั้นของข้อมูล และระดับความเสี่ยง ครอบคลุมการเลือกใช้วิธีการเข้ารหัส การบริหารจัดการรหัสเข้ารหัส การตรวจสอบความถูกต้องของการเข้ารหัส และการจัดการเหตุการณ์ที่เกี่ยวข้อง เพื่อป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ดังนี้



3.3.1 ต้องจำแนกลำดับชั้นของข้อมูล ระบุข้อมูลที่จำเป็นต้องได้รับการเข้ารหัส และประเมินความเสี่ยงที่เกี่ยวข้องกับการจัดเก็บ การรับส่ง และการใช้งานข้อมูล

3.3.2 ต้องกำหนดนโยบายและแนวปฏิบัติในการเข้ารหัสข้อมูล รวมถึงการเลือกใช้ซอฟต์แวร์ วิธีการเข้ารหัส และการบริหารจัดการรหัสเข้ารหัสให้เหมาะสมกับลำดับชั้นของข้อมูลและผลการประเมินความเสี่ยง

3.3.3 ต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของการเข้ารหัสข้อมูล รวมถึงการตรวจจับการเข้าถึงหรือการใช้งานรหัส เข้ารหัสโดยไม่ได้รับอนุญาต

3.3.4 เมื่อพบเหตุการณ์ที่เกี่ยวข้องกับการรั่วไหลหรือความผิดปกติของการเข้ารหัส ต้องดำเนินการเพิกถอน เปลี่ยน หรือระงับการใช้งานรหัสเข้ารหัสโดยทันที และดำเนินการตามขั้นตอนการจัดการเหตุการณ์ที่กำหนดไว้



3.3.5 ต้องกู้คืนข้อมูลและระบบการเข้ารหัสจากการสำรองข้อมูล ทบทวนและปรับปรุงมาตรการบริหารจัดการรหัสเข้ารหัส และป้องกันไม่ให้เกิดเหตุซ้ำ

3.4 ระบบนิเวศและสภาพแวดล้อมสำหรับการพัฒนาบริการดิจิทัล การสนับสนุน และความมั่นคงปลอดภัยไซเบอร์

การบริหารจัดการระบบนิเวศและสภาพแวดล้อมที่เกี่ยวข้องกับการพัฒนา การให้บริการ และการสนับสนุนระบบดิจิทัลของกรมส่งเสริมการเกษตร โดยครอบคลุมการควบคุมสภาพแวดล้อมการทำงาน การจัดการซอฟต์แวร์ และชุดคำสั่ง การบริหารจัดการช่องโหว่ การใช้บริการจากภายนอก และการฟื้นฟูระบบภายหลังเหตุการณ์ เพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่องและยั่งยืน ดังนี้

3.4.1 ต้องระบุและจัดทำบัญชีทรัพย์สินดิจิทัล ซอฟต์แวร์ ฮาร์ดแวร์ ชุดคำสั่ง ผู้ให้บริการภายนอก และช่องโหว่ที่เกี่ยวข้องกับระบบ รวมถึงความสัมพันธ์ในห่วงโซ่อุปทานดิจิทัล



3.4.2 ต้องควบคุมสภาพแวดล้อมการพัฒนา การทดสอบ และการใช้งานจริงให้แยกจากกันอย่างชัดเจน ควบคุมการเข้าถึง Source Code การติดตั้งซอฟต์แวร์ การปรับปรุงแพตช์ และการเข้าถึงระบบของผู้ให้บริการหรือผู้รับจ้างภายนอก

3.4.3 ต้องบันทึก เฝ้าระวังกิจกรรมที่เกี่ยวข้องกับการเข้าถึง การเปลี่ยนแปลงระบบ และการใช้งานทรัพยากร รวมถึงการตรวจจับช่องโหว่และพฤติกรรมที่ผิดปกติในระบบและโครงสร้างพื้นฐาน

3.4.4 เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ต้องควบคุม แก้ไข และจำกัดผลกระทบของเหตุการณ์ตามขั้นตอนที่กำหนด รวมถึงการประสานงานกับผู้เกี่ยวข้องและผู้ให้บริการภายนอก



3.4.5 ต้องดำเนินการกู้คืนระบบ บริการ และสภาพแวดล้อมให้กลับสู่สภาวะปกติอย่างปลอดภัย ทบทวนบทเรียนจากเหตุการณ์ที่เกิดขึ้น และปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

4. แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัตินี้จัดทำขึ้นเพื่อกำหนดบทบาท หน้าที่ และแนวทางการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกลุ่มบุคลากรที่เกี่ยวข้องกับระบบดิจิทัลของกรมส่งเสริมการเกษตรให้มีความชัดเจนและเป็นระบบ โดยมุ่งให้การป้องกัน ตรวจจับ และรับมือกับภัยคุกคามทางไซเบอร์เป็นความรับผิดชอบร่วมกันของทุกภาคส่วน เพื่อสนับสนุนการดำเนินภารกิจของกรมอย่างมั่นคง ปลอดภัย และต่อเนื่อง ทั้งนี้ ได้จำแนกกลุ่มผู้เกี่ยวข้องออกเป็น 5 กลุ่มหลัก ได้แก่



4.1 กลุ่มกำกับดูแลและเจ้าของงาน (Governance / Owner)



4.2 กลุ่มปฏิบัติการเทคโนโลยี (Infrastructure)



4.3 กลุ่มเฝ้าระวังและตอบสนองเหตุ (SOC / IR)



4.4 กลุ่มพัฒนาและผู้รับจ้าง ผู้ขาย หรือผู้ให้บริการภายนอก (DevOpSec)



4.5 กลุ่มผู้ใช้งานทั่วไป (User)

4.1 กลุ่มกำกับดูแลและเจ้าของงาน (Governance / Owner)

4.1.1 ผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

เป็นผู้กำหนดทิศทางความมั่นคงปลอดภัยไซเบอร์ขององค์กร เชื่อมโยง “ความเสี่ยง การตัดสินใจ ความต่อเนื่องของภารกิจ” จากนโยบายสู่การปฏิบัติ เพื่อการป้องกัน รับมือและการฟื้นฟูอย่างยั่งยืน โดยเห็นชอบนโยบายความมั่นคงปลอดภัยไซเบอร์ ทิศทางด้านดิจิทัล ข้อมูล รวมถึงการใช้ AI อนุมัติระดับความเสี่ยงที่องค์กรยอมรับได้ การควบคุม และจัดสรรทรัพยากรให้เพียงพอ กำหนดกลไกการรายงานและการตัดสินใจ ในประเด็นสำคัญเพื่อให้การดำเนินงานเป็นระบบ สอดคล้องภารกิจของกรมส่งเสริมการเกษตร

กำกับให้มีการรับรองขอบเขตของระบบสำคัญ ข้อมูลสำคัญ การเชื่อมโยงข้อมูล การเข้าถึง และการแลกเปลี่ยนข้อมูลตามนโยบาย และข้อกำหนดที่กำหนด และผู้ให้บริการที่ต้องอยู่ในการบริหารความเสี่ยงระดับองค์กร และรับทราบการประเมินความเสี่ยง การจัดลำดับความสำคัญของความเสี่ยง

อนุมัติแผนจัดการความเสี่ยงและแผนยกระดับมาตรการควบคุม กำกับให้มีมาตรการคุ้มครองข้อมูล การเข้าถึง การแลกเปลี่ยนข้อมูลตามนโยบาย และข้อกำหนดที่กำหนด รวมทั้งเห็นชอบมาตรการขั้นต่ำหรือมาตรฐานระดับองค์กร ที่ต้องบังคับใช้กับการพัฒนา จัดหาระบบและโครงการสำคัญ

รับทราบรายงานสถานะความเสี่ยง เหตุผิดปกติ และตัวชี้วัดภาพรวม และสั่งปรับระดับการเฝ้าระวังหรือมาตรการเสริมเมื่อมีสัญญาณความเสี่ยงสูง

ตัดสินใจเชิงบริหารเมื่อเกิดเหตุสำคัญ เช่น การยกระดับเหตุ อนุมัติการกักกันหรือจำกัดบริการ การสื่อสาร และการประสานหน่วยงานที่เกี่ยวข้อง พร้อมกำกับให้การแก้ไขแล้วเสร็จตามกรอบเวลา

ผู้บริหารอนุมัติแผนฟื้นฟูและการกู้คืนบริการ/ข้อมูลตามลำดับความสำคัญ ของภารกิจ รับรองบทเรียนหลังเหตุ และสั่งการปรับปรุงนโยบาย มาตรฐาน และแผนเพื่อป้องกันการเกิดเหตุซ้ำ

4.1 กลุ่มกำกับดูแลและเจ้าของงาน (Governance / Owner)

4.1.2 คณะกรรมการบริหารเทคโนโลยีสารสนเทศ

เป็นกลไกกำกับดูแลในการกำหนดนโยบาย ทิศทาง และกรอบการบริหารจัดการด้านเทคโนโลยีดิจิทัลและข้อมูลให้สอดคล้องกับภารกิจและยุทธศาสตร์ของกรมส่งเสริมการเกษตร โดยทำหน้าที่พิจารณาและให้ความเห็นชอบแผนงาน/โครงการสำคัญ การจัดหาระบบคอมพิวเตอร์และแผนปฏิบัติการดิจิทัล รวมถึงกำกับ ติดตาม และประเมินผลการดำเนินงานด้านดิจิทัลและข้อมูลของหน่วยงานในสังกัด ตลอดจนกำกับดูแลการเชื่อมโยงข้อมูลและการบริหารความเสี่ยง เพื่อให้การใช้ข้อมูลเกิดประโยชน์สูงสุด มีความมั่นคงปลอดภัย ตรวจสอบได้ และสามารถแต่งตั้งคณะทำงานหรือมอบหมายภารกิจเพิ่มเติมตามความจำเป็นเพื่อขับเคลื่อนภารกิจของกรมส่งเสริมการเกษตรให้บรรลุเป้าหมาย สอดคล้องภารกิจและการบริหารความเสี่ยงขององค์กร

พิจารณาความครบถ้วนของขอบเขตระบบ/ข้อมูลสำคัญและผลการประเมินความเสี่ยงในระดับภาพรวม พร้อมให้ข้อเสนอด้านการจัดลำดับความสำคัญก่อนเสนอผู้บริหารตัดสินใจ

พิจารณาและให้ความเห็นต่อแผนจัดการความเสี่ยงและการยกระดับมาตรการควบคุมในภาพรวมองค์กร รวมถึงกลั่นกรองข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับโครงการและการจัดหาระบบ เพื่อให้สอดคล้องมาตรฐานและเกิดผลจริง

รับทราบรายงานสถานะด้านการเฝ้าระวัง/ตรวจจับในภาพรวม และเสนอแนวทางยกระดับขีดความสามารถหรือแก้ไขช่องว่างเชิงระบบ

สนับสนุนการตัดสินใจในเหตุสำคัญด้วยข้อเสนอเชิงนโยบายและทางเลือกในการบริหารผลกระทบข้ามหน่วยงาน

คณะกรรมการรับทราบบทเรียนหลังเหตุและผลการปรับปรุง พร้อมเสนอการปรับมาตรฐาน แผนงาน หรือการลงทุนเชิงระบบเพื่อยกระดับระยะยาว

4.1 กลุ่มกำกับดูแลและเจ้าของงาน (Governance / Owner)

4.1.3 ฝ่ายตรวจสอบ

ฝ่ายตรวจมีบทบาทในการตรวจสอบอย่างเป็นอิสระเพื่อสร้างความเชื่อมั่นว่าการกำกับดูแล การบริหารความเสี่ยง และการควบคุมด้านดิจิทัล ข้อมูล และไซเบอร์ขององค์กรมีความเพียงพอ สอดคล้องนโยบาย และสามารถปฏิบัติได้จริงตลอดวงจรการบริหารความมั่นคงปลอดภัยไซเบอร์ ให้ความเชื่อมั่นอย่างเป็นอิสระ โดยจัดทำแผนตรวจสอบแบบอิงความเสี่ยง ตรวจสอบความสอดคล้องของนโยบาย โครงสร้างการกำกับดูแล บทบาท หน้าที่ และกระบวนการบริหารความเสี่ยง พร้อมรายงานข้อค้นพบต่อผู้บริหารและคณะกรรมการ และติดตามการปิดประเด็นโดยไม่ก้าวล่วงบทบาทผู้อนุมัติหรือผู้ปฏิบัติ

ทวนสอบความครบถ้วนของทะเบียนระบบ ข้อมูลสำคัญ การเชื่อมโยง และผู้ให้บริการ รวมถึงความเหมาะสมของวิธีประเมินความเสี่ยงและเหตุผลประกอบการจัดลำดับความเสี่ยง

ประเมินความเพียงพอและประสิทธิผลของมาตรการควบคุม ตรวจสอบหลักฐานการปฏิบัติและผลการปิดช่องว่างให้เป็นไปตามนโยบายและมาตรฐาน

ตรวจสอบความครอบคลุมของการบันทึกเหตุ การเฝ้าระวัง การแจ้งเตือน
และคุณภาพของรายงานสถานะ/เหตุผิดปกติตามรอบ

ประเมินความพร้อมของแผนตอบสนองเหตุและความครบถ้วนของหลักฐานการจัดการเหตุ ตลอดจนความสอดคล้องของการอนุมัติและการสื่อสารตามขั้นตอนที่กำหนด ในขอบเขตการตรวจสอบ

ตรวจสอบความพร้อมของแผนฟื้นฟู/กู้คืน ผลการทดสอบแผน และการดำเนินการแก้ไขถาวรตามบทเรียน พร้อมติดตามจนปิดข้อค้นพบ

4.1 กลุ่มกำกับดูแลและเจ้าของงาน (Governance / Owner)

4.1.4 เจ้าของระบบและข้อมูลดิจิทัล

เจ้าของระบบและข้อมูลดิจิทัลมีหน้าที่กำกับ “ความถูกต้องของข้อมูล ความต่อเนื่องของบริการ และระดับความเสี่ยงที่ยอมรับได้” ของระบบ/ข้อมูลที่รับผิดชอบ โดยทำหน้าที่ตัดสินใจเชิงเจ้าของงาน (business owner) กำหนดขอบเขต วัตถุประสงค์ ระดับความสำคัญ การจัดชั้นข้อมูล และหลักเกณฑ์การเข้าถึง การใช้ การแลกเปลี่ยนข้อมูล พร้อมกำกับให้การดำเนินงานของหน่วยเทคนิคและผู้ให้บริการสอดคล้องนโยบายและมาตรฐานองค์กร และประสานให้ผู้ดูแลระบบ/ผู้ปฏิบัติการดำเนินมาตรการตามที่กำหนด

จัดทำและทบทวนรายการระบบ ข้อมูลสำคัญ จุดเชื่อมโยง และผู้ให้บริการของระบบที่รับผิดชอบให้เป็นปัจจุบัน รวมถึงประเมินความเสี่ยง และจัดลำดับประเด็นเร่งด่วนเพื่อเสนอแผนแก้ไข

กำหนดมาตรการคุ้มครองข้อมูลและข้อกำหนดด้านความปลอดภัยของระบบ พร้อมกำกับการบังคับใช้จริง รวมทั้งกำหนดข้อกำหนดด้านความปลอดภัยใน TOR/สัญญาของระบบ และตรวจรับหลักฐานก่อนเปิดใช้งาน

กำกับให้มีการบันทึกเหตุและเฝ้าระวังตามระดับความสำคัญ ทบทวนรายงานผิดปกติตามรอบและแจ้งเหตุพร้อมข้อมูลประกอบเพื่อสนับสนุนการยืนยันเหตุอย่างทันท่วงที

ให้ข้อมูลผลกระทบเชิงงานระหว่างเหตุการณ์ และเงื่อนไขการให้บริการเพื่อประกอบการตัดสินใจและอนุมัติการดำเนินการที่กระทบผู้ใช้ หรือการใช้ข้อมูลในขอบเขตอำนาจของตน ภายใต้สายการสั่งการที่กำหนด

เจ้าของระบบกำหนดลำดับความสำคัญการกู้คืนของระบบที่รับผิดชอบ กำกับการกู้คืนให้ปลอดภัย ตรวจสอบความถูกต้องของข้อมูลหลังการกู้คืน และจัดทำข้อเสนอปรับปรุงเพื่อป้องกันการเกิดซ้ำ พร้อมติดตามให้แล้วเสร็จ

4.2 กลุ่มปฏิบัติการเทคโนโลยี (Infrastructure)

4.2.1 ผู้ดูแลระบบดิจิทัล (System Administrator)

ผู้ดูแลระบบดิจิทัลมีหน้าที่จัดทำและปรับปรุงทะเบียนทรัพย์สิน บริหารจัดการโครงสร้างพื้นฐาน รวมถึงระบบ AI อย่างเป็นระบบ ครอบคลุมวงจรการทำงานตั้งแต่การระบุ ป้องกัน ตรวจจับ ตอบสนอง และการฟื้นฟูระบบ โดยต้องบริหารจัดการความเสี่ยงทั้งด้านความมั่นคงปลอดภัยไซเบอร์ทั่วไป และความเสี่ยงของ AI เพื่อให้ระบบดำเนินงานได้อย่างมั่นคงปลอดภัย ตามกรอบการบริหารความเสี่ยงของกรมส่งเสริมการเกษตร

รวบรวม ทบทวน จัดทำและดูแลทะเบียนทรัพย์สินกายภาพ/ทรัพย์สินดิจิทัลในความรับผิดชอบของหน่วยงาน ประกอบด้วย เครื่องแม่ข่าย ระบบปฏิบัติการ ซอฟต์แวร์บริการ โครงสร้างพื้นฐาน คลาวด์ การตั้งค่าระบบ รวมถึงระบบหรือบริการที่มีการประยุกต์ใช้ AI เพื่อสนับสนุนการจำแนกระดับความสำคัญ และการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

การติดตั้ง กำหนดค่า และดูแลรักษาระบบดิจิทัลรวมถึงระบบ AI ให้เป็นไปตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย ครอบคลุมการจัดการบัญชีผู้ใช้และสิทธิ์การเข้าถึงข้อมูลและบริการที่เกี่ยวข้อง การอัปเดตแพตช์และซอฟต์แวร์ การสำรองข้อมูล การควบคุมการเปลี่ยนแปลงระบบ การป้องกันการใช้งานนอกวัตถุประสงค์หรือขัดต่อนโยบาย พร้อมจัดเก็บหลักฐานการดำเนินงานเพื่อให้สามารถตรวจสอบย้อนหลังได้

 จัดให้มีการบันทึกเหตุการณ์ของระบบตามข้อกำหนด ทั้งในระดับโครงสร้างพื้นฐาน ระบบปฏิบัติการ แอปพลิเคชัน และระบบหรือบริการที่ใช้ AI รวมถึงการตรวจสอบพฤติกรรมหรือการใช้งานที่ผิดปกติของระบบหรือบริการ เช่น การเรียกใช้งานที่ผิดรูปแบบ การเข้าถึงข้อมูลหรือโมเดลโดยไม่ได้รับอนุญาต หรือการเปลี่ยนแปลงค่าการทำงานที่ไม่สอดคล้องกับนโยบาย พร้อมแจ้งเตือนและส่งต่อข้อมูลให้หน่วยเฝ้าระวังและตอบสนองเหตุเมื่อพบความผิดปกติ

 สนับสนุนการดำเนินการกักกันหรือแก้ไขเชิงเทคนิคตามคำสั่งและแนวทางของทีมตอบสนองเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ เช่น การระงับการเข้าถึง ปรับสิทธิ์ผู้ใช้งาน ปิดหรือจำกัดการให้บริการบางส่วน แยกเครื่องหรือระบบที่ได้รับผลกระทบ หรือย้อนกลับการเปลี่ยนแปลงของระบบหรือการตั้งค่า พร้อมบันทึกขั้นตอนการดำเนินการและหลักฐานประกอบ

 การกู้คืนระบบดิจิทัลและระบบจากข้อมูลสำรอง ต้องทดสอบความพร้อมใช้งานและความถูกต้องของการทำงานหลังการกู้คืน รวมถึงตรวจสอบการตั้งค่าความปลอดภัย และการควบคุมการเข้าถึงของระบบและบริการก่อนเปิดให้บริการเต็มรูปแบบ เพื่อให้มั่นใจว่าระบบกลับมาดำเนินงานได้อย่างมั่นคงปลอดภัยและไม่ก่อให้เกิดความเสี่ยงซ้ำ

4.2 กลุ่มปฏิบัติการเทคโนโลยี (Infrastructure)

4.2.2 ผู้ดูแลเครือข่ายดิจิทัล (Network Administrator)

ผู้ดูแลเครือข่ายดิจิทัลมีบทบาทสำคัญในการดูแลโครงสร้างพื้นฐานการสื่อสารของหน่วยงาน ซึ่งเป็นฐานรองรับการให้บริการระบบดิจิทัลรวมถึงระบบที่มีการประยุกต์ใช้ AI ทั้งภายในและภายนอกองค์กร บทบาทดังกล่าวต้องคำนึงถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับเครือข่าย รวมถึงความเสี่ยงเฉพาะที่เกิดจากการเชื่อมต่อระบบ AI การรับส่งข้อมูล การเรียกใช้งานบริการ AI และการเข้าถึงโมเดลหรือข้อมูลผ่านเครือข่าย

- จัดทำและทบทวนข้อมูลโครงสร้างเครือข่าย อุปกรณ์เครือข่าย เส้นทางเชื่อมต่อ จุดเชื่อมโยงสำคัญ และการเชื่อมต่อไปยังระบบหรือบริการ รวมถึงบริการคลาวด์หรือ AI ภายนอกองค์กร เพื่อสนับสนุนการกำหนดขอบเขตระบบ การจำแนกทรัพย์สินเครือข่าย และการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงเฉพาะของการสื่อสารข้อมูลที่เกี่ยวข้องกับ AI

- กำหนดค่าและดูแลมาตรการด้านเครือข่ายให้เป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร โดยครอบคลุมการแบ่งโซนเครือข่าย การควบคุมการเข้าถึงเครือข่าย การกำหนดกฎการกรองทราฟฟิก การควบคุมการเชื่อมต่อระยะไกล และการจัดการอุปกรณ์เครือข่าย รวมถึงการจำกัดหรือควบคุมเส้นทางการสื่อสารที่เกี่ยวข้องกับ AI เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการรั่วไหลของข้อมูล พร้อมควบคุมการเปลี่ยนแปลงและจัดเก็บหลักฐานการดำเนินงานให้สามารถตรวจสอบย้อนหลังได้

 จัดให้มีการบันทึกข้อมูลเครือข่ายและการเฝ้าระวังทราฟฟิกตามข้อกำหนด วิเคราะห์สัญญาณผิดปกติในระดับเครือข่าย รวมถึงรูปแบบการสื่อสารที่อาจบ่งชี้ถึงการใช้งานระบบผิดปกติ รวมถึงการเรียกใช้งานบริการ AI ในปริมาณหรือรูปแบบที่ผิดปกติ และส่งต่อข้อมูลที่จำเป็นให้หน่วยเฝ้าระวังและตอบสนองเหตุ (SOC/IR) เพื่อยืนยันเหตุ ขยายผล และประเมินผลกระทบ

 ดำเนินการกักกันหรือจำกัดการสื่อสารทางเครือข่ายตามคำสั่งและแนวทางของทีมตอบสนองเหตุการณ์ เช่น การบล็อกปลายทางหรือบริการที่เกี่ยวข้องกับ AI การระงับเส้นทางการสื่อสาร การตัดการเชื่อมต่อ การแยกส่วนเครือข่าย หรือการปิดช่องทางที่ถูกใช้โจมตี เพื่อจำกัดผลกระทบและป้องกันการขยายวงของเหตุการณ์ พร้อมบันทึกการเปลี่ยนแปลงและการดำเนินการ

 ดำเนินการกู้คืนค่ากำหนดเครือข่ายและการเชื่อมต่อที่ได้รับผลกระทบ ตรวจสอบเสถียรภาพ ความปลอดภัย และความถูกต้องของการสื่อสารข้อมูล รวมถึงการเชื่อมต่อกับระบบหรือบริการ AI หลังการฟื้นฟู และยืนยันการกลับมาให้บริการตามลำดับความสำคัญที่กำหนด เพื่อให้ระบบเครือข่ายกลับสู่สภาพพร้อมใช้งานอย่างมั่นคงปลอดภัย

4.2 กลุ่มปฏิบัติการเทคโนโลยี (Infrastructure)

4.2.3 ผู้ดูแลคลาวด์/แพลตฟอร์ม (Cloud/Platform Administrator)

ผู้ดูแลคลาวด์และแพลตฟอร์มมีบทบาทสำคัญในการบริหารจัดการโครงสร้างพื้นฐานดิจิทัลที่เป็นฐานรองรับการพัฒนาและใช้งานระบบ AI ของหน่วยงาน ทั้งในรูปแบบแพลตฟอร์มภายในและบริการจากผู้ให้บริการภายนอก การปฏิบัติหน้าที่จึงต้องคำนึงถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงเฉพาะของระบบ AI เช่น การเข้าถึงทรัพยากร โมเดล และข้อมูลบนคลาวด์ การกำหนดสิทธิ์ การตั้งค่าความปลอดภัย และการพึ่งพาผู้ให้บริการ

 จัดทำและทบทวนรายการทรัพยากรคลาวด์และแพลตฟอร์มในความรับผิดชอบ เช่น โครงการ บัญชี ทรัพยากรหลัก สภาพแวดล้อมการใช้งาน การเชื่อมต่อ บริการที่เกี่ยวข้องกับ AI และสิทธิ์สำคัญ เพื่อสนับสนุนการจัดทำทะเบียนทรัพย์สิน การกำหนดขอบเขตระบบ และการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงความเสี่ยงของการใช้ AI บนคลาวด์

 กำหนดค่าและบังคับใช้มาตรการพื้นฐานด้านความปลอดภัยของคลาวด์และแพลตฟอร์มให้สอดคล้องกับนโยบายและแนวปฏิบัติขององค์กร โดยครอบคลุมการกำหนดและทบทวนสิทธิ์การเข้าถึง การตั้งค่าความปลอดภัยเริ่มต้น (Secure Baseline) การจัดการกุญแจ รหัสผ่าน และข้อมูลรับรอง การแยกสภาพแวดล้อม (เช่น พัฒนา ทดสอบ และใช้งานจริง) การควบคุมการเปลี่ยนแปลง รวมถึงการติดตามช่องโหว่และการอัปเดตที่เกี่ยวข้องกับแพลตฟอร์ม บริการคลาวด์ และบริการ AI ที่ใช้งาน

 เปิดใช้ ดูแล และทบทวนการบันทึกเหตุการณ์ของแพลตฟอร์มและบริการคลาวด์ รวมถึงบริการที่เกี่ยวข้องกับระบบ AI จัดทำการแจ้งเตือนเหตุการณ์สำคัญ วิเคราะห์รูปแบบการใช้งานที่ผิดปกติ เช่น การเข้าถึงทรัพยากร การเข้าถึงระบบ AI โดยไม่ได้รับอนุญาต หรือการใช้งานคลาวด์ที่มีความเสี่ยง และส่งต่อบันทึกและหลักฐานที่จำเป็นให้หน่วยเฝ้าระวังและตอบสนองเหตุ (SOC/IR) เพื่อการวิเคราะห์อย่างต่อเนื่อง

 ดำเนินการจำกัดสิทธิ์หรือกักกันทรัพยากรคลาวด์และแพลตฟอร์มตามคำสั่งและแนวทางของทีมตอบสนองเหตุการณ์ เช่น การปิดหรือหมุนเวียนกุญแจ (Key) การระงับบัญชีหรือสิทธิ์การเข้าถึง การแยกทรัพยากรหรือสภาพแวดล้อม การปรับนโยบายความปลอดภัยของแพลตฟอร์ม เพื่อจำกัดผลกระทบและป้องกันการขยายวงของเหตุการณ์ พร้อมจัดเก็บหลักฐานการดำเนินการอย่างครบถ้วน

 สนับสนุนการกู้คืนทรัพยากรคลาวด์และแพลตฟอร์มตามแผนฟื้นฟูของหน่วยงาน ทดสอบการกลับมาใช้งานของระบบและบริการที่เกี่ยวข้องกับระบบ AI ตรวจสอบความถูกต้องของการตั้งค่าและมาตรการความปลอดภัย และยืนยันความพร้อมก่อนเปิดให้บริการตามลำดับความสำคัญที่กำหนด

4.2 กลุ่มปฏิบัติการเทคโนโลยี (Infrastructure)

4.2.4 ผู้สนับสนุนระบบดิจิทัล/ผู้ให้บริการผู้ใช้งาน (Digital System Support / Helpdesk)

ผู้สนับสนุนระบบดิจิทัลและผู้ให้บริการผู้ใช้งานมีบทบาทสำคัญในฐานะด่านหน้าในการติดต่อกับผู้ใช้งาน ซึ่งรวมถึงผู้ใช้งานระบบดิจิทัลและระบบที่ประยุกต์ใช้ AI การดำเนินงานไม่เพียงมุ่งเน้นการแก้ไขปัญหาการใช้งานทั่วไป แต่ยังต้องสนับสนุนการใช้งานอย่างถูกต้อง ปลอดภัย และสอดคล้องกับนโยบายของกรมส่งเสริมการเกษตร คำนึงถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงจากการใช้งานนอกวัตถุประสงค์ การเปิดเผยข้อมูลโดยไม่เหมาะสม และผลกระทบต่อผู้ใช้งาน

รวบรวมและบันทึกข้อมูลปัญหาการใช้งาน เหตุผิดปกติที่ผู้ใช้งานแจ้ง และรูปแบบปัญหาที่เกิดซ้ำ ทั้งที่เกี่ยวข้องกับระบบดิจิทัลทั่วไปและระบบที่มีการใช้ AI เพื่อสนับสนุนการระบุความเสี่ยง จุดอ่อนเชิงปฏิบัติการ และประเด็นความเสี่ยงจากการใช้งาน AI เช่น การใช้งานนอกวัตถุประสงค์ หรือความเข้าใจคลาดเคลื่อนของผู้ใช้งาน

ให้คำแนะนำและสนับสนุนผู้ใช้งานให้ปฏิบัติตามนโยบายและแนวปฏิบัติขององค์กร รวมถึงแนวปฏิบัติการใช้ AI อย่างมั่นคงปลอดภัย สนับสนุนการจัดการบัญชีผู้ใช้งานตามกระบวนการที่กำหนด และประสานการแก้ไขปัญหาเบื้องต้นที่ไม่กระทบต่อความมั่นคงปลอดภัยไซเบอร์หรือการควบคุมการใช้งาน AI โดยไม่เปิดเผยข้อมูลหรือให้สิทธิ์เกินกว่าที่ได้รับอนุญาต

 เฝ้าระวังและสังเกตความผิดปกติจากการแจ้งปัญหาและพฤติกรรมการใช้งานของผู้ใช้งานที่อาจบ่งชี้ถึงเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์หรือความเสี่ยงจากการใช้ AI พร้อมทั้งแจ้งและส่งต่อข้อมูลที่เกี่ยวข้องให้ผู้ดูแลระบบหรือหน่วยงานที่รับผิดชอบเพื่อดำเนินการตรวจสอบต่อไป

 สนับสนุนการสื่อสารและการประสานงานภายในระหว่างการจัดการเหตุการณ์ตามคำสั่งของผู้ประสานงานเหตุ รวมถึงการช่วยเหลือผู้ใช้งานในระยะตอบสนอง เช่น การรีเซ็ตรหัสผ่าน การแจ้งแนวทางปฏิบัติชั่วคราว หรือการนัดหมายการแก้ไขปัญหา โดยไม่ดำเนินการใด ๆ ที่ขัดต่อนโยบายด้านความมั่นคงปลอดภัยไซเบอร์และการใช้ AI ขององค์กร

 สนับสนุนการกลับมาใช้งานของผู้ใช้งานหลังการแก้ไขหรือกู้คืนระบบ เช่น การยืนยันการใช้งานตามปกติ การสื่อสารขั้นตอนหรือข้อควรระวังหลังเหตุ รวมถึงการรวบรวมข้อเสนอแนะจากผู้ใช้งานเกี่ยวกับการใช้งานระบบดิจิทัลและ AI เพื่อนำไปใช้ปรับปรุงคุณภาพการให้บริการและมาตรการความมั่นคงปลอดภัยต่อไป

4.3 กลุ่มเฝ้าระวังและตอบสนองเหตุ (SOC / IR)

4.3.1 ทีมเฝ้าระวังภัยคุกคามไซเบอร์ (SOC Analyst / Helpdesk)

แนวปฏิบัติด้านการเฝ้าระวังและคัดกรองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์นำไปสู่การดำเนินการในทางปฏิบัติ ผ่านการบันทึกข้อมูลตามแบบฟอร์มที่ เพื่อให้การปฏิบัติงานเป็นไปอย่างเป็นระบบ มีมาตรฐานเดียวกัน สามารถตรวจสอบ ติดตาม และรายงานผลได้อย่างชัดเจน ประกอบด้วย

4.3.1.1 ข้อมูลทั่วไป

เลขที่เหตุ (Incident ID) :..... เวลาตรวจพบ : .....
ผู้ปฏิบัติงาน (Tier 1) : ..... ตำแหน่ง : .....

4.3.1.2 รายละเอียด

Source : ☐ FW ☐ NDR ☐ EDR ☐ e-mail ☐ Helpdesk ☐ อื่นๆ
Asset IP : .....
Owner / App : .....
Attack Type : .....
Description : .....

4.3.1.3 การดำเนินการ

☐ ตรวจสอบ Alert / Ticket ☐ เก็บหลักฐานเบื้องต้น
☐ Isolation : ..... ☐ EDR Scan : .....

4.3.1.4 ผลการคัดกรอง

ผลการพิจารณา :
◯ ไม่ใช่ภัยคุกคามไซเบอร์ (False Positive) ◯ ผิดปกติระดับต่ำ (เฝ้าระวังต่อ)
◯ เป็นภัยคุกคามไซเบอร์
ระดับความรุนแรง : ◯ วิกฤต ◯ สูง ◯ ปานกลาง ◯ ต่ำ ◯ ยังไม่สามารถระบุได้
อ้างอิงตาราง Severity Matrix / Escalation Criteria
เหตุผลประกอบการคัดกรอง : .....

4.3.1.5 การยกระดับเหตุ

◯ ปิด ◯ เฝ้าระวัง ☐ รายงาน IR Team (Tier 2)
ยกระดับไปยัง : ☐ IR Team ☐ Incident Coordinator
วันที่/เวลา ส่งต่อ/ปิดเคส : .../...../..... ..... : ..... น.
วิธีการแจ้ง : .....

4.3.1.6 ข้อสังเกต / ประเด็นที่ต้องติดตาม

.....

4.3 กลุ่มเฝ้าระวังและตอบสนองเหตุ (SOC / IR)

4.3.2 ทีมตอบสนองเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (IR Team)

ทีมตอบสนองเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์มีหน้าที่ดำเนินการควบคุม แก้ไข และลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการยืนยันแล้ว โดยปฏิบัติตามขั้นตอนและแบบฟอร์มที่กำหนด เพื่อให้การตอบสนองเป็นไปอย่างเป็นระบบ สามารถติดตาม ตรวจสอบ และรายงานผลการดำเนินการได้อย่างชัดเจน

4.3.2.1 ข้อมูลเหตุการณ์

Incident ID : ..... วันที่/เวลารับช่วงจาก Tier 1 : .....

วันที่/เวลาเริ่มวิเคราะห์ : .....

Asset / System / IP ที่เกี่ยวข้อง : .....เจ้าของระบบ/ข้อมูล : .....

4.3.2.2 การวิเคราะห์เหตุการณ์

☐ วิเคราะห์ Log / Timeline / Scope ☐ ควบคุมและจำกัดผลกระทบ (Containment)

☐ ระบุสาเหตุเชิงเทคนิค (Root Cause) ☐ ประเมินผลกระทบต่อระบบ / ข้อมูล / ผู้ใช้งาน

ระดับความรุนแรง : ◯ วิกฤต ◯ สูง ◯ ปานกลาง ◯ ต่ำ ◯ ไม่ใช่ภัยคุกคาม (False Positive)

ประเภทเหตุการณ์ : ☐ Malware ☐ Intrusion ☐ Data Leakage ☐ DoS ☐ Policy Violation

☐ Other: .....

สรุปการวิเคราะห์ : .....

4.3.2.3 การตอบสนองและฟื้นฟู

☐ ประสาน System Owner ☐ กำจัดภัยคุกคาม (Eradication)

☐ ฟื้นฟูระบบ / บริการ (Recovery) ☐ ทดสอบความพร้อมหลังแก้ไข

สรุปการตอบสนองและฟื้นฟู : .....

4.3.2.4 ผลการดำเนินการและการส่งต่อ

ผลการจัดการเหตุ

☐ ควบคุมและแก้ไขเรียบร้อย ☐ ต้องติดตามเพิ่มเติม ☐ ส่งต่อ Tier 3 (เชิงบริหาร)

ข้อเสนอแนะ : .....

ลงชื่อ Incident Response Team

.....

วันที่ .....

4.3 กลุ่มเฝ้าระวังและตอบสนองเหตุ (SOC / IR)

4.3.3 ผู้บริหารและผู้ประสานงานเหตุ (Executive Support / Incident Coordination & Post-Incident)

การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสูง (Tier 3) ซึ่งจะถูกเรียกใช้เมื่อเกิดเหตุการณ์ระดับ High หรือ Critical หรือเหตุการณ์ที่ส่งผลกระทบต่อภารกิจหลัก ข้อมูลสำคัญ ภาพลักษณ์ขององค์กร หรือกรณีที่มีความจำเป็นต้องใช้การตัดสินใจเชิงบริหาร ทั้งนี้ เพื่อสนับสนุนการสั่งการ การประสานงาน และการติดตามผลการดำเนินการอย่างเป็นระบบ รวมถึงการสรุปบทเรียนหลังเหตุการณ์

4.3.3.1 สรุปสถานการณ์ (Executive Summary)

Incident ID : .....

สรุปเหตุการณ์ : .....

4.3.3.2 การตัดสินใจเชิงบริหาร

☐ เห็นชอบแนวทางการจัดการเหตุ

☐ อนุมัติการฟื้นฟูและเปิดบริการ

☐ อนุมัติการสื่อสาร

☐ ภายใน.....

☐ ภายนอก .....

☐ อนุมัติการปิดเหตุ

ข้อสั่งการเพิ่มเติม : .....

4.3.3.3 บทเรียนและข้อเสนอเชิงนโยบาย

Lessons Learned : .....

ข้อเสนอปรับปรุง / นโยบาย / งบประมาณ : .....

ลงชื่อ ผู้บริหาร / ผู้ประสานงานเหตุ

.....

วันที่ .....

4.4 กลุ่มพัฒนาและผู้รับจ้าง/ผู้ขาย/ผู้ให้บริการภายนอก (DevOps)

4.4.1 ผู้พัฒนาภายในหน่วยงาน (Internal Developer)



ผู้พัฒนาภายในหน่วยงานรับผิดชอบคุณภาพและความมั่นคงปลอดภัยของซอฟต์แวร์ที่พัฒนาเอง รวมถึงระบบ AI และควบคุมความเสี่ยงจากข้อบกพร่องของโปรแกรมและการใช้งานไม่เหมาะสมของข้อมูลและสิทธิ์

ต้องระบุขอบเขตระบบ ฟังก์ชันสำคัญ ข้อมูลสำคัญ และเงื่อนไขด้านความมั่นคงปลอดภัยที่ต้องมีตั้งแต่ระยะออกแบบ รวมถึงระบุกรณีที่ระบบมีการประยุกต์ใช้ AI เช่น โมเดล ข้อมูลฝึก/ข้อมูลนำเข้า–ส่งออก จุดเชื่อมต่อกับบริการหรือแพลตฟอร์มภายนอก องค์ประกอบซอฟต์แวร์ ไลบรารี และโมเดลจากภายนอก ตลอดจนความเสี่ยงเชิงสถาปัตยกรรมและความเสี่ยงเฉพาะของ AI ที่อาจส่งผลต่อความถูกต้อง ความเป็นธรรม ความเป็นส่วนตัว และความมั่นคงปลอดภัยของระบบ

ต้องพัฒนาระบบตามแนวทางการพัฒนาที่ปลอดภัย โดยกำหนดมาตรฐานการเขียนโปรแกรม การทบทวนโค้ด และการควบคุมคุณภาพซอฟต์แวร์ ควบคุมการจัดการความลับ เช่น กุญแจ รหัสผ่าน โทเคน และข้อมูลรับรองของบริการ AI จัดการสิทธิ์การเข้าถึงซอร์สโค้ด ข้อมูล และโมเดลอย่างเป็นระบบ ควบคุมการเปลี่ยนแปลงซอฟต์แวร์ รวมถึงดำเนินการทดสอบด้านความมั่นคงปลอดภัยของซอฟต์แวร์และ AI ตามเกณฑ์ที่กำหนดก่อนนำขึ้นใช้งานจริง

ต้องจัดให้มีการตรวจพบความผิดปกติที่เกี่ยวข้องกับซอฟต์แวร์และ AI เช่น การบันทึกเหตุการณ์และกิจกรรมของระบบ การแจ้งเตือนข้อผิดพลาดหรือพฤติกรรมที่อาจกระทบความมั่นคงปลอดภัย การตรวจพบช่องโหว่จากการทดสอบหรือการสแกน รวมถึงการเฝ้าระวังพฤติกรรมผิดปกติของฟังก์ชันสำคัญหรือผลลัพธ์ของ AI ที่อาจบ่งชี้ถึงความเสี่ยงหรือการถูกโจมตี

 เมื่อพบช่องโหว่หรือเหตุผิดปกติ ต้องประเมินผลกระทบ จัดลำดับความเร่งด่วนของปัญหา แก้ไขหรือออกแพตช์ตามขั้นตอนที่กำหนด ควบคุมการเผยแพร่ซอฟต์แวร์หรือการปรับปรุงโมเดล AI และสนับสนุนข้อมูลเชิงเทคนิคที่จำเป็นให้แก่ทีมตอบสนองเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์จนสามารถจัดการและปิดประเด็นได้ครบถ้วน

 ต้องดำเนินการฟื้นฟูระบบให้กลับสู่สถานะที่มั่นคงปลอดภัยและสามารถใช้งานได้ตามปกติ ตรวจสอบความถูกต้องของการทำงานหลังการแก้ไข รวมถึงทบทวนและปรับปรุงแนวทางการออกแบบ การทดสอบ และมาตรฐานการพัฒนา เพื่อป้องกันไม่ให้เกิดปัญหาหรือความเสี่ยงซ้ำในอนาคต

4.4 กลุ่มพัฒนาและผู้รับจ้าง/ผู้ขาย/ผู้ให้บริการภายนอก (DevOps)

4.4.2 ผู้รับจ้างหรือผู้ให้บริการภายนอก (Vendor / Outsource)



ผู้รับจ้างหรือผู้ให้บริการภายนอกต้องส่งมอบซอฟต์แวร์ระบบ หรือบริการที่มีความมั่นคงปลอดภัยตามข้อกำหนดของหน่วยงาน รวมถึงกรณีที่มีการพัฒนา ใช้งาน หรือเชื่อมต่อกับระบบ AI และต้องบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงห่วงโซ่อุปทานซอฟต์แวร์และระบบ AI ให้สามารถตรวจสอบและติดตามย้อนกลับได้

ต้องยืนยันขอบเขตงาน สถาปัตยกรรม ระบบที่เกี่ยวข้อง ข้อมูลสำคัญ และข้อกำหนดด้านความมั่นคงปลอดภัยที่ระบุไว้ใน TOR หรือสัญญา รวมถึงกรณีที่ระบบมีการใช้ AI ต้องระบุโมเดล ข้อมูลที่ใช้ประมวลผลหรือฝึกสอน บริการ AI จากภายนอก ส่วนประกอบซอฟต์แวร์ ไลบรารี หรือโมเดลจากบุคคลที่สาม ตลอดจนความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่อุปทานซอฟต์แวร์และ AI

ต้องดำเนินการพัฒนา ปรับปรุง หรือให้บริการระบบตามมาตรฐานการพัฒนาที่ปลอดภัยจัดการสิทธิ์การเข้าถึงและการจัดการความลับในกระบวนการพัฒนาและให้บริการอย่างเหมาะสม จัดให้มีการทดสอบด้านความมั่นคงปลอดภัยของซอฟต์แวร์และ AI ก่อนส่งมอบ รวมถึงส่งมอบเอกสารและหลักฐานที่จำเป็นต่อการตรวจรับ เช่น รายงานผลการทดสอบ รายการส่วนประกอบซอฟต์แวร์ และแนวทางการใช้งานอย่างปลอดภัย

 ต้องจัดให้มีผลการตรวจสอบช่องโหว่และข้อบกพร่องที่เกี่ยวข้องกับซอฟต์แวร์ บริการ และ AI ก่อนส่งมอบ พร้อมจัดให้มีช่องทางรับแจ้งปัญหาหรือช่องโหว่ด้านความมั่นคงปลอดภัย และมีกลไกติดตามสถานะการแก้ไขอย่างเป็นระบบและตรวจสอบได้

 เมื่อเกิดช่องโหว่หรือเหตุการณ์ที่เกี่ยวข้องกับซอฟต์แวร์ บริการ หรือ AI ของผู้รับจ้าง ต้องดำเนินการแก้ไขตามระดับความรุนแรงและข้อตกลงระดับการให้บริการ (SLA) แจ้งผลกระทบ แนวทางลดความเสี่ยง และสถานะการแก้ไขให้หน่วยงานทราบอย่างทันท่วงที สนับสนุนการสืบสวนร่วมกับหน่วยงานเจ้าของระบบ และส่งมอบแพตช์หรือแนวทางแก้ไขที่ผ่านการทดสอบแล้ว

 ต้องสนับสนุนการกู้คืนบริการหรือข้อมูลตามขอบเขตความรับผิดชอบที่กำหนดในสัญญา พร้อมสรุปบทเรียนที่ได้รับ มาตรการป้องกันการเกิดซ้ำ และข้อเสนอแนะในการปรับปรุงกระบวนการพัฒนา การทดสอบ และการส่งมอบงานในรอบถัดไป เพื่อยกระดับความมั่นคงปลอดภัยของซอฟต์แวร์และ AI อย่างต่อเนื่อง

4.4 กลุ่มพัฒนาและผู้รับจ้าง/ผู้ขาย/ผู้ให้บริการภายนอก (DevOps)

4.4.3 ผู้พัฒนาระบบและความมั่นคงปลอดภัย (DevOps / AppSec)

DevOps/AppSec ทำหน้าที่วางและบังคับใช้ระบบ ความมั่นคงปลอดภัยเชิงวิศวกรรม ให้ฝังอยู่ในกระบวนการพัฒนา ทดสอบ และส่งมอบระบบ (CI/CD) รวมถึงระบบที่มีการใช้ AI โดยทำหน้าที่เป็นตัวกลางเชื่อมการพัฒนา โครงสร้างพื้นฐาน และหน่วยเฝ้าระวัง/ตอบสนองเหตุ (SOC/IR) ให้ทำงานสอดคล้องกันตลอดวงจรชีวิตของระบบ



ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและการปล่อยระบบ รวมถึงกรณีที่มีการใช้ AI ระบุจุดเสี่ยงในกระบวนการ (pipeline) เช่น โค้ด โมเดล AI อิมเมจ อาร์ติแฟกต์ รีจิสทรี และข้อมูลที่เกี่ยวข้อง ระบุสินทรัพย์ดิจิทัลที่ต้องได้รับการคุ้มครอง และกำหนดเกณฑ์การตัดสินใจด้านความเสี่ยงก่อนการปล่อยใช้งาน โดยคำนึงถึงความเสี่ยงเฉพาะของ AI เช่น ความถูกต้อง ความน่าเชื่อถือ และการพึ่งพาส่วนประกอบจากภายนอก

ต้องออกแบบและบังคับใช้มาตรการความมั่นคงปลอดภัยในสาย CI/CD เช่น การแยกสิทธิ์ของผู้ใช้งานและระบบอัตโนมัติ การกำหนดขั้นตอนอนุมัติการปล่อยงาน (Security Gating) การจัดการความลับและข้อมูลรับรอง การตรวจสอบโค้ด โมเดล AI และส่วนประกอบซอฟต์แวร์จากบุคคลที่สาม การเซ็นรับรองอาร์ติแฟกต์หรืออิมเมจ และการจัดการช่องโหว่ของซอฟต์แวร์และ AI อย่างเป็นวงรอบ

ต้องตั้งค่าการตรวจจับความผิดปกติในสายส่งมอบ เช่น การเปลี่ยนแปลงที่ไม่พึงประสงค์ในโค้ดหรือโมเดล AI การเข้าถึงซอร์สโค้ดหรือรีจิสทรีผิดปกติ การแจ้งเตือนจากการสแกนด้านความมั่นคงปลอดภัย และจัดส่งบันทึกหรือสัญญาณเตือนที่เกี่ยวข้องไปยัง SOC เพื่อการเฝ้าระวังและวิเคราะห์อย่างต่อเนื่อง

 เมื่อเกิดเหตุการณ์หรือพบช่องโหว่ ให้ดำเนินการปิดกั้นการปล่อยเวอร์ชันที่มีความเสี่ยง ย้อนกลับการเปลี่ยนแปลง (rollback) ตามขั้นตอนที่กำหนด ออกแพตช์หรือแนวทางแก้ไขเร่งด่วน กำกับให้การแก้ไขผ่านเกณฑ์ด้านความมั่นคงปลอดภัย และประสานงานกับทีม SOC/IR เพื่อควบคุมและลดผลกระทบในภาพรวม

 สนับสนุนการกู้คืนระบบและการปล่อยเวอร์ชันที่มีความมั่นคงปลอดภัยกลับสู่การให้บริการตามปกติ ตรวจสอบความครบถ้วนของมาตรการใน pipeline หลังเหตุการณ์ และทบทวนปรับปรุงแนวทาง เครื่องมือ และเกณฑ์การอนุมัติการปล่อยงาน เพื่อป้องกันไม่ให้เกิดเหตุซ้ำและยกระดับความมั่นคงปลอดภัยของระบบและ AI อย่างต่อเนื่อง

4.4 กลุ่มพัฒนาและผู้รับจ้าง/ผู้ขาย/ผู้ให้บริการภายนอก (DevOps)

4.4.4 ผู้กำกับสัญญา (Contract Manager)

ผู้กำกับสัญญารับผิดชอบการควบคุมและกำกับความเสี่ยงด้านคู่สัญญาให้เป็นไปตาม TOR/สัญญา ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ และกรณีที่เกี่ยวข้องกับ AI โดยทำหน้าที่เชิงบริหารเพื่อให้การดำเนินงานของคู่สัญญาเป็นไปตามเงื่อนไขที่กำหนด สามารถตรวจสอบและบังคับใช้ได้ตลอดอายุสัญญา



ต้องทบทวนและยืนยันข้อกำหนดด้านความมั่นคงปลอดภัยใน TOR/สัญญา เช่น ขอบเขตข้อมูลสำคัญ ข้อมูลส่วนบุคคล ข้อมูลที่ใช้กับ AI สิทธิ์การเข้าถึง เงื่อนไขการทดสอบความมั่นคงปลอดภัย การรายงานเหตุ และข้อกำหนดด้านการใช้ AI ระบุความเสี่ยงจากการพึ่งพาผู้ให้บริการหรือเทคโนโลยี AI จากภายนอก และกำหนดตัวชี้วัด หลักฐาน และเอกสารที่ใช้ประกอบการตรวจรับงานและการประเมินความสอดคล้อง

ต้องบังคับใช้เงื่อนไขด้านความมั่นคงปลอดภัยผ่านกระบวนการบริหารสัญญาและการตรวจรับงาน เช่น เงื่อนไขการควบคุมและทบทวนสิทธิ์การเข้าถึง ข้อกำหนดการเปลี่ยนแปลงระบบหรือโมเดล AI และการทดสอบก่อนใช้งานจริง เงื่อนไขการคุ้มครองข้อมูลและการจำกัดการนำข้อมูลไปใช้กับ AI ภายนอก รวมถึงข้อกำหนดการส่งมอบเอกสาร หลักฐาน และรายงานด้านความมั่นคงปลอดภัยตามที่กำหนดในสัญญา

 ต้องติดตามและตรวจสอบการปฏิบัติตามสัญญาและข้อตกลงระดับการให้บริการ (SLA) ด้านความมั่นคงปลอดภัยไซเบอร์ ตรวจสอบรายงานผลการทดสอบ ช่องโหว่ การแก้ไข และการประเมินความเสี่ยงจากคู่สัญญา รับทราบและบันทึกเหตุผิดปกติหรือเหตุการณ์ด้านความมั่นคงปลอดภัยจากคู่สัญญา และประสานให้มีการรายงานเข้าสู่กลไกการจัดการเหตุขององค์กรภายในระยะเวลาที่กำหนด

 เมื่อเกิดเหตุการณ์หรือการไม่ปฏิบัติตามข้อกำหนด ให้ประสานการใช้สิทธิ์ตาม TOR/สัญญาเพื่อเร่งรัดการแก้ไข กำกับระยะเวลา การส่งมอบหลักฐาน และการปิดช่องโหว่หรือความเสี่ยง สนับสนุนการสื่อสารและการทำงานร่วมกับทีมตอบสนองเหตุ (IR) และหน่วยเฝ้าระวัง (SOC) รวมถึงดำเนินการด้านสัญญาหรือมาตรการตามเงื่อนไขที่กำหนด

 ต้องกำกับการส่งมอบงานแก้ไข การกู้คืนบริการหรือระบบ และการทดสอบความพร้อมใช้งานให้ครบถ้วนตามเงื่อนไขสัญญา จัดทำสรุปบทเรียนด้านการบริหารคู่สัญญาและความเสี่ยงจากการใช้ AI และนำผลที่ได้ไปปรับปรุง TOR แม่แบบสัญญา และเงื่อนไขการตรวจรับงานในโครงการถัดไป เพื่อยกระดับการควบคุมความเสี่ยงด้านคู่สัญญาอย่างต่อเนื่อง

4.5 แนวปฏิบัติสำหรับผู้ใช้งานทั่วไป (User)

4.5.1 การเข้าใช้งานระบบด้วยบัญชี DOAE ID (Single Sign-On)

ผู้ใช้งานต้องเข้าใช้งานระบบและบริการดิจิทัลของกรมส่งเสริมการเกษตรด้วยบัญชีของตนเองเท่านั้น และต้องกำหนดรหัสผ่านที่มีความรัดกุมไม่ใช้ซ้ำกับระบบอื่น และออกจากระบบทุกครั้งเมื่อเลิกใช้งาน ทั้งนี้ ห้ามให้ผู้อื่นยืมบัญชีหรือใช้งานร่วมกัน เพื่อป้องกันการแอบอ้างตัวตนและการเข้าถึงระบบโดยมิชอบ รวมถึงการนำข้อมูลบัญชีไปใช้กับระบบ AI ที่อยู่นอกการควบคุมของหน่วยงาน

4.5.2 การใช้งานอีเมลและป้องกันการหลอกลวง (Phishing)

ผู้ใช้งานใช้อีเมลติดต่อราชการด้วยอีเมลของหน่วยงาน @doae.go.th ผ่านแพลตฟอร์มอีเมลฯ mailbox.doae.go.th ต้องใช้ความระมัดระวังในการใช้งานอีเมลและการติดต่อสื่อสาร โดยเฉพาะข้อความที่มีลักษณะเร่งด่วน หลอกลวง หรือชักชวนให้เปิดลิงก์ ดาวน์โหลดไฟล์ หรือกรอกข้อมูล

4.5.3 การใช้งานอินเทอร์เน็ตและเว็บไซต์อย่างปลอดภัย

ผู้ใช้งานต้องยืนยันตัวตนก่อนเข้าใช้งานผ่านเครือข่ายอินเทอร์เน็ตที่กรมส่งเสริมการเกษตรกำหนด หรือใช้งานอินเทอร์เน็ตผ่านช่องทางที่ปลอดภัย เข้าถึงเฉพาะเว็บไซต์ที่มีความน่าเชื่อถือและการเชื่อมต่อที่ปลอดภัย หลีกเลี่ยงเครือข่ายที่ไม่ทราบแหล่งที่มา และอัปเดตเว็บเบราว์เซอร์สม่ำเสมอ เพื่อป้องกันการโจมตีหรือการเชื่อมโยงไปยังระบบภายนอก

4.5.4 ความปลอดภัยของอุปกรณ์ดิจิทัล

ผู้ใช้งานต้องตั้งค่าความปลอดภัยของอุปกรณ์ เช่น ตั้งรหัสผ่านที่คาดเดายาก เปิดใช้การยืนยันตัวตนหลายขั้นตอน (2FA) ผ่าน SSO Horizon ด้วยบัญชี DOAE ID รวมถึงอัปเดตระบบและแอปพลิเคชัน และเปิดใช้ฟังก์ชันลบข้อมูลระยะไกลในกรณีอุปกรณ์สูญหาย ทั้งนี้ ห้ามดัดแปลงระบบ หรือใช้อุปกรณ์ที่อาจทำให้ข้อมูลของกรมถูกเข้าถึงโดยไม่ได้รับอนุญาต

4.5.5 การจัดการข้อมูลและเอกสารของทางราชการ

ผู้ใช้งานต้องจัดเก็บ ส่งต่อ และใช้งานข้อมูลหรือเอกสารของทางราชการผ่านบริการดิจิทัลที่กรมส่งเสริมการเกษตรกำหนดภายใต้แพลตฟอร์มพื้นที่จัดเก็บข้อมูลออนไลน์ของกรมส่งเสริมการเกษตร drive.doae.go.th หรือบริการภาครัฐที่ได้รับอนุญาตเท่านั้น พร้อมทั้งกำหนดสิทธิ์การเข้าถึงและลบข้อมูลที่ไม่จำเป็นเมื่อสิ้นสุดการใช้งาน ทั้งนี้ ห้ามนำข้อมูลราชการหรือข้อมูลส่วนบุคคลไปใช้งานในระบบอัตโนมัติหรือ AI ภายนอกที่อยู่นอกการควบคุมของหน่วยงาน

4.5.6 การใช้ลิงก์ย่อและรหัส QR Code

การเผยแพร่ลิงก์ย่อหรือรหัส QR Code เพื่อเชื่อมโยงไปยังระบบหรือข้อมูลของกรม ต้องใช้บริการที่หน่วยงานของรัฐจัดให้เท่านั้น เช่น qrcode.doae.go.th หรือ dg.th และต้องตรวจสอบปลายทางก่อนใช้งานหรือเผยแพร่ทุกครั้ง ห้ามใช้บริการจากแหล่งภายนอกหรือเชื่อมโยงกับข้อมูลที่ไม่ได้รับอนุญาต

4.5.7 การแชร์ไฟล์และการใช้งานระบบคลาวด์

การแชร์ไฟล์หรือใช้งานระบบคลาวด์ต้องดำเนินการผ่านบริการที่อยู่ภายใต้แพลตฟอร์มพื้นที่จัดเก็บข้อมูลออนไลน์ของกรมส่งเสริมการเกษตร drive.doae.go.th หรือระบบที่กรมอนุญาตเท่านั้น โดยต้องตรวจสอบสิทธิ์ผู้เข้าถึง และห้ามส่งต่อหรือซิงก์เอกสารราชการไปยังบัญชีหรืออุปกรณ์ส่วนบุคคล

4.5.8 การประชุมและติดต่อสื่อสารออนไลน์

ผู้ใช้งานต้องใช้ระบบประชุมและการสื่อสารออนไลน์ที่กรมกำหนด ตรวจสอบผู้เข้าร่วม ใช้ความระมัดระวังในการแชร์หน้าจอ และไม่บันทึกหรือเปิดใช้ฟังก์ชันอัตโนมัติที่อาจส่งข้อมูลออกนอกการควบคุมของหน่วยงาน เว้นแต่ได้รับอนุญาต

4.5.9 การใช้งานเครือข่ายสังคมออนไลน์

ผู้ใช้งานต้องไม่ส่งข้อมูลราชการ ข้อมูลสำคัญ ข้อมูลอ่อนไหว หรือข้อมูลส่วนบุคคลผ่านเครือข่ายสังคมออนไลน์หรือแอปพลิเคชันส่วนบุคคล เว้นแต่เป็นช่องทางทางการที่กรมกำหนด และต้องมีมาตรการป้องกันการรั่วไหลของข้อมูล

4.5.10 การแจ้งเหตุผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์

เมื่อพบเหตุผิดปกติจากการใช้งานระบบดิจิทัลหรืออุปกรณ์ เช่น พบอีเมลต้องสงสัย ระบบขัดข้อง ข้อมูลรั่วไหล ผู้ใช้งานต้องแจ้งไปยัง แพลตฟอร์ม DOAE Helpdesk ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยทันที และไม่ควรดำเนินการแก้ไขด้วยตนเอง

หลักการสำคัญ

ผู้ใช้งานต้องใช้งานระบบดิจิทัลของกรมส่งเสริมการเกษตรผ่านแพลตฟอร์มและช่องทางที่กำหนดเท่านั้น โดยมีการยืนยันตัวตน การควบคุมสิทธิ์และการจัดการข้อมูลภายใต้กรอบเดียวกัน คิดก่อนคลิก ระมัดระวังข้อมูลและแจ้งเหตุทันทีเมื่อพบความผิดปกติ เพื่อให้การใช้งานเป็นไปอย่างมั่นคงปลอดภัยและน่าเชื่อถือ

4.5 แนวปฏิบัติสำหรับผู้ใช้งานทั่วไป (User)

1. ใช้บัญชี DOAE ID ของตนเองเท่านั้น



เข้าใช้งานด้วยบัญชี (DOAE ID) ของตนเอง ห้ามให้ผู้อื่นยืมบัญชี และกำหนดรหัสผ่านแต่ละระบบต่างกัน

2. ใช้งานอีเมลปลอดภัย



ใช้อีเมล @doae.go.th ในการติดต่อราชการ ระวังอีเมลต้องสงสัยหลอกลวง (phishing) อย่าคลิกลิงก์หรือดาวน์โหลดไฟล์จากอีเมลที่ไม่รู้จัก

3. ใช้อินเทอร์เน็ตอย่างปลอดภัย



ใช้งานอินเทอร์เน็ตผ่านเครือข่ายของกรมฯ หรือช่องทางที่ปลอดภัยเท่านั้น ไม่เชื่อมต่อเครือข่ายที่ไม่รู้จัก และตรวจสอบที่อยู่เว็บไซต์ที่ปลอดภัย (HTTPS)

6. ใช้ลิงก์ย่อ และ QR Code



สร้างลิงก์ย่อ QR Code ผ่านqrcode.doae.go.th หรือหน่วยงานของรัฐเช่น dg.th และตรวจสอบปลายทางก่อนเผยแพร่

7. แชร์ไฟล์ผ่านคลาวด์ของกรมฯ



ใช้แพลตฟอร์มบริการพื้นที่จัดเก็บข้อมูลออนไลน์ ของกรมฯ ในการแชร์ข้อมูลสำคัญ ตรวจสอบสิทธิ์การเข้าถึง ห้ามส่งไฟล์ราชการผ่านบัญชีส่วนตัว หรือบริการฝากไฟล์ฟรี

8. ประชุมออนไลน์อย่างระมัดระวัง



ใช้ระบบที่กรมฯกำหนด ตรวจสอบผู้เข้าร่วม ระวังการแชร์หน้าจอที่อาจมีข้อมูลสำคัญ หรือข้อความส่วนตัวแสดงอยู่

4. ปกป้องอุปกรณ์ดิจิทัลเสมอ



ตั้งรหัสผ่านที่คาดเดายาก เปิดใช้การยืนยันตัวตนหลายขั้นตอน (2FA) หรือ OTP อัปเดตระบบและแอปพลิเคชัน ห้ามดัดแปลงระบบ ใช้อุปกรณ์ไม่ปลอดภัย

5. จัดการข้อมูลราชการผ่านระบบที่กำหนด



จัดเก็บและส่งต่อข้อมูลราชการผ่านบริการที่กรมฯกำหนด หรือบริการที่กรมฯอนุญาต เท่านั้นและห้ามนำข้อมูลสำคัญเข้าสู่ระบบ AI ภายนอก



9. ไม่ส่งข้อมูลสำคัญผ่านโซเชียลมีเดีย

ห้ามส่งข้อมูลราชการ ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว ผ่านแอปพลิเคชันโซเชียลมีเดียส่วนตัว เว้นแต่เป็นช่องทางที่กรมฯกำหนด



10. พบสิ่งผิดปกติแจ้ง DOAE Helpdesk ทันที

เมื่อพบเหตุผิดปกติ ระบบขัดข้อง หรือเหตุสงสัยข้อมูลรั่วไหล ห้ามแก้ไขด้วยตนเอง **แจ้ง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือ DOAE Helpdesk ทันที**



อภิธานศัพท์

DOAE ID	บัญชีผู้ใช้งานซึ่งเป็นบัญชีเดียวกับอีเมลกรมส่งเสริมการเกษตร @doae.go.th
SSO Horizon	ศูนย์กลางจัดการบัญชี DOAE ID บริการลงชื่อเข้าใช้งานจากจุดเดียว Single Sign-On
DOAE Helpdesk	แพลตฟอร์มบริหารครุภัณฑ์และบริการคอมพิวเตอร์ https://helpdesk.doae.go.th เป็นบริการเริ่มต้นในการลงทะเบียนตัวตนดิจิทัล / บันทึกข้อมูลการใช้เครื่องคอมพิวเตอร์ และเครือข่ายฯ / เปิดใช้งานอีเมลกรมส่งเสริมการเกษตร
DOAE QR	แพลตฟอร์มสร้างลิงก์ย่อและ QR Code https://qrcode.doae.go.th
DOAE eMail	แพลตฟอร์มอีเมลกรมส่งเสริมการเกษตร https://mailbox.doae.go.th
DOAE Drive	แพลตฟอร์มพื้นที่จัดเก็บข้อมูลออนไลน์ https://drive.doae.go.th

คณะผู้จัดทำ

นายวรวุฒิ อ้อยหวาน	ผู้อำนวยการกลุ่มระบบเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์
นายกิติศักดิ์ ปัญญาทรานนท์	นักวิชาการคอมพิวเตอร์ชำนาญการ
นายอนุวัฒน์ เปพาทย์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
นายสหรัฐ เขียวหวาน	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
นายนิรันดร อ่อนน้อมดี	เจ้าหน้าที่ระบบงานคอมพิวเตอร์

