บันทึกข้อความ

ส่วนราชการ กลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๔ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร ๑๒๘๓ ต่อ ๑๐๖

ที่ กษ ๐๘๐๔.๐๙/ ๙๕ **วันที่** ๑๓ มีนาคม ๒๕๖๙

เรื่อง รายงานผลการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์

เรียน ผอ.สวพ. ผ่าน ผอ.กพฐ๔

ตามแบบกำหนดและประเมินตัวชี้วัดด้านผลสัมฤทธิ์ของประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ของสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ให้ข้าราชการอบรมศึกษาการพัฒนาความรู้ผ่านระบบ Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐดิจิทัล โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตร อย่างน้อย ๒ เรื่อง และมีการสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชา นั้น

ข้าพเจ้า นางสาวอาทิมา เมืองหนู ตำแหน่ง วิศวกรโยธาปฏิบัติการ สังกัดกลุ่มพัฒนาโครสร้างพื้นฐานที่ ๔ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ได้ผ่านการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านระบบ Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐดิจิทัล จำนวน ๒ หลักสูตร ได้แก่

๑. ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Cybersecurity Risk Management)

๒. ไมโครซอฟท์ เวิร์ด (โปรแกรมประมวลผลคำเพื่องานเอกสาร)

จึงขอสรุปบทเรียนที่ได้รับการพัฒนาความรู้ในรอบการประเมินที่ ๑/๒๕๖๙ จำนวน ๑ หลักสูตร ได้แก่ เรื่อง ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Cybersecurity Risk Management) รายละเอียดปรากฏตามรายงานสรุปบทเรียน และได้แนบสำเนาใบประกาศนียบัตร จำนวน ๒ หลักสูตร มาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

อาทิมา เมืองหนู
(นางสาวอาทิมา เมืองหนู)
วิศวกรโยธาปฏิบัติการ

(นายวีระพงษ์ พิกุลประยงค์)
ผู้อำนวยการกลุ่มโครงสร้างพื้นฐานที่ ๔

ชื่อเรื่อง : ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์

(Understanding Cybersecurity Risk Management)

(โดย นางสาวอาทิมา เมืองหนู วิศวกรโยธาปฏิบัติการ)

วัตถุประสงค์

เพื่อให้เข้าใจถึงบริบทและองค์ประกอบของ **Cybersecurity และเพื่อ**เพื่อเรียนรู้หลักการบริหารความเสี่ยงด้านไซเบอร์ เพื่อเข้าใจ Framework และมาตรฐานสำคัญ เช่น NIST CSF, ISO 22301 และสามารถนำแนวคิดไปประยุกต์ใช้ในการจัดทำ BCP และการบริหารความต่อเนื่องทางธุรกิจเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศในองค์กรภาครัฐ/เอกชน

บทนำ

ปัจจุบันองค์กรพึ่งพาระบบดิจิทัลและข้อมูลเป็นหลัก ความเสี่ยงด้านไซเบอร์จึงส่งผลกระทบโดยตรงต่อ เช่น ความต่อเนื่องของงาน (Operational Disruption) ความเสียหายทางการเงิน ความเชื่อมั่นของประชาชนหรือลูกค้า ความปลอดภัยของข้อมูลส่วนบุคคล การบริหารความเสี่ยงไซเบอร์จึงไม่ใช่เรื่องของ IT เพียงอย่างเดียว แต่เป็นเรื่องของ “การบริหารจัดการองค์กร” ที่ต้องใช้แนวคิดเชิงระบบ (Framework-based & Risk-based Approach)

เนื้อหา

Cyber Security vs. Information Security เป็นพื้นฐานสำคัญที่สุด” ของการบริหารความเสี่ยงไซเบอร์

- Cyber Security (ความมั่นคงปลอดภัยไซเบอร์) คือ การปกป้อง “ระบบเครือข่าย ระบบคอมพิวเตอร์และระบบดิจิทัล” จากภัยคุกคามทางไซเบอร์
- Information Security (ความมั่นคงปลอดภัยสารสนเทศ) คือ การปกป้อง “ข้อมูล” ไม่ว่าจะอยู่ในรูปแบบใดก็ตาม โดยมีเป้าหมายหลักให้ข้อมูลเป็นความลับ มีความถูกต้องและพร้อมใช้งาน

ซึ่งสรุปแล้ว Cyber Security ก็คือส่วนหนึ่งของ Information Security

Cyber Security Risk Management คือ กระบวนการบริหารจัดการ“ความเสี่ยงจากภัยคุกคามทางไซเบอร์” อย่างเป็นระบบเพื่อป้องกัน ลดผลกระทบ และทำให้องค์กรดำเนินงานต่อได้ มีองค์ประกอบหลัก ดังนี้

1.Identifying Risk (การระบุความเสี่ยง) คือการค้นหาและระบุว่า "อะไรคือสิ่งที่อาจก่อให้เกิดความเสียหายต่อองค์กร"

2.Assess Risk (การประเมินความเสี่ยง) คือการวิเคราะห์ว่า โอกาสเกิด (Likelihood) เท่าไร ผลกระทบ (Impact) รุนแรงแค่ไหน

3.Control Risk (การควบคุม/ลดความเสี่ยง) คือการกำหนดมาตรการควบคุม

4.Review Controls (การทบทวนและปรับปรุง)

Frameworks คือ โครงสร้างแนวทางที่ช่วยให้องค์กรทำงานอย่างเป็นระบบ มีมาตรฐาน และควบคุมความเสี่ยงได้ ซึ่งมีหลายวิธี เช่น

- COSO (Committee of Sponsoring Organizations of the Treadway Commission) ใช้สำหรับ Enterprise Risk Management (ERM) เน้นบริหารความเสี่ยงระดับองค์กรทั้งหมด ไม่ใช่เฉพาะ IT
- ISO 27001 มาตรฐานสำหรับ Information Security Management System (ISMS)
- ISO 27032 ISO/IEC 27032 แนวทางด้าน **Cybersecurity** โดยเฉพาะเน้นการป้องกันภัยไซเบอร์ในโลกออนไลน์
- NIST (National Institute of Standards and Technology) หน่วยงานสหรัฐฯ ที่ออก Framework ด้าน Cybersecurity เป็น Framework ที่นิยมใช้มากที่สุด
- ISO 31000 มาตรฐานด้าน Risk Management ทั่วไปใช้ได้กับทุกอุตสาหกรรม
- ISO 27005 แนวทางบริหารความเสี่ยงด้าน Information Security ทำงานคู่กับ ISO 27001
- COBIT Framework สำหรับ IT Governance และ IT Management

NIST Cybersecurity Framework (CSF) ประกอบด้วย

- Framework Core คือ "โครงสร้างหลักของกิจกรรมด้าน Cybersecurity" ประกอบด้วย Functions (5 ฟังก์ชันหลัก) คือ Identify Protect Detect Respond Recover

Core บอกว่า "องค์กรควรทำอะไรบ้าง" ในภาพรวม

- Framework Implementation Tiers คือ "ระดับความพร้อม/ความเป็นผู้ใหญ่ (Maturity Level)" ขององค์กร **Tier ไม่ได้บอกว่า "ดีหรือไม่ดี" แต่บอกว่าองค์กรอยู่ระดับไหน**

- Framework Profiles คือ “การเลือกสิ่งที่เหมาะกับองค์กร” องค์กรจะกำหนด:Current Profile (ปัจจุบันทำอะไรอยู่) Target Profile (อยากไปถึงระดับไหน)

Business Continuity Planning (BCP) คือ การวางแผนล่วงหน้าเพื่อให้องค์กรสามารถดำเนินธุรกิจต่อไปได้ แม้เกิดเหตุการณ์ไม่คาดคิด เช่น น้ำท่วม ไฟไหม้ ไฟดับ

ISO 22301: Business Continuity Management คือ ระบบบริหารความต่อเนื่องทางธุรกิจ”เป้าหมายคือ ทำให้องค์กรเตรียมพร้อม รับมือ และฟื้นตัวจากเหตุการณ์หยุดชะงักได้อย่างเป็นระบบ มีโครงสร้างหลัก ดังนี้

- Context of the Organization วิเคราะห์บริบทองค์กร ผู้มีส่วนได้เสีย และความเสี่ยง
- Leadership ผู้บริหารต้องสนับสนุนและกำหนดนโยบาย BC
- Planning ประเมินความเสี่ยง ทำ BIA (Business Impact Analysis) และกำหนด RTO / RPO
- Support ทรัพยากร บุคลากร การสื่อสาร เอกสาร
- Operation การจัดทำและนำ BCP ไปใช้จริง
- Performance Evaluation ทดสอบแผน ตรวจสอบ ประเมินผล
- Improvement ปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)

Wrap Up คือ การสรุปปิดท้ายเนื้อหา การประชุม หรือการเรียน เพื่อทบทวนประเด็นสำคัญก่อนจบ คือ

- องค์กรต้องบริหารความเสี่ยง
- ต้องมี Framework เป็นแนวทาง
- ต้องมีแผน BCP เพื่อรับมือเหตุการณ์
- ต้องทดสอบและปรับปรุงอย่างต่อเนื่อง

ประโยชน์ที่ได้รับ

- เข้าใจโครงสร้างการบริหารความเสี่ยงด้านไซเบอร์อย่างเป็นระบบ
- สามารถวิเคราะห์และจัดลำดับความเสี่ยงในองค์กรได้
- เข้าใจบทบาทของ BCP และ ISO 22301
- สามารถประยุกต์ใช้ NIST CSF ในการพัฒนาองค์กร
- เพิ่มความพร้อมในการรับมือภัยคุกคามไซเบอร์

<u>แนวคิดการนำไปใช้ในการพัฒนาวิศวกรรมโยธาในกรมพัฒนาที่ดิน</u>

งานวิศวกรรมโยธาในกรมพัฒนาที่ดินมีการใช้ เช่น ระบบ GIS,ระบบฐานข้อมูลโครงการ,ระบบจัดซื้อจัดจ้าง,ระบบออกแบบและควบคุมงานก่อสร้าง,ระบบ Survey ซึ่งมีแนวทางประยุกต์ใช้ Cybersecurity Risk Management ดังนี้

- การทำ Risk Assessment กับระบบโครงสร้างพื้นฐานดิจิทัล วิเคราะห์ความเสี่ยงของระบบ GIS, Server, Cloud ประเมินความเสี่ยงข้อมูลแผนที่และข้อมูลที่ดิน
- ใช้ NIST CSF ในการจัดระบบควบคุม
- จัดทำ BCP สำหรับโครงการก่อสร้าง หากระบบ IT ล่ม งานภาคสนามจะดำเนินต่ออย่างไร มีระบบสำรองข้อมูลแบบ Offline หรือไม่
- บูรณาการกับงานวิศวกรรมโยธา ป้องกันการแก้ไขแบบก่อสร้างโดยไม่ได้รับอนุญาต ควบคุมความถูกต้องของข้อมูลปริมาณงาน (BOQ Integrity) ป้องกันการรั่วไหลของข้อมูลโครงการรัฐ
- สร้างวัฒนธรรมความปลอดภัยไซเบอร์ ฝึกอบรมวิศวกรและเจ้าหน้าที่ ใช้ PDCA ในการพัฒนาระบบอย่างต่อเนื่อง

โดยสรุปแล้ว Cybersecurity Risk Management เป็น “เครื่องมือเชิงกลยุทธ์” ที่ช่วยให้องค์กรป้องกันความเสียหาย รักษาความต่อเนื่องของงาน สร้างความเชื่อมั่น และพัฒนาองค์กรอย่างยั่งยืน

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

อาทิมา เมืองหนู

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์

(Understanding Cybersecurity Risk Management)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 22 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-22T21:19:12.835+07:00

38347c0c