

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต 12

รอบการประเมินที่ 2 / 2569 ตั้งแต่วันที่ 1 เมษายน 2569 – 30 กันยายน 2569

ประจำปีงบประมาณ พ.ศ. 2569

ชื่อ-นามสกุล นางภาณิศา สอนจันทร์.....ตำแหน่ง นักวิชาการเกษตรชำนาญการ.....

หน่วยงาน ศูนย์/สพด./กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินนราธิวาส.....

หัวข้อการพัฒนา ความเข้าใจการบริหารความเสี่ยงและความปลอดภัยไซเบอร์ (Understanding
.....Cybersecurity Risk Management).....

วิธีการพัฒนา TDGA e-Learning.....

วันที่พัฒนา 21 กรกฎาคม 2569.....สถานที่ ผ่านระบบออนไลน์ (https://tdga.dga.or.th/)

หน่วยงานที่จัดอบรม สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).....

สรุปสาระสำคัญ

Cybersecurity คือการปกป้องระบบ ข้อมูล และเครือข่ายจากภัยคุกคามทางดิจิทัลที่เพิ่มขึ้นอย่างต่อเนื่อง มีความสำคัญต่อทั้งบุคคลและองค์กร เพราะช่วยลดความเสี่ยงด้านการเงิน ชื่อเสียง และความเชื่อมั่นของลูกค้าในยุคดิจิทัลที่ทุกอย่างเชื่อมต่อกันตลอดเวลา

ความสำคัญของ Cybersecurity

๑. ปกป้องข้อมูลส่วนบุคคลและข้อมูลลูกค้า ลดความเสี่ยงจากการโจรกรรมข้อมูล เช่น รหัสผ่าน เลขบัญชี หรือข้อมูลสุขภาพ
๒. รักษาความต่อเนื่องทางธุรกิจ ป้องกันการหยุดชะงักจากการโจมตี เช่น Ransomware ที่ล็อกข้อมูลและเรียกค่าไถ่
๓. สร้างความเชื่อมั่นและความน่าเชื่อถือ ลูกค้าและคู่ค้าจะมั่นใจมากขึ้นเมื่อองค์กรมีมาตรการรักษาความปลอดภัยที่เข้มแข็ง
๔. ปฏิบัติตามกฎหมายและข้อกำหนด เช่น GDPR ในยุโรป หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในประเทศไทย
๕. ลดความเสียหายทางการเงินและชื่อเสียง การโจมตีไซเบอร์อาจทำให้สูญเสียรายได้ มูลค่าหุ้น และภาพลักษณ์องค์กร

Cybersecurity Risk หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์ซึ่งอาจส่งผลกระทบต่อข้อมูลระบบ และความต่อเนื่องทางธุรกิจ หากไม่จัดการอย่างเหมาะสม อาจนำไปสู่ความเสียหายทางการเงิน ชื่อเสียง และความเชื่อมั่นของลูกค้า

ความสำคัญของ Cybersecurity Risk

๑. ป้องกันความเสียหายทางการเงิน ค่าใช้จ่ายจากการโจมตีไซเบอร์ เช่น Ransomware เฉลี่ยสูงถึง ๕.๑๓ ล้านดอลลาร์ในปี ๒๐๒๖ และยังมีค่าไถ่เฉลี่ย ๑.๕๔ ล้านดอลลาร์
๒. รักษาความต่อเนื่องทางธุรกิจ หากระบบล่มหรือข้อมูลถูกล็อก องค์กรอาจหยุดดำเนินงานทันที

๓. สร้างความเชื่อมั่นของลูกค้าและคู่ค้า การจัดการความเสี่ยงไซเบอร์อย่างจริงจังช่วยเพิ่มความน่าเชื่อถือ
๔. ปฏิบัติตามกฎหมายและมาตรฐานสากล เช่น PDPA ในไทย หรือ NIST Cybersecurity Framework ที่ใช้ทั่วโลก
๕. ลดผลกระทบต่อชื่อเสียงองค์กร การรั่วไหลของข้อมูลลูกค้าอาจทำให้สูญเสียความไว้วางใจในระยะยาว

กระบวนการของ Cybersecurity Risk

ขั้นตอน	เป้าหมาย	ตัวอย่าง
กำหนดขอบเขต	ระบุระบบ/ข้อมูลที่จะประเมิน	ระบบคลาวด์, แอปธุรกิจ
ระบุทรัพย์สิน	จัดลำดับความสำคัญ	ข้อมูลลูกค้า, บัญชีผู้ใช้
ระบุภัยคุกคาม	หาต้นเหตุที่อาจโจมตี	Phishing, Ransomware
ระบุช่องโหว่	ตรวจหาจุดอ่อน	ไม่มี MFA, Patch ไม่อัปเดต
ประเมินโอกาส/ผลกระทบ	วัดความเสี่ยง	High likelihood + High impact
จัดลำดับความเสี่ยง	กำหนดสิ่งที่ต้องแก้ก่อน	Ransomware > Misconfiguration
วางแผนจัดการ	เลือกวิธีตอบสนอง	Mitigate, Transfer, Accept, Avoid
ติดตาม/ทบทวน	ปรับปรุงต่อเนื่อง	Audit ทุก ๖ เดือน

Risk Assessment คือ กระบวนการสำคัญในการระบุ วิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้นกับองค์กรหรือกิจกรรม เพื่อให้สามารถวางแผนจัดการและลดผลกระทบได้อย่างมีประสิทธิภาพ โดยเป็นส่วนหนึ่งของมาตรฐานการบริหารความเสี่ยงสากล เช่น ISO ๓๑๐๐๐

ความสำคัญของ Risk Assessment

๑. ช่วยให้องค์กรเข้าใจความเสี่ยงที่แท้จริง ระบุได้ว่าความเสี่ยงใดมีผลกระทบสูงและต้องจัดการก่อน
๒. สนับสนุนการตัดสินใจเชิงกลยุทธ์ ข้อมูลจากการประเมินช่วยให้ผู้บริหารเลือกแนวทางที่เหมาะสม
๓. ลดความเสียหายและค่าใช้จ่าย การเตรียมมาตรการล่วงหน้าช่วยลดผลกระทบจากเหตุการณ์วิกฤต
๔. สร้างความมั่นคงและความเชื่อมั่น ลูกค้าและคู่ค้าจะมั่นใจมากขึ้นเมื่อองค์กรมีระบบจัดการความเสี่ยงที่ชัดเจน

Risk Management คือ กระบวนการบริหารความเสี่ยงอย่างเป็นระบบ เพื่อช่วยให้องค์กรหรือโครงการสามารถรับมือกับความไม่แน่นอน ลดผลกระทบ และใช้ทรัพยากรได้อย่างมีประสิทธิภาพ โดยอาศัยการระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยงอย่างต่อเนื่อง

ความสำคัญของ Risk Management

๑. ช่วยให้องค์กรรับมือกับความไม่แน่นอน เช่น ความผันผวนของตลาดหรือภัยธรรมชาติ
๒. ลดผลกระทบทางการเงินและชื่อเสียง โดยการเตรียมมาตรการล่วงหน้า
๓. สนับสนุนการตัดสินใจเชิงกลยุทธ์ ทำให้ผู้บริหารเลือกแนวทางที่เหมาะสมกับระดับความเสี่ยงที่ยอมรับได้
๔. สร้างความมั่นคงและความเชื่อมั่น ทั้งภายในองค์กรและต่อคู่ค้า/ลูกค้า

๕. ใช้ทรัพยากรอย่างมีประสิทธิภาพ โดยจัดลำดับความสำคัญของความเสี่ยงที่ต้องจัดการก่อน

Business Continuity Planning (BCP) คือการวางแผนเพื่อให้ธุรกิจสามารถดำเนินงานต่อไปได้แม้เกิดเหตุการณ์ไม่คาดคิด เช่น ภัยธรรมชาติ การโจมตีทางไซเบอร์ หรือวิกฤตเศรษฐกิจ โดยมีเป้าหมายเพื่อรักษาความต่อเนื่อง ลดผลกระทบ และฟื้นตัวได้อย่างรวดเร็ว

ความสำคัญของ BCP

๑. ลดผลกระทบต่อการดำเนินงาน เช่น ระบบล่มหรือการหยุดชะงักของซัพพลายเชน
๒. รักษาความเชื่อมั่นของลูกค้าและคู่ค้า เพราะธุรกิจยังคงให้บริการได้แม้เกิดวิกฤต
๓. ลดความเสียหายทางการเงินและชื่อเสียง
๔. สนับสนุนการปฏิบัติตามกฎหมายและมาตรฐานสากล เช่น ISO ๒๒๓๐๑
๕. เพิ่มความยืดหยุ่น (Resilience) ให้ธุรกิจพร้อมรับมือกับความไม่แน่นอน

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

นำความรู้ที่ได้รับไปใช้ในการปฏิบัติงานได้อย่างถูกต้อง และสามารถนำไปสื่อสาร และถ่ายทอดความรู้ให้แก่ผู้อื่นได้