แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินอุตรดิตถ์

ด้วยข้าพเจ้า นางสาวนิตยา ภูมิราช ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ สังกัด สถานีพัฒนาที่ดินอุตรดิตถ์ สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cyber Security Awareness ระหว่างวันที่ ๑ เมษายน ๒๕๖๘ ถึงวันที่ ๗ มิถุนายน ๒๕๖๘ เป็นเวลารวมทั้งสิ้น ๖ วัน ณ สถานีพัฒนาที่ดินอุตรดิตถ์ ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy

บัดนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ พร้อมทั้งแนบใบประกาศ เพื่อโปรดพิจารณา ดังนี้

๑. การพัฒนาความรู้ฯ ดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ เพื่อเข้าใจความรู้พื้นฐานของ Cyber Security และรูปแบบภัยคุกคามของ Cyber Security

๑.๒ เพื่อสร้างความตระหนักรู้ด้าน Cyber Security ในชีวิตประจำวัน

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

๒.๑ Cybersecurity ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์หรือข่ายโครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาตในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ได้แก่ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐, พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล, มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

๒.๒ ความรู้พื้นฐานของ Cybersecurity

๑) Cybersecurity หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้นเบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

๒) Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระยุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓) Availability หรือ ความพร้อมใช้งานของข้อมูล การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่นข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคารข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๒.๓ รูปแบบภัยคุกคามของ Cybersecurity ในปัจจุบันมีภัยคุกคามหลายประมาท และเป็นภัยคุกคาม ยกตัวอย่าง เช่น

๑) Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware

๒) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

๓) Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS,เว็บไซต์หรือ ช่องทางSocial โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำชื่อนำชัลมูลดังกล่าวของเหยื่อใช้ในการทำธุรม

๔) Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ เช่น CMS Web Server หรือ Database Server วิธีการโจมตี
Cross-Site Scripting, SQL Injection, Path Traversal

๕) Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS. เว็บไซต์ หรือ ซ่องทาง Social โดยเป็นการส่งจำนจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญ หรือก่อกวน

๖) DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๗) Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเวปไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการไม่ทราบ ซึ่งผู้ไจมตีต้องกรนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของข้อมูลนั้นๆ

๘) Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้นซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

๙) Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงางานตอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐) Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๑๑) Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

๒.๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) การใช้งานคอมพิวเตอร์ ควรมีการแยก User ใช้งานกันของแต่ละบุคคล ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

๒) การใช้ Password ที่ดี มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ ๕ #) มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดา ได้ง่าย เช่น password ๑๒๓๔๕๖ วันเกิด หมายเลขโทรศัพท์ มีการเปลี่ยน Password อย่างสม่ำเสมอ ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ ไม่ควรบอก Password แก่ผู้อื่น

๓) การใช้ E-mail ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน ไม่ควรบอก Password แก่ผู้อื่น ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

๔) การใช้ Website ไม่เข้าเว็บไซที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ ไม่ควรทำการบันทึก Password ต่างๆ บน Browser เว็บไซต์สำหรับทำธุรกรรมที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Browsing ควรมีการติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕) การใช้ Messaging ไม่ควรบันทึก Password ไว้ที่โปรแกรม กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

๖) Fake News หรือ ข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE Facebook กระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น วิธีการสังเกตุข่าวปลอม มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ ระบุที่มาของข่าวไม่ได้ มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์ สำนวนการเขียนออกแนวการโฆษณา

๗) การใช้ Conference ใช้สถานที่เหมาะสมกับการ Conference ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง แชร์เอกสารต่างๆ อย่างระมัดระวัง ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ มีการขออนุญาตผู้เข้าว่าร่วมประชุม Conference ก่อนที่จะรับที่จะบันทึกภาพและเสียงในการประชุม

๘)_ การใช้ Cloud Storage แยก User ในการใช้งานของแต่ละบุคคล ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น ปิดการเข้าถึงไฟล์ หรือปิดการแชไฟล์เมื่อไม่มีความจำเป็น ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

๙) การใช้ WIFI ไม่ควรใช้งาน WIF! ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

๑๐) การใช้ Mobile ปัดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา กำหนด Application permission ให้เหมาะสม มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๑๑) การใช้ Internet Connection เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

๓. ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง ได้แก่

๓.๑ มีความรู้ความเข้าใจเกี่ยวกับความรู้พื้นฐานของด้านความมั่นคงทางไซเบอร์และรูปแบบภัยคุกคามของ Cyber Security

๓.๒ มีความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ในชีวิตประจำวัน

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯ ครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

๔.๑ นำความรู้เรื่องที่ได้รับการอบรมไปใช้และเฝ้าระวังด้านความมั่นคงทางไซเบอร์ของหน่วยงาน

๔.๒ นำความรู้ที่ได้รับไปประชาสัมพันธ์ สื่อสารให้แก่เจ้าหน้าที่ในสถานีพัฒนาที่ดิน กลุ่มเกษตรกรและประชาชนที่มีความสนใจ ได้อย่างถูกต้องและเหมาะสม

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

ความเสียหายจากการกระทำที่รู้เท่าไม่ถึงการณ์ของบุคคลากร อาจทำให้ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่

เพิ่มทักษะการใช้ความรู้รูปแบบภัยคุกคามของ Cyber Security แก่เจ้าหน้าที่ผู้ปฏิบัติงาน ส่งเสริมให้มีความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ในชีวิตประจำวันให้กับเจ้าหน้าที่ผู้ปฏิบัติงาน

จึงเรียนมาเพื่อโปรดพิจารณา

(นางสาวนิตยา ภูมิราช)
นักวิชาการเกษตรปฏิบัติการ
ผู้เข้ารับการพัฒนาความรู้