แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๑/๒๕๖๙ ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ – ๓๑ มีนาคม ๒๕๖๙
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ - นามสกุล นายธภัทร ชูประเสริฐ **ตำแหน่ง** นักวิชาการเกษตรปฏิบัติการ
หน่วยงาน ศูนย์ศึกษาการพัฒนาเขาหินซ้อนอันเนื่องมาจากพระราชดำริ
หัวข้อการพัฒนา Basic Cybersecurity Series
หลักสูตรพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์เบื้องต้น
วิธีการพัฒนา การฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์
วันที่พัฒนา ๑๐ กุมภาพันธ์ ๒๕๖๙ **สถานที่** ศูนย์ศึกษาการพัฒนาเขาหินซ้อนอันเนื่องมาจากพระราชดำริ
หน่วยงานที่จัดอบรม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity) ระดับต้น
๒. เพื่อให้ผู้เรียนสามารถนำความรู้ที่ได้พัฒนาไปใช้ในการปฏิบัติงานได้อย่างถูกต้อง

สรุปสาระสำคัญ

๑. ความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity) ระดับต้น ประกอบไปด้วยพื้นฐานและการบริหารจัดการความเสี่ยง (Risk Management) ซึ่งการบริหารความเสี่ยงคือหัวใจสำคัญของการรักษาความปลอดภัยสารสนเทศ โดยมุ่งเน้นที่การจัดการกับ "ความไม่แน่นอน" ของเหตุการณ์ที่อาจส่งผลกระทบต่อเป้าหมายองค์กร ทั้งครอบคลุมทั้งความเป็นไปได้ที่จะเกิดความเสียหายต่อธุรกิจ ความไม่แน่นอนของเหตุการณ์และการคลาดเคลื่อนจากการคาดการณ์ โดยการประเมินความเสี่ยงปัจจุบันขององค์กรจะใช้มาตรฐาน ISO ๓๑๐๐๐ และ COSO/ERM เป็นหลัก ส่วน ISO/IEC ๒๗๐๐๕ จะใช้สำหรับเทคนิคการประเมินความเสี่ยงด้านสารสนเทศโดยเฉพาะ ขณะที่ ISO/IEC ๒๗๐๐๑ เป็นมาตรฐานสำหรับการจัดการภาพรวม (ISMS)

ความปลอดภัยคือหน้าที่ของทุกคนในองค์กร ซึ่งประกอบด้วย

๑) Executives คือ ผู้วางนโยบายและตัดสินใจระดับสูงขององค์กร
๒) Managers คือ ผู้กำกับดูแลและถ่ายทอดนโยบายสู่การปฏิบัติในองค์กร
๓) Practitioners เป็นผู้ปฏิบัติงานที่นำมาตรการไปใช้จริง เช่น ตำแหน่งสายวิชาการในหน่วยงานต่างๆ ในองค์กร

ส่วน Hacker เป็นภัยคุกคามภายนอก ไม่ใช่บุคคลที่มีบทบาทบริหารจัดการความเสี่ยงในองค์กร

๒. กรอบมาตรฐาน NIST Cybersecurity Framework (NIST CSF) เป็นกรอบการทำงานระดับสากลที่ประกอบด้วย ๕ ฟังก์ชันหลัก เพื่อให้องค์กรรับมือภัยคุกคามอย่างเป็นระบบ ดังนี้

๑) การระบุ Identify เป็นการทำความเข้าใจความเสี่ยงและจุดอ่อน เช่น การประเมินช่องโหว่ Vulnerability Assessment (VA)
๒) การป้องกัน Protect เป็นการวางมาตรการควบคุมเพื่อลดผลกระทบ
๓) การตรวจจับ Detect การเฝ้าระวังเพื่อระบุความผิดปกติ
๔) การตอบสนอง Respond การดำเนินการเมื่อเกิดเหตุการณ์คุกคาม
๕) การกู้คืน Recover เป็นการฟื้นฟูระบบให้กลับมาให้บริการปกติ)

๓. เทคนิคการตรวจหาจุดอ่อนและการเฝ้าระวัง (VA & Monitoring) หลังจากระบุช่องโหว่ได้แล้ว ขั้นตอนที่ต้องทำคือ Vulnerability Analysis เพื่อวิเคราะห์หาสาเหตุรากเหง้า (Root Cause) ของจุดอ่อนนั้น โดยใช้เครื่องมือเฝ้าระวังการเฝ้าระวังภัยคุกคามใช้ระบบ SIEM (Security Information and Event Management) ในการรวม Log และวิเคราะห์ความผิดปกติ โดยทีมปฏิบัติการของศูนย์ที่ทำหน้าที่เฝ้าระวังภัยคุกคามไซเบอร์ตลอด ๒๔ ชั่วโมง เรียกว่า CSOC (Cyber Security Operations Center)

๔. การตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response) เมื่อพบเหตุการณ์ที่ไม่ปกติ เช่น เครื่องคอมพิวเตอร์ถูก Remote Desktop เข้ามาโดยไม่ได้รับอนุญาต จะต้องมีการแจ้งเตือน และรีบแจ้งทีม Cyber Security หรือทีม IT ตามช่องทาง โดยมีข้อห้ามสำคัญ คือไม่ควรโพสต์แจ้งเหตุการณ์ร้ายแรงผ่านโซเชียลส่วนตัว เพราะอาจสร้างความตื่นตระหนกและทำให้ข้อมูลรั่วไหล และการยับยั้งความเสียหาย (Containment) หากพบเครื่องติด Ransomware สิ่งแรกที่ต้องทำคือปลดเครื่องออกจากเครือข่ายสำนักงานทันทีเพื่อหยุดการระบาด

๕. ความต่อเนื่องทางธุรกิจและการกู้คืน (BCP & Recovery) จะต้องมีแผนรับมือ มีการระบุรายชื่อผู้ติดต่อ, หน้าที่ความรับผิดชอบ และช่องทางสื่อสารให้ชัดเจน**มี**การซักซ้อม และควรทดสอบแผน BCP (Business Continuity Plan) แบบ Table Top Exercise สม่ำเสมอ เช่น ปีละ ๒ ครั้งและจะต้องมีการสำรองข้อมูล (Backup) การสำรองข้อมูล ในเครื่องเดิม (แม้แยก Partition) ถือว่าไม่เหมาะสม ควรเก็บไว้ในสื่อภายนอก Cloud หรือ Backup Server ที่อยู่คนละพื้นที่กับข้อมูลจริง เพื่อให้ระบบสามารถกลับมาให้บริการได้อย่างต่อเนื่องโดยเร็วที่สุด

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. ผู้เรียนได้ความรู้ ความเข้าใจเกี่ยวกับด้านความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity) ระดับต้น

๒. ผู้เรียนเกิดความ ความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity)

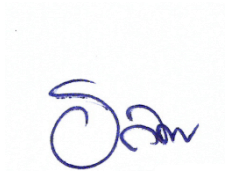
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ที่ได้พัฒนาไปใช้ในการปฏิบัติงานได้อย่างถูกต้อง

การนำองค์ความรู้ไปประยุกต์ใช้

สามารถนำความรู้ที่ได้รับจากการถ่ายทอดไปสื่อสาร และถ่ายทอดความรู้ให้แก่เกษตรกรและผู้อื่น เพื่อตระหนักรู้ถึงความปลอดภัยทางไซเบอร์

แนวทางการถ่ายทอดองค์ความรู้สู่เกษตรกร

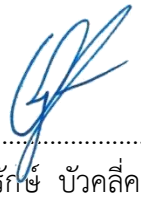
จากการได้รับการอบรม หลักสูตรดังกล่าวข้างต้น นักวิชาการเกษตร สามารถถ่ายทอดความรู้ความเข้าใจความเข้าใจเกี่ยวกับด้านความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเกษตรกรด้านการใช้ประโยชน์และลดการสูญเสียทรัพย์สิน และชีวิตได้



(ลงนาม)..... .....

(นายธภัทร ชูประเสริฐ)

นักวิชาการเกษตรปฏิบัติการ



(ลงนาม).....

(นายอนุรักษ์ บัวคลี่คลาย)

ผู้อำนวยการศูนย์ศึกษาการพัฒนาเขาหินซ้อน

อันเนื่องมาจากพระราชดำริ