แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินเพชรบูรณ์

ด้วย นางสาววรรธกร ไป่ทาฟอง ตำแหน่ง เจ้าพนักงานธุรการชำนาญงาน สังกัด สถานีพัฒนาที่ดินเพชรบูรณ์ สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้เพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) หลักสูตร พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ (Basic Cybersecurity Series) หมวดหมู่ ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Series) เมื่อวันที่ ๑๒ พฤษภาคม ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ ชั่วโมง ๓๐ นาที ซึ่งหลักสูตรดังกล่าวจัดโดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานราชการ ดังนี้

๑. วัตถุประสงค์

เพื่อเสริมสร้างความรู้ความเข้าใจด้านความมั่นคงปลอดภัยทางไซเบอร์ ความรู้พื้นฐานด้านความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์และกระบวนการป้องกันระบบ เครือข่าย อุปกรณ์ และข้อมูลดิจิทัลจากการโจมตีการเข้าถึงโดยมิชอบ

๒. เนื้อหาและหัวข้อวิชา

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) คือ กระบวนการป้องกันระบบ เครือข่าย อุปกรณ์และข้อมูลดิจิทัลจากการโจมตี การเข้าถึงโดยมิชอบ หรือการทำลาย เพื่อให้ข้อมูลที่เป็นความลับถูกต้องครบถ้วนและพร้อมใช้งาน CIA Triad โดยอาศัยการผสานรวมบุคคล กระบวนการ และเทคโนโลยี ซึ่งการใช้ CIA Triad ควรพิจารณาในทุกกรณีที่เกี่ยวข้องกับการจัดการข้อมูลและระบบสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัยสูงสุด

๒.๑ การพัฒนาซอฟต์แวร์และระบบไอที: ในระหว่างการออกแบบและพัฒนาซอฟต์แวร์หรือระบบใหม่ ควรใช้แนวคิด CIA Triad เพื่อให้มั่นใจว่าระบบนั้นมีความปลอดภัยต่อการใช้งาน ทั้งนี้ควรรวมไปถึงการทดสอบระบบหลังพัฒนาเสร็จสิ้นด้วย

๒.๒ การจัดการข้อมูลที่สำคัญ: เมื่อมีการเก็บรวบรวมหรือประมวลผลข้อมูลที่มีความสำคัญ เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน หรือข้อมูลลับทางธุรกิจ ควรใช้หลักการ CIA Triad เพื่อป้องกันข้อมูลจากการเข้าถึงหรือแก้ไขโดยไม่ได้รับอนุญาต

๒.๓ การดำเนินธุรกรรมออนไลน์: ในการทำธุรกรรมออนไลน์ เช่น การชำระเงินผ่านอินเทอร์เน็ต การส่งข้อมูลที่เป็นความลับ ควรใช้หลักการ CIA Triad เพื่อให้มั่นใจว่าข้อมูลไม่ถูกโจรกรรมหรือแก้ไขระหว่างการส่งต่อ

๒.๔ การจัดการระบบเครือข่าย: เมื่อมีการบริหารจัดการระบบเครือข่ายขององค์กร ควรใช้หลักการ CIA Triad เพื่อป้องกันการโจมตีทางไซเบอร์ เช่น การโจมตี DDoS หรือการเข้าถึงข้อมูลภายในเครือข่ายโดยไม่ได้รับอนุญาต

๒.๕ การจัดทำและปฏิบัติตามนโยบายความปลอดภัย: ในการวางนโยบายความปลอดภัยขององค์กร ควรใช้หลักการ CIA Triad เพื่อสร้างนโยบายที่ครอบคลุมและมีประสิทธิภาพในการป้องกันข้อมูลและระบบจากภัยคุกคาม

๒.๖ การสำรองข้อมูลและการกู้คืนระบบ ในการวางแผนสำรองข้อมูลและการกู้คืนระบบหลังจากเกิดเหตุการณ์ไม่คาดฝัน เช่น ภัยธรรมชาติหรือการโจมตีทางไซเบอร์ ควรใช้หลักการ CIA Triad เพื่อให้มั่นใจว่าข้อมูลยังคงมีความครบถ้วนและสามารถใช้งานได้เมื่อจำเป็น

การป้องกันความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ที่สำคัญ คือ การตั้งรหัสผ่านที่ซับซ้อน,อัปเดตซอฟต์แวร์ทันที , ติดตั้ง Antivirus , สำรองข้อมูลสม่ำเสมอ, และระมัดระวัง Phishing โดยควรมุ่งเน้น ๓ ระดับป้องกันภัยทั่วไป คือ ตั้งรหัสผ่าน , เปิดใช้งาน MFA , ป้องกันระบบ (ใช้ Firewall, ทำ System Hardening) และสร้างความทนทาน (วางแผนรับมือเหตุฉุกเฉิน) เพื่อรับมือภัยคุกคามที่ไม่รู้จัก

๑. ป้องกันที่ตัวบุคคล (Individual/Human Layer)
   ๑) รหัสผ่าน (Passwords) ใช้รหัสผ่านที่ซับซ้อน แตกต่างกันในแต่ละบัญชี และไม่เปิดเผยรหัสผ่าน
   ๒) การยืนยันตัวตน (Authentication) เปิดใช้งานการยืนยันตัวตนแบบหลายขั้นตอน (Multi - Factor Authentication - MFA) ทุกครั้งที่มีโอกาส
   ๓) การรับรู้ความเสี่ยง (Awareness) ระวังอีเมลหรือลิงก์แปลกปลอม (Phishing) ไม่คลิกทันที และตรวจสอบแหล่งที่มา
๒. ป้องกันที่อุปกรณ์และซอฟต์แวร์ (Technical Layer):
   ๑) อัปเดตระบบ (Updates) อัปเดตซอฟต์แวร์, แอปพลิเคชันและระบบปฏิบัติการ(OS) ให้เป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่
   ๒) โปรแกรมรักษาความปลอดภัย (Security Software) ติดตั้งโปรแกรมป้องกันไวรัส (Antivirus/Anti-malware) และเปิดใช้งาน Firewall
   ๓) สำรองข้อมูล (Backups) สำรองข้อมูลสำคัญ (Data Backup) อย่างสม่ำเสมอ และจัดเก็บไว้ในที่ปลอดภัย (เช่น Cloud หรือ External Hard Drive) เพื่อป้องกัน Ransomware
๓. ป้องกันที่เครือข่ายและระบบงาน (Network/Organizational Layer)
   ๑) การควบคุมการเข้าถึง (Access Control) จำกัดสิทธิ์การเข้าถึงข้อมูลตามบทบาทหน้าที่ (Least Privilege)
   ๒) เครือข่ายปลอดภัย (Secure Network) หลีกเลี่ยง Wi-Fi สาธารณะ หรือใช้ VPN โดยไม่จำเป็น
   ๓) การประเมินความเสี่ยง (Risk Assessment) ทำการประเมินความเสี่ยงทางไซเบอร์ขององค์กรอย่างน้อยปีละ ๑ ครั้ง เพื่อระบุภัยคุกคามและกำหนดแนวทางแก้ไข

การตรวจสอบและเฝ้าระวังทางไซเบอร์ (Cybersecurity Monitoring) คือ กระบวนการเชิงรุกในการตรวจสอบ ตรวจจับ และวิเคราะห์ความปลอดภัยของเครือข่าย อุปกรณ์ และข้อมูลในองค์กรแบบเรียลไทม์ โดยมีเป้าหมายเพื่อระบุช่องโหว่และภัยคุกคามที่ซ่อนอยู่ เช่น Ransomware, Phishing, หรือ DDoS เพื่อป้องกันการโจมตีหรือลดความเสียหายที่อาจเกิดขึ้น

การตรวจสอบช่องโหว่ทางไซเบอร์ (Vulnerability Assessment) คือกระบวนการค้นหาจุดอ่อนในระบบเครือข่าย ซอฟต์แวร์ และอุปกรณ์ไอทีอย่างเป็นระบบ เพื่อประเมินความเสี่ยงและจัดลำดับความสำคัญในการแก้ไขก่อนที่จะถูกโจมตีจริง โดยมักใช้เครื่องมืออัตโนมัติในการสแกน เพื่อหาช่องโหว่ที่ทราบแล้วและปิดความเสี่ยงที่อาจทำให้ข้อมูลรั่วไหลซึ่งอาจก่อให้เกิดความเสียหายกับองค์กร

๓. ประโยชน์ที่ได้รับ มีความรู้ความเข้าใจและเห็นความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และมีความรู้ขั้นพื้นฐานด้านความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์และกระบวนการป้องกันระบบเครือข่าย อุปกรณ์ และข้อมูลดิจิทัลจากการโจมตีการเข้าถึงโดยมิชอบ

๔. แนวทางในการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน สามารถนำความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และความรู้ขั้นพื้นฐานด้านความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ การเฝ้าระวังภัยและเพื่อป้องกันระบบ เครือข่าย อุปกรณ์ ข้อมูลดิจิทัลต่าง ๆ จากการโจมตีการเข้าถึงโดยมิชอบจากภัยคุกคามทางข้อมูลขององค์กร

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา จัดให้มีการฝึกอบรมเพื่อเพิ่มพูนความรู้ความเข้าใจและการสนับสนุนด้านอุปกรณ์ที่มีประสิทธิภาพเพื่อป้องกันข้อมูลความปลอดภัยขององค์กร

(นางสาววรรธกร ไป่ทาฟอง)
เจ้าพนักงานธุรการชำนาญงาน

(นายภัจจ์ งามสิทธิโชค)
ผู้อำนวยการสถานีพัฒนาที่ดินเพชรบูรณ์