บันทึกข้อความ

ส่วนราชการ กลุ่มวิเคราะห์สภาพการใช้ที่ดิน กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๑๘๙

ที่ กษ ๐๘๓๗.๐๒/ ๑๕๖ **วันที่** ๖ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอส่งรายงานการฝึกอบรม

เรียน ผอ.กลุ่มวิเคราะห์สภาพการใช้ที่ดิน

ด้วย ดิฉันนางสาวสลิลา เอี่ยมอิทธิพล นักวิชาการเกษตรชำนาญการพิเศษ เข้ารับการอบรมหลักสูตรการใช้เครื่องมือดิจิทัลเพื่อการทำงานภาครัฐ (Essential Digital Tools for Workplace) และการอบรมหลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity Series) จัดโดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล และเรียนรู้ผ่านสื่อออนไลน์ระบบ TDGA E - Learning ตั้งแต่วันที่ ๑ - ๒ กุมภาพันธ์ ๒๕๖๙ นั้น

บัดนี้ ได้รับใบประกาศนียบัตรผ่านการฝึกอบรมหลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอส่งใบประกาศนียบัตร และรายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้ที่ได้แนบมาพร้อมนี้ เพื่อใช้ประกอบการพิจารณาเกณฑ์การประเมินผลสำเร็จของงานตามตัวชี้วัดกลาง ระดับความสำเร็จของการพัฒนาความรู้ รอบการประเมินที่ ๑ ปีงบประมาณ ๒๕๖๙

จึงเรียนมาเพื่อโปรดทราบ และแจ้ง ผอ.กนผ. ลงนามในหนังสือที่ได้แนบมาพร้อมนี้

(นางสาวสลิลา เอี่ยมอิทธิพล)
นักวิชาการเกษตรชำนาญการพิเศษ

เรียน ผอ.กนผ.
เพื่อโปรดทราบ และลงนามในเอกสารที่แนบ

(นางสาวอมรรัตน์ สระเพ็ชร)
นักวิชาการเกษตรชำนาญการพิเศษ
ผู้อำนวยการกลุ่มวิเคราะห์สภาพการใช้ที่ดิน

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ นางสาวสลิลา นามสกุล เอี่ยมอิทธิพล
ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ กลุ่ม/ฝ่าย กลุ่มวิเคราะห์สภาพการใช้ที่ดิน
หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ
พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น (Basic Cybersecurity Series)
สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ
ระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-Learning)
หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ตั้งแต่วันที่ ๑ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙ ถึงวันที่ ๒ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙
เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/สัมมนา/พัฒนาความรู้ฯ

การอบรมครั้งนี้มีวัตถุประสงค์ เพื่อตระหนักและเทราบถึงวิธีการป้องกัน Cybersecurity และให้ผู้เรียนเข้าใจความหมายและเห็นถึงความสำคัญของการประยุกต์ใช้งาน Cybersecurity

๑. การประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

ความเสี่ยง คือ เหตุการณ์ การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย ความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้

การบริหารจัดการความเสี่ยง หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารสิ่งที่เกี่ยวข้องกับกิจกรรม หน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด

สภาพแวดล้อมกับความเสี่ยง ได้แก่

- สภาพแวดล้อมภายนอก เช่น ความสลับซับซ้อนทางสังคม ภาวะทางเศรษฐกิจ เสถียรภาพของรัฐบาล สภาพทางภูมิศาสตร์ และนวัตกรรม
- สภาพแวดล้อมภายใน เช่น โครงสร้างขององค์กร ผลผลิตและผลลัพธ์ อัตรากำลัง และคุณภาพบุคลากร

ความสำคัญของการบริหารความเสี่ยง

- เพื่อส่งเสริมให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายใน
- เพื่อให้ฝ่ายบริหารเกิดความมั่นใจว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย
- เพื่อสะท้อนการพัฒนาในด้านการกำกับดูแลที่ดีขององค์กร การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน

- เพื่อเป็นกลไกในการผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยง

กระบวนการบริหารจัดการความเสี่ยง

- กำหนดวัตถุประสงค์
- ระบุความเสี่ยง
- ประเมินความเสี่ยง
- ประเมินมาตรการควบคุม
- การจัดการความเสี่ยง
- รายงานผล
- การติดตาม และทบทวน

ประเภทความเสี่ยง

- ความเสี่ยงด้านยุทธศาสตร์
- ความเสี่ยงด้านปฏิบัติการ
- ความเสียงด้านการเงิน
- ความเสี่ยงด้านกฎหมาย
- ความเสี่ยงด้านเทคโนโลยี

กระบวนการจัดการความเสี่ยงตามมาตรฐาน COSO ERM

COSO ERM เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กรอย่างเป็นระบบ จนกระทั่งเป็นที่รู้จักและมีความนิยม ต่อมา COSO ได้กำหนดคำนิยามและรูปแบบต่าง ๆ ในการจัดการกับความเสี่ยง โดยได้กำหนดออกมาเป็น COSO ERM (COSO Enterprise Risk Management)

การประเมินความเสี่ยง เป็นการวัดระดับความรุนแรงของความเสี่ยงว่ามีมากน้อยเพียงใด โดยนำความเสี่ยงที่ได้จากการระบุความเสี่ยงมาทำการประเมินหาค่าระดับความเสี่ยง โดยแบ่งออกเป็น ๒ มิติ แต่ละมิติจะมีคะแนน ในการประเมินออกเป็น ๕ ระดับ ประกอบด้วย (๑) เกิดขึ้นได้ยาก (๒) เกิดขึ้นบ้างเป็นบางครั้ง (๓) เกิดขึ้นค่อนข้างบ่อย (๔) เกิดขึ้นบ่อย (๕) เกิดขึ้นเป็นประจำ

๒. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework)

กรอบมาตรฐานที่ได้รับการยอมรับในระดับสากล เช่น NIST Cybersecurity Framework (CSF) ซึ่งประกอบด้วย ๕ ฟังก์ชันหลัก ได้แก่ Identify, Protect, Detect, Respond และ Recover สามารถนำไปปรับใช้ในองค์กรเพื่อสร้างระบบการป้องกันที่ยั่งยืน

๓. การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment)

Vulnerability Assessment (VA) คือ กระบวนการที่ได้รับการตรวจสอบ หรือระบุช่องโหว่ที่มีอยู่ในระบบหรือแอปพลิเคชัน โดยใช้เครื่องมือตรวจสอบช่องโหว่และเทคนิคการสแกนเพื่อค้นหาปัญหาด้านความปลอดภัย ซึ่งกระบวนการนี้ช่วยให้ทราบถึงช่องโหว่ที่เปิดเผยในระบบหรือแอปพลิเคชัน จนนำไปสู่วิธีการแก้ไขได้อย่างถูกจุดเพื่อเพิ่มความปลอดภัย

Vulnerability Scanning Tool เพื่อตรวจสอบความปลอดภัยระบบเครือข่าย ค้นหาช่องโหว่ที่ใช้งานภายในองค์กร เช่น ระบบปฏิบัติการ (OS) ซอฟต์แวร์ อุปกรณ์ Network อุปกรณ์ Security ฯลฯ ซึ่งนับเป็นเรื่องสำคัญที่ใช้ระบุระดับความรุนแรงของช่องโหว่ที่เกิดขึ้นตามการอ้างอิงของ CVE และ CVSS

ประโยชน์ Vulnerability Assessment

- ช่วยในการประเมินระดับความเสี่ยงที่มาจากช่องโหว่
- ช่วยในการสร้างรายงานที่เกิดจากช่องโหว่ที่พบ
- ช่วยในการตรวจสอบว่าระบบสอดคล้องกับมาตรฐาน
- ช่วยในการค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย

รูปแบบของ VA Scan

- Host Assessment การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญ ซึ่งอาจจะเป็นเป้าหมายในการโจมตีได้ หากไม่ได้รับการทดสอบ
- Network and Wireless Assessment การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริง เพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต
- Database Assessment การประเมินความเสี่ยงในเรื่องของ Database หรือระบบที่เกี่ยวข้องกับข้อมูล

Remediation คือ การแก้ไขจุดประสงค์ของขั้นตอนสุดท้ายนี้คือ การอุดช่องโหว่ โดยส่วนใหญ่จะเป็นการร่วมมือกันระหว่างทีมงานที่ดูแลเรื่อง Security กับทีม Operation ซึ่งเป็นผู้ที่สามารถบอกได้ว่าการอุดช่องโหว่แบบใด ระดับไหนจะมีประสิทธิภาพสูงสุดโดยที่ไม่กระทบกับระบบปัจจุบัน หรืออาจจะกระทบน้อยลง

๔. การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

Detect Function การเฝ้าระวังภัยคุกคาม ต้องทำอย่างต่อเนื่อง โดยมีวัตถุประสงค์เพื่อ

- ลดความเสียหายที่อาจเกิดขึ้นได้ หรือสามารถจำกัดวงของความเสียหายที่เกิดขึ้นได้
- สามารถลดโอกาสหรือระยะเวลาของผู้โจมตีที่จะทำการโจมตีได้
- กระบวนการเฝ้าระวังที่ดี สามารถให้ข้อมูลที่เป็นประโยชน์ในกระบวนการ การตอบสนองต่อเหตุการณ์ และการกู้คืนระบบได้

ตัวอย่างของการ Detect Function เช่น พบการ Login ที่ผิดพลาด การ Login สู่ระบบนอกเวลางาน พบการ Login มาจากต้นทางที่น่าสงสัย การเรียกใช้งานโปรแกรมที่ผิดปกติ การทำงานของ CPU ที่มากผิดปกติ และมีการติดต่อไปยัง IP address ที่ถูกระบุว่าเป็น Malicious

ตัวอย่างเครื่องมือหรือระบบที่ใช้ในการเฝ้าระวัง เช่น

- ระบบ Intrusion Detection Systems (IDS)
- ระบบ Intrusion Prevention Systems (IPS)
- ระบบ Security Information and Event Management (SIEM)
- ระบบ Endpoint Detection and Response (EDR)

๕. การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

หน่วยงานควรจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ โดยกำหนดบทบาทหน้าที่ของแต่ละบุคคลให้มีความเหมาะสม ควรมีการซ้อมแผนรับมืออย่างน้อยปีละ ๑ ครั้ง

ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

- การเตรียมการ เช่น การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การตั้งทีมตอบสนองต่อเหตุการณ์ การฝึกอบรมพนักงานด้านการรับรู้ความปลอดภัยทางไซเบอร์ การเตรียมเครื่องมือต่าง ๆ

- การระบุภัยคุกคาม ขั้นตอนนี้เกี่ยวข้องกับการตรวจจับเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น ซึ่งสามารถเกิดขึ้นได้ ผ่านการแจ้งเตือนจากระบบที่ติดตั้งไว้

- การควบคุม เป้าหมายในขั้นตอนนี้คือการหยุดการโจมตี และลดความเสียหายให้น้อยที่สุด เช่น การตัดการเชื่อมต่อกับระบบเครือข่าย

- การกำจัดภัยคุกคามที่ตรวจพบ เช่น การลบไฟล์ Malware เป็นต้น

Crisis Communication Plan คือ หน่วยงานควรมีแผนการสื่อสารในภาวะวิกฤต เพื่อให้ข่าวสารที่เผยแพร่ออกไปในช่วงเกิดเหตุการณ์โจมตี มีความครบถ้วน และรวดเร็ว เพื่อให้ผู้ที่มีส่วนได้ส่วนเสียจะได้เตรียมตัวรับมือได้ทัน ควรมีการกำหนดช่องทางในการกระจายข่าวให้เหมาะสม และควรกำหนดให้มีโฆษกในกรณีที่จำเป็นต้องให้ข่าวกับสื่อมวลชน

ขั้นตอนการกู้คืนระบบ (Recover)

- จัดทำแผนความต่อเนื่องทางธุรกิจ เพื่อให้มั่นใจได้ว่า เมื่อเกิดเหตุการณ์หยุดชะงักกับระบบที่สำคัญแล้ว จะสามารถดำเนินการกู้คืนระบบ เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง

- การสำรองข้อมูล ควรทำอย่างสม่ำเสมอ และต้องมีการทดสอบชุดข้อมูลสำรองว่าสามารถใช้งานได้

- ปรับปรุงมาตรการรักษาความปลอดภัย เรียนรู้จากเหตุการณ์และใช้มาตรการรักษาความปลอดภัยเพิ่มเติมเพื่อป้องกันเหตุการณ์ที่คล้ายกันในอนาคต

Basic Cybersecurity

- การปกป้องข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ และข้อมูลการเงิน เป็นเป้าหมายหลักของการโจมตีทางไซเบอร์ การถูกขโมยข้อมูลส่วนบุคคล สามารถนำไปสู่การสูญเสียทางการเงินหรือการถูกนำไปใช้ในทางที่ผิด

- การป้องกันการโจมตีทางไซเบอร์ แนวคิดหลักจะเป็นการดำเนินการเพื่อให้คงไว้ซึ่งหลัก CIA คือ Confidentiality Availability และ Integrity ของข้อมูลและระบบที่ให้บริการเป็นหลัก

- การรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ การป้องกันภัยคุกคามทางไซเบอร์นั้น ไม่ว่าเราจะลงทุนป้องกันและดำเนินการป้องกันดีแค่ไหน ก็ไม่สามารถรับรองได้ว่าสินทรัพย์ของเราจะปลอดภัย ๑๐๐%

- การสร้างความเชื่อมั่นและความน่าเชื่อถือ ในโลกธุรกิจ ความปลอดภัยทางไซเบอร์มีความสำคัญต่อการสร้างความเชื่อมั่นให้กับลูกค้า และพันธมิตรทางธุรกิจ องค์กร ที่มีมาตรการรักษาความปลอดภัยที่ดีจะได้รับความเชื่อถือจากลูกค้า

๒.๒ ประสบการณ์/ประโยชน์ที่ได้รับการประยุกต์ใช้กับหน่วยงาน

☑ ต่อตนเอง

๑) เพิ่มความรู้และทักษะด้าน Cybersecurity

๒) สามารถนำไปใช้ในงานจริง เช่น การประเมินความเสี่ยง การตรวจสอบช่องโหว่ การตอบสนองต่อเหตุการณ์

๓) สร้างความมั่นใจในการทำงานและการปกป้องข้อมูลส่วนบุคคล

☑ ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน

๑) สามารถลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจจะเกิดขึ้นภายในหน่วยงาน

๒) สามารถปฏิบัติให้สอดคล้องกับมาตรฐานและกฎหมาย

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

ในบางช่วงเวลาคลิปวีดีโอเกิดการขัดข้อง

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

เนื้อหาครอบคลุมและเป็นระบบ มีการจัดลำดับหัวข้อชัดเจน ตั้งแต่การประเมินความเสี่ยง กรอบมาตรฐาน ไปจนถึงการตอบสนองและการฟื้นฟู ทำให้ผู้เรียนเข้าใจภาพรวมของ Cybersecurity Framework ได้ครบถ้วน-

ลงชื่อ .....

(นางสาวสลิลา เอี่ยมอิทธิพล)

ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ

ผู้รายงาน

วันที่ ๖ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙

(✓) ทราบ

ลงชื่อ .....

(นายนันทพล หนองหารพิทักษ์)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ ๖ เดือน ก.พ. พ.ศ. ๒๕๖๙

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ สลิลา เอี่ยมอิทธิพล

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 2 กุมภาพันธ์ 2569

สำเนาถูกต้อง

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-02T16:30:49.109+07:00
cf0bc89c

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ สลิลา เอี่ยมอิทธิพล

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การใช้เครื่องมือดิจิทัลเพื่อการทำงานภาครัฐ

(Essential Digital Tools for Workplace)

จำนวนชั่วโมงการเรียนรู้ 3:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 2 กุมภาพันธ์ 2569

สำเนาถูกต้อง

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-02T08:13:54.118+07:00
d95322d8