แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินพิจิตร

ด้วย นายกีรติกร ฤทธิเกรียง ตำแหน่ง นักวิชาการเกษตรชำนาญการ สังกัด สถานีพัฒนาที่ดินพิจิตร สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร พัฒนาทักษะความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น ในวันที่ ๑๐ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ วัน ณ สถานีพัฒนาที่ดินพิจิตร ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์

๑.๑ สร้างความตระหนักรู้ด้านไซเบอร์ (Cybersecurity Awareness) ให้เข้าใจความสำคัญ และผลกระทบของภัยคุกคามทางไซเบอร์ที่มีต่อตนเองและองค์กร

๑.๒ พัฒนาทักษะการใช้งานอย่างปลอดภัย สามารถใช้อุปกรณ์และเครือข่ายเทคโนโลยีได้อย่างปลอดภัย รวมถึงป้องกันและแก้ไขปัญหาเบื้องต้นได้

๑.๓ เข้าใจแนวทางการบริหารความเสี่ยง (Risk Management) ทำให้สามารถประเมินความเสี่ยงและช่องโหว่ (Vulnerability) ของระบบเพื่อเตรียมความพร้อมรับมือ

๑.๔ เข้าใจกฎหมายและกรอบมาตรฐานของ พ.ร.บ. ไซเบอร์ และมาตรฐานความมั่งคงปลอดภัยขั้นต่ำที่จำเป็น

๑.๕ รับมือและฟื้นฟูเบื้องต้น ทำให้เข้าใจกระบวนการตรวจจับ (Detect) ตอบสนอง (Respond) และฟื้นฟู (Recover) เมื่อเกิดเหตุภัยคุกคาม

๒. เนื้อหาและหัวข้อวิชา

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีวิธีการปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่ายโครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ปัจจุบันหน่วยงานภาครัฐ และเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมาย และรูปแบบในการโจมตีมีหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

๒.๑ กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

๒.๒.๑ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒.๒.๒ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๒.๒.๓ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

๒.๒.๔ มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ ระบบบริหารจัดการความปลอดภัยของข้อมูล

๒.๒ หลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

๒.๒.๑ Confidentiality (C) หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้น ความลับที่กำหนดไว้ เช่น ข้อมูลเงินเดือน ของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วน ทรัพยากรบุคคลเท่านั้น

๒.๒.๒ Intergrity (I) หรือ การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร

๒.๒.๓ - Availability (A) หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลธนาคารด้านการเงินข้อมูลบัญชีธนาคาร

๒.๓ รูปแบบภัยคุกคามของ Cybersecurity

๒.๓.๑ Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบ ต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึง Server ต่าง ๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา เช่น ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

๒.๓.๒ Wed-based attacks คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว จะนำเหยื่อไปที่เป้าหมายปลายทาง ที่เป็นเว็บที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๒.๓.๓ Phishing คือ วิธีการโจมตีเหยื่อหาช่องทางต่าง ๆ เช่น E-mail, SMS เว็บไซต์ หรือช่องทาง Social โดยใช้หลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น username, Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๒.๓.๔ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ

๒.๓.๕ Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูลข้อความหรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

๒.๓.๖ DDos คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่อง โจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๒.๓.๗ Data breach คือ เกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของ Application หรือระบบที่ทำให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๒.๓.๘ Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ หากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้นซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกันนำหลักการ Zero Trust มาใช้ภายในองค์กร

๒.๓.๙ Botnet หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการอย่างที่ถูกโปรแกรมไว้ ส่วนมากจะแฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets ที่ไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๒.๓.๑๐ Ransomware คือ Walware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้ว จะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าถ่ายของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๒.๓.๑๑ Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำ การติดตั้งโปรแกรมที่ใช้ในการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อตามประเมินผลเพื่อสร้างรายได้กลับไปที่ Hacke

๒.๔ มองการณ์ไกลและมีวิสัยทัศน์ดิจิทัล ผู้นำต้องมองเห็นโอกาสและความเสี่ยงจากเทคโนโลยีใหม่ ๆ พร้อมกำหนดทิศทางองค์กรให้สอดคล้องกับแนวโน้มในอนาคต

๓. ประโยชน์ที่ได้รับ

๓.๑ เข้าใจพื้นฐานความปลอดภัยทางไซเบอร์และสามารถระบุภัยคุกคามเบื้องต้นได้

๓.๒ ลดความเสี่ยงจากการโจมตีทางไซเบอร์ทั้งระดับบุคคลและองค์กร

๓.๓ มีความรู้เรื่องกฎหมายและจริยธรรมที่เกี่ยวข้องมาใช้ในการทำงานด้านไซเบอร์

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน สามารถนำความตระหนักรู้และทักษะการป้องกันภัยคุกคามทางไซเบอร์พื้นฐาน เช่น การโจมตีเว็บไซต์ การจัดการรหัสผ่าน และความปลอดภัยของเครือข่าย ไปปรับใช้ในการป้องกันข้อมูลขององค์กรและข้อมูลส่วนบุคคล และปฏิบัติตามกฎหมาย PDPA พ.ร.บ. ไซเบอร์ และรับมือภัยคุกคามในชีวิตประจำวัน

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา ให้ผู้บังคับบัญชาช่วยให้คำแนะนำและสนับสนุนงบประมาณในการอบรมเกี่ยวกับการพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อนำทักษะมาประยุกต์ใช้ได้จริงและเพื่อยกระดับศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานให้ทันสมัยและเป็นที่ยอมรับ

(นายกีรติกร ฤทธิเกรียง)
นักวิชาการเกษตรชำนาญการ

(นายมนตชัย พรมลอองวัน)
ผู้อำนวยการสถานีพัฒนาที่ดินพิจิตร

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

กีรติกร ฤทธิเกรียง

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 10 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (เกษร)
Date: 2026-02-10T14:02:25.235+07:00

37925f11

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

กีรติกร ฤทธิเกรียง

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ปฏิบัติงานภาครัฐ

(PDPA for Government Officer)

จำนวนชั่วโมงการเรียนรู้ 2:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 10 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
Date: 2026-02-10T14:04:02.144+07:00

99a859c4