



บันทึกข้อความ

36

สพ.สว. ๕๗
กษ. ๐๘๐๔.๐๘/๗๘
๑๐.๐๘

ส่วนราชการ กลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๓ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร.๕๑๐๗

ที่ กษ ๐๘๐๔.๐๘/๗๘

วันที่ ๙ กันยายน ๒๕๖๙

เรื่อง รายงานผลการอบรมตามตัวชี้วัดความสำเร็จของการพัฒนาความรู้ของบุคลากรในหน่วยงาน

เรียน ผอ.สวพ. ผ่าน ผอ.กพฐ.๓

ตามแบบกำหนด และประเมินตัวชี้วัดด้านผลสัมฤทธิ์ ในรอบการประเมินที่ ๒ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ (๑ เมษายน ๒๕๖๙ – ๓๐ กันยายน ๒๕๖๙) ของสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ซึ่งให้ข้าราชการอบรมศึกษาการพัฒนาความรู้ของบุคลากรในหน่วยงาน ให้ครบถ้วนตามเงื่อนไขของหลักสูตร จำนวน ๒ เรื่อง นั้น

ข้าพเจ้า ได้พัฒนาความรู้ตามตัวชี้วัดความสำเร็จ ของการพัฒนาบุคลากรในหน่วยงานในรอบการประเมิน ครั้งที่ ๒/๒๕๖๙ โดยมีรายละเอียด ดังนี้

๑. พัฒนาความรู้ในเรื่อง หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity) ผ่านระบบออนไลน์ (TDGA E-learning) หลักสูตรด้านดิจิทัลของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA) (มีใบรับรองประกาศนียบัตร)

๒. พัฒนาความรู้ในเรื่อง หลักการสร้างภาพข้อมูลและการออกแบบแดชบอร์ดอย่างมีประสิทธิภาพ (The Principle of Data Visualization and Dashboard Design) (TDGA E-learning) หลักสูตรด้านดิจิทัลของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA) (มีใบรับรองประกาศนียบัตร)

ในการนี้ ข้าพเจ้าขอสรุปรายงานการพัฒนาความรู้ตามตัวชี้วัดความสำเร็จ ของการพัฒนาบุคลากรในหน่วยงาน โดยสรุปบทเรียนที่ได้รับการพัฒนา จำนวน ๑ เรื่อง พร้อมด้วยสำเนาประกาศนียบัตร ตามเอกสารแนบท้ายบันทึกนี้

จึงเรียนมาเพื่อโปรดทราบ

(นายอภิเชษ คำสุวรรณ)

นายช่างโยธาชำนาญงาน

- ทรง

- ผอ.สว. (คุณทศพร) รกบม

(นายจักรกฤษณ์ วิโอ)

ผู้อำนวยการสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน

สรุปผลการเรียนรู้

๑. หัวข้อการพัฒนาความรู้

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity)

๒. เนื้อหาโดยสังเขป

ในยุคดิจิทัลที่องค์กรต่างๆ พึ่งพาเทคโนโลยีสารสนเทศและการสื่อสารในการดำเนินธุรกิจ ความท้าทายด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) และการบริหารความเสี่ยง (Risk Management) จึงเป็นหัวใจสำคัญที่จะช่วยให้องค์กรสามารถดำเนินงานได้อย่างราบรื่น ปลอดภัย และมีความต่อเนื่อง

๑. ทำความเข้าใจความเสี่ยงและมาตรฐานสากล

ความเสี่ยง (Risk) ไม่ได้หมายถึงเพียงแค่ความเสียหายทางการเงินที่เกิดขึ้นจริง แต่ยังครอบคลุมถึง "ความไม่แน่นอนของเหตุการณ์" และ "การคลาดเคลื่อนของการคาดการณ์" ที่อาจส่งผลกระทบต่อวัตถุประสงค์ขององค์กร การรับมือกับความเสี่ยงเหล่านี้จำเป็นต้องอาศัยกรอบมาตรฐานสากลที่เป็นที่ยอมรับ เช่น ISO ๓๑๐๐๐ สำหรับการบริหารความเสี่ยงทั่วไป และ COSO/ERM สำหรับการบริหารความเสี่ยงระดับองค์กร รวมถึงกรอบมาตรฐานด้านความปลอดภัยไซเบอร์อย่าง NIST Cybersecurity Framework (CSF) ซึ่งประกอบด้วยขั้นตอนหลัก ได้แก่ การระบุความเสี่ยง (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการกู้คืนระบบ (Recover)

๒. การประเมินช่องโหว่และการเฝ้าระวังภัยคุกคาม

การป้องกันที่ดีต้องเริ่มต้นจากการรู้เท่าทันจุดอ่อนของตนเอง ผ่านกระบวนการเช่น Vulnerability Assessment (VA) ซึ่งจัดอยู่ในขั้นตอนการระบุ (Identify) เพื่อค้นหาช่องโหว่ของระบบและนำมาวิเคราะห์สาเหตุเชิงลึก (Vulnerability Analysis) นอกจากนี้ องค์กรยังต้องมีเครื่องมือตรวจสอบที่ทันสมัย เช่น ระบบ SIEM (Security Information and Event Management) ควบคู่ไปกับการจัดตั้งทีมเฝ้าระวังภัยคุกคาม เฉพาะกิจอย่าง CSOC (Cyber Security Operations Center) ที่คอยมอนิเตอร์ความผิดปกติตลอด ๒๔ ชั่วโมง

๓. การรับมือและแผนรองรับภาวะวิกฤต (Incident Response & BCP)

ความปลอดภัยไซเบอร์ไม่ใช่หน้าที่ของฝ่ายไอทีหรือแฮกเกอร์ฝ่ายเดียว แต่เป็น **ความรับผิดชอบของบุคลากรทุกคนในองค์กร** เมื่อเกิดเหตุการณ์ผิดปกติหรือการโจมตีทางไซเบอร์ (เช่น การแพร่ ๑ ของมัลแวร์เรียกค่าไถ่หรือ Ransomware) สิ่งที่ต้องปฏิบัติอย่างเร่งด่วนคือการแยกเครื่องที่ติดเชื้อออกจากระบบเครือข่ายทันที ห้ามเพิกเฉยหรือโพสต์ข้อความตื่นตระหนกบนสื่อสังคมออนไลน์เด็ดขาด

นอกจากนี้ องค์กรจำเป็นต้องมี **แผนรับมือภัยคุกคาม (Incident Response Plan)** และ **แผนความต่อเนื่องทางธุรกิจ (BCP)** ที่ระบุรายชื่อผู้ติดต่อ หน้าที่รับผิดชอบ และช่องทางการสื่อสารที่ชัดเจน พร้อมทั้งมีการทดสอบแผนอย่างสม่ำเสมอ เช่น การทำ Table Top Exercise ปีละ ๒ ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดวิกฤตขึ้นจริง ทีมงานจะสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

๔. ความสำคัญของการสำรองและการกู้คืนข้อมูล (Backup & Recovery)

การสำรองข้อมูลเป็นเกราะป้องกันสุดท้ายที่สำคัญ แต่ต้องดำเนินการอย่างถูกวิธี เช่น การเก็บข้อมูลไว้บนระบบ Cloud หรือ Backup Server ที่แยก Data Center ออกจากระบบจริงอย่างเด็ดขาด หลีกเลี่ยงการเก็บไว้ใน USB Drive หรือ Partition เดียวกันกับข้อมูลหลักในระยะยาว เพราะจุดประสงค์หลักของการทำ

System Recovery ไม่ใช่แค่การปิดช่องโหว่ แต่คือการทำให้ระบบสามารถกลับมาให้บริการได้อย่างต่อเนื่อง เพื่อลดความเสียหายสูงสุดแก่ธุรกิจนั่นเอง

๓. ประโยชน์ที่ได้รับ

๓.๑ **เข้าใจหลักการและแนวปฏิบัติพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์:** ตระหนักถึงความสำคัญของการปกป้องระบบคอมพิวเตอร์ เครือข่าย และข้อมูลสำคัญภายใต้หลักการ CIA Triad (ความลับ ความถูกต้อง และความพร้อมใช้งาน)

๓.๒ **รู้เท่าทันภัยคุกคามทางดิจิทัลในรูปแบบต่างๆ:** สามารถแยกแยะและระบุความเสี่ยงจากภัยคุกคามรอบตัว เช่น การโจมตีด้วย Phishing, มัลแวร์ (Malware/Ransomware) และวิศวกรรมสังคม (Social Engineering) ได้อย่างถูกต้อง

๓.๓ **มีแนวทางปฏิบัติเพื่อป้องกันตนเองและองค์กร:** รู้วิธีการจัดการรหัสผ่านที่ปลอดภัย การเปิดใช้งานการยืนยันตัวตนแบบหลายขั้นตอน (MFA/๒FA) การอัปเดตระบบเพื่อปิดช่องโหว่ รวมถึงการสำรองข้อมูลอย่างถูกวิธี

๓.๔ **รู้วิธีปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินทางไซเบอร์:** เข้าใจขั้นตอนการระงับเหตุเบื้องต้น เช่น การตัดการเชื่อมต่อเครือข่ายเมื่อเครื่องติดมัลแวร์ และการประสานงานแจ้งเตือนผู้เกี่ยวข้องหรือทีม IT Support ได้อย่างทันทั่วทั้ง

๔. แนวคิดในการนำไปใช้ในการพัฒนางานของตนเองและหน่วยงาน

๔.๑ **ยกระดับความตระหนักรู้ด้านความปลอดภัย (Security Awareness):** นำความรู้เรื่องภัยคุกคามไซเบอร์มาปรับใช้ในการปฏิบัติงานประจำวัน เช่น การตรวจสอบอีเมลและลิงก์แปลกปลอมอย่างรอบคอบ เพื่อป้องกันความเสี่ยงที่อาจสร้างความเสียหายแก่ระบบของหน่วยงาน

๔.๒ **เสริมสร้างความปลอดภัยในการจัดการข้อมูลและรหัสผ่าน:** ปฏิบัติตามมาตรฐานความปลอดภัยด้านไอที เช่น การตั้งรหัสผ่านที่ซับซ้อน การเปลี่ยนรหัสผ่านตามรอบเวลา และการเปิดใช้งานการยืนยันตัวตนแบบหลายขั้นตอน (MFA/๒FA) ในการเข้าถึงระบบงาน

๔.๓ **สำรองข้อมูลสำคัญอย่างสม่ำเสมอ:** จัดให้มีกระบวนการสำรองข้อมูล (Data Backup) ของหน่วยงานอย่างเป็นระบบ และแยกเก็บข้อมูลสำรองไว้นอกเหนือจากเครื่องคอมพิวเตอร์หลัก เพื่อป้องกันความเสียหายจากเหตุการณ์ไม่คาดฝันหรือการโจมตีด้วย Ransomware

๔.๔ **อัปเดตระบบและซอฟต์แวร์ให้ทันสมัยอยู่เสมอ:** ให้ความสำคัญกับการอัปเดตระบบปฏิบัติการและแอปพลิเคชันใช้งาน เพื่อปิดช่องโหว่ทางเทคโนโลยีที่อาจเป็นช่องทางให้ผู้ไม่หวังดีเข้ามาโจมตีระบบ

๔.๕ **ปฏิบัติตามขั้นตอนการรับมือเหตุการณ์ฉุกเฉิน (Incident Response):** เตรียมความพร้อมและทำความเข้าใจแนวปฏิบัติเมื่อเกิดเหตุการณ์ผิดปกติ เช่น การตัดการเชื่อมต่อเครือข่ายทันทีเมื่อพบเครื่องคอมพิวเตอร์ติดมัลแวร์ และประสานงานแจ้งทีม IT Support หรือผู้เกี่ยวข้องอย่างรวดเร็วเพื่อจำกัดวงความเสียหาย

๕. ใบประกาศนียบัตร

๑. หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity)
๒. AI Governance & Ethics : หลักการจริยธรรม ธรรมาภิบาล และข้อกฎหมายในการประยุกต์ใช้ AI

๓. แนวทางปฏิบัติด้านการจัดซื้อจัดจ้าง รุ่น ๐๒ ปี ๒๕๖๔



ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

อภิเชก คำสุวรรณ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
หลักการสร้างภาพข้อมูลและการออกแบบแดชบอร์ดอย่างมีประสิทธิภาพ
(The Principle of Data Visualization and Dashboard Design)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 4 กันยายน 2569

Ah.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



Sponsored by P.O. Box 60000, Washington, D.C. 20540
Capital Government Development Agency (CDGA)
Organization ID: 12345
Date: 2024-08-15 10:10 AM EDT

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

อภิเชก คำสุวรรณ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนากิจกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 4 กันยายน 2569

(นางไอรดา เหลืองวิล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



ประกาศนียบัตรนี้ใช้ได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น
Digital Government Development Agency (DGA)
เลขที่ 2024-09-0072555-0001-01-00