สรุปการจัดกิจกรรมจัดการความรู้

ของสำนักงานพัฒนาฝีมือแรงงานเลย

ประจำปีงบประมาณ ๒๕๖๕ รอบที่ ๒ (๑ เมษายน ๒๕๖๕ – ๓๐ กันยายน ๒๕๖๕)

หน่วยงาน สำนักงานพัฒนาฝีมือแรงงานเลย

กิจกรรม การจัดการความรู้ “การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์”

วัน/เวลา/สถานที่ วันที่ ๖ พฤษภาคม พ.ศ.๒๕๖๕ เวลา ๑๐.๐๐ น.
ณ ห้องประชุมสำนักงานพัฒนาฝีมือแรงงานเลย

กลุ่มเป้าหมาย บุคลากรของสำนักงานพัฒนาฝีมือแรงงานเลย

สำนักงานพัฒนาฝีมือแรงงานเลย ได้จัดกิจกรรมการจัดการความรู้ให้กับบุคลากรในสังกัด เพื่อสร้างสัมพันธภาพระหว่างบุคลากรในหน่วยงาน และเพื่อส่งเสริมให้บุคลากรพัฒนาทักษะด้านดิจิทัลของตนเอง เพื่อให้สามารถปฏิบัติงานได้ก้าวทันเทคโนโลยี ขับเคลื่อนองค์การไปสู่รัฐบาลดิจิทัลอย่างมีธรรมาภิบาลโดยผู้เข้าร่วมประชุม ประกอบด้วย ผู้อำนวยการและบุคลากรของหน่วยงานและได้คัดเลือกความรู้ที่ดำเนินการแลกเปลี่ยนความคิดเห็น เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

ขอบเขตของการจัดการองค์ความรู้จากการพัฒนาความรู้ที่จำเป็นด้านทักษะดิจิทัล

กิจกรรมที่นำไปใช้ประโยชน์ในการปฏิบัติงานได้แก่ การตรวจสอบและป้องกันการเข้าถึงข้อมูลของคอมพิวเตอร์ที่ใช้ในการปฏิบัติงาน

เป้าหมายในการจัดการองค์ความรู้

๑. ช่วยให้เกิดความคล่องตัวในการปฏิบัติงาน
๒. ช่วยให้เกิดการสร้างงานที่มีมูลค่าสูง
๓. ประชาชนสามารถเข้าถึงบริการได้ง่าย
๔. เกิดความคุ้มค่าในการใช้ทรัพยากร
๕. มีความสะดวก รวดเร็ว ในการให้บริการ
๖. ตรงต่อความต้องการของประชาชน

ประโยชน์ที่ได้รับจากการจัดการองค์ความรู้

๑. เจ้าหน้าที่มีความตื่นตัว ระมัดระวังและตระหนักถึงภัยคุกคามทางคอมพิวเตอร์
๒. การรักษาความลับของข้อมูลและการรักษาความถูกต้องของข้อมูล
๓. ช่องทางการให้บริการมีความมั่นคง ปลอดภัย
๔. การลดความเสียหายของข้อมูลและอุปกรณ์คอมพิวเตอร์
๕. การเข้าถึงข้อมูลได้ง่าย สะดวก รวดเร็วและมีความปลอดภัย
๖. สามารถรักษาความลับของข้อมูลของประชาชนทำให้เกิดความเชื่อมมั่นในการเข้ามาใช้บริการ

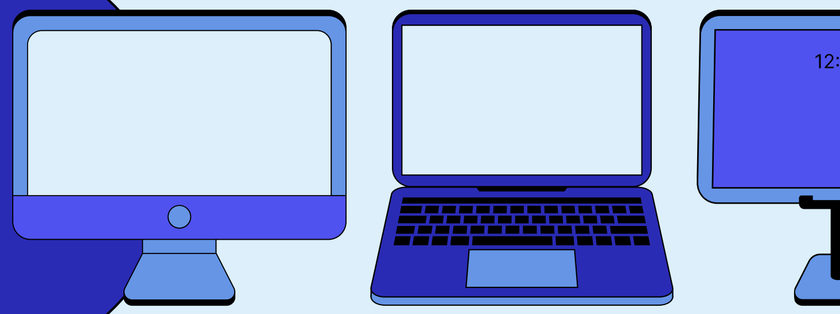
ปัญหาและข้อเสนอแนะในการจัดการองค์ความรู้

๑. เจ้าหน้าที่ยังขาดความระมัดระวังในการป้องกันภัยคุกคามทางไซเบอร์
๒. การตั้งรหัสผ่านง่ายทำให้กิดความเสี่ยงในการเข้าถึงข้อมูลโดยบุคคลอื่น
๓. ขาดการสำรองข้อมูลเพื่อป้องกันการเสียหาย

ขั้นตอนและกระบวนการดำเนินงานมีดังนี้

กระบวนการการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness)

หมวด Digital Literacy
สำนักงานพัฒนาฝีมือแรงงานเลย



1.ส่งเสริมให้บุคลากรพัฒนาทักษะด้านดิจิทัลของตนเอง เพื่อให้สามารถปฏิบัติงานได้ก้าวทันเทคโนโลยี ขับเคลื่อนองค์การไปสู่รัฐบาลดิจิทัลอย่างมีธรรมาภิบาล

3.จัดทำเนื้อหาความรู้ให้มีรูปแบบที่เข้าใจง่าย เหมาะสมและครบถ้วน

5. กำหนดให้บุคลากรเรียนรู้ได้ผ่านออนไลน์

ขั้นตอนแรก

ขั้นตอนที่ 2

2.กำหนดความรู้ที่จำเป็นในการขับเคลื่อนของหน่วยงาน “การสร้างการตระหนักรู้ด้านความมั่นคงทางไซเบอร์”

ขั้นตอนที่ 3

ขั้นตอนที่ 4

4.จัดเก็บองค์ความรู้ให้เป็นระบบ เข้าถึงง่าย สะดวกรวดเร็ว เช่น เว็บไซต์/เฟสบุ๊คหน่วยงาน

ขั้นตอนที่ 5

ขั้นตอนที่ 6

6. ประเมินผลการนำความรู้มาใช้ประโยชน์ในการปฏิบัติงาน

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (CYBERSECURITY AWARENESS)

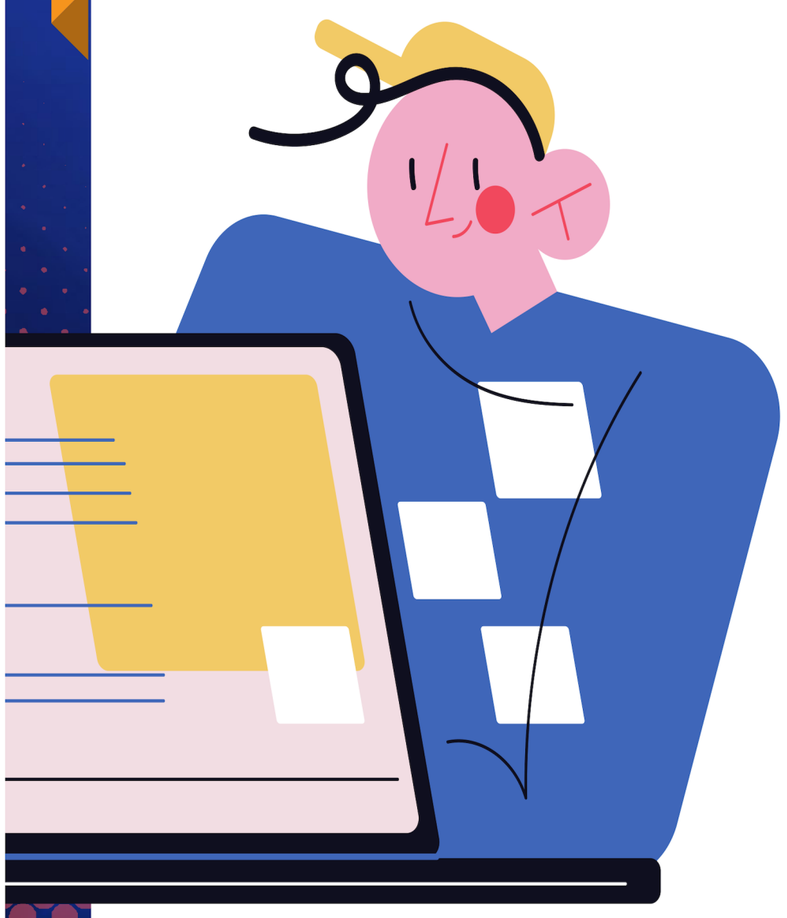
หมวด **DIGITAL LITERACY**

สำนักงานพัฒนาฝีมือแรงงานเลย

ความมั่นคงปลอดภัยทางไซเบอร์ (CYBERSECURITY) คืออะไร

คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ในปัจจุบันหน่วยงานของรัฐและภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ



ความรู้พื้นฐานของ CYBERSECURITY

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (CIA Triad)

C : Confldentlality การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้

I : Integrity การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้อง

A : Availability ความพร้อมใช้งานข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการบริการข้อมูล

รูปแบบภัยคุกคามของ **CYBERSECURITY**

ความตระหนักรู้ด้าน **CYBERSECURITY** ในชีวิตประจำวัน

1.ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

2.ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์หรือเลิกใช้งาน

3.ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

4.มีการ update patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

5.มีการ update version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

6.ไม่ควรจด Password และติด Password ไว้ที่หน้าจอและใช้ Password ที่ดีและไม่ควรบอก Password แก่ผู้อื่น

7.ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

8.ไม่เปิดไฟล์แนบจาก E-mai หรือช่องทาง Social ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

9.ไม่กด Link ใน E-mail หรือช่องทาง Social โดยไม่ตรวจเช็คให้ดี

10.เชื่อมต่อ Wifi ที่บ้านหรือที่ทำงาน หรือเชื่อมต่ออินเตอร์เน็ตจากเครือข่ายโทรศัพท์ ไม่ควรเชื่อมต่อ wifi สาธารณะ

กิจกรรมการจัดการองค์ความรู้
“การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์”
สำนักงานพัฒนาฝีมือแรงงานเลย