

แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ
นางสาวศศิธร หุ่นทอง นักวิชาการเกษตรชำนาญการ สถานีพัฒนาที่ดินสุรินทร์
สำนักงานพัฒนาที่ดินเขต ๓ กรมพัฒนาที่ดิน
หลักสูตร “พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น”
(Basic Cybersecurity Series)
วันที่ ๑๐ เดือนกันยายน ๒๕๖๙ เป็นเวลา ๑ วัน
ผ่านระบบการเรียนออนไลน์ โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
Thailand Digital Government Academy (TDGA)

สรุปบทเรียน

๑. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

- วิเคราะห์สินทรัพย์ (Asset Identification): รวบรวมและจัดหมวดหมู่ข้อมูลรวมถึงอุปกรณ์ในองค์กร เช่น เครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ ฐานข้อมูลเกษตรกร หรือระบบสารสนเทศภายใน เพื่อดูว่าสิ่งใดมีความสำคัญระดับสูง
- ประเมินความเสี่ยงและผลกระทบ (Risk & Impact Analysis): คำนวณความเสียหายหากข้อมูลรั่วไหลหรือระบบล่ม โดยพิจารณาจากโอกาสเกิด (Likelihood) และระดับความเสียหาย (Impact) เพื่อจัดลำดับความสำคัญในการแก้ไข
- วางแผนลดความเสี่ยง (Risk Mitigation): กำหนดมาตรการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เช่น การเพิ่มมาตรการยืนยันตัวตนในระบบที่มีความเสี่ยงสูง

๒. ความต้านทานและตอบสนองต่อภัยคุกคาม (Cyber Resilience)

- แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan - BCP): วางโครงสร้างการทำงานสำรองไว้ล่วงหน้า เพื่อให้หน่วยงานยังสามารถให้บริการประชาชนหรือดำเนินงานต่อไปได้ แม้ระบบคอมพิวเตอร์หลักจะถูกลบทำลาย
- ระบบสำรองข้อมูล (Data Backup Strategy): ปฏิบัติตามกฎหมาย ๓-๒-๑ สำรองข้อมูลไว้ ๓ ชุด บนสื่อบันทึกต่างกัน ๒ ชนิด และเก็บไว้ Off-site หรือ Cloud ที่ปลอดภัยอย่างน้อย ๑ ชุด
- การซ้อมแผนรับมือ (Tabletop Exercise): จัดการทดสอบจำลองสถานการณ์ภัยคุกคาม (เช่น โดน Ransomware) เพื่อฝึกซ้อมให้บุคลากรเข้าใจบทบาทหน้าที่เมื่อเกิดเหตุจริง

๓. กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

- การปฏิบัติตามกฎหมาย (Regulatory Compliance): ดำเนินการให้ถูกต้องตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)
- การนำมาตรฐานสากลมาปรับใช้: อ้างอิงกรอบการทำงานระดับสากล เช่น NIST CSF (Identify, Protect, Detect, Respond, Recover) หรือ ISO/IEC ๒๗๐๐๑ เพื่อจัดทำเป็นนโยบายความปลอดภัย (Cybersecurity Policy) ของหน่วยงาน
- การสร้างความตระหนักรู้ (Security Awareness Training): อบรมสร้างภูมิคุ้มกันดิจิทัลให้เจ้าหน้าที่ทุกคน เนื่องจากบุคลากรคือปราการด่านแรกในการป้องกันภัยไซเบอร์

๔. การป้องกันและการประเมินช่องโหว่ (Protect & Vulnerability Assessment)

- การจัดการช่องโหว่ (Patch Management): สแกนหาจุดอ่อนของระบบอย่างสม่ำเสมอ และเร่งอัปเดตซอฟต์แวร์/ระบบปฏิบัติการทันทีที่มีแพตช์ความปลอดภัยใหม่ออกมา
- การจำกัดสิทธิ์การเข้าถึง (Access Control & Least Privilege): กำหนดสิทธิ์ให้ผู้ใช้งานเข้าถึงข้อมูลเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น เพื่อลดความเสียหายหากบัญชีผู้ใช้ถูกแฮก
- การป้องกันเครือข่ายและอุปกรณ์ (Network & Endpoint Protection): ติดตั้ง Firewall, ระบบป้องกันไวรัส (EDR/Antivirus) และตั้งค่าให้เครื่องคอมพิวเตอร์ล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งาน

๕. การตรวจสอบและเฝ้าระวังภัยคุกคาม (Detect)

- การจัดการประวัติระบบ (Log Management): บันทึกและจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log files) ตามที่กฎหมายกำหนด เพื่อใช้ตรวจสอบเส้นทางการใช้งานและสิ่งผิดปกติ
- ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS): ใช้เครื่องมือช่วยเฝ้าระวังพฤติกรรมน่าสงสัยในระบบเครือข่าย เช่น การพยายามสแกนหาช่องโหว่หรือการแอบส่งข้อมูลออกไปยัง IP แปลกปลอม
- การแจ้งเตือนภัยคุกคาม (Alerting & Monitoring): ตั้งค่าระบบแจ้งเตือนไปยังผู้ดูแลระบบทันทีที่พบความผิดปกติ เพื่อให้ยับยั้งเหตุได้ก่อนเกิดความเสียหายวงกว้าง

๖. การเผชิญเหตุและการฟื้นฟูความเสียหาย (Respond & Recover)

- การควบคุมและจำกัดวงความเสียหาย (Containment): เมื่อพบการบุกรุก ต้องเร่งตัดการเชื่อมต่ออุปกรณ์ที่ติดเชื่อออกจากเครือข่ายทันที เพื่อไม่ให้ไวรัสหรือแฮกเกอร์แพร่กระจายไปยังเครื่องอื่น
- การสืบสวนหาสาเหตุ (Digital Forensics): ตรวจสอบร่องรอยดิจิทัลเพื่อหาสาเหตุของช่องโหว่ วิธีการที่ผู้โจมตีใช้ และ scope ของข้อมูลที่ได้รับผลกระทบ
- การกู้คืนและปรับปรุงระบบ (Recovery & Lessons Learned): ตรวจสอบความสะอาดของระบบ กู้คืนข้อมูลจากชุด Backup นำระบบกลับมาเปิดใช้งาน และนำข้อผิดพลาดมาปรับปรุงมาตรการป้องกันเพื่อไม่ให้เกิดซ้ำ



(นางสาวศศิธร หุ่นทอง)
นักวิชาการเกษตรชำนาญการ

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ศศิธร หุ่นทอง

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 10 กันยายน 2569

สำหรับคุณ
ศศิธร ✓

(นางสาวศศิธร หุ่นทอง)
นักวิชาการเกษตรชำนาญการ

A.L.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



5e145ec8

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (พ.ร.)
Digital Government Development Agency (Public
Organization) (DGA)
Date: 2026-09-10T10:59:11.671+07:00