วัตถุประสงค์และขอบเขต

การรักษาความปลอดภัยทางไซเบอร์มีความสำคัญต่อการดำเนินงานให้ประสบความสำเร็จของกลุ่มบริษัทในเครือ ASCC นโยบายนี้กำหนดกรอบการทำงานและมาตรการเพื่อสร้างและรักษาแนวปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ มีจุดมุ่งหมายเพื่อปกป้องข้อมูลที่สำคัญ รักษาความปลอดภัยของทรัพย์สินที่สำคัญ และลดภัยคุกคามทางไซเบอร์ ซึ่งจะเป็นการปกป้องชื่อเสียง ทรัพย์สิน และความเชื่อถือของผู้มีส่วนได้ส่วนเสียของบริษัท

วัตถุประสงค์

วัตถุประสงค์หลักของนโยบายนี้คือ:

• **ปกป้องข้อมูลสารสนเทศ**: รับรองการรักษาความลับ และความพร้อมใช้งานของข้อมูลสำคัญ ทรัพย์สินทางปัญญาและข้อมูลของลูกค้า จากการเข้าถึง การเปิดเผย การดัดแปลง หรือการทำลายโดยไม่ได้รับอนุญาต

• **ป้องกันการโจมตีทางไซเบอร์:** ใช้มาตรการป้องกันและตรวจจับการโจมตีทางไซเบอร์ เช่น มัลแวร์ (Malware), ฟิชชิง (Phishing) แรนซัมแวร์ (Ransomware) โดยสร้างระบบการควบคุมและตรวจสอบความปลอดภัยที่เข้มงวด

• **สร้างกรอบการจัดการความเสี่ยงทางไซเบอร์:** พัฒนาและดำเนินการตามกรอบการจัดการความเสี่ยงทางไซเบอร์ที่ครอบคลุมเพื่อระบุ ประเมิน และลดความเสี่ยงทางไซเบอร์ให้สอดคล้องกับกลยุทธ์การจัดการความเสี่ยงโดยรวมของบริษัท

• **เพิ่มขีดความสามารถในการตอบสนองต่อเหตุการณ์:** มีทีมงานเฉพาะเพื่อตอบสนองต่อเหตุการณ์ทางไซเบอร์อย่างทันท่วงทีและมีประสิทธิภาพ ลดผลกระทบและสามารถอำนวยความสะดวกในการกู้คืนอย่างรวดเร็ว

• **ส่งเสริมความตระหนักและการฝึกอบรมของพนักงาน:** ให้ความรู้แก่พนักงานเกี่ยวกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ แนวปฏิบัติ บทบาทและความรับผิดชอบในการปกป้องข้อมูลของบริษัท ส่งเสริมวัฒนธรรมของการตระหนักรู้และความรับผิดชอบด้านความปลอดภัยในโลกไซเบอร์

หน้าที่และความรับผิดชอบ

ความรับผิดชอบในการจัดการ:

• ให้ความสำคัญในการจัดลำดับเรื่องของความปลอดภัยทางไซเบอร์เป็นองค์ประกอบที่สำคัญของการดำเนินงานของบริษัท

• กำหนดบทบาทและความรับผิดชอบสำหรับความปลอดภัยทางไซเบอร์ภายในบริษัท

• จัดสรรทรัพยากรที่เหมาะสมและฝึกอบรมด้านความปลอดภัยในโลกไซเบอร์

• ตรวจสอบและปรับปรุงนโยบายความปลอดภัยทางไซเบอร์และขั้นตอนอย่างสม่ำเสมอ

ความรับผิดชอบของทีมไอทีและความปลอดภัย:

• ใช้และรักษาการควบคุมทางเทคนิคที่มีประสิทธิภาพ เช่น ไฟร์วอลล์ (Firewalls) ระบบตรวจจับการบุกรุก และการเข้ารหัส

• ดำเนินการประเมินช่องโหว่และทดสอบการเจาะระบบและเครือข่ายอย่างสม่ำเสมอ

• ตรวจสอบและวิเคราะห์การรับส่งข้อมูลเครือข่าย ข้อมูลบันทึก และเหตุการณ์ด้านความปลอดภัยเพื่อการตรวจจับและ ตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างทันท่วงที

• ตรวจสอบให้แน่ใจว่ามีกระบวนการจัดการเพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ทันที

ความรับผิดชอบของพนักงาน:

• ปฏิบัติตามนโยบายความปลอดภัยทางไซเบอร์ ขั้นตอน และแนวทางปฏิบัติของบริษัท

• รายงานเหตุการณ์ด้านความปลอดภัยหรือช่องโหว่ที่น่าสงสัยไปยังฝ่ายไอที

• เข้าร่วมโปรแกรมอบรมความรู้และความปลอดภัยทางไซเบอร์ในช่องทางต่างๆที่บริษัทจัดให้

• รักษาอุปกรณ์ที่บริษัทได้จัดเตรียมให้ รหัสผ่าน และรักษาข้อมูลความลับการเข้าถึงจากการใช้งานโดยไม่ได้รับอนุญาต

มาตรการรักษาความปลอดภัยทางไซเบอร์

ก. การควบคุมการเข้าถึง:

1.ใช้รหัสผ่านที่รัดกุมและการยืนยันตัวตนแบบหลายปัจจัยสำหรับการเข้าถึงระบบและข้อมูลของบริษัท

2. จำกัดสิทธิ์การเข้าถึงโดยยึดหลักการกำหนดสิทธิ์

3. ตรวจสอบและอัปเดตสิทธิ์การเข้าถึงและการอนุญาตของผู้ใช้อย่างสม่ำเสมอ

ข. การป้องกันข้อมูล:

1. ป้องกันการเข้ารหัสข้อมูลที่สำคัญ ทั้งก่อนและหลังการใช้งาน โดยใช้รหัสที่มีความปลอดภัยได้มาตรฐาน

2. ใช้มาตรการป้องกันการสูญหายของข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่ไม่ได้รับอนุญาต

3. สำรองข้อมูลสำคัญเป็นประจำและทดสอบกระบวนการกู้คืน

ค. ความตระหนักและการฝึกอบรมด้านความปลอดภัย:

1. จัดให้มีการฝึกอบรมความตระหนักด้านความปลอดภัยในโลกไซเบอร์อย่างสม่ำเสมอแก่พนักงานทุกคน

2. พนักงานมีความรู้ความเข้าใจและสามารถตอบสนองต่อการโจมตีในรูปแบบต่างๆ

3. ให้ความรู้แก่พนักงานเกี่ยวกับการท่องเว็บอย่างปลอดภัยในโลกโซเชียล และการจัดการอีเมลหรือไฟล์แนบที่น่าสงสัย

4. การตอบสนองต่อเหตุการณ์:

1. ทบทวนแผนรับมือ ความรับผิดชอบ และขั้นตอนในการจัดการเหตุการณ์ความปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ

2. ตรวจสอบความพร้อมของทีมอย่างสม่ำเสมอ ให้แน่ใจว่ามีการฝึกอบรมและมีการเตรียมพร้อมที่เหมาะสม

Version	**Date**	**Reason for Revision**	**Reviewer**	**Approved By**
1.0	June 2023	New Document	IT and Facilities officer, CFO	CEO