การพัฒนาทักษะการสร้างความตระหนักรู้ความมั่นคงปลอดภัยทางไซเบอร์ (ทักษะด้านดิจิทัล 2569)

ชื่อผู้สรุปองค์ความรู้ นางสาวกัญญาพัชร วงศ์พรหม

ที่มา : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สรุปเนื้อหา

ได้เรียนรู้เกี่ยวกับความหมายและพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น วิธีการป้องกันความปลอดภัยในการใช้ภัยทางคอมพิวเตอร์ ว่ามีวิธีรับมืออะไรได้บ้าง และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงาน และชีวิตประจำวัน

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

2. การบริหารความเสี่ยง หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการติดตามและสื่อสารสิ่งที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุดและเพิ่มโอกาสแก่องค์กรมากที่สุด

3. ความสำคัญของการบริหารความเสี่ยง

3.1. เพื่อส่งเสริม ให้องค์กรมีการบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายใน

3.2. เพื่อสะท้อนการพัฒนา ในด้านการกำกับดูแลที่ดีขององค์กร การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน

3.3. เพื่อให้ฝ่ายบริหารเกิดความมั่นใจ ว่าการดำเนินงานจะบรรลุวัตถุประสงค์ได้ตามเป้าหมาย

3.4. เพื่อเป็นกลไก ในการผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยง

4. ประเภทความเสี่ยง Risk Type มี 5 ประเภท ดังนี้

4.1 Strategic คือ การบรรลุเป้าหมาย และวัตถุประสงค์ ชื่อเสียง/ภาพลักษณ์สำนักงาน เช่น การเปลี่ยนแปลงนโยบายระดับรัฐ กฎหมายสั่ง นโยบายขององค์กร รูปแบบธุรกิจ และข้อร้องเรียน

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

4.3 Financial คือ การบริหารจัดการงบประมาณ ค่าใช้จ่าย เช่น การขาดสภาพคล่อง งบประมาณที่ได้รับไม่สอดคล้องกับสภานการณ์ของภารกิจที่เปลี่ยนแปลงไป

4.4 Compliance คือ การปฏิบัติตามกฎหมาย ระเบียบที่เกี่ยวข้อง เช่น การปฏิบัติงานไม่เป็นไปตามคำสั่ง ประกาศ ระเบียบ ข้อบังคับขององค์กร

4.5 Information Technology คือ การรักษาความลับ และความมั่นคงปลอดภัยทางไซเบอร์ ความถูกต้องเชื่อถือได้ของระบบ เช่น การเปิดเผยข้อมูล การแก้ไขทำลายข้อมูลโดยไม่ได้รับอนุญาต

5. ปัจจัยความเสี่ยง (Risk Factor)

ปัจจัยความเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้องค์กรไม่บรรลุวัตถุประสงค์ที่ กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน กระบวนงานใด เมื่อใด และจะเกิดขึ้นได้อย่างไรและ ทำไมถึงเกิด ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการ ป้องกันความเสี่ยงในภายหลังได้อย่างถูกต้อง

6. ปัจจัย...

6. ปัจจัยความเสี่ยงพิจารณาได้จาก

6.1 ปัจจัยภายนอก เช่น เศรษฐกิจ สังคม การเมือง กฎหมาย ฯลฯ

6.2 ปัจจัยภายใน เช่น กฎระเบียบ ข้อบังคับภายในองค์กร ประสบการณ์ของเจ้าหน้าที่ ระบบการทำงาน ความโลภและจริยธรรมของแต่ละบุคคล ฯลฯ

7. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด ผลกระทบ และระดับของความเสี่ยงนั้นๆ

7.1 โอกาสที่จะเกิด หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ ความเสี่ยง

7.2 ผลกระทบ หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิด เหตุการณ์ความเสี่ยง

7.3 ระดับของความเสี่ยง หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

8. องค์ประกอบของการบริหารความเสี่ยงทางการทุจริต

องค์ประกอบของการบริหารความเสี่ยงทางการทุจริต ประกอบด้วย 8 ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง ดังนี้

8.1 สภาพแวดล้อมภายในองค์กร (Internal Environment) สภาพแวดล้อมภายในองค์กรเป็นพื้นฐานที่สสำคัญสำหรับการบริหารความเสี่ยงทางการทุจริต มีอิทธิพล ต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม วิธีการปฏิบัติงาน สภาพแวดล้อมภายใน องค์กรประกอบด้วยหลายปัจจัย เช่น จริยธรรม วิธีการทำงานของทั้งผู้บริหารและเจ้าหน้าที่ รวมถึงปรัชญา และวัฒนธรรมในการบริหารงาน ความเสี่ยงในการเกิดการทุจริตเป็นส่วนที่สำคัญและมีผลต่อการกำหนดกลยุทธ์เพื่อนำไปดำเนินการให้องค์กรบรรลุเป้าหมายทั้งด้านผลการปฏิบัติงาน และการยอมรับของสังคม

8.2 การกำหนดวัตถุประสงค์

คือขั้นตอนแรกสำหรับกระบวนการบริหารความเสี่ยงทางการทุจริต องค์กรควรมั่นใจว่าวัตถุประสงค์ขององค์กรที่กำหนดขึ้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์ ดำเนินการด้วยการใช้ทรัพยากรขององค์กรอย่างมีประสิทธิภาพ โดยคำนึงถึงผลประโยชน์ขององค์กรและผู้มีส่วนได้ส่วนเสียขององค์กรเป็นเป็นอย่างดี

8.3 การระบุความเสี่ยงหรือการบ่งชี้เหตุการณ์ (Event Identification) คือการระบุสถานการณ์ ปัจจัย และกิจกรรมที่มีความเสี่ยงในการเกิดการทุจริต ซึ่งองค์กรไม่สามารถ มั่นใจได้ว่าเหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดขึ้นหรือไม่ หรือมีผลลัพธ์ที่เกิดขึ้นจะเป็นอย่างไร ประกอบด้วย ปัจจัยภายในและภายนอกที่ส่งผลต่อการปฏิบัติงานหรือปฏิบัติหน้าที่เพื่อให้บรรลุเป้าหมายและวัตถุประสงค์ขององค์กร

8.4 การประเมินความเสี่ยง (Risk Assessment) คือการประเมินโอกาสและผลกระทบของเหตุการณ์ที่อาจเกิดขึ้นต่อตามเหตุการณ์ ปัจจัย กิจกรรมที่ บ่งชี้ ขณะที่การเกิดเหตุการณ์ใดเหตุการณ์หนึ่งอาจส่งผลกระทบได้ในระดับต่ำหรือสูง เหตุการณ์ที่เกิดขึ้นอย่าง ต่อเนื่องอาจมีผลกระทบในระดับสูง การประเมินความเสี่ยงประกอบด้วย 2 มิติ ดังนี้

8.4.1 โอกาสที่อาจเกิดขึ้น หรือเหตุการณ์มีโอกาสเกิดขึ้นมากน้อยเพียงใด

8.4.2 ผลกระทบ หากมีเหตุการณ์เกิดขึ้นองค์กรจะได้รับผลกระทบมากน้อยเพียงใด

8.5 การจัดการ...

8.5 การจัดการความเสี่ยง หรือการตอบสนองความเสี่ยง (Risk Response) เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วต้องทำการประเมินวิธีการบริหารจัดการความ เสี่ยงทางการทุจริตที่สามารถนำไปปฏิบัติได้ โดยการพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงการปิดโอกาสความเสี่ยงทางการทุจริตทั้งหมดให้ได้ เพื่อให้การบริหารความเสี่ยงทางการทุจริตมีประสิทธิผล

9. คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

9.1 ควรมีการแยก user ใช้งานกันของแต่ละบุคคล

9.2 ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

9.3 ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

9.4 มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

9.5 มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

9.6 ไม่ควรจด password และติด password ไว้ที่หน้าจอ 7. มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น

10. Password การใช้ Password ที่ดี คือ

10.1 มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ

10.2 มีความยาวของ Password อย่างน้อย 8 ตัวอักษร

10.3 ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password,123456,วันเกิด,หมายเลขโทรศัพท์

10.4 มีการเปลี่ยน Password อย่างสม่ำเสมอ

10.5 ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

10.6 ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

10.7 ไม่ควรบอก Password แก่ผู้อื่น

11. E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

11.1 ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

11.2 ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

11.3 ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค

11.4 เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม