แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มวิชาการเพื่อการพัฒนาที่ดิน

ด้วย นายเทอดศักดิ์ อนากาศ ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ สังกัด กลุ่มวิชาการเพื่อการพัฒนาที่ดิน สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้เพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) หลักสูตร ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding Cybersecurity Risk Management) เมื่อวันที่ ๙ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ ชั่วโมง ๓๐ นาที ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์

๑.๑ เพื่อให้ผู้เรียนเข้าใจความหมายและกระบวนการของ Cybersecurity Risk Management

๑.๒ เพื่อให้ผู้เรียนเข้าใจหลักการพื้นฐานของ Risk Management

๑.๓ เพื่อให้ผู้เรียนเข้าใจแนวทางการจัดทำแผน Business Continuity Planning

๒. เนื้อหาและหัวข้อวิชา

๒.๑ Cyber Security vs. Information Security เรียนรู้ความหมายของ Cyber Security และ Information Security

ความหมายของ Cyber Security (ความปลอดภัยทางไซเบอร์) เป้าหมาย: ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต, การโจมตี (Hacking), มัลแวร์ และการจารกรรมข้อมูลที่อยู่บนเครือข่ายอินเทอร์เน็ตหรือระบบ IT ขอบเขต: ครอบคลุมทรัพย์สินดิจิทัล, แอปพลิเคชัน, เครือข่าย, Cloud และอุปกรณ์เชื่อมต่อต่าง ๆ (IoT) ลักษณะ: มุ่งเน้นไปที่ภัยคุกคามทางไซเบอร์ (Cyber Attacks) และการรักษาความปลอดภัยของข้อมูลในรูปแบบดิจิทัล

ความหมายของ Information Security (ความปลอดภัยของข้อมูล) เป้าหมาย: รักษาความปลอดภัยของสารสนเทศและสินทรัพย์ข้อมูลไม่ให้รั่วไหล ไม่ว่าจะเก็บอยู่ในรูปแบบใดก็ตาม ขอบเขต: ครอบคลุมทั้งข้อมูลที่จัดเก็บในคอมพิวเตอร์ (Digital), เอกสารกระดาษ (Paper-based), ความปลอดภัยทางกายภาพ (Physical Security), กระบวนการทำงาน และบุคลากร หลักการ: ยึดหลัก \(CIA\) Triad (Confidentiality-ความลับ, Integrity-ความถูกต้อง, Availability-ความพร้อมใช้งาน)

ข้อแตกต่างที่สำคัญ ขอบเขต: Information Security กว้างกว่า ครอบคลุมทุกรูปแบบข้อมูล, Cyber Security เฉพาะเจาะจงที่ข้อมูลดิจิทัล.เป้าหมายหลัก: Cyber Security ป้องกัน "การโจมตีทางไซเบอร์", Information Security ป้องกัน "ข้อมูลสูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต"

๒.๒ Cyber Security Risk Management ความเข้าใจเบื้องต้นของ Cyber Security Risk Management

Cyber Security Risk Management คือ กระบวนการที่องค์กรใช้ในการ ระบุ ประเมิน และตอบสนอง ต่อความเสี่ยงทางไซเบอร์ เพื่อลดโอกาสการเกิดเหตุการณ์และจำกัดผลกระทบที่อาจเกิดขึ้นกับ

ข้อมูลและระบบสารสนเทศ โดยมีเป้าหมายหลักเพื่อให้ธุรกิจสามารถดำเนินงานได้อย่างต่อเนื่องแม้จะเผชิญกับภัยคุกคาม

๒.๓ Frameworks กรอบการดำเนินงานและมาตราฐานที่เกี่ยวข้อง

กระบวนการบริหารความเสี่ยง ๕ ขั้นตอนหลัก ตามมาตรฐานสากลและแนวทางของไทย (เช่น NIST CSF และ ISO/IEC ๒๗๐๐๕) กระบวนการมักประกอบด้วย

๑) การระบุความเสี่ยง (Risk Identification): สำรวจสินทรัพย์ดิจิทัล (Assets) ระบุภัยคุกคาม (Threats) และหาจุดอ่อนหรือช่องโหว่ (Vulnerabilities) ที่มีอยู่

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis): ประเมินโอกาสที่จะเกิดเหตุการณ์และผลกระทบ (Impact) ที่จะตามมา หากความเสี่ยงนั้นเกิดขึ้นจริง

๓) การประเมินค่าความเสี่ยง (Risk Evaluation): นำผลวิเคราะห์มาจัดลำดับความสำคัญ เพื่อตัดสินใจว่าความเสี่ยงใดต้องจัดการก่อนหลังตามระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)

๔) การตอบสนองต่อความเสี่ยง (Risk Treatment): เลือกใช้วิธีจัดการที่เหมาะสม เช่น

- การลดความเสี่ยง (Reduce): ติดตั้งระบบป้องกันเพื่อลดโอกาสเกิด
- การถ่ายโอนความเสี่ยง (Share/Transfer): เช่น การทำประกันภัยไซเบอร์
- การหลีกเลี่ยง (Avoid): ยกเลิกกิจกรรมที่เสี่ยงเกินไป
- การยอมรับความเสี่ยง (Accept): หากต้นทุนการป้องกันสูงกว่าความเสียหาย

๕) การติดตามและทบทวน (Monitor and Review): ตรวจสอบประสิทธิภาพของมาตรการที่ใช้และปรับปรุงให้ทันต่อภัยคุกคามใหม่ๆ อยู่เสมอ ซึ่งกรอบการทำงานที่นิยม (Frameworks) ได้แก่

- NIST Cybersecurity Framework ๒.๐: เน้น ๖ ฟังก์ชันหลัก คือ Govern (กำกับดูแล), Identify (ระบุ), Protect (ป้องกัน), Detect (ตรวจจับ), Respond (ตอบสนอง) และ Recover (กู้คืน)
- ISO/IEC ๒๗๐๐๑ & ๒๗๐๐๕: มาตรฐานสากลด้านการจัดการความมั่นคงปลอดภัยสารสนเทศและการบริหารความเสี่ยง

๒.๔ NIST Cybersecurity Framework ความเข้าใจเบื้องต้นของ NIST Cybersecurity Framework

NIST Cybersecurity Framework (CSF) คือชุดแนวทางปฏิบัติ มาตรฐาน และแนวทางที่สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) ของสหรัฐอเมริกาพัฒนาขึ้น เพื่อช่วยให้องค์กรทุกขนาดและทุกประเภทสามารถ จัดการและลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ได้อย่างเป็นระบบ ซึ่งประกอบไปด้วย ๖ ฟังก์ชันหลัก (Core Functions) ของ NIST CSF ๒.๐ ได้แก่

๑) Govern (กำกับดูแล): เน้นการกำหนดกลยุทธ์ นโยบาย บทบาทหน้าที่ และการบริหารจัดการความเสี่ยงในระดับองค์กรเพื่อให้สอดคล้องกับเป้าหมายธุรกิจ

๒) Identify (ระบุ): ทำความเข้าใจสภาพแวดล้อมทางธุรกิจ สินทรัพย์ (เช่น อุปกรณ์ ข้อมูล) และความเสี่ยง เพื่อวางรากฐานในการจัดการความปลอดภัย

๓) Protect (ป้องกัน): กำหนดมาตรการป้องกันเพื่อควบคุมความเสียหายหรือป้องกันไม่ให้เกิดเหตุการณ์ เช่น การจัดการสิทธิ์เข้าถึง (Access Control) และการฝึกอบรมบุคลากร

๔) Detect (ตรวจจับ): การเฝ้าระวังและตรวจสอบเพื่อค้นหาเหตุการณ์ที่ผิดปกติหรือการบุกรุกในระบบได้อย่างรวดเร็ว

๕) Respond (ตอบสนอง): การวางแผนและดำเนินการเมื่อตรวจพบเหตุการณ์ผิดปกติ เพื่อจำกัดความเสียหายและสื่อสารกับผู้เกี่ยวข้องอย่างมีประสิทธิภาพ

๖) Recover (กู้คืน): การดำเนินกิจกรรมเพื่อกู้คืนระบบหรือบริการที่ได้รับความเสียหายให้กลับมาใช้งานได้ตามปกติ และนำบทเรียนมาปรับปรุงแผนงาน

๒.๕ Business Continuity Planning (BCP) เรียนรู้การวางแผนความต่อเนื่องทางธุรกิจ

Business Continuity Planning (BCP) หรือ แผนบริหารความต่อเนื่องทางธุรกิจ คือ แผนกลยุทธ์ที่กำหนดขั้นตอนการปฏิบัติงานเพื่อช่วยให้องค์กรสามารถ ดำเนินธุรกิจต่อไปได้ หรือกลับมาเปิดดำเนินการให้เร็วที่สุดหลังจากเกิดเหตุการณ์วิกฤตที่ทำให้หยุดชะงัก เช่น ภัยธรรมชาติ (น้ำท่วม, ไฟไหม้), โรคระบาด, หรือการโจมตีทางไซเบอร์ ประกอบด้วย ๕ ขั้นตอนหลักในการทำแผน BCP ได้แก่

๑) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA): ระบุว่ากระบวนการใดสำคัญที่สุดต่อธุรกิจ หากหยุดชะงักจะเกิดความเสียหายเท่าไหร่ และต้องกู้คืนภายในกี่ชั่วโมง (RTO)

๒) การประเมินความเสี่ยง (Risk Assessment): ค้นหาโอกาสที่จะเกิดเหตุการณ์ต่าง ๆ เช่น ไฟดับ หรือ ข้อมูลถูกโจรกรรม และประเมินระดับผลกระทบ

๓) การกำหนดกลยุทธ์ความต่อเนื่อง (Strategy Development): วางแนวทางแก้ปัญหา เช่น การมีสำนักงานสำรอง, การสำรองข้อมูลบน Cloud หรือการมีซัพพลายเออร์สำรอง

๔) การจัดทำและนำแผนไปใช้ (Plan Development & Implementation): เขียนเอกสารขั้นตอนการปฏิบัติงานที่ชัดเจน รวมถึงจัดตั้ง BCP Team และกำหนดระบบการแจ้งเหตุ (Call Tree)

๕) การซักซ้อมและทบทวน (Testing & Maintenance): ทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าพนักงานเข้าใจและแผนยังทันสมัยต่อสถานการณ์ปัจจุบัน

๒.๖ ISO ๒๒๓๐๑ Business Continuity Management เรียนรู้มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ISO ๒๒๓๐๑ (BCM)

ISO ๒๒๓๐๑ คือมาตรฐานสากลสำหรับการจัดทำ ระบบบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ซึ่งออกแบบมาเพื่อช่วยให้องค์กรทุกขนาดและทุกประเภทสามารถเตรียมความพร้อม ตอบสนอง และฟื้นฟูการดำเนินงานจากการหยุดชะงักที่ไม่คาดคิด เช่น ภัยธรรมชาติ การโจมตีทางไซเบอร์ หรือวิกฤตการณ์ต่าง ๆ

องค์ประกอบสำคัญของ ISO ๒๒๓๐๑ (BCM) ในการดำเนินการตามมาตรฐานนี้มีกระบวนการหลักที่สำคัญ ดังนี้:

๑) Business Impact Analysis (BIA): การวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุว่ากิจกรรมใดสำคัญที่สุดและต้องกู้คืนภายในระยะเวลาเท่าใด

๒) Risk Assessment: การประเมินความเสี่ยงเพื่อระบุภัยคุกคามและจุดอ่อนที่อาจทำให้ธุรกิจหยุดชะงัก

๓) Business Continuity Strategy: การกำหนดกลยุทธ์เพื่อรักษาความต่อเนื่องของกระบวนงานหลัก (Critical Business Processes)

๔) Business Continuity Plan (BCP): การจัดทำแผนรองรับสภาวะวิกฤตที่มีขั้นตอนการปฏิบัติงานที่ชัดเจน

๕) Exercise and Testing: การทดสอบและซ้อมแผนสม่ำเสมอ เพื่อให้มั่นใจว่าบุคลากรมีความพร้อมและแผนสามารถใช้งานได้จริง

ประโยชน์ของการได้รับรองมาตรฐาน ISO ๒๒๓๐๑ ได้แก่

๑) ความยืดหยุ่น (Resilience): ช่วยให้องค์กรสามารถฟื้นตัวจากการหยุดชะงักได้อย่างรวดเร็วและมีประสิทธิภาพ

๒) ความเชื่อมั่น: สร้างความมั่นใจให้แก่ลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียว่าธุรกิจจะไม่หยุดนิ่งแม้ในภาวะวิกฤต

๓) ลดความสูญเสีย: ช่วยลดผลกระทบทางการเงินและความเสียหายต่อชื่อเสียงภาพลักษณ์ขององค์กร

๔) ความได้เปรียบทางการแข่งขัน: องค์กรที่มีมาตรฐานนี้มักได้รับความไว้วางใจในการทำธุรกิจในห่วงโซ่อุปทานระดับสากล

๓. ประโยชน์ที่ได้รับ

การบริหารความเสี่ยงไซเบอร์เป็นกลยุทธ์สำคัญที่ช่วยให้ธุรกิจอยู่รอดได้ในยุคดิจิทัล ประโยชน์ที่ได้รับจากการทำ Cybersecurity Risk Management อย่างเป็นระบบมีดังนี้

๓.๑ ลดโอกาสและผลกระทบจากภัยคุกคาม (Risk Mitigation) ช่วยให้องค์กรไม่เพียงแค่ "ตั้งรับ" แต่เป็นการ "รุก" โดยการระบุจุดอ่อน (Vulnerabilities) ก่อนที่แฮกเกอร์จะเจอ ทำให้ลดโอกาสที่จะถูกโจมตี และหากเกิดเหตุขึ้นจริง ผลกระทบต่อข้อมูลและทรัพย์สินจะน้อยลงอย่างมาก

๓.๒ รักษาความต่อเนื่องทางธุรกิจ (Business Continuity) เมื่อมีความเสี่ยงที่ได้รับการจัดการอย่างดี ระบบงานที่สำคัญ (Critical Systems) จะไม่หยุดชะงักนานเกินไป ช่วยให้ธุรกิจยังสามารถให้บริการลูกค้าได้แม้จะอยู่ภายใต้การโจมตี หรือกู้คืนระบบได้อย่างรวดเร็ว (ลด Downtime)

๓.๓ ประหยัดค่าใช้จ่ายในระยะยาว (Cost-Effectiveness) การลงทุนในระบบป้องกันและแผนบริหารความเสี่ยง มีราคา "ถูกกว่า" การต้องจ่ายค่าไถ่ (Ransomware) ค่าปรับทางกฎหมาย หรือค่าเสียหายจากการกู้คืนข้อมูลและชื่อเสียงที่เสียไปหลายเท่าตัว

๓.๔ สร้างความเชื่อมั่นให้ลูกค้าและคู่ค้า (Trust & Reputation) ในโลกที่ข้อมูลรั่วไหลเป็นข่าวรายวัน องค์กรที่มีระบบบริหารความเสี่ยงที่ชัดเจน (เช่น ทำตามมาตรฐาน NIST หรือ ISO) จะได้รับความไว้วางใจมากกว่า ซึ่งเป็นแต้มต่อสำคัญในการทำธุรกิจและสร้างความน่าเชื่อถือในระยะยาว

๓.๕ ปฏิบัติตามกฎหมายและข้อบังคับ (Compliance) ช่วยให้องค์กรปฏิบัติได้ถูกต้องตามกฎหมาย เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ของไทย ซึ่งหากละเลยอาจมีโทษทั้งทางแพ่ง อาญา และทางปกครอง

๓.๖ การตัดสินใจที่แม่นยำขึ้น (Informed Decision Making) ผู้บริหารสามารถตัดสินใจได้ว่าจะลงทุนในเทคโนโลยีใดก่อน-หลัง โดยอิงจาก ข้อมูลความเสี่ยงจริง ไม่ใช่การคาดเดา ทำให้การใช้งบประมาณด้านความปลอดภัยมีประสิทธิภาพสูงสุด

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน

๔.๑ การตัดสินใจเชิงกลยุทธ์ที่แม่นยำ (Strategic Decision Making) ช่วยให้ผู้บริหารระดับสูงมองเห็นภาพรวมของภัยคุกคามในรูปแบบของ "ตัวเลขและความสำคัญ" แทนที่จะเป็นศัพท์เทคนิค ทำให้สามารถจัดสรรงบประมาณและทรัพยากรไปยังจุดที่วิกฤตที่สุดได้อย่างคุ้มค่า ไม่สูญเปล่ากับระบบที่ไม่จำเป็น

๔.๒ ยกระดับธรรมาภิบาลขององค์กร (Corporate Governance) การบริหารความเสี่ยงเป็นส่วนหนึ่งของความรับผิดชอบของคณะกรรมการและผู้บริหาร การมีระบบ Cybersecurity Risk

Management ที่ดีช่วยยืนยันว่าหน่วยงานมีการกำกับดูแลที่ดี (Governance) โปร่งใส และมีมาตรฐานในการปกป้องผลประโยชน์ขององค์กรและผู้มีส่วนได้ส่วนเสีย

๔.๓ สร้างความได้เปรียบทางการแข่งขัน (Competitive Advantage) ในยุคที่คู่ค้าและลูกค้าให้ความสำคัญกับความปลอดภัยของข้อมูล หน่วยงานที่มีระบบบริหารความเสี่ยงที่เข้มแข็ง (เช่น มีใบรับรอง ISO ๒๗๐๐๑) จะได้รับความไว้วางใจในการทำโปรเจกต์สำคัญหรือการเชื่อมต่อระบบกับพันธมิตรระดับสากลมากกว่าคู่แข่ง

๔.๔ การจัดการวัฒนธรรมความปลอดภัยในองค์กร (Cybersecurity Culture) กระบวนการบริหารความเสี่ยงช่วยให้บุคลากรในทุกระดับตระหนักถึงหน้าที่และความรับผิดชอบของตนเอง เปลี่ยนจากความกลัวเป็นการสร้าง "ความตระหนักรู้" (Awareness) ทำให้พนักงานกลายเป็นเกราะป้องกันด่านแรกที่มีประสิทธิภาพ (Human Firewall)

๔.๕ การบริหารจัดการห่วงโซ่อุปทาน (Supply Chain Security) ช่วยให้หน่วยงานสามารถประเมินและคัดเลือกผู้ให้บริการ (Vendors) หรือ Outsource ได้อย่างปลอดภัย ลดความเสี่ยงที่ภัยคุกคามจะหลุดรอดเข้ามาผ่านทางคู่ค้า ซึ่งเป็นช่องโหว่ยอดนิยมในการโจมตีสมัยใหม่

๔.๖ ความยืดหยุ่นและการฟื้นตัวที่รวดเร็ว (Cyber Resilience) ประโยชน์ที่ชัดเจนที่สุดคือเมื่อเกิดเหตุการณ์จริง หน่วยงานที่มีการบริหารความเสี่ยงจะ "ไม่สติแตก" เพราะมีแผนเผชิญเหตุที่ซักซ้อมไว้แล้ว ทำให้สามารถลดความเสียหายและกู้คืนระบบกลับมาสร้างรายได้หรือให้บริการประชาชนได้เร็วกว่าปกติ

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) การสนับสนุนจากผู้บริหารระดับสูง เพราะการบริหารความเสี่ยงต้องใช้ทรัพยากรการอนุมัติงบประมาณการสนับสนุนการจัดซื้อเครื่องมือและเทคโนโลยีป้องกันที่จำเป็น รวมถึงการกำหนดนโยบาย เมื่อผู้บริหารให้ความสำคัญ พนักงานจะรับรู้ว่าความปลอดภัยไซเบอร์เป็นเรื่องที่ต้องปฏิบัติตามอย่างเคร่งครัด และการยอมรับระดับความเสี่ยงผู้บริหารต้องเป็นผู้ตัดสินใจว่าความเสี่ยงระดับใดที่องค์กรยอมรับได้ และระดับใดที่ต้องลงทุนเพิ่มเพื่อป้องกัน

(นายเทอดศักดิ์ อนากาศ)
นักวิชาการเกษตรชำนาญการพิเศษ

(นางชุติมา จันทร์เจริญ)
ผู้อำนวยการกลุ่มวิชาการเพื่อการพัฒนาที่ดิน