บันทึกข้อความ

ส่วนราชการ กลุ่มวิเคราะห์สภาพการใช้ที่ดิน กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๒๐๓

ที่ กษ ๐๘๓๗.๐๒/๑๕๑ **วันที่** ๕ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอสรุปบทเรียนจากการพัฒนาความรู้ผ่านระบบ e-training

เรียน ผอ. กลุ่มวิเคราะห์สภาพการใช้ที่ดิน

ตามที่ กองนโยบายและแผนการใช้ที่ดิน มอบหมายให้ข้าราชการเข้ารับการพัฒนาความรู้ผ่านระบบ e-training เพื่อประกอบการประเมินผลการปฏิบัติราชการของข้าราชการ นั้น

บัดนี้ ข้าพเจ้า นางสาวเนตรนภา กาศวิเศษ ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ ได้รับการพัฒนาความรู้ผ่านระบบ e-training ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิตัล รวมจำนวน ๒ เรื่อง คือ Basic Cybersecurity Series: หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น และแนวทางปฏิบัติกระบวนการทางดิจิทัลภาครัฐเพื่อสนับสนุนการดำเนินการตาม พ.ร.บ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ รายละเอียดตามประกาศนียบัตรจำนวน ๒ ใบ และผลการสรุปบทเรียนการพัฒนาความรู้ผ่านระบบ e-training ทั้ง ๒ เรื่อง คือ Basic Cybersecurity Series: หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น และ แนวทางปฏิบัติกระบวนการทางดิจิทัลภาครัฐเพื่อสนับสนุนการดำเนินการตาม พ.ร.บ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ ที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

(นางสาวเนตรนภา กาศวิเศษ)
นักวิชาการเกษตรชำนาญการพิเศษ

เรียน ผอ.กนผ.
เพื่อโปรดพิจารณา

(นางสาวอมรรัตน์ สระเพ็ชร)
นักวิชาการเกษตรชำนาญการพิเศษ
ผู้อำนวยการกลุ่มวิเคราะห์สภาพการใช้ที่ดิน

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน
****

ส่วนที่ 1 ข้อมูลทั่วไป

ชื่อ นางสาวเนตรนภา นามสกุล กาศวิเศษ
ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ กลุ่ม/ฝ่าย กลุ่มวิเคราะห์สภาพการใช้ที่ดิน
หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้
Basic Cybersecurity Series: หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น
สถานที่อบรม/สัมมนา/พัฒนาความรู้ E-training
หน่วยงานที่จัดฝึกอบรม/ประชุม/สัมมนา สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิตัล
ตั้งแต่วันที่ 26 เดือน มกราคม พ.ศ. 2569 ถึงวันที่ 28 เดือน มกราคม พ.ศ. 2569
เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....

ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

2.1 รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/สัมมนา/พัฒนาความรู้

เนื้อหาสาระสำคัญ

Basic Cybersecurity Series: หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

วัตถุประสงค์การอบรม Basic Cybersecurity Series มีดังนี้

1. เพื่อให้ผู้เข้ารับการอบรมมีความรู้ความเข้าใจพื้นฐานเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
2. เพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบัน
3. เพื่อส่งเสริมให้สามารถใช้งานเทคโนโลยีดิจิทัลและระบบสารสนเทศได้อย่างปลอดภัย
4. เพื่อเป็นพื้นฐานในการพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับที่สูงขึ้นต่อไป

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง แนวคิด มาตรการ และกระบวนการที่ใช้ในการปกป้องระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลสารสนเทศจากการเข้าถึง การใช้งาน การเปิดเผย หรือการทำลายโดยไม่ได้รับอนุญาต ในยุคที่หน่วยงานและองค์กรพึ่งพาระบบดิจิทัลเป็นหลัก ความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นปัจจัยสำคัญที่ส่งผลต่อความต่อเนื่องของการดำเนินงานและความเชื่อมั่นของผู้ใช้งาน

ความมั่นคงปลอดภัยทางไซเบอร์ไม่ได้จำกัดอยู่เพียงด้านเทคนิคหรืออุปกรณ์เท่านั้น แต่ครอบคลุมถึงพฤติกรรมของผู้ใช้งาน กระบวนการทำงาน และนโยบายขององค์กร ตัวอย่างเช่น กรณีที่บุคลากรใช้รหัสผ่านเดียวกันกับหลายระบบ หากระบบใดระบบหนึ่งถูกเจาะ ระบบอื่น ๆ ก็อาจได้รับผลกระทบตามไปด้วย แสดงให้เห็นว่าพฤติกรรมของผู้ใช้งานมีผลต่อความปลอดภัยของระบบโดยตรง

ตัวอย่างเหตุการณ์ที่เกิดขึ้นบ่อยในชีวิตประจำวัน เช่น การคลิกลิงก์จากอีเมลหรือข้อความที่ไม่น่าเชื่อถือ ซึ่งอาจนำไปสู่การติดมัลแวร์หรือการถูกขโมยข้อมูลส่วนบุคคล เหตุการณ์ดังกล่าวสะท้อนให้เห็นว่า ความรู้พื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งจำเป็นสำหรับผู้ใช้งานทุกคน ไม่เฉพาะผู้ที่มีหน้าที่ดูแลระบบเท่านั้น

หลักการพื้นฐานของความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งประกอบด้วยองค์ประกอบสำคัญ 3 ประการ ได้แก่

1. ความลับของข้อมูล (Confidentiality) คือ การป้องกันไม่ให้ข้อมูลถูกเปิดเผยหรือเข้าถึงโดย

ผู้ที่ไม่มีสิทธิ์

2. ความถูกต้องครบถ้วนของข้อมูล (Integrity) คือ การรักษาข้อมูลให้ถูกต้อง ไม่ถูกแก้ไขดัดแปลง หรือทำลายโดยไม่ได้รับอนุญาต

3. ความพร้อมใช้งานของระบบและข้อมูล (Availability) คือ การทำให้ระบบและข้อมูลสามารถใช้งานได้ตามความจำเป็นอย่างต่อเนื่อง

ภัยคุกคามทางไซเบอร์ที่พบบ่อยในชีวิตประจำวันและในการทำงาน ได้แก่

- มัลแวร์ (Malware) ซึ่งรวมถึงไวรัส โทรจัน สปายแวร์ และแรนซัมแวร์ ที่สามารถสร้างความเสียหายต่อระบบสารสนเทศ ข้อมูล และการดำเนินงานขององค์กร
- ฟิชชิ่ง (Phishing) เป็นการหลอกลวงผ่านอีเมล เว็บไซต์ หรือข้อความ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลทางการเงิน
- การโจมตีทางวิศวกรรมสังคม (Social Engineering) ซึ่งอาศัยการหลอกล่อ ชักจูง หรือสร้างความน่าเชื่อถือ เพื่อให้ผู้ใช้งานกระทำการที่ก่อให้เกิดความเสี่ยงด้านความปลอดภัย

แนวทางการป้องกันและลดความเสี่ยงด้านไซเบอร์ในระดับพื้นฐาน ที่สามารถนำไปใช้ได้จริง เช่น

- การตั้งรหัสผ่านที่มีความปลอดภัยและไม่ซ้ำกัน
- การจัดการรหัสผ่านอย่างเหมาะสม
- การใช้งานอีเมลและอินเทอร์เน็ตอย่างระมัดระวัง
- การอัปเดตระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอ

ความปลอดภัยของข้อมูลและข้อมูลส่วนบุคคล

ความปลอดภัยของข้อมูลและข้อมูลส่วนบุคคลเป็นประเด็นสำคัญอย่างยิ่งในยุคดิจิทัล เนื่องจากข้อมูลถือเป็นทรัพย์สินที่มีคุณค่าและมีความอ่อนไหว การรั่วไหล การถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม อาจก่อให้เกิดความเสียหายทั้งในระดับบุคคล องค์กร และสังคมโดยรวม การอบรมจึงมุ่งเน้นให้ผู้เข้าอบรมตระหนักถึงความสำคัญของการปกป้องข้อมูล และเข้าใจบทบาทหน้าที่ของตนเองในการดูแลรักษาความปลอดภัยของข้อมูลสารสนเทศ

ข้อมูลส่วนบุคคล ซึ่งหมายถึงข้อมูลที่สามารถระบุตัวบุคคลได้ ไม่ว่าจะเป็นข้อมูลทั่วไป เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ ที่อยู่ หรือข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลด้านสุขภาพ ข้อมูลทางการเงิน และข้อมูลประจำตัวประชาชน ซึ่งข้อมูลเหล่านี้จำเป็นต้องได้รับการดูแลและปกป้องเป็นพิเศษ

ความเสี่ยงจากการถูกโจมตีทางไซเบอร์ ความผิดพลาดจากการใช้งานของบุคลากร และการขาดมาตรการควบคุมที่เหมาะสม การตระหนักถึงความเสี่ยงดังกล่าวช่วยให้สามารถวางแนวทางป้องกันได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

แนวทางปฏิบัติในการรักษาความปลอดภัยของข้อมูลและข้อมูลส่วนบุคคล เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูลตามความจำเป็น การจัดเก็บข้อมูลอย่างเป็นระบบและปลอดภัย การหลีกเลี่ยงการเปิดเผยข้อมูลผ่านช่องทางที่ไม่ปลอดภัย รวมถึงการสำรองข้อมูลเพื่อป้องกันการสูญหายหรือความเสียหายที่อาจเกิดขึ้น

การสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยทางไซเบอร์

การสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นปัจจัยสำคัญที่ช่วยเสริมสร้างความปลอดภัยของระบบสารสนเทศอย่างยั่งยืน เนื่องจากภัยคุกคามทางไซเบอร์จำนวนมากเกิดจากพฤติกรรมของผู้ใช้งานที่ขาดความตระหนักรู้หรือไม่ปฏิบัติตามแนวทางด้านความปลอดภัยอย่างเหมาะสม การอบรมจึงมุ่งเน้นให้ผู้เข้าอบรมเข้าใจว่า ความมั่นคงปลอดภัยทางไซเบอร์ไม่ใช่หน้าที่ของบุคลากรด้านเทคโนโลยีสารสนเทศเพียงฝ่ายเดียว แต่เป็นความรับผิดชอบร่วมกันของทุกคนในองค์กร

การปลูกฝังจิตสำนึกด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยส่งเสริมให้ผู้เข้าอบรมตระหนักถึงผลกระทบที่อาจเกิดขึ้นจากการกระทำเพียงเล็กน้อย เช่น การเปิดอีเมลหรือไฟล์แนบจากแหล่งที่ไม่

น่าเชื่อถือ การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการละเลยการปฏิบัติตามมาตรการด้านความปลอดภัย ซึ่งอาจนำไปสู่ความเสียหายต่อข้อมูลและระบบขององค์กรในวงกว้าง

การสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ยังครอบคลุมถึงการส่งเสริมพฤติกรรมที่เหมาะสมในการใช้งานเทคโนโลยีดิจิทัล เช่น การใช้ทรัพยากรสารสนเทศอย่างมีความรับผิดชอบ การรายงานเหตุการณ์หรือความผิดปกติที่อาจเกี่ยวข้องกับความปลอดภัยทางไซเบอร์อย่างทันท่วงที และการเรียนรู้เพื่อปรับตัวให้ทันต่อภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นอย่างต่อเนื่อง

2.2 ประสบการณ์/ประโยชน์ที่ได้รับ/การประยุกต์ใช้กับหน่วยงาน

☑ ต่อตนเอง

มีความรู้ ความเข้าใจ และทักษะพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ สามารถรับรู้และประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้น สามารถนำแนวทางการป้องกันไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน และมีพื้นฐานความรู้สำหรับการพัฒนาต่อยอดด้าน Cybersecurity ในอนาคต

☑ ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน

สามารถนำความรู้ทักษะพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่ได้มาเผยแพร่แก่บุคลากรอื่น ๆ ได้

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

บางครั้งสัญญาณอินเตอร์เน็ตมีปัญหา ทำให้การอบรมไม่ต่อเนื่อง

2.4 ข้อคิดเห็นและข้อเสนอแนะ

ควรมีการสนับสนุนให้บุคลากรอบรมหลักสูตรนี้ เพื่อให้บุคลากรมีความรู้ ความเข้าใจ และทักษะพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ และสามารถนำแนวทางการป้องกันไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน และมีพื้นฐานความรู้สำหรับการพัฒนาต่อยอดด้าน Cybersecurity ในอนาคต

ลงชื่อ .....

(นางสาวเนตรนภา กาศวิเศษ)

ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ

ผู้รายงาน

วันที่ 5 เดือน กุมภาพันธ์ พ.ศ. 2569

ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา

( ) ทราบ

.....

.....

ลงชื่อ .....

(นายนันทพล หนองหารพิทักษ์)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ ..... เดือน ..... พ.ศ. .....

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ เนตรนภา กาศวิเศษ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 28 มกราคม 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล