ประกาศที่ PF051

นโยบายความปลอดภัยทางไซเบอร์

1. วัตถุประสงค์และขอบเขต

การรักษาความปลอดภัยทางไซเบอร์มีความสำคัญต่อกลุ่มบริษัท ASCC จึงกำหนดนโยบายกรอบการทำงานและมาตรการเพื่อสร้างและรักษาแนวปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ ปกป้องข้อมูลที่ละเอียดอ่อน รักษาความปลอดภัยของทรัพย์สิน และลดภัยคุกคามทางไซเบอร์ ซึ่งเป็นการปกป้องชื่อเสียง ทรัพย์สิน และความน่าเชื่อถือของผู้มีส่วนได้ส่วนเสีย

2. วัตถุประสงค์

2.1 เพื่อป้องกันข้อมูลและสารสนเทศ

การรักษาความลับและความพร้อมการเข้าใช้งานของข้อมูลที่สำคัญ ทรัพย์สินทางปัญญาและข้อมูลลูกค้า จากการเข้าถึง การเปิดเผย การดัดแปลง หรือการทำลายโดยไม่ได้รับอนุญาต

2.2 เพื่อป้องกันการโจมตีทางไซเบอร์

ใช้มาตรการป้องกันและตรวจจับการโจมตีทางไซเบอร์ เช่น มัลแวร์ ฟิชชิ่ง แรนซัมแวร์ และการใช้งานสื่อออนไลน์ โดยสร้างระบบการควบคุมและตรวจสอบความปลอดภัย

2.3 เพื่อกำหนดกรอบการจัดการความเสี่ยงทางไซเบอร์

พัฒนาระบบ และดำเนินการตามกรอบการจัดการความเสี่ยงทางไซเบอร์ที่ระบุไว้ ประเมิน และลดความเสี่ยงทางไซเบอร์ให้สอดคล้องกับกลยุทธ์การจัดการความเสี่ยงโดยรวมของบริษัทฯ

2.4 เพื่อความสามารถในการตอบสนองต่อเหตุการณ์

จัดทำแผนฉุกเฉิน และกำหนดทีมตอบสนองต่อเหตุการณ์ทางไซเบอร์แบบทันทีและมีประสิทธิภาพ ลดผลกระทบและกู้คืนได้อย่างรวดเร็ว

2.5 เพื่อส่งเสริมความตระหนักและการฝึกอบรมของพนักงาน

ให้ความรู้แก่พนักงานเกี่ยวกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ แนวปฏิบัติที่เหมาะสม และบทบาทความรับผิดชอบในการปกป้องข้อมูลของบริษัทฯ ส่งเสริมวัฒนธรรมของการตระหนักรู้และความรับผิดชอบด้านความปลอดภัยในโลกไซเบอร์

3. หน้าที่และความรับผิดชอบ

3.1 ความรับผิดชอบของผู้บริหาร

3.1.1 แสดงความเป็นผู้นำในการจัดลำดับความสำคัญของความปลอดภัยทางไซเบอร์เป็นองค์ประกอบที่สำคัญของการดำเนินงานของบริษัท

3.1.2 กำหนดบทบาทและความรับผิดชอบที่ชัดเจนสำหรับความปลอดภัยทางไซเบอร์ภายในกลุ่มบริษัท

3.1.3 จัดสรรทรัพยากรที่เหมาะสมสำหรับการริเริ่มและการฝึกอบรมด้านความปลอดภัยทางไซเบอร์

3.1.4 ตรวจสอบและปรับปรุงนโยบายความปลอดภัยทางไซเบอร์และขั้นตอนที่เกี่ยวข้องอย่างสม่ำเสมอ

3.2 ความรับผิดชอบของทีมไอทีและทีมความปลอดภัย

3.2.1 ปรับปรุง และรักษาการป้องกันทางเทคนิค ได้แก่ ไฟร์วอลล์ (Firewall) ระบบตรวจจับการบุกรุก และการเข้ารหัส

3.2.2 ดำเนินการประเมินช่องโหว่และทดสอบการเจาะระบบและเครือข่ายอย่างสม่ำเสมอ

3.2.3 ตรวจสอบและวิเคราะห์การรับ-ส่งข้อมูลบนเครือข่าย ข้อมูลบันทึก และเหตุการณ์ด้านความปลอดภัยเพื่อการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างทันท่วงที

3.2.4 ตรวจสอบให้แน่ใจว่ามีกระบวนการจัดการแพตช์เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ทันที

3.3 ความรับผิดชอบของพนักงาน

3.3.1 ปฏิบัติตามนโยบายความปลอดภัยทางไซเบอร์ ขั้นตอน และแนวทางปฏิบัติของบริษัท

3.3.2 รายงานเหตุการณ์ด้านความปลอดภัยหรือช่องโหว่ที่น่าสงสัยไปยังฝ่ายไอทีและ CFO ของกลุ่ม

3.3.3 เข้าร่วมโปรแกรมอบรมความรู้และความปลอดภัยทางไซเบอร์ที่บริษัทฯจัดให้

3.3.4 ดูแลอุปกรณ์ที่บริษัทมอบให้ รักษารหัสผ่าน และข้อมูลจากการเข้าถึงเพื่อใช้งานโดยไม่ได้รับอนุญาต

4. มาตรการรักษาความปลอดภัยทางไซเบอร์

4.1 การควบคุมการเข้าถึง

4.1.1 ใช้รหัสผ่านที่คาดเดาได้ยากและการยืนยันตัวตนแบบหลายขั้นตอนสำหรับการเข้าถึงระบบและข้อมูลของบริษัท

4.1.2 จำกัดสิทธิ์การเข้าถึงอย่างน้อยสิทธิ์พื้นฐาน

4.1.3 ตรวจสอบและปรับปรุงสิทธิ์การเข้าถึงว่ามีความถูกต้อง และได้รับอนุญาติ

4.2 การป้องกันข้อมูล

4.2.1 เข้ารหัสข้อมูลที่สำคัญ ทั้งระหว่างการจัดส่งและการจัดเก็บ โดยใช้การเข้ารหัสตามมาตรฐานอุตสาหกรรม

4.2.2 ใช้มาตรการป้องกันการสูญหายของข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลโดยไม่ได้รับอนุญาต

4.2.3 กำหนดแผนสำรองข้อมูลสำคัญเป็นประจำและทดสอบกระบวนการกู้คืน

4.3 ความตระหนักและการฝึกอบรมด้านความปลอดภัย

4.3.1 จัดให้มีการฝึกอบรมความตระหนักด้านความปลอดภัยในโลกไซเบอร์อย่างสม่ำเสมอแก่พนักงานทุกคน

4.3.2 ทำแบบจำลองฟิชชิ่งเพื่อทดสอบความตระหนักของพนักงาน และการจัดการกับฟิชชิ่ง

4.3.3 ให้ความรู้แก่พนักงานเกี่ยวกับนิสัยการท่องเว็บให้ปลอดภัย เทคนิควิศวกรรมในสังคมออนไลน์ และการจัดการอีเมลหรือไฟล์แนบที่น่าสงสัย

4.4 การตอบสนองต่อเหตุการณ์

4.4.1 ทบทวนแผนรับมือเหตุการณ์ที่กำหนดบทบาท ความรับผิดชอบ และขั้นตอนในการจัดการเหตุการณ์ความปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ

4.4.2 ทบทวนการตอบสนองเหตุการณ์ฉุกเฉินของทีมที่ได้กำหนดไว้อย่างสม่ำเสมอ และให้มั่นใจว่ามีการฝึกอบรม และเตรียมทรัพยากรที่จำเป็นอย่างเหมาะสม