แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๓

รอบการประเมินที่ ๑ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นางสาวจุฑาทัศย์ รัตนพงศ์ ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

กลุ่ม/ฝ่าย/สพด สถานีพัฒนาที่ดินชัยภูมิ

หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

สถานที่ สถานีพัฒนาที่ดินชัยภูมิ

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

Cybersecurity คือการนำเครื่องมือด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกัน และรับมือการโจมตีอุปกรณ์ เครือข่าย และระบบจากบุคคลที่สามที่ไม่ได้รับอนุญาต ซึ่งปัจจุบันมีความสำคัญมากเนื่องจากรูปแบบการโจมตีมีความหลากหลายและสร้างความเสียหายต่อองค์กรมากขึ้น

กฎหมาย และมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

กฎหมายที่เกี่ยวข้อง

- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562: เป็นกฎหมายหลักที่กำหนดกลไกในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560: กฎหมายที่กำหนดความผิดและบทลงโทษเกี่ยวกับการใช้งานคอมพิวเตอร์ในทางที่ผิด
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA): กฎหมายที่ดูแลเรื่องสิทธิและการคุ้มครองข้อมูลส่วนบุคคลเพื่อไม่ให้ถูกนำไปใช้โดยไม่ได้รับอนุญาต

มาตรฐานความปลอดภัย

- ISO 27001: เป็นมาตรฐานสากลสำหรับระบบบริหารจัดการความปลอดภัยของข้อมูล (Information Security Management System: ISMS) เพื่อช่วยให้องค์กรจัดการความปลอดภัยของสินทรัพย์ข้อมูลได้อย่างเป็นระบบ
- OWASP Top Ten: มาตรฐานหรือแนวทางที่ใช้ศึกษาเพื่อป้องกันภัยคุกคามสำหรับเว็บไซต์และเว็บแอปพลิเคชัน

ความรู้พื้นฐานของ Cybersecurity

หลักการ CIA Triad (หัวใจสำคัญของความปลอดภัย)

เป็นหลักปฏิบัติพื้นฐาน 3 ประการ เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล :

Confidentiality (การรักษาความลับ) : การกำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ เช่น ข้อมูลเงินเดือนควรเข้าถึงได้เฉพาะผู้จัดการฝ่ายบุคคลเท่านั้น

Integrity (การรักษาความถูกต้อง) : การรักษาสิทธิในการแก้ไขข้อมูลเพื่อให้ข้อมูลมีความถูกต้องแม่นยำอย่างต่อเนื่อง เช่น ข้อมูลบัญชีธนาคารต้องถูกต้องและไม่ถูกแก้ไขโดยมิชอบ

Availability (ความพร้อมใช้งาน) : การทำให้ข้อมูลพร้อมให้เข้าถึงและใช้งานได้ตลอดเวลาเมื่อต้องการ

รูปแบบภัยคุกคาม

Malware

Malware คือ ซอฟต์แวร์หรือชุดคำสั่ง (Code) ที่ถูกสร้างขึ้นมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ เมื่อถูกติดตั้งหรือเปิดใช้งานในระบบ จะทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงทรัพยากรของเครื่อง และอาจแชร์ข้อมูลไปยังเครื่องอื่นๆ ในเครือข่ายหรือเซิร์ฟเวอร์ได้

ประเภทของ Malware ที่สำคัญ

ชื่อเรียก Malware นั้นครอบคลุมถึงซอฟต์แวร์อันตรายหลายประเภท เช่น:

- ไวรัส (Virus): โปรแกรมที่แพร่กระจายตัวเองและสร้างความเสียหายต่อไฟล์หรือระบบ
- เวิร์ม (Worms): โปรแกรมที่สามารถแพร่กระจายตัวเองผ่านระบบเครือข่ายได้โดยอัตโนมัติ
- โทรจัน (Trojans): โปรแกรมที่หลอกลวงว่าปลอดภัยเพื่อจูงใจให้ผู้ใช้ติดตั้ง แต่แฝงจุดประสงค์ร้ายไว้ภายใน
- Ransomware (มัลแวร์เรียกค่าไถ่): ทำการล็อกไฟล์โดยการเข้ารหัสข้อมูลทั้งหมดในเครื่อง ทำให้ไม่สามารถเปิดใช้งานไฟล์ได้ เพื่อใช้ในการเรียกค่าไถ่แลกกับรหัสปลดล็อก
- Botnets: โปรแกรมแฝงตัวเพื่อรอรับคำสั่งจากผู้ไม่ประสงค์ดีในการโจมตีเป้าหมายอื่นๆ ต่อไป

แนวทางการป้องกัน Malware

เอกสารได้แนะนำข้อปฏิบัติเพื่อความปลอดภัยไว้ดังนี้:

- ติดตั้งและอัปเดต: ควรติดตั้งโปรแกรม Anti-Malware และหมั่นอัปเดตอย่างสม่ำเสมอ
- อัปเดตระบบ: อัปเดต Patch ของระบบปฏิบัติการ (OS) และเวอร์ชันของโปรแกรมต่างๆ ให้เป็นปัจจุบันอยู่เสมอ
- มีความตระหนักก่อนเปิดไฟล์: ไม่ควรเปิดอีเมลหรือไฟล์แนบจากผู้ส่งที่ไม่ชัดเจนหรือไม่น่าสงสัย และตรวจสอบลิงก์ก่อนคลิกทุกครั้ง
- สำรองข้อมูล: ควรสำรองข้อมูลเป็นประจำและแยกเก็บไฟล์สำรองไว้อย่างปลอดภัย (โดยเฉพาะเพื่อป้องกัน Ransomware)
- การใช้งานเว็บและอุปกรณ์: หลีกเลี่ยงเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจน และตรวจสอบสิทธิ์การเข้าถึง (Permission) ของแอปพลิเคชันบนมือถือให้เหมาะสม

Phishing

Phishing คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่างๆ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social Media โดยผู้โจมตีจะใช้วิธี หลอกล่อให้เหยื่อหลงเชื่อ เพื่อขโมยข้อมูลส่วนตัวที่สำคัญ เช่น:

- ชื่อผู้ใช้งาน (Username)

- รหัสผ่าน (Password)
- ข้อมูลสำคัญอื่นๆ เพื่อนำไปใช้ทำธุรกรรมในชื่อของเหยื่อ

ข้อควรปฏิบัติเพื่อป้องกัน Phishing (เน้นที่ E-mail)

เนื่องจาก E-mail เป็นช่องทางยอดนิยมในการทำ Phishing เอกสารจึงแนะนำข้อปฏิบัติไว้ดังนี้:

- ไม่เปิดอีเมล: หลีกเลี่ยงการเปิดอีเมลที่น่าสงสัย หรือมาจากผู้ส่งที่ไม่ชัดเจน
- ไม่เปิดไฟล์แนบ: ห้ามเปิดไฟล์ที่แนบมากับอีเมลที่น่าสงสัย
- ไม่คลิกลิงก์: ห้ามคลิกลิงก์ในอีเมลโดยไม่มีการตรวจสอบก่อน
- ตรวจสอบซ้ำ: หากเป็นเรื่องสำคัญหรือเกี่ยวกับการทำธุรกรรม ควรตรวจสอบผ่านช่องทางอื่นเพิ่มเติมก่อนดำเนินการ

วิธีการสังเกตและจัดการเบื้องต้น

- ตัวอย่างกลโกง: มักจะมีการส่งข้อความหลอกล่อ เช่น แจ้งว่าการจัดส่งพัสดุมีปัญหา หรือแจ้งว่ามีข้อความที่ยังไม่ได้ตรวจสอบ เพื่อให้เราคลิกลิงก์ไปยังเว็บไซต์ปลอมที่ดูคล้ายของจริง (เช่น เว็บธนาคารปลอม)
- การรายงาน: สำหรับผู้ใช้ Gmail สามารถใช้ฟีเจอร์ "Report Phishing" เพื่อแจ้งเตือนระบบเกี่ยวกับอีเมลอันตรายได้
- ความตระหนักรู้: ก่อนจะเปิดลิงก์หรือไฟล์ใดๆ ที่ได้รับมา ควรมีความตระหนักและระมัดระวังอยู่เสมอ

Ransomware

- Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการ "ล็อคไฟล์" ข้อมูลทั้งหมด
- วิธีการทำงานคือการ "เข้ารหัสไฟล์" (Encryption) ทำให้เจ้าของเครื่องไม่สามารถเปิดใช้งานไฟล์ข้อมูลนั้นได้
- จุดประสงค์หลักคือการ "เรียกค่าไถ่" เพื่อแลกกับรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ให้กลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน Ransomware

เอกสารแนะนำแนวทางปฏิบัติเพื่อป้องกันความเสียหายจากมัลแวร์เรียกค่าไถ่ไว้ 3 ข้อหลัก:

- สำรองข้อมูลเป็นประจำ: ควรทำการสำรองข้อมูลอย่างสม่ำเสมอและต้องแยกเก็บไฟล์สำรองข้อมูลไว้ต่างหาก (Off-site storage)
- ติดตั้ง Anti-Malware: ติดตั้งโปรแกรมป้องกันมัลแวร์และหมั่นอัปเดตซอฟต์แวร์ให้เป็นปัจจุบันเสมอ
- สร้างความตระหนักรู้: ก่อนจะเปิดไฟล์ต่างๆ ที่ได้รับมา ควรใช้ความระมัดระวังและตรวจสอบให้ดีก่อนทำการเปิด

ผลกระทบที่เกิดขึ้น

- นอกจากการถูกเรียกค่าไถ่แล้ว Ransomware ยังเป็นส่วนหนึ่งของปัญหา Data Breach หรือการรั่วไหลของข้อมูล

- อาจทำให้ข้อมูลสำคัญของบุคคลหรือองค์กรถูกนำไปเผยแพร่สู่สาธารณะ
- ส่งผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กรอย่างรุนแรง

Data Breach

Data Breach คือ เหตุการณ์ที่มีการรั่วไหลของข้อมูล ซึ่งอาจมีสาเหตุมาจาก 2 ส่วนหลักคือ:

- ช่องโหว่ของระบบ: การที่ระบบมีจุดอ่อนที่ทำให้ข้อมูลไหลออกไปได้
- การโจมตีเพื่อขโมยข้อมูล: การจงใจโจมตีเว็บไซต์ แอปพลิเคชัน หรือระบบให้บริการต่างๆ เพื่อเอาข้อมูลไป โดยส่วนใหญ่เจ้าของข้อมูลหรือผู้ให้บริการมักจะไม่ทราบว่ามีการรั่วไหลเกิดขึ้น

วัตถุประสงค์ของผู้โจมตี

ผู้ที่ทำการโจมตีเพื่อทำ Data Breach มักมีวัตถุประสงค์เพื่อ:

- นำชุดข้อมูลที่ขโมยได้ไป ขาย ในตลาดมืดหรือบุคคลอื่น
- นำข้อมูลมาใช้เพื่อ เรียกค่าไถ่ จากเจ้าของข้อมูล

ผลกระทบที่เกิดขึ้น

เมื่อเกิดการรั่วไหลของข้อมูล จะส่งผลเสียในหลายด้าน ดังนี้:

- ข้อมูลสำคัญถูกเผยแพร่: ข้อมูลส่วนตัวหรือข้อมูลลับขององค์กรถูกนำไปเปิดเผยสู่สาธารณะ
- ความสูญเสียทางการเงิน: ในกรณีที่ถูกเรียกค่าไถ่ข้อมูล
- ความน่าเชื่อถือ: สร้างความเสียหายต่อชื่อเสียงและความเชื่อมั่นที่ผู้อื่นมีต่อองค์กรอย่างรุนแรง

กฎหมายที่เกี่ยวข้อง

การดูแลเรื่อง Data Breach และการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย มีกฎหมายสำคัญที่เกี่ยวข้องคือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

DDoS

- DDoS คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย
- ลักษณะการโจมตี: เป็นการใช้เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นต้นทางในการโจมตีจำนวนมาก ยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน

จุดประสงค์ของการโจมตี

- เพื่อทำให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายของเป้าหมาย ไม่สามารถใช้งานได้ หรือระบบล่ม ในที่สุด
- ความเกี่ยวข้องกันกับภัยคุกคามอื่น
- ในเอกสารระบุว่า DDoS เป็น 1 ใน 15 ภัยคุกคามที่สำคัญ (Top Threats) ประจำปี 2020 ตามรายงานของ ENISA (องค์กรของยุโรปที่ดูแลเรื่องภัยคุกคามไซเบอร์)
- มีความเชื่อมโยงกับ Botnets (Robot Network) ซึ่งเป็นโปรแกรมที่ถูกเขียนขึ้นเพื่อแฝงตัวในอุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายตามที่ผู้ไม่ประสงค์ดีกำหนด

แนวทางการป้องกันภัยคุกคามเบื้องต้น

แม้เอกสารจะไม่ได้ระบุวิธีป้องกัน DDoS โดยเฉพาะเจาะจง แต่ได้แนะนำแนวปฏิบัติเพื่อความปลอดภัยของระบบที่เกี่ยวข้องไว้ดังนี้:

- การดูแลรักษาเครื่องคอมพิวเตอร์: ติดตั้ง Anti-Malware, อัปเดต Patch ระบบปฏิบัติการ (OS) และอัปเดตเวอร์ชันของโปรแกรมต่างๆ สม่ำเสมอ เพื่อป้องกันไม่ให้เครื่องกลายเป็นส่วนหนึ่งของ Botnets ที่ถูกนำไปใช้โจมตีผู้อื่น
- ความปลอดภัยของ IoT: เปลี่ยนรหัสผ่านเริ่มต้น (Default Password) และอัปเดตเฟิร์มแวร์เป็นเวอร์ชันล่าสุดเสมอ เพราะอุปกรณ์ IoT มักถูกแฮ็กเพื่อใช้เป็นฐานในการโจมตี DDoS

Inside Threat

- เป็นภัยคุกคามที่เกิดจากบุคลากร "ภายในองค์กร" เอง
- อาจเกิดได้จากทั้ง "ความตั้งใจ" หรือ "ความไม่ตั้งใจ" ของบุคลากรก็ได้
- มักเกิดขึ้นผ่านช่องทางการใช้งานตามปกติ เช่น การใช้เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน

ความรุนแรงของ Inside Threat

- Inside Threat จัดเป็นภัยที่มีความรุนแรงสูง เนื่องจากภายในองค์กรมักมีการป้องกันในระดับที่ต่ำกว่าการป้องกันจากภายนอก
- ผู้ไม่ประสงค์ดีหรือบุคลากรที่ประมาทสามารถเข้าถึงข้อมูลได้ง่ายกว่าคนนอก ทำให้ผลลัพธ์ของความเสียหายมีความรุนแรงมาก

วิธีการป้องกัน

เอกสารแนะนำให้นำหลักการ **Zero Trust** มาใช้ภายในองค์กร ซึ่งมีแนวคิดหลักคือ:

- ตรวจสอบทุกครั้ง: ต้องมีการตรวจสอบผู้เข้าระบบทุกครั้งที่มีการใช้งาน
- ให้สิทธิ์เท่าที่จำเป็น (Least Privilege): ให้สิทธิ์การใช้งานแก่ผู้ใช้ให้น้อยที่สุดหรือเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น

ตัวอย่างที่เกี่ยวข้องกับความปลอดภัยภายใน (CIA Triad)

เพื่อให้เข้าใจการป้องกันภัยภายในได้ชัดเจนขึ้น เอกสารได้ยกตัวอย่างการจำกัดสิทธิ์ (Confidentiality) ไว้ เช่น:

- ข้อมูลเงินเดือน: ควรให้เฉพาะผู้จัดการฝ่ายทรัพยากรบุคคลเข้าถึงได้เท่านั้น
- เบอร์โทรศัพท์พนักงาน: จัดเป็นข้อมูลภายในที่พนักงานทุกคนสามารถเข้าถึงได้

Cryptojacking

Cryptojacking คือ ภัยคุกคามทางไซเบอร์รูปแบบหนึ่งที่ผู้ไม่ประสงค์ดีจะ "แอบติดตั้งมัลแวร์" ลงในเครื่องคอมพิวเตอร์หรืออุปกรณ์ของเหยื่อ เพื่อแอบใช้ทรัพยากรของเครื่องนั้นๆ เช่น หน่วยประมวลผล (CPU) หรือการ์ดจอ (GPU) ในการประมวลผลเหรียญดิจิทัล (Cryptocurrency) หรือที่เรียกกันว่า "การขุดเหรียญ" โดยที่เจ้าของเครื่องไม่รู้ตัว

วิธีการและผลกระทบ

- การแพร่กระจาย: มักแฝงมากับไฟล์ดาวน์โหลด, โฆษณาบนเว็บไซต์ที่ฝัง Code อันตรายไว้ หรือการคลิกลิงก์ที่หลอกลวง
- อาการของเครื่องที่ติด Cryptojacking:
    - เครื่องคอมพิวเตอร์ทำงานช้าลงอย่างเห็นได้ชัด (เนื่องจาก CPU ถูกใช้งานหนักตลอดเวลา)
    - เครื่องเกิดความร้อนสูงเกินปกติ
    - พัดลมระบายอากาศทำงานดังและเร็วขึ้น
    - ค่าไฟฟ้าเพิ่มสูงขึ้นจากการที่เครื่องทำงานหนัก 24 ชั่วโมง

แนวทางการป้องกัน

เพื่อให้ปลอดภัยจากการถูกแอบใช้เครื่องไปขุดเหรียญ เอกสารแนะนำข้อปฏิบัติดังนี้:

- อัปเดตซอฟต์แวร์: หมั่นอัปเดต Patch ของระบบปฏิบัติการและโปรแกรมป้องกันมัลแวร์ (Anti-Malware) ให้เป็นเวอร์ชันล่าสุดเสมอ
- ระวังแหล่งดาวน์โหลด: หลีกเลี่ยงการดาวน์โหลดโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือโปรแกรมละเมิดลิขสิทธิ์
- การใช้งานอินเทอร์เน็ต: ระมัดระวังการเข้าเว็บไซต์ที่น่าสงสัยและไม่คลิกลิงก์แปลกๆ ที่ได้รับจากช่องทางต่างๆ

ความตระหนักรู้ด้าน Cybersecurity แนวทางการป้องกันและข้อควรปฏิบัติ

- **การจัดการรหัสผ่าน (Password):**
    - ควรมีความยาวอย่างน้อย 8 ตัวอักษร และมีความซับซ้อน (ตัวเล็ก, ตัวใหญ่, ตัวเลข, อักขระพิเศษ)
    - เปลี่ยนรหัสผ่านสม่ำเสมอ และใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication)
    - หลีกเลี่ยงรหัสที่คาดเดาง่าย เช่น "123456" หรือวันเกิด
- **ความปลอดภัยในการทำงาน:**
    - E-mail: ไม่เปิดอีเมลหรือไฟล์แนบจากผู้ส่งที่น่าสงสัย และไม่คลิกลิงก์โดยไม่ตรวจสอบ
    - คอมพิวเตอร์: แยก User การใช้งาน, Logout เมื่อไม่อยู่หน้าจอ, และอัปเดตระบบปฏิบัติการ (Patch) สม่ำเสมอ
    - อินเทอร์เน็ตและ WiFi: หลีกเลี่ยง WiFi สาธารณะที่ไม่มีรหัสผ่าน และเปลี่ยนรหัสผ่านเริ่มต้น (Default Password) ของ Router
    - IoT Devices: เปลี่ยนรหัสผ่านเริ่มต้นและอัปเดตเฟิร์มแวร์เป็นเวอร์ชันล่าสุดเสมอ

Fake News (ข่าวปลอม)

เป็นภัยคุกคามใกล้ตัวที่มีความน่ากลัวอย่างมาก ข่าวปลอมมักถูกสร้างให้ดูมีความน่าเชื่อถือ เพื่อให้ผู้รับสารหลงเชื่อ สามารถสร้างกระแสและปลุกปั่นได้อย่างมีประสิทธิภาพ มีการกระจายข่าวได้อย่างรวดเร็วผ่านช่องทางออนไลน์ เช่น LINE และ Facebook

วิธีการสังเกตข่าวปลอม

- พาดหัวข่าวเกินจริง: มีการใช้ข้อความที่เกินกว่าความเป็นจริงเพื่อดึงดูดความสนใจ
- ระบุที่มาไม่ได้: ไม่สามารถตรวจสอบแหล่งที่มาของข่าวได้ชัดเจน
- ไม่ระบุเวลา: มักจะไม่ระบุวันที่และเวลาที่เกิดเหตุการณ์อย่างชัดเจน
- สำนวนการเขียน: มีลักษณะการเขียนคล้ายกับการโฆษณาชวนเชื่อ

ข้อควรปฏิบัติเพิ่มเติม

- ตรวจสอบที่มา: ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ หากยังไม่ทราบที่มาของข้อมูลที่ชัดเจน
- แหล่งตรวจสอบ: สามารถตรวจสอบข้อมูลได้ที่ ศูนย์ต่อต้านข่าวปลอม ประเทศไทย (Anti-Fake News Center Thailand) ผ่านทางเว็บไซต์ www.antifakenewscenter.com

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ ไม่ได้หมายถึงการปฏิเสธเทคโนโลยี แต่คือการสร้างสมดุลระหว่าง ความปลอดภัย (Security) และ ความสะดวกสบาย (Convenience) หากทุกคนมีความตระหนักรู้และปฏิบัติตามแนวทางที่ถูกต้อง โลกไซเบอร์ก็จะกลายเป็นพื้นที่ที่ปลอดภัยสำหรับทุกคน

ลงนาม.....

(นางสาวจุฑาทัศย์ รัตนพงศ์)
นักวิชาการเกษตรปฏิบัติการ

ลงนาม.....

(นายไลซันต์ ตั้งภูมิ)
ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินชัยภูมิ
รับรองผลการพัฒนาความรู้

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ จุฑาทัศย์ รัตนพงศ์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 22 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (dpa.)
Date: 2026-02-22T16:40:21.823+07:00
b87f031e