การจัดการองค์ความรู้ Knowledge Management (KM) ประจำปีงบประมาณ พ.ศ. 2569

ชื่อองค์ความรู้: การรักษาความปลอดภัยข้อมูลข่าวสาร (Information Security)

1. ผู้รับผิดชอบ: นายชาติชาย เทียมสนิท หัวหน้าฝ่ายแผนงานและนโยบาย สถาบันพัฒนาบุคลากรดิจิทัล

2. ที่มาและความสำคัญ

ในสภาพแวดล้อมดิจิทัลของประเทศไทยที่กำลังพัฒนาอย่างรวดเร็ว
สถาบันพัฒนาบุคลากรดิจิทัลภายใต้มีบทบาทสำคัญในการเตรียมความพร้อมให้กำลังแรงงานมีทักษะทางเทคโนโลยีที่ทันสมัย ตอบโจทย์ต่อความท้าทายล่าสุด โดยเฉพาะอย่างยิ่งภัยคุกคามทางไซเบอร์และการรั่วไหลของข้อมูล ซึ่งมีแนวโน้มรุนแรงและซับซ้อนมากขึ้น นอกจากภารกิจหลักในการพัฒนากำลังแรงงานแล้วนั้น สถาบันฯ ได้เล็งเห็นถึงความจำเป็นเร่งด่วนที่บุคลากรของทางสถาบันเอง
จะต้องมีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความปลอดภัยข้อมูลข่าวสาร
ในการปฏิบัติงานประจำวัน
เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคลของประชาชน
การรักษาความปลอดภัยข้อมูลข่าวสารโดยพื้นฐานแล้ว คือ
การปกป้องข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัยตามหลักการ CIA Triad อันประกอบด้วย
ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability)
ซึ่งสมรรถนะด้านนี้มีความสำคัญอย่างยิ่งต่อทุกคนในยุคปัจจุบัน โดยเฉพาะอย่างยิ่งเจ้าหน้าที่ภาครัฐ
เพราะไม่เพียงแต่ช่วยป้องกันการโจมตีจากผู้ไม่หวังดีและการลดความเสี่ยงจากการถูกเรียกค่าไถ่ข้อมูล
(Ransomware) เท่านั้น แต่ยังช่วยสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการภาครัฐ
และขับเคลื่อนการบริหารราชการแผ่นดินในรูปแบบดิจิทัลได้อย่างมั่นคงและยั่งยืน

3. วัตถุประสงค์

3.1 เพื่อเพิ่มความมั่นคงปลอดภัยในการทำงาน:
เรียนรู้และปฏิบัติตามแนวทางการรักษาความปลอดภัยข้อมูลข่าวสาร
เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ การติดมัลแวร์ หรือการหลอกลวงแบบฟิชชิง (Phishing)
ช่วยให้ระบบงานหลักของสถาบันฯ ทำงานได้อย่างต่อเนื่องและปลอดภัย
3.2 ปกป้องข้อมูลสำคัญและข้อมูลส่วนบุคคลของประชาชน: ป้องกันไม่ให้ข้อมูลการฝึกอบรม ข้อมูลประวัติ หรือข้อมูลส่วนบุคคลที่อยู่ภายใต้การดูแลของสถาบันฯ รั่วไหลสู่สาธารณะ

ซึ่งสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

3.3 ส่งเสริมความตระหนักรู้และนโยบายความปลอดภัยที่เป็นระบบ:

เพื่อสร้างความเข้าใจในระดับองค์กรเกี่ยวกับแนวทางปฏิบัติที่ปลอดภัย เช่น การตั้งรหัสผ่านที่รัดกุม การควบคุมสิทธิ์การเข้าถึงข้อมูล และการจัดการกับเหตุการณ์ละเมิดความปลอดภัยอย่างถูกวิธีและมีจริยธรรม

3.4 พัฒนาเป็นหลักสูตรใน DSD Online Training:

เพื่อเผยแพร่องค์ความรู้ด้านการรักษาความปลอดภัยข้อมูลข่าวสารให้แก่ประชาชนทั่วไปเข้ารับการฝึกอบรมออนไลน์ได้ฟรีผ่านทาง DSD Online Training

4. กฎหมาย/ระเบียบ/ข้อบังคับ/แผนปฏิบัติการและอื่น ๆ ที่เกี่ยวข้อง

4.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562: มุ่งเน้นการกำหนดนโยบาย มาตรการและมาตรฐานขั้นต่ำในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

4.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA): กำหนดหลักเกณฑ์ มาตรการและการรักษาความปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคลจากการจัดเก็บ รวบรวม หรือเผยแพร่โดยมิชอบ

4.3 แผนปฏิบัติการดิจิทัลเพื่อการพัฒนาฝีมือแรงงาน และ

แผนปฏิบัติการด้านการพัฒนาทรัพยากรบุคคลของกรมพัฒนาฝีมือแรงงาน พ.ศ. 2566 - 2570

5. หน่วยงาน/ผู้เกี่ยวข้อง

สถาบันพัฒนาบุคลากรดิจิทัล กรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน

6. ขั้นตอนการดำเนินการ

6.1 ศึกษาแนวคิดหลักของการรักษาความปลอดภัยข้อมูลข่าวสารรวมถึงความสำคัญ บทบาท และความมั่นคงปลอดภัยทางไซเบอร์

6.2 ทำความเข้าใจภัยคุกคามในรูปแบบต่างๆ และมาตรการป้องกันขั้นพื้นฐาน เช่น การตรวจจับอีเมลหลอกลวง (Phishing) การใช้ระบบตรวจสอบตัวตนแบบหลายปัจจัย (MFA) การจัดการช่องโหว่ระบบ และการสำรองข้อมูล

6.3 ค้นคว้าจากแหล่งข้อมูลที่น่าเชื่อถือ เช่น มาตรฐานสากล ISO/IEC 27001, แนวทางปฏิบัติจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และคู่มือความปลอดภัยต่างๆ

6.4 ลงมือปฏิบัติตามมาตรการความปลอดภัยและประเมินความเสี่ยงเบื้องต้นของระบบงานในสถาบันฯ

รวมถึงติดตามข่าวสาร ความก้าวหน้าทางเทคโนโลยีสารสนเทศ และรูปแบบภัยคุกคามใหม่ๆ อย่างสม่ำเสมอ

6.5 วิเคราะห์ผลลัพธ์และช่องโหว่ที่พบในระบบงาน โดยพิจารณาถึงความเสี่ยง ความครอบคลุมของการป้องกัน และความสอดคล้องกับนโยบายภาครัฐ พร้อมระบุจุดแข็ง จุดอ่อน และข้อบกพร่องที่ต้องแก้ไขทันที

6.6 เปรียบเทียบมาตรการหรือเครื่องมือความปลอดภัยในรูปแบบต่างๆ
เพื่อค้นหาแนวทางป้องกันที่เหมาะสมและคุ้มค่าที่สุดสำหรับแต่ละระบบงาน

6.7 ทำความเข้าใจข้อจำกัดทางด้านระบบ บุคลากร และงบประมาณ
แล้วเรียนรู้วิธีจัดการความเสี่ยงเพื่อไม่ให้ส่งผลกระทบต่อการให้บริการประชาชน

6.8 จัดทำเอกสารสรุปองค์ความรู้ (KM) แนวทางปฏิบัติที่ดี (Best Practices)
และนโยบายการรักษาความปลอดภัยข้อมูลข่าวสารสำหรับบุคลากรภายใน

6.9 นำเสนอและถ่ายทอดองค์ความรู้ที่ได้ให้แก่เจ้าหน้าที่ในสถาบันฯ เพื่อปรับปรุงกระบวนการทำงานให้ปลอดภัย ผ่านการอบรมเชิงปฏิบัติการหรือการจำลองสถานการณ์ภัยคุกคาม

6.10 เผยแพร่องค์ความรู้ดังกล่าวและแจ้งเตือนภัยคุกคามรูปแบบใหม่ผ่านช่องทางสื่อของทางสถาบันฯ

7. ข้อมูล/ระบบ/เทคโนโลยีที่ใช้ในกระบวนการงาน (ถ้ามี)

7.1 มาตรฐานสากล ISO/IEC 27001 (Information Security Management Systems)

7.2 กรอบแนวทางความปลอดภัยไซเบอร์ (NIST Cybersecurity Framework)

7.3 บทความและแหล่งเรียนรู้:

7.3.1 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.):
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และแนวทางปฏิบัติตามกฎหมายไซเบอร์: https://www.ncsa.or.th

7.3.2 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.):
แนวทางปฏิบัติและเกณฑ์มาตรฐานการคุ้มครองข้อมูลส่วนบุคคล: https://www.pdpc.or.th

7.3.3 ศูนย์ต่อต้านข่าวปลอมประเทศไทย (Anti-Fake News Center) และ THAICERT:
รายงานสถานการณ์ภัยคุกคามประจำปีและกลโกงทางเทคโนโลยี

8. ผลที่คาดว่าจะได้รับ/ผลลัพธ์ที่ได้

8.1 การทำงานมีความมั่นคงปลอดภัยสูงและมีประสิทธิภาพ:
บุคลากรสามารถปฏิบัติงานบนระบบดิจิทัลได้อย่างมั่นใจ

ลดอัตราการเกิดเหตุการณ์ระบบล่มอันเนื่องมาจากมัลแวร์ หรือการหยุดชะงักจากการถูกโจมตีทางไซเบอร์ ทำให้ข้อมูลระบบราชการไม่สูญหายและมีความถูกต้องครบถ้วน

8.2 บริการภาครัฐมีความน่าเชื่อถือและได้รับความไว้วางใจจากประชาชน:

ช่องทางการสื่อสารและการให้บริการของสถาบันฯ (เช่น ระบบลงทะเบียน แชทบอท หรือฐานข้อมูลหลักสูตร) มีมาตรการปกป้องข้อมูลที่รัดกุม ป้องกันการเข้าถึงโดยมิชอบตลอด 24 ชั่วโมง

ช่วยลดโอกาสที่ข้อมูลส่วนบุคคลของประชาชนจะรั่วไหล

ส่งผลให้ภาพลักษณ์ของหน่วยงานมีความมั่นคงปลอดภัยในระดับสูง

8.3 วัฒนธรรมองค์กรที่ตระหนักรู้ด้านความปลอดภัย: เจ้าหน้าที่มีพฤติกรรมการใช้งานไอทีที่ปลอดภัย ไม่เปิดลิงก์สุ่มเสี่ยง ตระหนักถึงความรับผิดชอบต่อข้อมูล และพร้อมปฏิบัติตามกฎหมายดิจิทัลอย่างเคร่งครัด

8.4 มีหลักสูตรการรักษาความปลอดภัยข้อมูลข่าวสารพื้นฐาน (Cybersecurity & Information Security Awareness) เป็นหลักสูตรใน DSD Online Training เผยแพร่ให้แก่ผู้ใช้แรงงานและผู้ที่สนใจ

9. ข้อเสนอแนะ

เพื่อต่อยอดการสร้างความมั่นคงปลอดภัยสารสนเทศให้เจ้าหน้าที่ของกรมพัฒนาฝีมือแรงงานอย่างยั่งยืน กรมพัฒนาฝีมือแรงงานมีความจำเป็นต้องจัดทำโครงการฝึกอบรมด้านการรักษาความปลอดภัยข้อมูลข่าวสาร และการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง

โดยเริ่มจากการกำหนดนโยบายความมั่นคงปลอดภัยที่ชัดเจนและประกาศใช้อย่างเป็นทางการ

เพื่อให้ทุกคนเข้าใจทิศทางและข้อบังคับร่วมกัน นอกจากนี้

ควรมีการแต่งตั้งคณะทำงานหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

รวมถึงเจ้าหน้าที่เทคนิคเฉพาะทางในการมอนิเตอร์ระบบ

เพื่อให้สอดรับกับภารกิจหลักและการป้องกันภัยคุกคามได้อย่างทันท่วงที

อีกทั้ง การสร้างวัฒนธรรมองค์กรที่ส่งเสริมความตระหนักรู้เป็นสิ่งสำคัญอย่างยิ่ง

โดยควรจัดกิจกรรมทดสอบความพร้อมเป็นระยะ เช่น การจำลองส่งอีเมลฟิชชิง

ไปยังเจ้าหน้าที่เพื่อประเมินความเข้าใจ และสนับสนุนการปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบัน

รวมถึงการสื่อสารประชาสัมพันธ์อินโฟกราฟิกเตือนภัยร้ายทางไซเบอร์อย่างสม่ำเสมอ

ซึ่งจะช่วยกระตุ้นให้เกิดพฤติกรรมการทำงานที่ปลอดภัยและลดความเสี่ยงที่เกิดจากความผิดพลาดของมนุษย์ (Human Error) ได้อย่างมีประสิทธิภาพที่สุด