

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ.....นางสาวอัจฉรี.....นามสกุล.....สิงห์โต.....

ตำแหน่ง.....นักวิชาการเกษตรชำนาญการ.....กลุ่ม/ฝ่าย.....วางแผนการจัดการที่ดินในพื้นที่เสี่ยงภัยทางการเกษตร.....

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้.....พัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น...

สถานที่อบรม/สัมมนา/พัฒนาความรู้.....การเรียนรู้ผ่านระบบอิเล็กทรอนิกส์ (e-Learning)

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้.....สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล.....

ตั้งแต่วันที่.....๒๖.....เดือน.....พฤษภาคม.....พ.ศ.๒๕๖๔....

ถึงวันที่.....๒๖.....เดือน.....พฤษภาคม.....พ.ศ.๒๕๖๔....

เพื่อ ☐ อบรม ☐ สัมมนา ☒ อื่นๆ ระบุ.....การเรียนรู้ผ่านสื่ออิเล็กทรอนิกส์.....

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

ในปัจจุบันเทคโนโลยีสารสนเทศและระบบเครือข่ายมีบทบาทสำคัญต่อการดำเนินงานของหน่วยงานทั้งภาครัฐ ภาคเอกชน และการใช้ชีวิตประจำวันของประชาชน การใช้งานอินเทอร์เน็ต การเก็บข้อมูลบนระบบดิจิทัล และการเชื่อมต่ออุปกรณ์ต่าง ๆ ผ่านเครือข่าย ทำให้เกิดความสะดวกและเพิ่มประสิทธิภาพในการทำงาน อย่างไรก็ตาม การพัฒนาเทคโนโลยีดังกล่าวก็มาพร้อมกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในด้านความรุนแรงและความซับซ้อน ดังนั้น การรักษาความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นสิ่งสำคัญที่ทุกองค์กรจำเป็นต้องให้ความสำคัญ และสามารถแยกตามหัวข้อดังนี้

๑. แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นกระบวนการและมาตรการที่องค์กรนำมาใช้เพื่อปกป้องข้อมูล ระบบเครือข่าย และอุปกรณ์สารสนเทศจากภัยคุกคามต่าง ๆ โดยมีเป้าหมายสำคัญในการรักษาองค์ประกอบหลัก ๓ ประการ ได้แก่

๑.๑ ความลับของข้อมูล (Confidentiality) ข้อมูลต้องถูกเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๑.๒ ความถูกต้องครบถ้วนของข้อมูล (Integrity) ข้อมูลต้องไม่ถูกแก้ไข เปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต

๑.๓ ความพร้อมใช้งานของระบบ (Availability) ระบบและข้อมูลต้องสามารถใช้งานได้เมื่อมีความจำเป็น

องค์กรควรกำหนดนโยบายด้านความปลอดภัยทางไซเบอร์อย่างชัดเจน รวมถึงกำหนดสิทธิ์การเข้าถึงข้อมูล การใช้งานรหัสผ่านที่ปลอดภัย การสำรองข้อมูล และการฝึกอบรมบุคลากรให้มีความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อช่วยลดความเสี่ยงที่อาจเกิดขึ้นจากความผิดพลาดของผู้ใช้งาน

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) การประเมินความเสี่ยงเป็นกระบวนการสำคัญที่ช่วยให้องค์กรสามารถวิเคราะห์และประเมินความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศและข้อมูลสำคัญ โดยมีวัตถุประสงค์เพื่อค้นหาจุดอ่อน วิเคราะห์โอกาสเกิดภัยคุกคาม และกำหนดแนวทางในการลดความเสี่ยงอย่างเหมาะสม

ขั้นตอนสำคัญของการประเมินความเสี่ยง ประกอบด้วย

๒.๑ การระบุทรัพย์สินสารสนเทศ เช่น ฐานข้อมูล ระบบเครือข่าย หรืออุปกรณ์คอมพิวเตอร์

๒.๒ การระบุภัยคุกคามที่อาจเกิดขึ้น เช่น การโจมตีจากแฮกเกอร์ หรือมัลแวร์

๒.๓ การวิเคราะห์ช่องโหว่ของระบบ

✓

๒.๔ การประเมินระดับความเสี่ยงและผลกระทบ

๒.๕ การกำหนดมาตรการควบคุมและป้องกัน

การประเมินความเสี่ยงช่วยให้องค์กรสามารถจัดลำดับความสำคัญของปัญหา และวางแผนบริหารจัดการความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น

๓. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework) กรอบมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นแนวทางที่ช่วยให้องค์กรสามารถบริหารจัดการความปลอดภัยได้อย่างเป็นระบบและมีมาตรฐานสากล โดยหนึ่งในกรอบมาตรฐานที่ได้รับความนิยมคือ NIST Cybersecurity Framework ซึ่งแบ่งกระบวนการออกเป็น ๕ ด้านหลัก ได้แก่

๓.๑ Identify (การระบุความเสี่ยงและทรัพย์สิน) คือ ขั้นตอนแรกของกรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีวัตถุประสงค์เพื่อให้องค์กรทราบว่า “สิ่งใดสำคัญ” และ “มีความเสี่ยงอะไรบ้าง” ที่อาจส่งผลกระทบต่อระบบสารสนเทศ ข้อมูล และการดำเนินงานขององค์กร

๓.๒ Protect (การป้องกันความเสี่ยง) คือ ขั้นตอนในกรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มุ่งเน้นการกำหนดมาตรการเพื่อป้องกันและลดโอกาสการเกิดภัยคุกคามทางไซเบอร์ รวมถึงลดผลกระทบที่อาจเกิดขึ้นต่อข้อมูล ระบบ เครือข่าย และทรัพยากรสารสนเทศขององค์กร

๓.๓ Detect (การตรวจจับภัยคุกคาม) ขั้นตอนในกรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มุ่งเน้นการตรวจสอบ เฝ้าระวัง และค้นหาความผิดปกติหรือภัยคุกคามที่เกิดขึ้นกับระบบสารสนเทศและเครือข่ายขององค์กร เพื่อให้สามารถตรวจพบเหตุการณ์ได้อย่างรวดเร็วและลดความเสียหายที่อาจเกิดขึ้น

๓.๔ Respond (การตอบสนองต่อเหตุการณ์) คือ ขั้นตอนในกรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับการดำเนินการเมื่อเกิดเหตุการณ์หรือภัยคุกคามทางไซเบอร์ขึ้น เพื่อควบคุมสถานการณ์ ลดความเสียหาย และแก้ไขปัญหาให้ระบบสามารถกลับมาดำเนินงานได้อย่างปลอดภัย

๓.๕ Recover (การฟื้นฟูระบบหลังเกิดเหตุ) คือ ขั้นตอนในกรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มุ่งเน้นการกู้คืนระบบ ข้อมูล และการดำเนินงานขององค์กรให้กลับมาใช้งานได้ตามปกติ หลังจากเกิดเหตุการณ์หรือภัยคุกคามทางไซเบอร์

๔. การป้องกันความเสี่ยง (Protect) การป้องกันความเสี่ยงเป็นมาตรการสำคัญที่ช่วยลดโอกาสในการเกิดภัยคุกคามทางไซเบอร์ โดยองค์กรควรดำเนินมาตรการด้านเทคนิคและด้านบริหารจัดการควบคู่กันไป ตัวอย่างมาตรการป้องกัน ได้แก่

๔.๑ การติดตั้งโปรแกรมป้องกันไวรัสและมัลแวร์

๔.๒ การใช้ Firewall เพื่อควบคุมการเข้าถึงเครือข่าย

๔.๓ การเข้ารหัสข้อมูลสำคัญ

๔.๔ การกำหนดสิทธิ์ผู้ใช้งานตามระดับหน้าที่

๔.๕ การอัปเดตระบบและซอฟต์แวร์อย่างสม่ำเสมอ

๔.๖ การสำรองข้อมูลเพื่อป้องกันการสูญหาย

๔.๗ การสร้างความตระหนักรู้ด้านไซเบอร์ให้กับบุคลากร

การป้องกันที่ดีจะช่วยลดโอกาสที่องค์กรจะตกเป็นเป้าหมายของการโจมตีทางไซเบอร์ และช่วยลดความเสียหายที่อาจเกิดขึ้นได้อย่างมาก

๕. การประเมินช่องโหว่ (Vulnerability Assessment) การประเมินช่องโหว่เป็นกระบวนการตรวจสอบระบบ

คอมพิวเตอร์ เครือข่าย และแอปพลิเคชัน เพื่อค้นหาจุดอ่อนที่อาจถูกผู้ไม่หวังดีใช้เป็นช่องทางในการโจมตีระบบ การประเมินช่องโหว่อาจดำเนินการโดยใช้เครื่องมือสแกนช่องโหว่อัตโนมัติ หรือการตรวจสอบโดยผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ ซึ่งผลการตรวจสอบจะช่วยให้องค์กรทราบถึงจุดอ่อนของระบบ และสามารถดำเนินการแก้ไขได้อย่างเหมาะสม ตัวอย่างช่องโหว่ที่พบได้บ่อย ได้แก่

๕.๑ การใช้รหัสผ่านที่ไม่ปลอดภัย

๕.๒ ซอฟต์แวร์ที่ไม่ได้อัปเดต

๕.๓ การตั้งค่าระบบที่ไม่เหมาะสม

๕.๔ การเปิดพอร์ตหรือบริการที่ไม่จำเป็น

การประเมินช่องโหว่เป็นกระบวนการที่ควรดำเนินการอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้อุปกรณ์กลายเป็นสาเหตุของการถูกโจมตีทางไซเบอร์

๖. การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) การตรวจสอบและเฝ้าระวังภัยคุกคามเป็นกระบวนการติดตาม วิเคราะห์ และตรวจจับพฤติกรรมที่ผิดปกติในระบบเครือข่ายและระบบสารสนเทศ เพื่อให้สามารถค้นพบเหตุการณ์ผิดปกติได้อย่างรวดเร็ว องค์กรอาจใช้เครื่องมือและเทคโนโลยีต่าง ๆ เช่น

๖.๑ ระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS)

๖.๒ ระบบป้องกันการบุกรุก (IPS)

๖.๓ ระบบเฝ้าระวังเครือข่าย

๖.๔ การวิเคราะห์ Log หรือบันทึกเหตุการณ์

๖.๕ ระบบแจ้งเตือนภัยอัตโนมัติ

การเฝ้าระวังที่มีประสิทธิภาพช่วยให้องค์กรสามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว ลดความเสียหาย และป้องกันการลุกลามของปัญหาไปยังระบบอื่น

๗. การเผชิญเหตุภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ องค์กรจำเป็นต้องมีแผนรับมือเหตุการณ์ (Incident Response Plan)

เพื่อดำเนินการแก้ไขปัญหาอย่างรวดเร็วและลดผลกระทบที่อาจเกิดขึ้น ขั้นตอนสำคัญในการตอบสนองต่อเหตุการณ์ ได้แก่

๗.๑ การตรวจสอบและยืนยันเหตุการณ์

๗.๒ การควบคุมและจำกัดความเสียหาย

๗.๓ การแยกระบบที่ได้รับผลกระทบ

๗.๔ การวิเคราะห์สาเหตุของเหตุการณ์

๗.๕ การแก้ไขและป้องกันไม่ให้เกิดเหตุซ้ำ

หลังจากควบคุมสถานการณ์แล้ว องค์กรต้องดำเนินการฟื้นฟูระบบและข้อมูลให้กลับมาใช้งานได้ตามปกติ เช่น การกู้คืนข้อมูลจากระบบสำรอง การตรวจสอบความสมบูรณ์ของระบบ และการปรับปรุงมาตรการด้านความปลอดภัยเพิ่มเติม

๒.๒ ประสบการณ์/ประโยชน์ที่ได้รับ/การประยุกต์ใช้กับหน่วยงาน

☒ ต่อตนเอง

๑. การมีระบบรักษาความปลอดภัยที่ดีช่วยสร้างความมั่นใจให้แก่ประชาชน ลูกค้า หรือหน่วยงานที่เกี่ยวข้องว่าข้อมูลและบริการขององค์กรมีความปลอดภัยและน่าเชื่อถือ

๒. การบริหารจัดการด้านไซเบอร์อย่างเป็นระบบช่วยให้องค์กรสามารถตรวจสอบ วิเคราะห์ และจัดการปัญหาได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น

☒ ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน

๑. จัดให้มีการสำรองข้อมูลสำคัญอย่างสม่ำเสมอ และจัดทำแผนกู้คืนระบบเมื่อเกิดเหตุการณ์ฉุกเฉิน เพื่อให้สามารถกลับมาดำเนินงานได้อย่างรวดเร็ว

๒. ส่งเสริมให้บุคลากรมีความรู้ด้านความปลอดภัยไซเบอร์

๓. หน่วยงานสามารถนำแนวทาง Identify, Protect, Detect, Respond และ Recover มาประยุกต์ใช้

เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์มีความเป็นระบบและมีประสิทธิภาพมากยิ่งขึ้น

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

๒.๔.๑ ควรมีการยกตัวอย่างเหตุการณ์จริงเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ผู้เรียนเห็นภาพและเข้าใจผลกระทบ

ที่อาจเกิดขึ้นกับองค์กรได้ชัดเจนมากยิ่งขึ้น

๒.๔.๒ ควรปรับเนื้อหาให้สอดคล้องกับสถานการณ์ภัยคุกคามทางไซเบอร์ในปัจจุบัน เนื่องจากรูปแบบการโจมตีมีการเปลี่ยนแปลง และพัฒนาอยู่ตลอดเวลา



(นางสาวอัจฉรี สิงห์โต)

นักวิชาการเกษตรชำนาญการ

ผู้รายงาน

วันที่ ๕ เดือน มิถุนายน พ.ศ. ๒๕๖๙..

ส่วนที่ ๓ ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....
.....
.....



ลงชื่อ.....

(นาย นันทพล หนองทรพิทักษ์)

ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

ตำแหน่ง.....

วันที่ ๑๗ มิ.ย. ๒๕๖๙ พ.ศ.....

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

อัจฉรี สิงห์โต

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนากิจกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 28 พฤษภาคม 2569

A.L.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

ศิริมาลฤกษ์
จิรณัฐ สิงห์โต



Signed by: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพง.)
Date: 2026-05-28T14:06:40.193+07:00

Za2ef297

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

อัจฉรี สิงห์โต

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
หลักสูตรทักษะเอไอระดับพื้นฐาน (AI Basics)

จำนวนชั่วโมงการเรียนรู้ 2:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 28 พฤษภาคม 2569

A.L.

นางสาวกนกพร
อัจฉรี สิงห์โต

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (กกปร.)
Date: 2026-05-28T14:36:31+07:00
bb655f49