

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร

กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ-นามสกุล นางสาวณัฐธิดา สิงห์ประเสริฐ

ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน ฝ่าย บริหารทั่วไป

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ :

การสร้างตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

สถานที่อบรม/สัมมนา/พัฒนาความรู้ :

TDGA

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ :

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA E-LEARNING)

ตั้งแต่วันที่ ๑๐ เดือน สิงหาคม พ.ศ. ๒๕๖๔ ถึงวันที่ ๑๐ เดือน สิงหาคม พ.ศ. ๒๕๖๔

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

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/สัมมนา/พัฒนาความรู้

๑. ความเสี่ยง คือ เหตุการณ์ การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบ/หรือสร้างความเสียหายความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จ ต่อการบรรลุเป้าหมายและวัตถุประสงค์ ทั้งในระดับองค์กร ระดับหน่วยงาน และระดับบุคคลได้

๒. การบริหารความเสี่ยง หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตามและสื่อสารสิ่งที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กรเพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุดและเพิ่มโอกาสแก่องค์กรมากที่สุด

๓. ความสำคัญของการบริหารความเสี่ยง

๓.๑. เพื่อส่งเสริม ให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายใน

๓.๒. เพื่อสะท้อนการพัฒนา ในด้านการกำกับดูแลที่ดีขององค์กร การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน

๓.๓. เพื่อให้ฝ่ายบริหารเกิดความมั่นใจ ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย

๓.๔. เพื่อเป็นกลไก ในการผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยง

๔. ประเภทความเสี่ยง Risk Type มี ๕ ประเภท ดังนี้

๑. Strategic คือ การบรรลุเป้าหมาย และวัตถุประสงค์ ชื่อเสียง/ภาพลักษณ์สำนักงาน เช่น การเปลี่ยนแปลงนโยบายระดับรัฐ,กฎหมายสั่ง,นโยบายขององค์กร,รูปแบบธุรกิจ และข้อร้องเรียน

๒. Operational คือ ความพร้อมของบุคลากร,รูปแบบ วิธีการ กระบวนการดำเนินงาน และการขึ้นทะเบียนบริการใหม่ เช่น การรักษาบุคลากร,อัตรากำลัง,ขาดการบูรณาการ

๓. Financial คือ การบริหารจัดการงบประมาณ ค่าใช้จ่าย เช่น การขาดสภาพคล่อง,งบประมาณที่ได้รับไม่สอดคล้องกับสถานการณ์ของภารกิจที่เปลี่ยนแปลงไป

๔. Compliance คือ การปฏิบัติตามกฎหมาย ระเบียบที่เกี่ยวข้อง เช่น การปฏิบัติงานไม่เป็นไปตามคำสั่ง ประกาศ ระเบียบ ข้อบังคับขององค์กร

๕. Information Technology คือ การรักษาความลับ และความมั่นคงปลอดภัยทางไซเบอร์, ความถูกต้องเชื่อถือได้ของระบบ เช่น การเปิดเผยข้อมูล, การแก้ไขทำลายข้อมูลโดยไม่ได้รับอนุญาต

๕. ปัจจัยความเสี่ยง (Risk Factor)

ปัจจัยความเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้องค์กรไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน กระบวนการใด เมื่อใดและจะเกิดขึ้นได้อย่างไรและ ทำไมถึงเกิด ทั้งนี้สาเหตุของความความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการ ป้องกันความเสี่ยงในภายหลังได้อย่างถูกต้อง

๖. ปัจจัยความเสี่ยงพิจารณาได้จาก

๑. ปัจจัยภายนอก เช่น เศรษฐกิจ สังคม การเมือง กฎหมาย ฯลฯ

๒. ปัจจัยภายใน เช่น กฎระเบียบ ข้อบังคับภายในองค์กร ประสิทธิภาพของเจ้าหน้าที่ ระบบการทำงาน ความโลภและจริยธรรมของแต่ละบุคคล ฯลฯ

๗. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด ผลกระทบ และระดับของความเสี่ยงนั้นๆ

๑) โอกาสที่จะเกิด หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ ความเสี่ยง

๒) ผลกระทบ หมายถึง ขนาดความรุนแรงของความเสี่ยงที่จะเกิดขึ้นหากเกิด เหตุการณ์ความเสี่ยง

๓) ระดับของความเสี่ยง หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละ ปัจจัยเสี่ยง แบ่งเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

๘. องค์ประกอบของการบริหารความเสี่ยงทางการทุจริต

องค์ประกอบของการบริหารความเสี่ยงทางการทุจริต ประกอบด้วย ๘ ประการ ซึ่งครอบคลุม แนวทางการกำหนดนโยบาย การบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง ดังนี้

๑. สภาพแวดล้อมภายในองค์กร (Internal Environment) สภาพแวดล้อมภายในองค์กรเป็นพื้นฐานที่สำคัญสำหรับการบริหารความเสี่ยงทางการทุจริต มีอิทธิพล ต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม วิธีการปฏิบัติงาน สภาพแวดล้อมภายใน องค์กรประกอบด้วยหลายปัจจัย เช่น จริยธรรม วิธีการทำงานของทั้งผู้บริหารและเจ้าหน้าที่ รวมถึงปรัชญาและ วัฒนธรรมในการบริหารงาน ความเสี่ยงในการเกิดการทุจริตเป็นส่วนที่สำคัญและมีผลต่อการกำหนดกลยุทธ์เพื่อ นำไปดำเนินการให้องค์กรบรรลุเป้าหมายทั้งด้านผลการปฏิบัติงานและการยอมรับของสังคม

๒. การกำหนดวัตถุประสงค์ คือขั้นตอนแรกสำหรับกระบวนการบริหารความเสี่ยงทางการทุจริต องค์กรควรมั่นใจว่า วัตถุประสงค์ ขององค์กรที่กำหนดขึ้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์ ดำเนินการด้วยการใช้ทรัพยากรขององค์กร อย่างมีประสิทธิภาพ โดยคำนึงถึงผลประโยชน์ขององค์กรและผู้มีส่วนได้ส่วนเสียขององค์กรเป็นเป็นอย่างดี

๓. การระบุความเสี่ยงหรือการบ่งชี้เหตุการณ์ (Event Identification) คือการระบุสถานการณ์ ปัจจัย และกิจกรรมที่มีความเสี่ยงในการเกิดการทุจริต ซึ่งองค์กรไม่สามารถ มั่นใจได้ว่าเหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดขึ้นหรือไม่ หรือมีผลลัพธ์ ที่เกิดขึ้นจะเป็นอย่างไร ประกอบด้วย ปัจจัยภายในและภายนอกที่ส่งผลต่อการปฏิบัติงานหรือปฏิบัติหน้าที่ เพื่อให้บรรลุเป้าหมายและวัตถุประสงค์ขององค์กร

๔. การประเมินความเสี่ยง (Risk Assessment) คือการประเมินโอกาสและผลกระทบของเหตุการณ์ที่อาจเกิดขึ้นต่อตาม เหตุการณ์ ปัจจัย กิจกรรมที่ บ่งชี้ ขณะที่การเกิดเหตุการณ์ใดเหตุการณ์หนึ่งอาจส่งผลกระทบได้ในระดับต่ำหรือสูง เหตุการณ์ ที่เกิดขึ้นอย่าง ต่อเนื่องอาจมีผลกระทบในระดับสูง การประเมินความเสี่ยงประกอบด้วย ๒ มิติ ดังนี้

๔.๑) โอกาสที่อาจเกิดขึ้น หรือเหตุการณ์มีโอกาสเกิดขึ้นมากน้อยเพียงใด

๔.๒) ผลกระทบ หากมีเหตุการณ์เกิดขึ้นองค์กรจะได้รับผลกระทบมากน้อยเพียงใด

๕. การจัดการความเสี่ยง หรือการตอบสนองความเสี่ยง (Risk Response) เมื่อความเสี่ยงได้รับการบ่งชี้และประเมิน ความสำคัญแล้วต้องทำการประเมินวิธีการบริหารจัดการความ เสี่ยงทางการทุจริตที่สามารถนำไปปฏิบัติได้ โดยการพิจารณา

ทางเลือกในการดำเนินการจะต้องคำนึงถึงการปิด โอกาสความเสี่ยงทางทฤษฎีทั้งหมดให้ได้ เพื่อให้การบริหารความเสี่ยงทางทฤษฎีมีประสิทธิภาพ

Computer สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก user ใช้งานกันของแต่ละบุคคลไม่ควรใช้บัญชีผู้ใช้ (User Account) ร่วมกัน ไม่ว่าจะเป็นคอมพิวเตอร์ส่วนตัวหรือคอมพิวเตอร์ในองค์กร รวมถึงการแบ่งแยกประเภทบัญชีระหว่าง Administrator (สำหรับติดตั้ง/ตั้งค่าระบบ) และ Standard User (สำหรับการใช้งานทั่วไป) ช่วยระบุตัวตนและตรวจสอบย้อนหลังได้ง่ายเมื่อเกิดปัญหา อีกทั้งยังช่วยจำกัดสิทธิ์การเข้าถึงข้อมูล ความเป็นส่วนตัว และป้องกันไม่ให้ภัยคุกคาม เช่น มัลแวร์ เข้าถึงไฟล์สำคัญของระบบได้ หากรหัสผ่านของบัญชีทั่วไปหลุดไป

๒. ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ ป้องกันผู้ไม่หวังดีสวมรอยเข้าใช้งานเครื่องคอมพิวเตอร์ (Unauthorized Access) เพื่อแอบดูข้อมูล ลบไฟล์ แอบส่งอีเมลในนามของเรา หรือติดตั้งโปรแกรมประสงค์ร้ายโดยที่เราไม่รู้ตัว

๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ ติดตั้งโปรแกรมป้องกันมัลแวร์หรือไวรัสที่มีประสิทธิภาพ และเปิดระบบอัปเดตข้อมูลสายพันธุ์ไวรัส (Virus Signature Database) แบบอัตโนมัติ พร้อมทั้งตั้งเวลาสแกนระบบดิสก์ (Full System Scan) เป็นประจำ สายพันธุ์ของมัลแวร์ ไวรัส หรือแรนซัมแวร์ (Ransomware) ถูกพัฒนาขึ้นใหม่ทุกวัน หากไม่อัปเดตฐานข้อมูลเป็นปัจจุบัน โปรแกรมจะไม่สามารถตรวจจับและป้องกันไฟล์อันตรายชนิดใหม่ๆ ได้

๔. มีการอัปเดต Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ เปิดใช้งานระบบ Automatic Updates ระบบปฏิบัติการ ไม่ว่าจะเป็น Windows, macOS หรือ Linux เพื่อรับแพตช์ความปลอดภัย (Security Patches) ทั้งนี้ ผู้ไม่หวังดี (Hackers) มักค้นหาช่องโหว่ (Vulnerabilities) ของระบบปฏิบัติการเพื่อใช้เป็นช่องทางในการแฮกเครื่อง การอัปเดต Patch คือการปิดช่องโหว่เหล่านั้นเพื่อไม่ให้ถูกโจมตีผ่านระบบเครือข่าย

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอตรวจสอบและอัปเดตเวอร์ชันของโปรแกรมต่างๆ ที่ใช้งานอยู่เสมอ โดยเฉพาะเว็บเบราว์เซอร์ (เช่น Chrome, Edge), โปรแกรมอ่านไฟล์ PDF, ซอฟต์แวร์สำนักงาน ซอฟต์แวร์ที่ไม่ได้รับการอัปเดตอาจมีช่องโหว่ที่แฮกเกอร์สามารถใช้ไฟล์อันตราย (เช่น ไฟล์ PDF หรือไฟล์เอกสารล่อกลวง) หรือเว็บไซต์อันตรายมาเจาะระบบผ่านตัวโปรแกรมเพื่อยึดเครื่องคอมพิวเตอร์ได้

๖. ไม่ควรจด password และติด password ไว้ที่หน้าจอ ๗. มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น
Password การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร ๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์ ๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ

๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๗. ไม่ควรบอก Password แก่ผู้อื่น

E-mail สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๓. ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

๒.๒ ประสบการณ์/ประโยชน์ที่ได้รับ/การประยุกต์ใช้กับหน่วยงาน

๑. ได้เรียนรู้เกี่ยวกับความหมายและพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

๒. ได้เรียนรู้วิธีการป้องกันความปลอดภัยในการใช้ภัยทางคอมพิวเตอร์

๓. นำความรู้ที่ได้รับมาประยุกต์ใช้เพื่อความปลอดภัยทั้งในการทำงานและชีวิตประจำวัน

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

-

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

-

ลงชื่อ.....ณัฐธิดา.....

(นางสาวณัฐธิดา สิงห์ประเสริฐ)

ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน

ผู้รายงาน

วันที่.....๒๐.....เดือน.....สิงหาคม..... พ.ศ.๒๕๖๙....

ส่วนที่ ๓ ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

.....

ลงชื่อนพ/ดร.....

(นายเน้นทพล หอนงหารพิทักษ์)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่.....เดือน.....๒๐ ส.ค. ๒๕๖๙.....

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ณัฐธิดา สิงห์ประเสริฐ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 10 สิงหาคม 2569

A L.

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

สำเนาถูกต้อง

ณัฐธิดา สิงห์ประเสริฐ



097bcaa6

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
Digital Government Development Agency (Public
Organization) (DGA)
Date: 2026-08-10T15:24:35.009+07:00

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ณัฐธิดา สิงห์ประเสริฐ

ได้ผ่านการอบรมด้วยระบบการเรียนรู้ออนไลน์ในบทเรียน
ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์
(Understanding Cybersecurity Risk Management)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 10 สิงหาคม 2569

Signature

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

สำเนาถูกต้อง

ศิริจิต สิงห์ปวงสุข

