แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๓

รอบการประเมินที่ ๑ / ๒๕๖๙ ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ - ๓๑ มีนาคม ๒๕๖๙

ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล เลิศอุไร เลิศไกร ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน

กลุ่ม/ฝ่าย/สพด กลุ่มวิชาการเพื่อการพัฒนาที่ดิน

หัวข้อการพัฒนา Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

สถานที่ กลุ่มวิชาการเพื่อการพัฒนาที่ดิน สำนักงานพัฒนาที่ดินเขต ๓

วันที่ ๑๖ กุมภาพันธ์ ๒๕๖๙

วิทยากร/ผู้ให้ความรู้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

หน่วยงานที่จัดอบรมสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy

สรุปสาระสำคัญ

หลักสูตรทั้ง ๖ หัวข้อ คือ

๑. แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์

เน้นการสร้าง Cyber Resilience หรือความสามารถในการเตรียมตัว รับมือ และฟื้นฟูระบบให้กลับมาทำงานได้อย่างรวดเร็วเมื่อเกิดเหตุ โดยใช้หลักการพื้นฐาน CIA Triad ได้แก่

- Confidentiality: การรักษาความลับของข้อมูล
- Integrity: การรักษาความถูกต้องของข้อมูล
- Availability: การทำให้ระบบพร้อมใช้งานเสมอ

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) กระบวนการวิเคราะห์เพื่อหาโอกาสที่ภัยคุกคามจะส่งผลกระทบต่อองค์กร ประกอบด้วย ๓ ขั้นตอนหลัก

๑. Risk Identification: ระบุสินทรัพย์ดิจิทัล ภัยคุกคาม และช่องโหว่

๒. Risk Analysis: วิเคราะห์ระดับผลกระทบและความน่าจะเป็น

๓. Risk Evaluation: ประเมินว่าความเสี่ยงอยู่ในระดับที่ยอมรับได้หรือไม่ เพื่อกำหนดแนวทางจัดการ

๓. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) แนวทางที่เป็นสากล เช่น NIST CSF ๒.๐ ซึ่งช่วยให้หน่วยงานบริหารจัดการความเสี่ยงได้อย่างเป็นระบบ ประกอบด้วยฟังก์ชันหลัก ได้แก่ Govern, Identify, Protect, Detect, Respond, และ Recover

๔. การป้องกันความเสี่ยง (Protect) และการประเมินช่องโหว่ (Vulnerability Assessment) เน้นการ "ปิดประตูบ้าน" ก่อนถูกโจมตี โดยมีแนวทางสำคัญคือ

- Vulnerability Assessment (VA): การใช้เครื่องมือสแกนหาจุดอ่อนในระบบเพื่อเร่งแก้ไข
- การป้องกันเบื้องต้น: เช่น การอัปเดต Patch สม่ำเสมอ, การตั้งรหัสผ่านที่คาดเดายาก และการใช้การยืนยันตัวตนสองปัจจัย (๒FA)

๕. การตรวจสอบ และเฝ้าระวังภัยคุกคาม (Detect) การวางระบบเพื่อ "ตรวจจับ" กิจกรรมที่ผิดปกติได้อย่างรวดเร็ว เช่น

- การตรวจสอบการเชื่อมต่อระยะไกล (Remote Access)
- การวิเคราะห์ Log File หรือบันทึกกิจกรรมในระบบ เพื่อหาพฤติกรรมน่าสงสัย

๖. การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

Respond: ขั้นตอนเมื่อเกิดภัยคุกคาม เช่น การตัดการเชื่อมต่อเพื่อจำกัดความเสียหายและการรายงานเหตุการณ์

Recover: การกู้คืนข้อมูลจากระบบสำรอง (Backup) และการปรับปรุงระบบให้กลับมาใช้งานได้ตามปกติเพื่อสร้างความต่อเนื่องทางธุรกิจ

(ลงนาม).....

(นางสาวเลิศอุไร เลิศไกร)

ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน

(ลงนาม).....

(นายจิรยุทธ์ คำขจร)

ตำแหน่ง ผู้อำนวยการกลุ่มวิชาการเพื่อการพัฒนาที่ดิน

ผู้รับรองผลการพัฒนาความรู้

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ เลิศอุไร เลิศไกร

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 16 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-16T19:58:21.555+07:00
d20c384a