บันทึกข้อความ

ส่วนราชการ สถานีพัฒนาที่ดินกรุงเทพมหานคร สำนักงานพัฒนาที่ดินเขต ๑ โทร. ๐ ๒๔๕๓ ๒๒๑๗

ที่ กษ ๐๘๐๘.๑๙/ ๑๕๖ **วันที่** ๑๓ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอส่งสรุปผลการพัฒนาความรู้ของข้าราชการรอบการประเมินที่ ๑/๒๕๖๙

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินกรุงเทพมหานคร

ตามที่ กรมพัฒนาที่ดิน ให้บุคลากรภายในหน่วยงานของกรมพัฒนาที่ดินทั้งส่วนกลาง และส่วนภูมิภาค พัฒนาทักษะด้านดิจิทัล โดยเรียนรู้ผ่านสื่อออนไลน์TDGA E-learning เพื่อประเมินผลการพัฒนาความรู้ของบุคลากรประจำปีงบประมาณ พ.ศ.๒๕๖๙ รอบที่ ๑ระหว่างวันที่ ๑ ตุลาคม ๒๕๖๘ – ๓๑ มีนาคม ๒๕๖๙ และรอบที่ ๒ ระหว่างวันที่ ๑ เมษายน - ๓๐ กันยายน ๒๕๖๙ โดยมีวัตถุประสงค์เพื่อเป็นเครื่องมือในการพัฒนาทักษะด้านดิจิทัลของบุคลากรกรมพัฒนาที่ดิน ให้มีความรู้ความเข้าใจ และนำความรู้ที่ได้ไปประยุกต์กับการปฏิบัติงาน นั้น

บัดนี้ กระผมได้ทำการเรียนรู้ผ่านสื่อการเรียนการสอน จำนวน ๒ หลักสูตร ได้แก่ การเรียนรู้ผ่านสื่อออนไลน์ TDGA E-learning หลักสูตร “หลักการสร้างภาพข้อมูลและการออกแบบแดชบอร์ดอย่างมีประสิทธิภาพ” (The Principle of Data Visualization and Dashboard Design) และการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) โดยสถาบันพัฒนาบุคคลากรภาครัฐด้านดิจิทัลเรียบร้อยแล้ว จึงขอส่งแบบรายงานสรุปผลการพัฒนาความรู้ของข้าราชการ จำนวน ๑ หลักสูตร “การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์” (Cybersecurity Awareness) พร้อมแนบหลักฐานผ่านเรียนรู้ผ่านสื่อออนไลน์ TDGA E-learning ทั้ง ๒ หลักสูตรดังกล่าวมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

(นายกฤษฎา จงดี)
เจ้าพนักงานการเกษตรปฏิบัติงาน

(นางสาวนัทฐา ทักษ์รัตนศรัณย์)
ผู้อำนวยการสถานีพัฒนาที่ดินกรุงเทพมหานคร

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ กฤษฎา จงดี

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

หลักการสร้างภาพข้อมูลและการออกแบบแดชบอร์ดอย่างมีประสิทธิภาพ

(The Principle of Data Visualization and Dashboard Design)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 2 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

90d856b8

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-02T13:16:34.510+07:00

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ กฤษฎา จงดี

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 9 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

8991d6a2

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (DPA)
Date: 2026-02-09T13:25:56.681+07:00

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

ชื่อ-นามสกุล นายกฤษฎา จงดี **ตำแหน่ง** เจ้าพนักงานการเกษตรปฏิบัติงาน .
กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินกรุงเทพมหานคร สำนักงานพัฒนาที่ดินเขต ๑ .
หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) .
สถานที่ TDGA E-learning **วันที่** ๙ กุมภาพันธ์ ๒๕๖๙ .
วิทยากร/ผู้ให้ความรู้ คุณพลากร ลาภอลงกรณ์ ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) .

หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy.

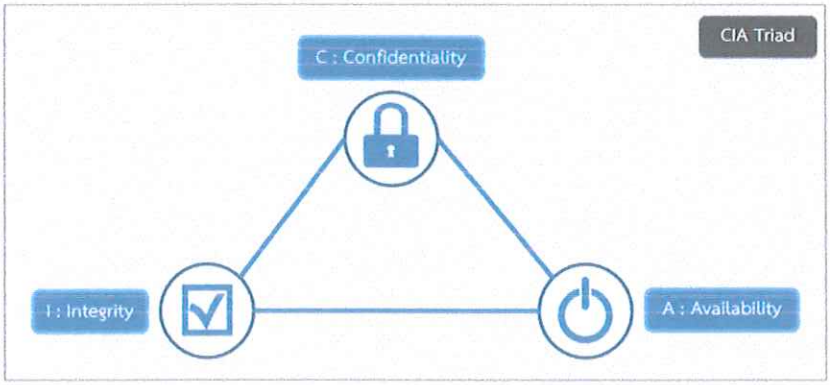
สรุปสาระสำคัญของเนื้อหา

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์คือ การนำเครื่องมือทางด้านเทคโนโลยี วิธีการ ปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่สามารถโดยไม่ได้รับอนุญาต

ปัจจุบันหน่วยงานภาครัฐ และเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมาย และรูปแบบในการโจมตีมีหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

• ข้อมูลส่วนเงินเดือนของพนักงานในบริษัทจัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

• เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการ ให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ CyberSecurity

- Malware
- Web-based attacks
- Phishing
- Web application attacks
- Spam
- DDoS
- Data breach
- Insider threat
- Botnets
- Ransomware
- Cryptojacking

๑. Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบ ต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึง ทรัพยากรของระบบคอมพิวเตอร์ และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึง Server ต่างๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา เช่น ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

๒. Wed-based attacks คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อ แก้ไขเว็บไซต์ โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๓. Phishing คือวิธีการโจมตีเหยื่อหาช่องทางต่างๆ เช่น E-mail, SMS เว็บไซต์หรือช่องทาง Social โดย ใช้หลอกล่อเหยื่อด้วยวิธีการต่างๆที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น username, Password หรือข้อมูลสำคัญอื่นๆเพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔. Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น cms
- Web Server หรือ database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site pcripting
- SQL injection

๕. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูลข้อความหรือโฆษณาต่างๆ

ผ่านช่องทาง ต่างๆ ไปยังผู้รับ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

๖. DDos คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์,ระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่อง โจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์,ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๗. Data breach คือเกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของ เว็บไซต์, ข้อมูลของ Application หรือระบบที่ทำให้บริการต่างๆโดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัวหรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘. Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ ตั้งใจหากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้นซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกันนำหลักการ Zero Trust มาใช้ภายในองค์กร

๙. Botnet หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้ง โปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการอย่างที่ถูกโปรแกรมไว้ส่วนมากจะแฝงตัวบเครื่องของเหยื่อจะไม่ทราบว่ามี การติด Botnets ที่ไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐. Ransomware คือ Walware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าถ่ายของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำโดยทำการแยกที่เก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีการตระหนักก่อนที่จะทำการเปิด

๑๑. Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำ การติดตั้งโปรแกรมที่ใช้ในการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อตามประเมินผลเพื่อสร้างรายได้กลับไปที่ Hacker

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

คอมพิวเตอร์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานการของแต่ละบุคคล

๒. ควรออกจากระบบเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti Malware และมีการอัพเดทอย่างสม่ำเสมอ

๔. มีการอัพเดทระบบปฏิบัติการ OS อย่างสม่ำเสมอ

๕. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ Password ที่ดีและไม่บอก Password แก่ผู้อื่น

Password

๑. การใช้ Password ที่ดีคือหนึ่งมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ตัวเลข และอักขระพิเศษ

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓. ความหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น Password ๑,๒,๓,๔,๕,๖ วันเกิด และหมายเลขโทรศัพท์

๔. มีการเปลี่ยน password อย่างสม่ำเสมอ

อีเมล์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด Gmail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๓. ไม่คลิกลิงค์ใน E-mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆควรมีการเช็คผ่านเข้าทางอื่นๆเพิ่มเติม

เว็บไซต์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ได้เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจนเช่นการใช้งานช่องทาง Social ต่างๆ

๒. ไม่ควรทำการบันทึก Password ต่างๆบนบราวเซอร์

๓. เว็บไซต์สำหรับทำธุรการที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน https

๔. ควรมีการอัพเดทเวอร์ชั่นของเราสม่ำเสมอ

๕. ในกรณีเครื่องคอมพิวเตอร์ที่ไม่ใช่เรื่องส่วนตัวควรใช้งาน Browser ในโหมดเซฟเว็บ Save Web browsing

๖. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น Google Chrome , mozilla Firefox เป็นต้น

Message

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรให้ระบบจำ Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิดลิงก์หรือฝ่ายต่างๆที่ได้รับมา

๔. มีการ update Version ของโปรแกรมอย่างสม่ำเสมอ

๕. ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News

ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ดูมีความน่าเชื่อถือ ทำให้ผู้ที่ได้ข่าวสารหลงเชื่อสามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านช่องทางออนไลน์เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็ว มากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้
๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
๔. สำนวนการเขียนออกมาแนวการโฆษณา

Conference

สิ่งที่ต้องควรปฏิบัติเพื่อความปลอดภัย
๑. ใช้สถานที่เหมาะสมกับการ Conference
๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
๓. แชร์ข้อมูลต่างๆ อย่างระมัดระวัง
๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
๕. มีการ update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

Cloud storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย
๑. แยก User ในการใช้งานของแต่ละบุคคล
๒. ควรกำหนดผู้เข้าสู่ไฟล์ได้เท่าที่จำเป็นเท่านั้น
๓. ปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
๕. มีการ update Version ในโปรแกรมอย่างสม่ำเสมอ
๖. มีการตั้ง Password ที่ดีและมันบอก Password แก่ผู้อื่น

ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง

ช่วยให้เข้าใจภัยคุกคามทางไซเบอร์ที่พบบ่อย และวิธีในการปกป้องข้อมูลจากภัยคุกคาม ช่วยลดความเสี่ยงการถูกโจมตีทางไซเบอร์ มีความรู้ในการสังเกตและรับมือกับภัยรูปแบบต่างๆ เช่น การหลอกลวงทางสังคม (Social Engineering)

ความเห็นของผู้บังคับบัญชา

(/) ทราบ

.....

.....

.....

(ลงนาม).....
(นายกฤษฎา จงดี)
เจ้าพนักงานการเกษตรปฏิบัติงาน

(ลงนาม).....
(นางสาวนัทฐา ทักษ์รัตนศรัณย์)
ผู้อำนวยการสถานีพัฒนาที่ดินกรุงเทพมหานคร
ผู้รับรองผลการพัฒนาความรู้