บันทึกข้อความ

ส่วนราชการ กลุ่มวางแผนการจัดการที่ดินในพื้นที่เสี่ยงภัยทางการเกษตร กองนโยบายและแผนการใช้ที่ดิน โทร. ๑๓๒๐

ที่ กษ ๐๘๓๗.๐๖/๔๔๗ **วันที่** ๖ มิถุนายน ๒๕๖๘

เรื่อง ขอส่งสรุปการเรียนรู้ผ่านสื่ออิเล็กทรอนิกส์

เรียน ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

ตามที่ กรมพัฒนาที่ดิน ได้กำหนดตัวชี้วัดรายบุคคลด้านการพัฒนาบุคลากร รอบการประเมินที่ ๒ (๑ เมษายน ๒๕๖๘ – ๓๐ กันยายน ๒๕๖๘) นั้น

บัดนี้ ข้าพเจ้าได้เรียนรู้ทักษะด้านดิจิทัลผ่านสื่อศูนย์กลางการเรียนรู้ทักษะดิจิทัลสำหรับภาครัฐ (Digital Government Learning Platform) ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล หลักสูตร Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น จบหลักสูตรเรียบร้อยแล้ว จึงขอส่งสรุปการเรียนรู้ จำนวน ๑ เรื่อง

จึงเรียนมาเพื่อโปรดพิจารณา

อิสราภรณ์ ทัพยาสิทธินันท์

(นางสาวอิสราภรณ์ ทัพยาสิทธินันท์)
เจ้าหน้าที่วิเคราะห์นโยบายและแผน

เรียน ผอ.นผ.
เพื่อโปรดทราบสรุปผลการเรียนรู้ฯ

(นางสาวพิมพิลัย นวลละออง)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
ผู้อำนวยการกลุ่มวางแผนการจัดการที่ดิน
ในพื้นที่เสี่ยงภัยทางการเกษตร

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ.....น.ส.อิสราภรณ์.....นามสกุล.....หัทยาสิทธินันท์.....
ตำแหน่ง..เจ้าหน้าที่วิเคราะห์นโยบายและแผน...กลุ่มวางแผนการจัดการที่ดินในพื้นที่เสี่ยงภัยทางการเกษตร
หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ...Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น.....
สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ ...Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล.....
หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ..... Digital Government Learning Platform สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล .....
ตั้งแต่วันที่...๓๐...เดือน...พฤษภาคม.....พ.ศ...๒๕๖๘.....ถึงวันที่...๓๐.....เดือน.....พฤษภาคม...พ.ศ...๒๕๖๘...

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

กระบวนการบริหารความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ความเสี่ยง คือ เหตุการณ์ การกระทำใดๆที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และอาจส่งผลกระทบหรือสร้างความเสียหายความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบรรลุเป้าหมายและวัตถุประสงค์ทั้งในระดับหน่วยงานและระดับบุคคลได้

การวางแผนเพื่อลดความเสี่ยง

การบริหารความเสี่ยง Risk Management เป็นวิธีการหรือกลยุทธ์ที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม หรือกระบวนการดำเนินงานขององค์กรเพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุดและเพิ่มโอกาสแก่องค์กรมากที่สุด

สภาพแวดล้อมกับความเสี่ยง แบ่งออกเป็น ๒ แบบ คือ

สภาพแวดล้อมภายนอก

-Socio-cultural Factors ความสลับซับซ้อนทางสังคม โครงสร้างประชากร การศึกษา อาชีพ และอื่นๆ
-Economic Factors เป็นภาวะทางเศรษฐกิจ การจ้างงาน อัตราดอกเบี้ย และอื่นๆ
-Political and Legal Factors เสถียรภาพของรัฐบาล นโยบายรัฐ กฎหมาย ฯลฯ
-Physical Factors สภาพทางภูมิศาสตร์ ดินฟ้าอากาศ ภัยธรรมชาติ
-Technological Factors นวัตกรรม ความมีอยู่ของเทคโนโลยี ฯลฯ

สภาพแวดล้อมภายใน

-Structure and Policy โครงสร้างองค์กร กลยุทธ์ ฯลฯ
-Service ผลผลิต และผลลัพธ์ ความพึงพอใจของผู้รับบริการ ฯลฯ
-Manpower อัตรากำลัง คุณภาพบุคลากร การบริหารบุคคล ฯลฯ
-Money ประสิทธิภาพด้านการเงิน การระดมทุน
-Materials วัสดุ อุปกรณ์ เครื่องจักร ฯลฯ
-Management กระบวนการ ภาวะความเป็นผู้นำ วัฒนธรรมองค์กร สารสนเทศ ฯลฯ

ความสำคัญของการบริหารความเสี่ยง

-เพื่อส่งเสริม ให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายใน

-เพื่อสะท้อนการพัฒนา ในด้านการกำกับดูแลที่ดีขององค์กร การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน

-เพื่อให้ฝ่ายบริหารเกิดความมั่นใจ ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย

-เพื่อเป็นกลไก ในการผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยง

กระบวนการบริหารจัดการความเสี่ยง ไม่ได้หมายถึงแต่ตัวเราเท่านั้น ในองค์กรจะต้องมีผู้ปฏิบัติงานหน้างานต้องเป็นผู้ประเมินความเสี่ยงเอง เพราะเราจะรู้การปฏิบัติงานของเราได้ดีที่สุด หลังจากนั้นจึงส่งต่อให้กับ Managers, Executives, Practitioners โดยนำมาตรฐานที่องค์กรประยุกต์ใช้มาประเมินความเสี่ยง

ประเภทความเสี่ยง Risk Type

๑.เชิงยุทธศาสตร์ Strategic

๒.สภาพความพร้อมของการให้บริการ Operational

๓.ด้านการเงิน Financial

๔.ด้านกฎหมาย กฎระเบียบ Compliance

๕.เทคโนโลยี Information Technology

กระบวนการจัดการความเสี่ยง ตามมาตรฐาน COSO ERM (COSO Enterprise Risk Mamgement)

COSO ERM เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กรอย่างเป็นระบบ จนกระทั่งเป็นที่รู้จักและมีความนิยม

การตอบสนองความเสี่ยง

การจัดทำแผนจัดการความเสี่ยง

๑.การยอมรับความเสี่ยง สามารถเลือกวิธียอมรับความเสี่ยง ถ้าความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

๒.การลด/ควบคุมความเสี่ยง เป็นการกำหนดกิจกรรมเพื่อลดความเสี่ยง เช่น การแก้ไขปรับปรุงการทำงาน

๓.การหลีกเลี่ยงความเสี่ยง เป็นการตัดสินใจที่จะไม่เข้าไปเกี่ยวข้องกับสถานการณ์ ความเสี่ยงนั้น

๔.การกระจาย/ถ่ายโอนความเสี่ยง เป็นการถ่ายโอนความรับผิดชอบหรือภาระของการสูญเสียให้กับบุคคลอื่น

ตามเอกสารประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ กรอบมาตรฐานแบ่งได้ออกเป็น ๕ หัวข้อหลัก

๑.การระบุความเสี่ยง (Identify)

๒.การป้องกันความเสี่ยง (Protect)

๓.การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔.การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) โดยเราจะต้องมีการจัดทำแผน ว่าถ้าเกิดเหตุเราต้องทำอย่างไรต่อไป

๕.การฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

การป้องกันความเสี่ยงโดยการประเมินช่องโหว่

Vulnerability Assessment (VA) กระบวนการที่ใช้ในการตรวจสอบและระบุช่องโหว่ที่มีอยู่ในระบบหรือแอปพลิเคชั่น โดยใช้เครื่องมือตรวจสอบ

Vulnerability Scanning Tool เพื่อตรวจสอบความปลอดภัยระบบเครือข่ายซึ่งใช้งานภายในองค์กร เช่นระบบปฏิบัติการ (OS)

รูปแบบของ VA Scan

-Host Assessment การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญ

-Network and Wireless Assessment การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริงเพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

-Database Assessment ประเมินความเสี่ยงในเรื่องของ Database

-Application Scans ด้านความปลอดภัยใน Web Application และ Source Code

ขั้นตอนการทำ VA

-Vulnerability Identification เป็นขั้นตอนการเตรียมรายการของช่องโหว่ใน App ผู้ที่วิเคราะห์จะทำการทดสอบความแข็งแรงของระบบ Security

-Vulnerability Analysis ขั้นตอนของการหาสาเหตุหรือต้นตอที่เจอช่องโหว่มาจากข้อที่ ๑

-Risk Assessment การจัดลำดับความสำคัญของช่องโหว่

-Remediation ขั้นตอนสุดท้ายคือ การอุดช่องโหว่

การมีความรู้เกี่ยวกับความมั่นคงทางปลอดภัยทางไซเบอร์เบื้องต้น เป็นสิ่งที่จำเป็นสำหรับทุกคนในยุคดิจิตอล ไม่เพียงแต่ป้องกันข้อมูลส่วนบุคคลและคอมพิวเตอร์ของเราเองยังเพื่อสร้างความมั่นคงแก่องค์กรและสร้างความเชื่อมั่นให้ลูกค้า และพันธมิตรทางการค้า เป็นสิ่งที่เตรียมพร้อมสำหรับภัยคุกคามทางไซเบอร์อาจจะเกิดขึ้นในอนาคต สามารถศึกษาได้จากมาตรฐานสากล เช่น ISO/IEC ๒๗๐๐๑ Version ๒๐๒๒ และ NIST Cybersecurity Framework เพื่อให้เกิดประโยชน์สูงสุด

๒.๒ ประสบการณ์/ประโยชน์ที่ได้รับ /การประยุกต์ใช้กับหน่วยงาน

☑ ต่อตนเอง สามารถนำบทเรียนไปปรับใช้ในระบบความปลอดภัยในอุปกรณ์ของตนเอง โดยที่เราสามารถรู้เท่าทันของมิจฉาชีพได้

☑ ต่อหน่วยงาน / การนำมาประยุกต์ใช้กับหน่วยงาน สามารถนำบทเรียนที่ได้เรียนไปปรับใช้ในองค์กร เพื่อให้ข้อมูลขององค์กรมีความปลอดภัยมากยิ่งขึ้น ยากต่อการโจรกรรมข้อมูล

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-ศัพท์บางตัวเป็นศัพท์เฉพาะที่เข้าใจยาก จึงต้องค้นคว้าศึกษาเพิ่มเติม

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

-ต้องการให้มีการแยกบทเรียน แต่ละเนื้อหาให้ชัดเจนมากกว่านี้

ลงชื่อ.....

(...น.ส.อิสราภรณ์...หัทยาสิทธินันท์...)

ตำแหน่ง.....เจ้าหน้าที่วิเคราะห์นโยบายและแผน.....

ผู้รายงาน

วันที่ ...๖...เดือน ...มิถุนายน....พ.ศ. ...๒๕๖๘...

ส่วนที่ ๓ ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

.....

ลงชื่อ.....

(นายนันทพล หนองหารพิทักษ์)

ตำแหน่ง ผู้เชี่ยวชาญด้านวางแผนการใช้ที่ดิน

รักษาราชการแทน ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่.....เดือน.....พ.ศ. .....

๑๓ มิ.ย. ๒๕๖๘

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

อิสราภรณ์ หัทยาสิทธินันท์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series : หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

รวมระยะเวลาทั้งสิ้น 1 : 30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 30 พฤษภาคม 2568

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

อิสราภรณ์ หัทยาสิทธินันท์
สำเนาถูกต้อง

111ba88b

Signed by สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (องค์การมหาชน) (depa)
Date: 2025-05-30T15:42:56.112+07:00