ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

แนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อเป็นหลักในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับการดำเนินงานและวัตถุประสงค์ในการดำเนินธุรกิจ และได้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศและกำหนดให้พนักงานของบริษัทต้องปฏิบัติตามอย่างเคร่งครัด โดยครอบคลุมพนักงานและหน่วยงานทั้งหมดของบริษัทและหน่วยงานภายนอกที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับสารสนเทศของบริษัท โดยมีสาระสำคัญ ดังนี้

1) กำหนดให้หน่วยงาน Information Technology ทำหน้าที่ทบทวน หรือปรับปรุงนโนบาย กรอบการดำเนินงาน และ/หรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้สอดคล้องกับมาตรฐานสากล กฎหมาย และข้อกำหนดต่าง ๆ ที่เกี่ยวข้อง พร้อมทั้งมีหน้าที่รับผิดชอบบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อป้องกันภัยคุกคามทางไซเบอร์จากกระบวนการทางธุรกิจและจากกระบวนการผลิต

2) กำหนดข้อปฏิบัติการใช้บริการด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับหลักมาตรฐานสากลเพื่อป้องกันการโจมตีทางไซเบอร์ตลอดจนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับการบริหารความเสี่ยงในระดับองค์กร โดยขอบเขตของการปฏิบัติและบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงสินทรัพย์และบุคลากรทั้งหมดขององค์กรอีกทั้งหน่วยงานภายนอก

ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

แนวปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ

3) ติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุกด้านไซเบอร์ให้ครอบคลุมระบบสารสนเทศของบริษัท ควบคุมการจัดการ เข้าถึงข้อมูล การแลกเปลี่ยนข้อมูล การสำรองและทำลายข้อมูล พร้อมทั้งจัดให้มีการเฝ้าระวังโดยหน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ และรายงานข้อมูลภัยคุกคามด้านไซเบอร์ให้แก่ผู้บริหารรับทราบ

4) จัดทำแผนการตอบสนองเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์เพื่อการจัดการเหตุการณ์ผิดปกติได้อย่างรวดเร็วและมีประสิทธิภาพ ตลอดจนมีการติดตามเหตุการณ์ที่เกิดขึ้นและจัดทำแผนฟื้นฟูหลังจากเกิดเหตุการณ์ผิดปกติเพื่อลดผลกระทบต่อกระบวนการธุรกิจ รวมถึงจัดให้มีการซ้อมแผนเพื่อประเมินความถูกต้องและมีประสิทธิผลของแผน

5) สร้างความตระหนักรู้และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้กับพนักงานทุกคน ผ่านการสื่อความและจัดอบรม ให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) เพื่อให้พนักงานมีความเข้าใจและสามารถรับมือกับ ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ พร้อมทั้งมีความรับผิดชอบต่อความปลอดภัยของข้อมูลในงานของตนเอง และ เฝ้าระวังพฤติกรรมหรือกิจกรรมที่อาจเป็นภัยด้านด้านความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

โครงสร้างการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์

ทีวีโอมีการกำกับดูแลผ่านคณะกรรมการตรวจสอบและบริหารความเสี่ยง ซึ่งรับผิดชอบในการกำหนดนโยบาย กรอบการบริหารความเสี่ยงองค์กร (Enterprise Risk Management) โดยมีการจัดการผ่านคณะทำงานด้านการบริหารความเสี่ยง (Risk Management Working Group) และมีหน่วยงานด้านเทคโนโลยีสารสนเทศซึ่งเป็นเจ้าของความเสี่ยงระดับปฏิบัติการ หน้าที่บริหารจัดการ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และนำสู่การปฏิบัติการลดความเสี่ยงดังกล่าวโดยหน่วยงานที่เกี่ยวข้องต่อไป ทั้งนี้ภัยคุกคามทางไซเบอร์ถือเป็นภัยคุกคามหนึ่งที่มีโอกาสให้เกิดผลกระทบหรือมีความเสี่ยงต่อข้อมูลและระบบเทคโนโลยีสารสนเทศ และมีโอกาสที่จะสร้างผลเสียหายต่อลูกค้า ผู้มีส่วนได้ส่วนเสีย และคู่ค้าธุรกิจได้

วัตถุประสงค์

ทีวีโอมีความมุ่งมั่นในการพัฒนาและนำระบบเทคโนโลยีสารสนเทศมาใช้งานโดยให้มีการปฏิบัติที่สอดคล้องกับข้อกำหนดทางกฎหมายไอทีที่สำคัญ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562 เป็นต้น โดยมีวัตถุประสงค์ดังนี้

- เพื่อป้องกันข้อมูลสำคัญรั่วไหลหรือถูกทำลายจาก Ransomware/Virus เช่น ข้อมูลส่วนบุคคลต่างๆ
- เพื่อให้มีการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Risk) ที่สามารถระบุความเสี่ยง (Identify) ป้องกัน (Protect) ตรวจพบ (Detect) รับมือ (Respond)
- กู้ระบบคืนสู่สภาวะปกติ (Recover) และสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง

ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

มาตรการจัดการความเสี่ยง

เพื่อสร้างความมั่นใจในความสามารถป้องกันภัยคุกคามทาง Cybersecurity ที่อาจจะเกิดกับบริษัทได้อีกในอนาคต บริษัทจึงได้กำหนดมาตรการจัดการความเสี่ยงดังนี้

- ปรับปรุงระบบสำรองข้อมูล ให้ครอบคลุมทั้งระบบสารสนเทศหลักของบริษัท เช่น ระบบ ERP และระบบสารสนเทศอื่นๆ เพื่อป้องกันปัญหาในการกู้คืนข้อมูลจากความเสี่ยงด้าน Cyber Security
- กำหนดให้มีการทดสอบแผนสำรองฉุกเฉิน และการกู้คืนข้อมูลกรณีถูกโจมตีไซเบอร์เป็นประจำอย่างน้อยปีละ 1 ครั้ง
- ให้มีการทดสอบเจาะระบบ และตรวจความผิดปกติ/ช่องโหว่ อย่างน้อย 1 ครั้ง ใน 2 ปี โดยหน่วยงานอิสระภายนอกที่มีความเชี่ยวชาญเฉพาะทาง
- จัดให้มีช่องทางสำหรับแจ้งเหตุการณ์ที่น่าสงสัยหรือปัญหาด้านความมั่นคงปลอดภัยสารสนเทศ ผ่านช่องทาง MIS@tvothai.com

ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

ผลการดำเนินการประจำปี 2567

- ติดตั้งโปรแกรมป้องกัน Ransomware และ Full scan ในเครื่อง Server และเครื่องลูกข่ายทั้งหมด เพื่อให้มั่นใจว่าไม่มี Ransomware ใน System
- ดำเนินการทดสอบแผนสำรองฉุกเฉิน และการกู้คืนข้อมูล
- เพิ่มกระบวนการยืนยันตัวตนในการเข้าใช้งานระบบคอมพิวเตอร์
- Block การเข้าถึง/ส่งออกข้อมูลทาง Internet ของกลุ่มประเทศในกลุ่มเสี่ยง Ransomware ที่ตรวจพบผ่านอุปกรณ์ Firewall ของบริษัท
- จัดอบรมพนักงานเพื่อให้ความรู้แก่พนักงานเกี่ยวกับกฎหมาย PDPA และวิธีการปฏิบัติที่ถูกต้องในการจัดการข้อมูลส่วนบุคคล รวมไปถึงการให้ความรู้และความตระหนักต่อภัยทางไซเบอร์ (Cybersecurity Awareness) และทำแบบทดสอบความเข้าใจเรื่องความปลอดภัยทางไซเบอร์และ Phishing Mail

เอกสารที่เกี่ยวข้อง

- ระเบียบการใช้งานเครื่องคอมพิวเตอร์และเครื่อข่ายคอมพิวเตอร์ของบริษัท