แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๑/๒๕๖๙ ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ – ๓๑ มีนาคม ๒๕๖๙
ประจำปีงบประมาณ พ.ศ.๒๕๖๙

ชื่อ-นามสกุล นางสาวชลธิชา เมฆโสภณ **ตำแหน่ง** เจ้าพนักงานธุรการชำนาญงาน
หน่วยงาน สถานีพัฒนาที่ดินฉะเชิงเทรา
หัวข้อการพัฒนา การรักษาความปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี
วิธีการพัฒนา OCSC Learning Portal ศูนย์การเรียนรู้ทางสื่ออิเล็กทรอนิกส์แบบบูรณาการ
วันที่พัฒนา ๑๖ กุมภาพันธ์ ๒๕๖๙ **สถานที่** ออนไลน์
หน่วยงานที่จัดอบรม สำนักงานคณะกรรมการข้าราชการพลเรือน
วัตถุประสงค์

๑. เพื่อให้มีความเข้าใจและตระหนักรู้ถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์
๒. เพื่อให้มีการเตรียมความพร้อมในการปฏิบัติงานทางด้านความปลอดภัยทางไซเบอร์
๓. เพื่อให้สามารถประยุกต์ใช้เทคโนโลยีในกระบวนการทำงาน เพื่อลดขั้นตอนและเพิ่มประสิทธิภาพในการทำงาน

สรุปสาระสำคัญ

การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เป็นรากฐานสำคัญของการบริหารจัดการระบบสารสนเทศภาครัฐ เนื่องจากหน่วยงานรัฐมีการจัดเก็บและประมวลผลข้อมูลสำคัญจำนวนมาก เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน และข้อมูลเชิงนโยบาย ในยุคดิจิทัล หน่วยงานภาครัฐมีการใช้เทคโนโลยีสารสนเทศในการดำเนินงานอย่างกว้างขวาง ส่งผลให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น การโจมตีทางไซเบอร์สามารถก่อให้เกิดความเสียหายต่อข้อมูล ระบบ และความเชื่อมั่นของประชาชน ดังนั้น ผู้ปฏิบัติงานด้านเทคโนโลยีจำเป็นต้องมีความรู้และความเข้าใจด้าน Cybersecurity อย่างถูกต้องและเป็นระบบ

หลักการพื้นฐานของความมั่นคงปลอดภัยไซเบอร์

หลัก CIA Triad

หลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศประกอบด้วย ๓ องค์ประกอบ ได้แก่
Confidentiality (ความลับ) : การป้องกันไม่ให้ข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต
Integrity (ความถูกต้องครบถ้วน) : การทำให้มั่นใจว่าข้อมูลไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต
Availability (ความพร้อมใช้งาน) : การทำให้ระบบและข้อมูลสามารถใช้งานได้เมื่อจำเป็น

แนวคิดด้านความเสี่ยง

Threat (ภัยคุกคาม) : สิ่งที่อาจก่อให้เกิดอันตราย เช่น แฮกเกอร์ มัลแวร์
Vulnerability (ช่องโหว่) : จุดอ่อนในระบบที่อาจถูกโจมตี
Risk (ความเสี่ยง) : โอกาสที่ภัยคุกคามจะใช้ช่องโหว่และก่อให้เกิดผลกระทบ
Impact (ผลกระทบ) : ความเสียหายที่เกิดขึ้นจากเหตุการณ์

ภัยคุกคามและรูปแบบการโจมตี

มัลแวร์ (Malware) มัลแวร์เป็นซอฟต์แวร์ประสงค์ร้ายที่ออกแบบมาเพื่อทำลาย ขโมย หรือเข้าควบคุมระบบคอมพิวเตอร์ เช่น Virus ต้องอาศัยไฟลหรือโปรแกรมอื่นในการแพร่กระจาย, Worm แพร่กระจายตัวเองผ่านเครือข่ายได้โดยอัตโนมัติ, Trojan Horse แผงตัวมากับโปรแกรมที่ดูปลอดภัยเพื่อหลอกให้ติดตั้ง, Ransomware เข้ารหัสไฟล์และเรียกค่าไถ่เพื่อแลกกับการถอดรหัส และ Spyware แอบเก็บข้อมูลผู้ใช้

Social Engineering เป็นการใช้เทคนิคทางจิตวิทยาหลอกล่อเหยื่อ เช่น Phishing หลอกผ่านอีเมล์, Spear Phishing เจาะจงเป้าหมาย, Vishing หลอกผ่านโทรศัพท์ และ Whaling เจาะจงผู้บริหารระดับสูง

การโจมตีรูปแบบอื่น เช่น Brute-force Attack เดารหัสผ่าน, Dictionary Attack ใช้ชุดคำศัพท์เดารหัส, Distributed Denial of Service (DDoS) ทำให้ระบบล่ม (กระทบ Availability) และ Zero-Day Exploit ใช้ช่องโหว่ที่ยังไม่มี Patch แก้ไข

เทคโนโลยีและมาตรการป้องกัน

๑. มาตรการด้านเครือข่าย

Firewall ระบบที่ควบคุมและกรองการรับส่งข้อมูลตามกฎที่กำหนด

Intrusion Detection System (IDS) ระบบที่ตรวจจับและป้องกันการโจมตีโดยอัตโนมัติ

Intrusion Prevention System (IPS) ระบบที่ตรวจจับและป้องกันการโจมตีโดยอัตโนมัติ

Virtual Private Network (VPN) เทคโนโลยีที่เข้ารหัสการสื่อสารผ่าน Public Network

Web Application Firewall (WAF) ระบบป้องกันการโจมตีที่มุ่งเป้าไปยังเว็บแอปพลิเคชัน

๒. การปกป้องข้อมูล

Encryption เพื่อรักษาความลับ

Hashing เพื่อตรวจสอบความถูกต้อง

Multi-Factor Authentication (MFA) เพิ่มความปลอดภัยการยืนยันตัวตน

Data Loss Prevention (DLP) เทคโนโลยีป้องกันข้อมูลรั่วไหล

๓. การเฝ้าระวังและตอบสนอง

Security Information and Event Management (SIEM) ระบบรวบรวมและวิเคราะห์ Log จากหลายแหล่งเพื่อเฝ้าระวังเหตุการณ์

Endpoint Detection and Response (EDR) ตรวจจับและตอบสนองที่เครื่องปลายทาง

การบริหารจัดการและการควบคุมความมั่นคงปลอดภัย

๑. Secure Configuration

ปิดบริการและพอร์ตที่ไม่จำเป็น

เปลี่ยนรหัสผ่านเริ่มต้น

ใช้หลัก Least Privilege

๒. Patch Management

การติดตั้งแพตช์เพื่อแก้ไขช่องโหว่ที่ถูกค้นพบใหม่ ลดความเสี่ยงจากการถูกโจมตี

๓. การสำรองข้อมูล (Backup)

การสำรองข้อมูลอย่างสม่ำเสมอช่วยลดผลกระทบจาก Ransomware และเหตุการณ์สูญหายของข้อมูล

แผนและนโยบายที่เกี่ยวข้อง

Acceptable Use Policy (AUP) นโยบายกำหนดแนวทางการใช้งานทรัพยากร IT ขององค์กร

Incident Response Plan (IRP) แผนรับมือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

Disaster Recovery Plan (DRP) แผนกู้คืนระบบหลังเกิดเหตุร้ายแรง

Business Continuity Plan (BCP) แผนดำเนินธุรกิจต่อเนื่องในสถานการณ์วิกฤต

Password Policy นโยบายรหัสผ่าน

แผนเหล่านี้ช่วยให้องค์กรสามารถตอบสนองต่อเหตุการณ์และดำเนินงานต่อได้อย่างต่อเนื่อง

กฎหมายและข้อกำหนดที่เกี่ยวข้อง

หน่วยงานภาครัฐต้องปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของภาครัฐ

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. มีความเข้าใจในหลักการพื้นฐานของ Cybersecurity

๒. สามารถระบุภัยคุกคาม วิเคราะห์ความเสี่ยง และเลือกใช้มาตรการป้องกันที่เหมาะสมได้อย่างมีประสิทธิภาพ

๓. สามารถนำหลักการไปประยุกต์ใช้จะสามารถลดความเสี่ยงด้านไซเบอร์ และยกระดับความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างยั่งยืน

(นางสาวชลธิชา เมฆโสภณ)
เจ้าพนักงานธุรการชำนาญงาน

(นายบุญสม พรหมสุวรรณ์)
ผู้อำนวยการสถานีพัฒนาที่ดินฉะเชิงเทรา

สำนักงานคณะกรรมการ
ดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

สำนักงานคณะกรรมการข้าราชการพลเรือน

ร่วมกับ

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

ขอมอบประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

นางสาวชลธิชา เมฆโสภณ

ได้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์

วิชา การรักษาความปลอดภัยไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยี
(Cybersecurity Principle for Technology Practitioners)

(รวมระยะเวลาทั้งสิ้น 2 ชั่วโมง)

ให้ไว้ ณ วันที่ 17 กุมภาพันธ์ พ.ศ. 2569

(นายปิยวัฒน์ ศิวรักษ์)
เลขาธิการคณะกรรมการข้าราชการพลเรือน

(นายเวทางค์ พ่วงทรัพย์)
เลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

CERTIFICATE
OCSC
Learning Space

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

– ชลธิชา เมฆโสภณ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 24 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-24T18:34:35.601+07:00

e22e6e0e

CYBERSECURITY

สำหรับผู้ปฏิบัติงานด้านเทคโนโลยีภาครัฐ

ผู้สรุป: นางสาวชลธิา เมฆโสภณ | สถานีพัฒนาที่ดินฉะเชิงเทรา สพข.2 | วันที่ 16 กุมภาพันธ์ 2569

ทำไม Cybersecurity สำคัญ?

- หน่วยงานรัฐจัดเก็บข้อมูลสำคัญจำนวนมาก
- เสี่ยงต่อการโจมตีทางไซเบอร์
- ส่งผลกระทบต่อข้อมูล ระบบ และความเชื่อมั่นประชาชน

หลักการพื้นฐาน (CIA Triad)

Confidentiality
- ปกป้องข้อมูลลับ

Integrity
- ข้อมูลถูกต้องครบถ้วน

Availability
- ระบบพร้อมใช้งาน

แนวคิดด้านความเสี่ยง

- **Threat** = ภัยคุกคาม
- **Vulnerability** = ช่องโหว่
- **Risk** = โอกาสเกิดความเสียหาย

Malware
- Virus
- Worm
- Trojan
- Ransomware

Social Engineering
- Phishing
- Spear Phishing
- Vishing

ภัยคุกคามอื่น ๆ
- Brute-force
- DDoS
- Zero-Day

เทคโนโลยีและมาตรการป้องกัน

ด้านเครือข่าย
- Firewall
- IDS / IPS
- VPN
- WAF

ปกป้องข้อมูล
- Encryption
- MFA
- DLP

เฝ้าระวัง
- SIEM
- EDR

มาตรการเชิงปฏิบัติ
- กำหนดค่าการเข้าถึง
- การจัดการแพตช์
- การสำรองข้อมูล

ประโยชน์ที่ได้รับ
- ☑ เข้าใจหลัก **Cybersecurity**
- ☑ วิเคราะห์ความเสี่ยงได้
- ☑ เลือกใช้มาตรการป้องกันเหมาะสม
- ☑ ลดความเสี่ยงด้านไซเบอร์อย่างยั่งยืน