



บันทึกข้อความ

ส่วนราชการ สถานีพัฒนาที่ดินภูเก็ต สำนักงานพัฒนาที่ดินเขต ๑๑ โทร ๐ ๗๖๖๘ ๕๒๕๓

ที่ กษ ๐๘๑๘.๐๖/ภก.๓๖๙

วันที่ ๑๗ สิงหาคม ๒๕๖๙

เรื่อง ขอสรุปบทเรียนการพัฒนาความรู้ รอบการประเมินที่ ๒/๒๕๖๙

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินภูเก็ต

ตามที่กรมพัฒนาที่ดิน กำหนดให้ข้าราชการทั่วไป ดำเนินการจัดทำตัวชี้วัดรายบุคคลด้านการพัฒนาบุคลากร “ระดับความสำเร็จของการพัฒนาความรู้” รอบการประเมินที่ ๒ (๑ เมษายน ๒๕๖๙ - ๓๐ กันยายน ๒๕๖๙) ของปีงบประมาณ พ.ศ.๒๕๖๙ โดยให้มีการพัฒนาความรู้ครบถ้วนตามเงื่อนไขของหลักสูตร ๒ เรื่อง และมีการสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชาทราบ ภายในวันที่ ๑๔ กันยายน ๒๕๖๙ นั้น

บัดนี้ ข้าพเจ้า นางสาวฐิตาภา จอมเลิศ ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ สังกัดสถานีพัฒนาที่ดินภูเก็ต สำนักงานพัฒนาที่ดินเขต ๑๑ กรมพัฒนาที่ดิน ได้มีการพัฒนาความรู้ครบถ้วนตามเงื่อนไขของหลักสูตรแล้ว จึงขอสรุปบทเรียนตามหลักสูตรดังกล่าว ตามรายละเอียดที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

(นางสาวฐิตาภา จอมเลิศ)
นักวิชาการเกษตรปฏิบัติการ

- ทวณ

ใน 3:

17 ส.ค. ๒๕๖๙

สรุปบทเรียนการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์
วิชา“ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล
(Cyber Security and Digital Awareness)” ของสำนักงาน ก.พ.

เป้าหมายการเรียนรู้

๑. ผู้เข้ารับการอบรมสามารถอธิบายเกี่ยวกับรูปแบบของภัยคุกคามทางดิจิทัลในลักษณะต่างๆ
๒. ผู้เข้ารับการอบรมสามารถอธิบายความสำคัญ และความจำเป็นของความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล
๓. ผู้เข้ารับการอบรมสามารถประยุกต์ใช้เทคโนโลยีดิจิทัลในยุคปัจจุบัน รวมทั้งสามารถปฏิบัติตามและใช้กฎหมายด้านดิจิทัล (Digital Government)

ความรู้พื้นฐานเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล

ความมั่นคงปลอดภัยทางไซเบอร์ คือการปกป้องระบบคอมพิวเตอร์ เครือข่าย และข้อมูลจากการเข้าถึง การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต โดยมีหลักการพื้นฐานที่เรียกว่า CIA Triad

- Confidentiality (ความลับ) : การปกป้องข้อมูลไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงได้
- Integrity (ความถูกต้องแท้จริง) : การรับประกันว่าข้อมูลจะไม่ถูกแก้ไข ปรับเปลี่ยน หรือทำลาย
- Availability (ความพร้อมใช้งาน) : การทำให้ระบบและข้อมูลพร้อมใช้งาน สำหรับผู้มีสิทธิ์เสมอเมื่อต้องการ

แนวคิดและความสำคัญ

ในยุคดิจิทัล องค์กรและบุคคลพึ่งพาระบบสารสนเทศในการจัดเก็บข้อมูลสำคัญและทำธุรกรรม หากเกิดการโจมตีทางไซเบอร์ อาจส่งผลกระทบต่อขั้นรุนแรง ได้แก่

- ความเสียหายทางการเงินและทรัพย์สิน
- การสูญเสียความน่าเชื่อถือและภาพลักษณ์ขององค์กร
- ความสูญเสียด้านข้อมูลส่วนบุคคลและข้อมูลความลับทางธุรกิจ

รูปแบบของภัยคุกคามทางดิจิทัล

ภัยคุกคามในปัจจุบันมีหลากหลายรูปแบบที่พบได้บ่อย ได้แก่

- Malware (มัลแวร์) : ซอฟต์แวร์ประสงค์ร้าย เช่น Virus, Trojan (ซ่อนตัวในไฟล์ที่ดูปลอดภัย) Spyware (แอบขโมยข้อมูล) และ Ransomware (เรียกค่าไถ่)
- Phishing : การส่งข้อความหรืออีเมลหลอกลวงเพื่อหลอกเอาข้อมูลสำคัญ
- Spoofing : การปลอมแปลงแหล่งที่มาของข้อมูล เช่น IP Spoofing หรือ Email Spoofing
- Man-in-the-Middle (MitM) : การดักจับและแอบเปลี่ยนแปลงแก้ไขข้อมูลระหว่างผู้ใช้งานกับระบบ
- Denial of Service (DoS/DDoS) : การส่งข้อมูลปริมาณมหาศาลเพื่อทำให้ระบบช้าลงหรือล่มจนใช้งานไม่ได้

ความเสี่ยงในการใช้เทคโนโลยีดิจิทัลในยุคปัจจุบัน

- การพึ่งพาอุปกรณ์พกพา (Smartphones, Laptops) และระบบ Cloud ในการทำงาน
- การเชื่อมต่อผ่านเครือข่ายสาธารณะที่ไม่ปลอดภัย
- พฤติกรรมความเสี่ยงของผู้ใช้ เช่น การ ตั้งรหัสผ่านที่เดาง่าย การหลงเชื่อข้อความหลอกลวง และการขาดความตระหนักรู้ (Digital Awareness)

เครื่องมือและซอฟต์แวร์ที่ช่วยในการรักษาความปลอดภัยทางไซเบอร์

- Antivirus/Anti-Malware : โปรแกรมตรวจจับและกำจัดซอฟต์แวร์ประสงค์ร้าย
- Firewall : ปรการคัดกรองและควบคุมของข้อมูลเข้า-ออกจากเครือข่าย
- SSL/TLS : โพรโตคอลการเข้ารหัสข้อมูล (Encryption) ระหว่างรับส่งข้อมูลผ่านอินเทอร์เน็ต
- VPN (Virtual Private Network) : การสร้างช่องทางการสื่อสารส่วนตัวที่ปลอดภัย
- SIEM (Security Information and Event Management) : เครื่องมือรวบรวมและวิเคราะห์ข้อมูล Log เพื่อตรวจจับสิ่งผิดปกติในระบบ

บทบาทขององค์กรในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

- การกำหนดนโยบายความมั่นคงปลอดภัย (Security Policy) ที่ชัดเจน
- การควบคุมสิทธิ์การเข้าถึงข้อมูลตามหลัก Least Privilege (ให้สิทธิ์เท่าที่จำเป็น)
- การประเมินความเสี่ยงและจัดทำแผนรับมือเหตุการณ์ภัยคุกคาม (Incident Response Plan)
- การจัดฝึกอบรมสร้างความตระหนักรู้ด้านไซเบอร์ (Cyber Security Awareness Training) ให้แก่บุคลากร

ความมั่นคงปลอดภัยทางไซเบอร์กับการทำงาน

- Work from Anywhere : การกำหนดแนวทางรักษาความปลอดภัยสำหรับการทำงานนอกสถานที่
- BYOD (Bring Your Own Device) : มาตรการกำกับดูแลการนำอุปกรณ์ส่วนตัวมาใช้ในการทำงาน
- การแยกแยะบัญชีผู้ใช้งานส่วนตัวและบัญชีผู้ใช้งานสำหรับการทำงานออกจากกัน

วิธีการป้องกันภัยคุกคามทางดิจิทัล

- Strong Passwords : การตั้งรหัสผ่านที่ซับซ้อน คาดเดายาก และไม่ใช้รหัสผ่านซ้ำกัน
- Multi-Factor Authentication (MFA) : การใช้การยืนยันตัวตนหลายขั้นตอนเพื่อเพิ่มความปลอดภัย
- Data Encryption : การเข้ารหัสข้อมูลทั้งในระหว่างการจัดเก็บและระหว่างการรับส่งข้อมูล
- Software Updates : การอัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ เพื่อปิดช่องโหว่

กฎหมายด้านดิจิทัล (Digital Laws)

กฎหมายสำคัญที่เกี่ยวกับการใช้งานเทคโนโลยีและข้อมูล ได้แก่

- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กำหนดโทษสำหรับการเข้าถึงระบบ/ข้อมูลโดยมิชอบ การเข้าถึงมาตรการป้องกัน หรือการนำเข้าข้อมูลเท็จ
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) กำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดมาตรการป้องกันและรับมือภัยคุกคามทางไซเบอร์ในระดับโครงสร้างพื้นฐานสำคัญของประเทศ

กรณีศึกษา

- การโจมตีด้วย Ransomware ในองค์กรใหญ่ การหยุดชะงักของระบบบริการและกระบวนการกู้คืนข้อมูล
- กรณี Phishing และ Social Engineering การหลอกลวงพนักงานเพื่อเอา credentials เข้าถึงระบบภายใน
- บทเรียนที่ได้รับ ความสำคัญของการสำรองข้อมูล (Backup) แบบออฟไลน์และการฝึกอบรมบุคลากรอย่างสม่ำเสมอ

ผู้สรุปบทเรียน

นางสาวฐิตาภา จอมเลิศ

นักวิชาการเกษตรปฏิบัติการ



สำนักงานคณะกรรมการข้าราชการพลเรือน
ขอมอบประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

นางสาวฐิตาภา จอมเลิศ

ได้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์

วิชา ปัญญาประดิษฐ์กับการทำงาน (Working with AI)

[รวมระยะเวลาทั้งสิ้น 2 ชั่วโมง]

ให้ไว้ ณ วันที่ 12 มิถุนายน พ.ศ. 2569

[นายปิยวัฒน์ ศิวรักษ์]
เลขาธิการคณะกรรมการข้าราชการพลเรือน





สำนักงานคณะกรรมการข้าราชการพลเรือน
ขอมอบประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

นางสาวฐิตาภา จอมเลิศ

ได้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์

วิชา ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล
[Cyber Security and Digital Awareness]

[รวมระยะเวลาทั้งสิ้น 3 ชั่วโมง]

ให้ไว้ ณ วันที่ 16 สิงหาคม พ.ศ. 2569

[นายปิยวัฒน์ ศิวรักษ์]
เลขาธิการคณะกรรมการข้าราชการพลเรือน

