



## บันทึกข้อความ

|                |              |
|----------------|--------------|
| เลขที่รับ..... | ผบร. สวพ. ๔๕ |
| วันที่.....    | ๑๓ ส.ค. ๒๕๖๔ |
| เวลา.....      | ๑๔.๐๙ น.     |

ส่วนราชการ กลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๔ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร ๑๒๘๓ ต่อ ๑๐๖  
ที่ กษ ๐๘๐๔.๐๙/๔๓๗ วันที่ ๑๓ สิงหาคม ๒๕๖๔

เรื่อง รายงานผลการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์

เรียน ผอ.สวพ. ผ่าน ผอ.กพฐ๔

ตามแบบกำหนดและประเมินตัวชี้วัดด้านผลสัมฤทธิ์ของประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ของสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ให้ข้าราชการอบรมศึกษาการพัฒนาความรู้ผ่านระบบ Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐดิจิทัล โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตร อย่างน้อย ๒ เรื่อง และมีการสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชา นั้น

ข้าพเจ้า นายสุทิน พันศิริธัญ ตำแหน่ง นายช่างโยธาอาวุโส สังกัดกลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๔ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ได้ผ่านการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านระบบ Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐดิจิทัล จำนวน ๒ หลักสูตร ได้แก่

๑. ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์(Understanding Cybersecurity Risk Management)

๒. การขับเคลื่อนด้วยข้อมูลสู่การเป็นรัฐบาลดิจิทัล(Data Driven Digital Government Transformation)

จึงขอสรุปบทเรียนที่ได้รับการพัฒนาความรู้ในรอบการประเมินที่ ๒/๒๕๖๔ จำนวน ๑ หลักสูตร ได้แก่ เรื่อง ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์(Understanding Cybersecurity Risk Management) รายละเอียดปรากฏตามรายงานสรุปบทเรียน และได้แนบสำเนาใบประกาศนียบัตร จำนวน ๒ หลักสูตร มาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

(นายสุทิน พันศิริธัญ)  
นายช่างโยธาอาวุโส

ผู้อำนวยการกลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๔

- ทธบ

- ผบร. (พิเศษ) เพื่องานรวม

(นายจักรกฤษณ์ มีโย)

ผู้อำนวยการสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน

**ชื่อเรื่อง : ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์**  
**(Understanding Cybersecurity Risk Management)**  
(โดย นายสุทิน พันศิริคุณ นายช่างโยธาวุธโส)

**วัตถุประสงค์**

๑. เพื่อให้มีความตระหนักรู้ในความมั่นคงปลอดภัยไซเบอร์
๒. เพื่อให้สามารถใช้เทคโนโลยีคอมพิวเตอร์ได้อย่างปลอดภัยและแก้ปัญหาเบื้องต้นได้เมื่อต้องพบปัญหา
๓. เพื่อให้การประเมินความเสี่ยงด้านไซเบอร์โดยมีแนวทางการดำเนินงานที่ถูกต้องเหมาะสม

**บทนำ**

หลักสูตรนี้มุ่งเน้นให้ผู้เข้าอบรมได้ตระหนักรู้ความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งมีความรู้และความเข้าใจในภัยคุกคามไซเบอร์รูปแบบต่าง ๆ โดยเฉพาะที่กำลังเป็นประเด็นสำคัญในปัจจุบัน นอกจากนี้ยังส่งเสริมให้ผู้เข้ารับการอบรมมีความรู้เบื้องต้นในวิธีการป้องกันภัยคุกคามไซเบอร์ที่เกิดขึ้นในอนาคตได้อย่างถูกต้องและทันทั่วถึง รวมทั้งมีความเข้าใจเบื้องต้นเกี่ยวกับการบริหารความเสี่ยง (Risk Management) และการประเมินความเสี่ยง (Risk Assessment) ระบบสารสนเทศให้มีความมั่นคงปลอดภัยทางไซเบอร์

**เนื้อหา**

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญต่อการดำเนินงานของหน่วยงานราชการ ความปลอดภัยทางไซเบอร์กลายเป็นปัจจัยสำคัญที่ไม่สามารถมองข้ามได้ การรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศไม่เพียงแต่เป็นการปกป้องทรัพย์สินทางดิจิทัลของหน่วยงาน แต่ยังเป็นการรักษาความน่าเชื่อถือในการให้บริการประชาชนและการดำเนินงานตามภารกิจของรัฐ

ความปลอดภัยของข้อมูล (Information Security) เป็นพื้นฐานสำคัญในการรักษาข้อจำกัดที่ได้รับอนุญาตในการเข้าถึงและเปิดเผยข้อมูล รวมถึงการปกป้องความเป็นส่วนตัวและข้อมูลที่เป็นกรรมสิทธิ์ของหน่วยงาน ขณะที่ไซเบอร์สเปซ (Cyberspace) หมายถึงพื้นที่เสมือนที่เกิดจากการเชื่อมต่อของคอมพิวเตอร์ ระบบเครือข่ายอินเทอร์เน็ต และอุปกรณ์ดิจิทัลต่างๆ เป็น "โลกดิจิทัล" ที่ผู้คน ข้อมูล และเทคโนโลยีได้ต่อกันผ่านเครือข่าย

๑. หลักการพื้นฐานด้านความปลอดภัยทางไซเบอร์ หลักการพื้นฐานด้านความปลอดภัยทางไซเบอร์ที่ใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย ๓ องค์ประกอบหลัก

๑.๑ ความลับ (Confidentiality) การป้องกันไม่ให้ข้อมูลถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต โดยวิธีการเข้ารหัส (Encryption), การกำหนดสิทธิ์ (Access Control), การยืนยันตัวตนหลายปัจจัย (MFA) ตัวอย่าง เช่น ข้อมูลบัตรประจำตัวประชาชนถูกเข้ารหัส ไม่สามารถอ่านได้หากไม่มี key ที่ถูกต้อง

๑.๒ ความถูกต้องแม่นยำ (Integrity) การรับประกันว่าข้อมูลไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับ

อนุญาตโดยวิธีการ Hashing, Digital Signature, Version Control ตัวอย่าง เช่น ระบบฐานข้อมูลประชาชน ต้องรับประกันว่าข้อมูลไม่ถูกแก้ไขโดยบุคคลที่ไม่มีสิทธิ์

๑.๓ ความพร้อมใช้งาน (Availability) ข้อมูลและระบบต้องพร้อมใช้งานเมื่อผู้มีสิทธิ์ ต้องการ โดยวิธีการ การสำรองข้อมูล (Backup), ความซ้ำซ้อน (Redundancy), การกระจายภาระงาน (Load Balancing), การ ป้องกัน DDoS ตัวอย่าง เช่น ระบบให้บริการออนไลน์ของหน่วยงานต้องเปิดให้บริการตลอด ๒๔/๗

## ๒. ตัวอย่างการรักษาความปลอดภัยทางไซเบอร์

๒.๑ ความปลอดภัยเครือข่าย (Network Security) การปฏิบัติในการป้องกันเครือข่ายจากการเข้าถึง โดย ไม่ได้รับอนุญาต การใช้งานในทางที่ผิด การรบกวน หรือการหยุดชะงักของบริการ

๒.๒ ความปลอดภัยแอปพลิเคชัน (Application Security) กระบวนการที่เกี่ยวข้องกับการตรวจจับ การ ซ่อมแซม และการเพิ่มความปลอดภัยของแอปพลิเคชันเพื่อป้องกันข้อมูลหรือโค้ดจากการถูกขโมยก่อนที่จะมีการ เผยแพร่

๒.๓ ความปลอดภัยคลาวด์ (Cloud Security) การผสมผสานของนโยบาย การควบคุมขั้นต้น และ เทคโนโลยีที่ทำงานร่วมกันเพื่อปกป้องโครงสร้างพื้นฐานและระบบบนคลาวด์

๒.๔ ความปลอดภัยโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) ชุดเครื่องมือพื้นฐานที่ ให้บริการด้านความปลอดภัย เช่น เครื่องสแกนไวรัส ระบบป้องกันการบุกรุก ซอฟต์แวร์มัลแวร์

## ๓. การจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

### ๓.๑ ประเภทการควบคุมความปลอดภัยของข้อมูล

๓.๑.๑ การควบคุมเชิงขั้นตอน (Procedural Controls) การควบคุมเหล่านี้ป้องกัน ตรวจจับ หรือ ลดความเสี่ยงด้านความปลอดภัยต่อทรัพย์สินทางกายภาพ รวมถึงการศึกษาเพื่อตระหนักถึงเรื่องความปลอดภัย กรอบการทำงานด้านความปลอดภัย การฝึกอบรม การปฏิบัติตามกฎระเบียบ และแผนการตอบสนองต่อ เหตุการณ์

๓.๑.๒ การควบคุมการเข้าถึง (Access Controls) การควบคุมเหล่านี้กำหนดว่าใครมีสิทธิ์เข้าถึงและ ใช้ข้อมูลของหน่วยงานและเครือข่าย รวมถึงการกำหนดข้อจำกัดในการเข้าถึงทางกายภาพของอาคาร และการ เข้าถึงเสมือนเช่นการอนุญาตการเข้าถึงที่มีสิทธิ์พิเศษ

๓.๑.๓ การควบคุมเชิงเทคนิค (Technical Controls) การควบคุมเหล่านี้เกี่ยวข้องกับการใช้ การยืนยัน ตัวตนของผู้ใช้หลายปัจจัยเมื่อเข้าสู่ระบบ ไฟร์วอลล์ และซอฟต์แวร์ป้องกันไวรัส

๓.๑.๔ การควบคุมตามกฎหมาย (Compliance Controls) การควบคุมเหล่านี้เกี่ยวข้องกั บกฎหมายความเป็นส่วนตัวและมาตรฐานความปลอดภัยทางไซเบอร์ ต้องการการประเมินความ เสี่ยง ด้านความ ปลอดภัยของข้อมูลและบังคับใช้ข้อกำหนดด้านความปลอดภัยของข้อมูล

## ๓.๒ กระบวนการจัดการความเสี่ยง (Risk Management Process)

๓.๒.๑ การระบุความเสี่ยง (Identifying Risk) การประเมินสภาพแวดล้อมขององค์กรเพื่อระบุความเสี่ยงในปัจจุบันหรือที่อาจเกิดขึ้นซึ่งอาจส่งผลกระทบต่อการดำเนินงาน

๓.๒.๒ การประเมินความเสี่ยง (Assess Risk) การวิเคราะห์ความเสี่ยงที่ระบุได้เพื่อดูว่ามีแนวโน้มที่จะส่งผลกระทบต่อหน่วยงานมากแค่ไหนและผลกระทบอาจเป็นอย่างไร

๓.๒.๓ การควบคุมความเสี่ยง (Control Risk) กำหนดวิธีการ ขั้นตอน เทคโนโลยี หรือมาตรการอื่นๆ ที่สามารถช่วยให้หน่วยงานลดความเสี่ยงได้

๓.๒.๔ การทบทวนการควบคุม (Review Controls) ประเมินอย่างต่อเนื่องว่าการควบคุมที่มีอยู่ มีประสิทธิภาพสามารถลดความเสี่ยงได้มากแค่ไหน และเพิ่มหรือปรับการควบคุมตามความจำเป็น

## ๔. แนวทางปฏิบัติที่ดีที่สุดเพื่อลดความเสี่ยง

๔.๑ โครงการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ การสร้างความตระหนักรู้และเสริมสร้างทักษะให้กับบุคลากรในหน่วยงาน

๔.๒ การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ การรักษาซอฟต์แวร์และระบบปฏิบัติการให้อยู่ในเวอร์ชันล่าสุด

๔.๓ โซลูชันการจัดการการเข้าถึงแบบสิทธิพิเศษ (PAM) การควบคุมและจัดการบัญชีผู้ใช้ที่มีสิทธิพิเศษในระบบ

๔.๔ การตรวจสอบสิทธิ์การเข้าถึงแบบหลายปัจจัย (MFA) การเพิ่มชั้นความปลอดภัยในการเข้าถึงระบบ

๔.๕ การสำรองข้อมูลแบบไดนามิก การสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอและทดสอบการกู้คืนข้อมูล

## ๕. การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

๕.๑ ความหมายและความสำคัญของ BCM การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management - BCM) เป็นกระบวนการเชิงรุกที่หน่วยงานใช้เพื่อเตรียมพร้อม วางแผน และตอบสนอง ต่อเหตุการณ์ที่อาจทำให้การดำเนินงานหยุดชะงัก เช่น ภัยธรรมชาติ ไฟไหม้ น้ำท่วม การโจมตีไซเบอร์ หรือ การระบาดของโรค โดยองค์ประกอบหลักของ BCM ประกอบด้วย

๕.๑.๑ Business Impact Analysis (BIA) การวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุกิจกรรม ที่สำคัญ และจำเป็นต่อการดำเนินงานของหน่วยงาน

๕.๑.๒ Risk Assessment (RA) การประเมินความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อ การดำเนินงาน

๕.๑.๓ Business Continuity Plan (BCP) แผนรองรับความต่อเนื่อง เช่น การมีเซิร์ฟเวอร์สำรอง การทำงานจากสถานที่อื่น

๕.๑.๔ Disaster Recovery Plan (DRP) แผนการกู้คืนระบบเทคโนโลยีสารสนเทศและข้อมูล

๕.๑.๕ Training & Testing การฝึกซ้อมและทดสอบแผนเป็นประจำเพื่อให้มั่นใจว่าแผนสามารถใช้งานได้จริง

## ๖. การจัดการเหตุการณ์ด้านความปลอดภัยและกรอบมาตรฐานสากล

๖.๑ การจัดการเหตุการณ์ด้านความปลอดภัยสามารถแบ่งออกเป็น ๓ ระดับตามความรุนแรงและผลกระทบ

๖.๑.๑ การจัดการเหตุการณ์ (Incident Management) เหตุการณ์เล็กๆ ที่สามารถควบคุมและแก้ไขได้ด้วยกระบวนการปกติ

๖.๑.๒ การจัดการภาวะฉุกเฉิน (Emergency Management) เหตุการณ์ที่มีความรุนแรงมากขึ้น ต้องมีการระดมทรัพยากรเพิ่มเติม และอาจกระทบความปลอดภัยของบุคลากรหรือการดำเนินงาน

๖.๑.๓ การจัดการภาวะวิกฤต (Crisis Management) เหตุการณ์รุนแรงขั้นสูงสุด มีผลกระทบต่อทั้งหน่วยงาน และอาจกระทบภาพลักษณ์ ความน่าเชื่อถือ กฎหมาย หรือการดำเนินงานของหน่วยงาน

## ๗. มาตรฐานสากลที่เกี่ยวข้อง

๗.๑ มาตรฐาน ISO ๒๒๓๐๑: ระบบจัดการความต่อเนื่องทางธุรกิจ ISO ๒๒๓๐๑ เป็นมาตรฐานสากลสำหรับระบบจัดการความต่อเนื่องทางธุรกิจ ที่ให้กรอบการทำงานที่เป็นระบบและมีประสิทธิภาพ

๗.๒ มาตรฐาน ISO ๒๗๐๐๕: การจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศ ISO ๒๗๐๐๕ เป็นมาตรฐานที่ให้แนวทางในการจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศ โดยมุ่งเน้นการระบุ ประเมิน และจัดการความเสี่ยงผ่านกระบวนการที่เป็นระบบ

## ๘. การบริหารความเสี่ยงด้านไซเบอร์

๘.๑ ผลกระทบ (Impact) ความเสียหายหรือผลกระทบที่อาจเกิดขึ้นต่อหน่วยงานหากเหตุการณ์เสี่ยงเกิดขึ้น

๘.๒ ความน่าจะเป็น (Likelihood) โอกาสหรือความถี่ที่เหตุการณ์เสี่ยงจะเกิดขึ้น

๘.๓ ภัยคุกคาม (Threat) อะไรก็ตามที่อาจก่อให้เกิดอันตรายหรือความเสียหายต่อทรัพย์สินหรือระบบ

๘.๔ ช่องโหว่ (Vulnerability) จุดอ่อนหรือข้อบกพร่องในระบบที่ภัยคุกคามสามารถใช้ประโยชน์ได้

## ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์กร

### ข้อสรุป

จากการศึกษาหลักการและแนวปฏิบัติด้านความปลอดภัยทางไซเบอร์ สามารถสรุปได้ว่า การรักษาความปลอดภัยข้อมูลในยุคดิจิทัลจำเป็นต้องมีการบูรณาการระหว่างเทคโนโลยี กระบวนการ และบุคลากรอย่างเป็นระบบ โดยหลัก CIA Triad ยังคงเป็นพื้นฐานสำคัญในการออกแบบระบบความปลอดภัย ขณะที่การจัดการ ความต่อเนื่องทางธุรกิจและการเตรียมพร้อมรับมือกับเหตุการณ์ไม่คาดคิดจะช่วยให้องค์กรสามารถดำเนินงาน ได้อย่างต่อเนื่องแม้ในสถานการณ์วิกฤต

### แนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์กร

๑. การพัฒนาแบบองค์รวม องค์กรควรนำหลักการความปลอดภัยทางไซเบอร์มาบูรณาการเข้ากับแผนยุทธศาสตร์องค์กร โดยไม่ถือเป็นเพียงเรื่องของหน่วยงาน IT เท่านั้น แต่เป็นความรับผิดชอบร่วมกัน ของทุกหน่วยงาน
๒. การสร้างวัฒนธรรมความปลอดภัย การพัฒนาความตระหนักรู้และสร้างวัฒนธรรมความปลอดภัยให้กับบุคลากรทุกระดับ ผ่านการฝึกอบรมอย่างต่อเนื่องและการสร้างแรงจูงใจในการปฏิบัติตามมาตรการความปลอดภัย
๓. การประยุกต์ใช้เทคโนโลยีที่เหมาะสม องค์กรควรเลือกใช้เทคโนโลยีและโซลูชันด้านความปลอดภัย ที่เหมาะสมกับบริบทและความต้องการขององค์กร โดยคำนึงถึงความคุ้มค่าการลงทุนและความเสี่ยงที่ยอมรับได้
๔. การพัฒนาขีดความสามารถในการตอบสนอง การจัดตั้งทีมตอบสนองต่อเหตุการณ์ด้านความปลอดภัย (Incident Response Team) และการฝึกซ้อมแผนรับมือกับสถานการณ์ต่างๆ อย่างสม่ำเสมอ เพื่อให้องค์กรสามารถรับมือกับภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพ
๕. การปรับปรุงและพัฒนาอย่างต่อเนื่อง การนำหลักการ PDCA (Plan-Do-Check-Act) มาใช้ใน การจัดการความปลอดภัยทางไซเบอร์ โดยมีการประเมินผล ปรับปรุง และพัฒนาระบบความปลอดภัยให้ทันต่อภัยคุกคามที่เปลี่ยนแปลงไปอย่างต่อเนื่อง

### ประโยชน์ที่ได้รับ

๑. มีความรู้ ความเข้าใจ เรื่อง Cybersecurity และ Cybersecurity Risk กระบวนการของ Cybersecurity Risk ความรู้เบื้องต้นของ Risk Assessment และ Risk Management แนวทางการ วางแผน ความต่อเนื่องทางธุรกิจ Business Continuity Planning (BCP)

# ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

สุทิน พันหิรัญ

ได้ผ่านการอบรมด้วยระบบการเรียนรู้ออนไลน์ในบทเรียน  
ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์  
(Understanding Cybersecurity Risk Management)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล  
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
ให้ ณ วันที่ 4 สิงหาคม 2569

*Ah.*

( นางไอรดา เหลืองวิไล )

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



# ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

สุทิน พันศิริบุญ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน  
การขับเคลื่อนด้วยข้อมูลสู่การเป็นรัฐบาลดิจิทัล  
(Data Driven Digital Government Transformation)

จำนวนชั่วโมงการเรียนรู้ 2:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล  
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
ให้ ณ วันที่ 4 สิงหาคม 2569

*A. L.*

( นางไอรดา เหลืองวิไล )

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



0576c034

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)  
Digital Government Development Agency (Public  
Organization) (DGA)  
Date: 2026-08-04T16:18:35.451+07:00