

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

ส่วนที่ 1 ข้อมูลทั่วไป

ชื่อ นางสาววารุณี นามสกุล อดิศักดิ์กุล ✓

ตำแหน่ง นักสำรวจดินปฏิบัติการ กลุ่ม นโยบายและวางแผนการใช้ที่ดิน

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา

Basic Cybersecurity Series: หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น
สถานที่อบรม/สัมมนา/พัฒนาความรู้

อบรมออนไลน์ผ่าน URL: <https://e-learning.dga.or.th/>

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

ตั้งแต่วันที่ 28 เดือน มิถุนายน พ.ศ. 2569 ถึงวันที่ 28 เดือน มิถุนายน พ.ศ. 2569

เพื่อ ☒ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ

.....

ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

ความมั่นคงปลอดภัยทางไซเบอร์ มีเป้าหมายในการป้องกันระบบ ข้อมูล และการบริการให้รอดพ้นจากภัยคุกคาม ความผิดพลาด หรือการสูญเสีย โดยใช้หลักการ CIA Triad Model ได้แก่ การรักษาความลับ (Confidentiality) เพื่อให้เฉพาะผู้ที่มีสิทธิ์เท่านั้นที่เข้าถึงข้อมูลได้ ความถูกต้องครบถ้วน (Integrity) เพื่อป้องกันไม่ให้ข้อมูลถูกแก้ไขหรือทำลายโดยมิชอบ และความพร้อมใช้งาน (Availability) เพื่อให้ระบบและข้อมูลพร้อมใช้งานตลอดเวลา ซึ่งหลักการนี้จะเกิดผลได้จริงต้องผ่านการขับเคลื่อนร่วมกันของ 3 ปัจจัย ได้แก่ คน (People) โดยการสร้างทักษะและความตระหนักรู้ กระบวนการ (Process) ในการดำเนินงานที่ชัดเจน และเทคโนโลยี (Technology) หรือเครื่องมือต่าง ๆ ซึ่งความปลอดภัยทางไซเบอร์ครอบคลุมในรูปแบบต่าง ๆ เช่น การใช้งานแอปพลิเคชัน ข้อมูลสารสนเทศ เครือข่าย การปฏิบัติงาน การเข้ารหัส การควบคุมการเข้าถึง การสร้างความตระหนัก และกำหนดระยะเวลาการกู้คืนระบบ

ในปัจจุบันเป็นยุคที่เทคโนโลยีและอินเทอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น ฉะนั้นความปลอดภัยทางไซเบอร์จึงเป็นเรื่องสำคัญ โดยเรื่องที่ควรทราบเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น มีดังนี้

1. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) คือ กระบวนการระบุ วิเคราะห์ และรับมือกับความเสี่ยงของระบบสารสนเทศ เพื่อปกป้องข้อมูลและช่วยให้องค์กรดำเนินงานได้อย่างปลอดภัยและต่อเนื่อง

1.1 ความเสี่ยง (Risk) คือ เหตุการณ์ที่ไม่แน่นอน ซึ่งส่งผลกระทบต่อการบรรลุเป้าหมายขององค์กร โดยมีองค์ประกอบสำคัญ คือ โอกาสเกิด ความเสียหายที่อาจเกิดขึ้น และความไม่แน่นอน การประเมินต้องพิจารณาทั้งปัจจัยภายนอก เช่น สังคม เศรษฐกิจ กฎหมาย ภัยธรรมชาติ และเทคโนโลยี และปัจจัยภายใน เช่น เงินทุน อุปกรณ์ และบุคลากร ทั้งนี้ ความเสี่ยงไม่มีทางเป็นศูนย์ ทำได้เพียงควบคุมให้อยู่ในระดับที่ยอมรับได้ นอกจากนี้ ความเสี่ยงต่างจากปัญหาตรงที่เป็นเรื่องของอนาคตที่มีข้อมูลอ้างอิง และต่างจากความไม่แน่นอนตรงที่ต้องอาศัยข้อมูลเชิงประจักษ์หรือสถิติมาประเมิน

1.2 กระบวนการบริหารความเสี่ยง มี 7 ขั้นตอน ได้แก่ 1) การกำหนดวัตถุประสงค์และขอบเขต 2) การระบุความเสี่ยง 3) การประเมินความเสี่ยงจาก โอกาสเกิด x ผลกระทบ 4) การประเมินมาตรการควบคุมที่มีอยู่ 5) การจัดทำแผนจัดการความเสี่ยง (RTP) 6) การรายงานผลต่อผู้บริหาร และ 7) การติดตาม ทบทวนอย่างน้อยปีละ 1 ครั้ง โดยองค์กรสามารถเลือกตอบสนองต่อความเสี่ยงได้ 4 รูปแบบ ได้แก่ 1) Accept ยอมรับเมื่อค่าป้องกันสูงกว่าความเสียหาย 2) Mitigate ลดหรือควบคุมตามมาตรฐาน เช่น ISO/NIST 3) Avoid หลีกเลี่ยง โดยปรับกระบวนการ และ 4) Transfer ถ่ายโอนความเสี่ยง เช่น ทำประกันภัยไซเบอร์

1.3 กรอบ COSO ERM และการประเมินความเสี่ยงด้านไซเบอร์ ในการบริหารความเสี่ยงระดับองค์กร ตามกรอบ COSO ERM จะครอบคลุม 5 ด้าน ได้แก่ 1) การกำกับดูแลและวัฒนธรรม 2) การกำหนดกลยุทธ์ 3) การประเมินและตอบสนอง 4) การทบทวนผล และ 5)การสารสนเทศและการสื่อสาร สำหรับการประเมิน ความเสี่ยงด้านไซเบอร์จะมุ่งเน้นการคุ้มครองตามหลัก CIA Triad ได้แก่ ความลับ (Confidentiality) ความ ถูกต้องแม่นยำ (Integrity) และความพร้อมใช้งาน (Availability) โดยเริ่มประเมินจากสินทรัพย์ (Asset) หรือกระบวนการทำงาน เชื่อมโยงกับภัยคุกคาม (Threat) และช่องโหว่ (Vulnerability) รวมถึงให้ผู้ดูแล สินทรัพย์ (Asset Owner) เป็นผู้ประเมินตนเอง และแยกบทบาทผู้ตรวจสอบออกจากผู้ประเมินเพื่อความโปร่งใส

2. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ (Cybersecurity Framework) ที่นำมาประยุกต์ใช้เพื่อรักษาความปลอดภัยทางไซเบอร์ของประเทศไทย ได้แก่ ISO (International Organization for Standardization) /IEC (The International Electrotechnical commission) ซึ่งเน้นการรักษา ความปลอดภัยของข้อมูลในระดับรัฐ และ NIST Security Framework (National Institute of Standards and Technology) ซึ่งเป็นกรอบการทำงานหลักที่นิยมใช้ในการรับมือภัยคุกคามทางไซเบอร์ โดยในหลักสูตรนี้ เน้น NIST Cybersecurity Framework เพื่อสอดคล้องกับ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ดังนี้

2.1 NIST cybersecurity framework ปัจจุบันเป็นเวอร์ชัน 2.0 ซึ่งประกอบด้วย 6 ฟังก์ชันหลัก (22 Categories, 106 Subcategories) ได้แก่ Govern (Governance) Identify Protect Detect Respond และ Recover เพื่อเน้นการกำกับดูแล การเข้าใจบริบทองค์กร การจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain) และ การกำหนดนโยบายให้สอดคล้องกับกลยุทธ์องค์กร

2.2 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยทางด้านไซเบอร์สำหรับ หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2562 อิงตาม 5 ฟังก์ชันหลัก ดังนี้

1) การระบุความเสี่ยง (Identify) จัดทำทะเบียนสินทรัพย์ ประเมินและจัดการความเสี่ยง (กำหนด KRI) ประเมินช่องโหว่ (Vulnerability Assessment) ของระบบสำคัญและระบบใหม่ ทำ Penetration Testing เท่าที่จำเป็น และควบคุมผู้ให้บริการภายนอก (Third Party Management) ตามหลัก CIA

2) การป้องกันความเสี่ยง (Protect) กำหนดการควบคุมการเข้าถึง (Access Control) ทำ System Hardening/Security Baseline ใช้การเชื่อมต่อระยะไกลที่ปลอดภัย (VPN/HTTPS) ควบคุมสื่อเก็บข้อมูล ถอดได้ สร้างความตระหนักรู้ (Cyber Awareness) และแบ่งปันข้อมูลอย่างปลอดภัยตามระดับความลับ

3) การตรวจสอบและเฝ้าระวัง (Detect) เฝ้าระวังภัยคุกคามไซเบอร์ของบริการสำคัญ จัดประเภท วิเคราะห์ และมีกระบวนการแจ้งเหตุเมื่อพบความผิดปกติ

4) การเผชิญเหตุ (Respond) จัดทำและฝึกซ้อมแผนรับมือภัยคุกคาม (Incident Response Plan) อย่างน้อยปีละ 1 ครั้ง มีแผนสื่อสารภาวะวิกฤต (Crisis Communication) และกำหนดผู้รับผิดชอบชัดเจน

5) การฟื้นฟูความเสียหาย (Recover) วางมาตรการฟื้นคืนระบบและข้อมูล ให้สอดคล้องกับแผน ต่อเนื่องทางธุรกิจ (BCP) แผนกู้คืนระบบ (IT DRP) และข้อตกลงระดับการบริการ (SLA) กับ Vendor

3. การป้องกันความเสี่ยง โดยการประเมินช่องโหว่ (Vulnerability Assessment: VA)

3.1 การประเมินช่องโหว่ คือ กระบวนการตรวจสอบและระบุช่องโหว่ในระบบหรือแอปพลิเคชัน โดยใช้ เครื่องมือสแกนอัตโนมัติและเทคนิคต่าง ๆ เพื่อค้นหาจุดอ่อนด้านความปลอดภัย และนำไปสู่วิธีแก้ไขที่ถูกต้อง

การประเมินช่องโหว่มีความสำคัญ ในการช่วยค้นหาและป้องกันภัยคุกคามล่วงหน้า เนื่องจากแฮกเกอร์ มีการปรับเปลี่ยนรูปแบบการโจมตีอยู่เสมอ การทำ VA อย่างสม่ำเสมอ อย่างน้อยปีละ 2 ครั้ง จะช่วยลด ความเสี่ยงจากการถูกโจมตีได้

3.2 Vulnerability Scanning Tool เพื่อตรวจสอบความปลอดภัยระบบเครือข่าย ค้นหาช่องโหว่ที่ใช้งาน ภายในองค์กร เช่น ระบบปฏิบัติการ (OS) software อุปกรณ์ network อุปกรณ์ security ซึ่งนับเป็นเรื่องสำคัญ ที่ใช้ระบุระดับความรุนแรงของช่องโหว่ที่เกิดขึ้นตามการอ้างอิงของ CVE และ CVSS

3.3 ประโยชน์ของการประเมินช่องโหว่ ได้แก่ 1) ประเมินความเสี่ยง วิเคราะห์ระดับความรุนแรงและ ผลกระทบที่อาจเกิดขึ้นหากไม่แก้ไขช่องโหว่ 2) สร้างรายงาน รวบรวมข้อมูลช่องโหว่พร้อมคำแนะนำ เพื่อให้ทีมความปลอดภัยตัดสินใจแก้ไขได้อย่างมีประสิทธิภาพ 3) ตรวจสอบมาตรฐาน ช่วยตรวจสอบว่า ระบบสอดคล้องกับมาตรฐานความปลอดภัย เช่น PCI DSS หรือ HIPAA หรือไม่ และ 4) ประหยัดต้นทุน ช่วยพบและแก้ปัญหาตั้งแต่ช่วงพัฒนาระบบ ประหยัดเวลาและค่าใช้จ่ายในอนาคต

3.4 รูปแบบของ VA scan ได้แก่ 1) Host Assessment ประเมินความเสี่ยงของ Server สำคัญ 2) Network and Wireless Assessment ประเมินความเสี่ยงของระบบเครือข่ายตาม Policy เพื่อป้องกันการ เข้าถึงโดยไม่ได้รับอนุญาต 3) Database Assessment ประเมินความเสี่ยงของระบบฐานข้อมูลและ Big Data และ 4) Application Scans สแกนหาช่องโหว่ใน Web Application และ Source Code แบบอัตโนมัติ

3.5 ขั้นตอนการทำการประเมินช่องโหว่

1) vulnerability identification (Testing) ทดสอบระบุช่องโหว่โดยใช้เครื่องมือสแกนอัตโนมัติ อ้างอิงฐานข้อมูลจาก Vendor

2) vulnerability analysis วิเคราะห์สาเหตุและต้นตอของช่องโหว่ เช่น การใช้ Open Source Library เวอร์ชันเก่า

3) risk assessment จัดลำดับความสำคัญของช่องโหว่เป็น Rank/Score ตามความรุนแรง ผลกระทบ และความยากง่ายในการโจมตี

4) remediation อุดช่องโหว่ โดยทีม Security และ Operation ร่วมมือกันปรับปรุงระบบ/ลง Patch ใหม่โดยไม่กระทบการทำงานปัจจุบัน

4. การตรวจสอบและเฝ้าระวังภัยคุกคามไซเบอร์ (Detect) คือ กระบวนการตรวจจับความผิดปกติของระบบ พฤติกรรมผู้ใช้งาน หรือการโจมตีที่อาจเกิดขึ้น เพื่อแจ้งเตือนและประสานงานไปยังผู้ที่เกี่ยวข้องให้ทำการ ตอบสนองและแก้ไขได้อย่างทันท่วงที การเฝ้าระวังต้องทำอย่างต่อเนื่องและมีประสิทธิภาพเพื่อตรวจจับ ความผิดปกติได้อย่างรวดเร็ว โดยมีวัตถุประสงค์หลักในการลดความเสียหายและจำกัดวงความเสียหายให้ แคบลง ช่วยลดโอกาสและระยะเวลาของผู้โจมตี ตลอดจนให้ข้อมูลที่เป็นประโยชน์ต่อการตอบสนองเหตุการณ์ และการกู้คืนระบบ

ตัวอย่างเหตุการณ์ผิดปกติที่ระบบสามารถตรวจจับได้ มีทั้งด้านพฤติกรรม การเข้าสู่ระบบ เช่น การพยายาม Login ล้มเหลวเป็นจำนวนมากจากต้นทางเดียว การ Login นอกเวลาทำงาน หรือการ Login มาจากต่างประเทศ ที่ไม่มีเจ้าหน้าที่ปฏิบัติงานจริง รวมถึงการใช้งานทรัพยากรผิดปกติ เช่น CPU พุ่งสูงถึง 100% ในช่วงเวลาสั้น ๆ หรือมีการรับส่งข้อมูลในเครือข่ายมากผิดปกติ นอกจากนี้ยังครอบคลุมถึงการตรวจพบการเรียกใช้งาน Program หรือ Library ที่น่าสงสัย การรันไฟล์มัลแวร์ (Malicious File) และการพยายามติดต่อไปยัง IP Address Domain หรือ URL ที่สุ่มเสี่ยง

ในการดำเนินงานมีเครื่องมือหรือระบบหลายประเภทที่ใช้ตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น ระบบตรวจจับการบุกรุก (IDS) ระบบป้องกันการบุกรุก (IPS) ระบบบริหารจัดการข้อมูลเหตุการณ์ ความปลอดภัย (SIEM) และระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ปลายทาง (EDR) นอกจากนี้ ยังสามารถนำระบบข้อมูลข่าวสารภัยคุกคาม (Threat Intelligence) มาเชื่อมต่อกับระบบ เพื่อยกระดับ ประสิทธิภาพและความแม่นยำในการตรวจจับให้ดียิ่งขึ้น

5. การเผชิญเหตุภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

5.1 การเผชิญเหตุภัยคุกคามทางไซเบอร์ (Respond) เป็นขั้นตอนการรับมือ เพื่อจำกัดวงความเสียหายให้อยู่ในระดับต่ำที่สุด หน่วยงานต้องจัดทำแผน กำหนดบทบาทหน้าที่ เสนอไทม์ไลน์ สื่อสารให้ผู้เกี่ยวข้องทราบ และซักซ้อมอย่างน้อยปีละ 1 ครั้ง โดยอ้างอิงตามมาตรฐาน NIST SP 800-61 ซึ่งมี 4 ขั้นตอนหลัก ดังนี้

1) การเตรียมการ จัดทำแผน ตั้งทีมตอบสนอง อบรมสร้างความตระหนักรู้แก่พนักงาน และเตรียมเครื่องมือตรวจจับ เช่น ระบบ IDS IPS Firewall และ EDR เป็นต้น

2) การระบุภัยคุกคาม ตรวจจับความผิดปกติที่เกิดขึ้น ผ่านการแจ้งเตือนของระบบ การพบเห็นของพนักงาน หรือสิ่งบอกเหตุอื่น ๆ

3) การควบคุม หยุดยั้งการโจมตีและจำกัดพื้นที่ความเสียหาย เช่น การตัดการเชื่อมต่อจากระบบเครือข่าย

4) การกำจัดภัยคุกคาม ขจัดภัยคุกคามที่พบ เช่น การลบไฟล์ Malware การบล็อก IP ที่เป็นอันตราย ทั้งนี้ หลังจากเสร็จสิ้นขั้นตอนต่าง ๆ แล้ว ต้องวิเคราะห์หาสาเหตุ บันทึกข้อเสนอนะ เพื่อปรับปรุงระบบ และควรจัดทำแผนการสื่อสารในภาวะวิกฤต โดยตั้งทีมโฆษกหรือผู้ให้ข่าวอย่างชัดเจน เพื่อกระจายข้อมูลที่ถูกต้องและรวดเร็ว

5.2 การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover) เป็นกระบวนการกู้คืนระบบให้กลับมาดำเนินงานได้ตามปกติอย่างต่อเนื่อง ประกอบด้วย

1) การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) จัดทำและทดสอบปรับปรุงแผนอย่างน้อยปีละ 1 ครั้ง เพื่อรองรับกรณีที่ระบบหยุดชะงัก

2) การสำรองข้อมูล ควรทำการสำรองข้อมูลอย่างสม่ำเสมอและหมั่นทดสอบการกู้คืนระบบ โดยใช้กลยุทธ์ 3-2-1 คือ สำเนาข้อมูลอย่างน้อย 3 ชุด เก็บข้อมูลไว้บนสื่อบันทึกข้อมูลที่ต่างชนิดกันอย่างน้อย 2 ประเภท เช่น Storage หลัก Tape External Drive และเก็บไว้ต่างสถานที่ (Offsite) อย่างน้อย 1 ชุด เช่น บน Cloud Storage

3) ปรับปรุงมาตรการรักษาความปลอดภัย นำบทเรียนจากเหตุการณ์มาแก้ไขจุดบกพร่อง การตั้งค่าอุปกรณ์ หรือมาตรการต่าง ๆ เพื่อป้องกันการเกิดเหตุซ้ำในอนาคต

2.2 ประสิทธิภาพ/ประโยชน์ที่ได้รับ/การประยุกต์ใช้กับหน่วยงาน

☒ ต่อตนเอง

ได้รับความรู้และเพิ่มความตระหนักรู้เกี่ยวกับความปลอดภัยทางไซเบอร์มากขึ้น ทั้งเรื่องความเสี่ยง การประเมินความเสี่ยง กรอบมาตรฐานความมั่นคงทางไซเบอร์ การประเมินช่องโหว่ รวมทั้งการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ เพื่อให้ทราบ ประเมิน และป้องกันภัยคุกคามทางไซเบอร์เบื้องต้นได้

☒ ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน

หน่วยงานมีข้อมูล Big Data รวมทั้งทรัพย์สินต่าง ๆ ที่สำคัญ ที่ต้องรักษาไว้ โดยเฉพาะข้อมูลดิจิทัล ซึ่งเป็นสินทรัพย์ที่มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ ฉะนั้นสิ่งที่องค์กรควรต้องทำ คือ การสำรวจสินทรัพย์ทางดิจิทัล จากนั้นประเมินความเสี่ยง ประเมินช่องโหว่ ควรมีการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ มีการกำหนดหน้าที่ให้ชัดเจน มีสื่อสารให้คนในองค์กรทราบอย่างชัดเจนเป็นแนวทางเดียวกัน เพื่อเป็นการป้องกันให้สินทรัพย์เหล่านี้ปลอดภัย ที่สำคัญควรมีการจัดทำแผนความปลอดภัยทางไซเบอร์ในทุก ๆ ปี

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

เนื้อหาที่มีรายละเอียดค่อนข้างเยอะ และเนื้อหาบางส่วนยากต่อการทำความเข้าใจ ทำให้เสียเวลาในการที่ต้องเรียน/ฟังซ้ำหลายรอบ

เนื่องจากการใช้อินเทอร์เน็ตเป็นสิ่งจำเป็นในยุคปัจจุบัน อย่างไรก็ตามการใช้งานดังกล่าวก็มาพร้อมกับความเสี่ยง/ภัยคุกคามในเรื่องของข้อมูลที่มีความสำคัญ เช่น ข้อมูลส่วนบุคคล ข้อมูลการเงิน และสินทรัพย์อื่น ๆ เสี่ยงต่อการโจมตีและการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม ฉะนั้นการตระหนักรู้และการเรียนรู้เกี่ยวกับความปลอดภัยทางด้านไซเบอร์จึงเป็นสิ่งจำเป็นอย่างมาก ทำให้สามารถนำมาป้องกัน ระวัง และรักษาสินทรัพย์ที่สำคัญให้มีความปลอดภัย

ลงชื่อ อนุช อติศักดิ์กุล
(นางสาววารุณี อติศักดิ์กุล)
ตำแหน่ง นักสำรวจดินปฏิบัติการ
ผู้รายงาน
วันที่ 19 เดือน สิงหาคม พ.ศ. 2569

(✓) ทราบ

ลงชื่อ.....
(นายบัณฑิต นองหารพิทักษ์)
ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน
ตำแหน่ง.....
วันที่ ๒๕ ตุลาคม ๒๕๖๕ พ.ศ.

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

วารุณี อติศักดิ์กุล

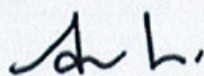
ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนากิจกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 28 มิถุนายน 2569



(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

สันทิชา ฤกษ์ดี

อภิสรา อติศักดิ์กุล



ประกาศนียบัตร

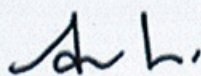
ให้ไว้เพื่อแสดงว่า

วารุณี อติศักดิ์กุล

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
การประยุกต์ใช้ความรู้ปัญญาประดิษฐ์
ในการพัฒนาหุ่นยนต์สนทนา (Chatbot) เพื่อการบริการภาครัฐ

จำนวนชั่วโมงการเรียนรู้ 1:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 29 พฤษภาคม 2569



(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (nsr)
Digital Government Development Agency (Public
Organization) (DGA)
Date: 2024-05-03T15:23:43.233+07:00

สำเนาถูกต้อง
วารุณี อติศักดิ์กุล