นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บทนำ

บริษัทจะมุ่งสร้างคุณค่าของสินค้าและบริการให้เหมาะสมกับความต้องการของลูกค้าในแต่ละพื้นที่ ควบคู่ไปกับการบริหารต้นทุนและค่าใช้จ่ายในการดำเนินธุรกิจให้อยู่ในระดับที่เหมาะสมเพื่อให้บริษัทสามารถส่งมอบความคุ้มค่าของสินค้าและบริการให้แก่ลูกค้าได้สูงที่สุด เพื่อให้บรรลุวิสัยทัศน์ในการเป็นช่องทางจัดจำหน่ายสินค้าวัสดุก่อสร้างและสินค้าตกแต่งบ้านที่ดีที่สุดในอาเซียน นอกจากการบริหารงานภายใต้หลักธรรมาภิบาล และมุ่งเน้นกระบวนการทำงานที่เป็นเลิศแล้ว บริษัทยังจะมุ่งพัฒนาช่องทางจัดจำหน่ายสินค้า การสร้างความสัมพันธ์กับลูกค้า การทำงานร่วมกับพันธมิตรทางธุรกิจ ควบคู่ไปกับการพัฒนาระบบเทคโนโลยีสารสนเทศและการพัฒนาบุคคลากร เพื่อรองรับการเติบโตและสร้างมูลค่าเพิ่มที่เหมาะสมให้แก่ผู้มีส่วนได้เสียและสังคมโดยรวม จึงได้จัดทำนโยบายความมั่นคงและความปลอดภัยของเทคโนโลยีสารสนเทศ เพื่อใช้กำกับดูแลและสนับสนุนการบริหารจัดการความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เพื่อสร้างความมั่นใจในการดำเนินกิจกรรมต่างๆของบริษัท และถูกต้องตามกฎหมายที่เกี่ยวข้อง

ระบบเทคโนโลยีสารสนเทศของบริษัททั้งหมด ทำงานบนระบบ Cloud 100% รวมถึงการรักษาความปลอดภัย เรื่อง Back up, Recovery, BCP ระบบ Cloud สามารถช่วยลดความจำเป็นในการใช้ระบบฮาร์ดแวร์ ลดการใช้ไฟฟ้าและทรัพยากรพลังงาน และลดค่าใช้จ่ายระบบฮาร์ดแวร์และบำรุงรักษาระบบต่าง ๆ และระบบ Cloud ยังสามารถช่วยลดการใช้คนในหลายด้าน ประหยัดเวลาในการจัดการระบบเครือข่ายและการดูแลรักษา การใช้ Server Cloud ช่วยลดการใช้งานของคนในด้านการดูแลและการจัดการระบบ บริการ Cloud จะมีแผงควบคุมแบบเว็บที่ใช้งานง่าย ช่วยให้ผู้ดูแลระบบสามารถติดตามและควบคุม Server Cloud ได้โดยง่ายผ่านอินเตอร์เฟซที่ใช้งานง่าย ยังมีการติดตามและบันทึกเหตุการณ์ที่เกิดขึ้นกับ Server อย่างละเอียดเป็นระยะเวลา ทำให้การตรวจสอบและการดำเนินการต่อไปเป็นไปได้อย่างรวดเร็ว

วัตถุประสงค์

1. เพื่อกำหนดหลักการและข้อบังคับในการบริหารจัดการด้านความปลอดภัยของเทคโนโลยีสารสนเทศ
2. เพื่อสร้างความรู้ให้กับบุคลากร ให้ปฏิบัติตามนโยบาย รวมถึงกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศได้ถูกต้อง
3. เพื่อป้องกันไม่ให้ระบบเทคโนโลยีสารสนเทศถูกบุกรุกและทำลาย ในรูปแบบต่างๆที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจ และกิจกรรมต่างๆ ของบริษัท

องค์ประกอบของนโยบาย

1. การพิสูจน์ตัวตนเข้าใช้งานระบบ (Accountability, Identification and Authentication)

1.1 การพิสูจน์ตัวตน (Authentication) คือ กระบวนการยืนยันตัวตนผู้ใช้งาน ในการเข้าสู่ระบบ

1.2 การกำหนดสิทธิ์ (Authorization) เป็นการระบุว่าผู้ใช้งาน สามารถใช้งานเมนูไหนได้บ้าง / หรือทำอะไรกับระบบได้บ้าง

1.3 การบันทึกการใช้งาน (Accountability) คือ การบันทึกรายละเอียดของการใช้โปรแกรม โดยบริษัทมีการยืนยันตัวตนเพื่อเข้าใช้งานดังนี้

1) การใช้สแกนลายนิ้วมือ หรือ สแกนหน้า เพื่อระบุตัวตน

2) การใช้ OTP / Email เพื่อยืนยันการดำเนินการ

3) การกำหนด Secret Key / Token เพื่อ Access ระบบ (เฉพาะคนที่มี Secret Key / Toke เท่านั้น ถึงจะสามารถเข้าใช้งานได้ ไม่รวมกับ User / Password)

2. การบริหารจัดการทรัพย์สิน (Assets Management)

2.1 ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งานอยู่

2.2 ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทในทางที่ไม่เหมาะสม ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงซอฟท์แวร์ ในเครื่องคอมพิวเตอร์ของบริษัท

2.3 เว้นแต่ได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงานที่รับผิดชอบ

2.4 ต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อนสูง ความชื้นสูง มีฝุ่นละออง และต้องระวังการตกกระแทก

2.5 หลีกเลี่ยงการใช้ของแข็งกดทับหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้

2.6 การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ต้องทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน

2.7 ห้ามดัดแปลงส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง หากมีความจำเป็นให้แจ้งผู้ดูแลหรือหัวหน้างาน

2.8 และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ให้มีสภาพเดิม

2.9 ผู้ใช้งานที่พ้นสภาพต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน

2.10 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย

2.11 ห้ามติดตั้ง software ที่ผิดลิขสิทธิ์ และ software ที่ไม่เกี่ยวข้องกับงาน

3. การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ (Data access control)

3.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้สารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น
   - อ่านอย่างเดียว
   - สร้างข้อมูล
   - แก้ไขข้อมูล
   - อนุมัติ
   - ยกเลิก
   - ลบ
2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน ที่ได้กำหนดไว้
3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องได้รับการพิจารณาอนุญาตจากผู้บริหารส่วนงาน

3.2 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

1) จัดแบ่งประเภทข้อมูล ออกเป็น
   - ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลพนักงาน ข้อมูลทางด้านการเงิน
2) จัดแบ่งระดับความสำคัญของข้อมูล คือ
   - ข้อมูลที่มีระดับความสำคัญมาก
   - ข้อมูลที่มีระดับความสำคัญปานกลาง
   - ข้อมูลที่มีระดับความสำคัญน้อย
3) จัดแบ่งระดับชั้นการเข้าถึง
   - ระดับชั้นสำหรับผู้บริหาร
   - ระดับชั้นสำหรับผู้ใช้งานทั่วไป
   - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

4) การกำหนดเวลาในการเข้าถึง

5) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

3.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

1) มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งานครอบคลุมในเรื่องต่อไปนี้

- จัดทำแบบฟอร์มขอใช้ระบบสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มอิเล็กทรอนิกส์เพื่อขอเข้าใช้งานระบบ
- ตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
- มีการระบุชื่อ นามสกุล ของผู้ใช้งาน
- มีการระบุ ตำแหน่ง หน่วยงานที่สังกัด
- มีการลงนามของผู้บังคับบัญชาของผู้ใช้งาน
- มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
- มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ
- มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน
- เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

2) การทบทวนสิทธิการเข้าใช้งาน ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้ระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออกเปลี่ยนตำแหน่ง โอน ย้าย เป็นต้น

3.4 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

1) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ

2) เจ้าของข้อมูล จะต้องทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆที่ให้ไว้ยังคงมีความเหมาะสม

3) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลแต่ละชั้นความลับข้อมูล

4) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ Encryptionรูปแบบต่าง ๆ เป็นต้น

5) ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่บำรุงรักษาเครื่องคอมพิวเตอร์ หรือนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

4. การรักษาความปลอดภัยของการสำรองข้อมูล (Backup Policy)

4.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรอง ข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

4.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศ แต่ละระบบ

4.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถ แสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูล สำรองอย่างสม่ำเสมอ

4.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ ภายในระยะเวลาที่เหมาะสม

5. การรักษาความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย(Network and Server Policy)

5.1 ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

5.2 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของบริษัท ต้องได้รับอนุญาตจากผู้ดูแลระบบอย่างเคร่งครัด

5.3 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้ง เพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

5.4 ต้องมีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะ ระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบ เครือข่ายที่มีการใช้งานร่วมกัน

5.5 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถใน การตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

5.6 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

5.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อม ทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.8 ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษา ความครบถ้วน ถูกต้องและระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือ บุคคลที่หน่วยงานมอบหมาย

5.9 ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึก การเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บ บันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

5.10 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

5.11 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

6. การรักษาความปลอดภัยของอินเตอร์เน็ตและอีเมล์ (Internet and E-mail Security Policy)

6.1 การตั้งรหัสผ่านที่ปลอดภัย

1) รหัสควรมีความยาวอย่างน้อย 8 ตัวอักษร ซึ่งรหัสจะต้องประกอบไปด้วยอักษรตัวใหญ่ อักษรตัวเล็ก ตัวเลข และสัญลักษณ์ ผสมกันยิ่งเพิ่มความปลอดภัยให้กับรหัสมากขึ้น
2) หลีกเลี่ยงการใช้วัน เดือน ปีเกิด ชื่อตัวเอง รวมไปถึงชื่อต่าง ๆ ที่เกี่ยวข้องกับตัวเรามาใช้
3) ไม่ควรใช้คำศัพท์ในพจนานุกรม ไม่ว่าจะเป็นคำศัพท์แบบเดี่ยว เช่น home หรือนำหลาย ๆ คำมารวมกัน เช่น Good Home เนื่องจากแฮกเกอร์สามารถใช้โปรแกรมการเดารหัสผ่าน โดยเปรียบเทียบจากฐานข้อมูลคำศัพท์

4) แยกรหัสผ่าน หากเป็นคนละบัญชีผู้ใช้งาน โดยเฉพาะรหัสผ่านที่ใช้เข้าถึงข้อมูลสำคัญ อาจจะใช้วิธีตั้ง Password เป็นพวกเดียวกัน แต่เปลี่ยนตัวเลขที่ตามหลังเพื่อแยกความแตกต่าง
5) อย่าแทนตัวอักษรบางตัวด้วยตัวเลขที่ดูคล้ายกัน เช่น ตั้งรหัสผ่านว่า H0use โดยใช้เลข 0 (เลขศูนย์) แทน o (อักษรโอ) คนทั่วไปก็สามารถคาดเดาได้ถึงแม้จะผสมกัน

6.2 เลือกเว็บเบราเซอร์ที่ปลอดภัย

การเลือกเบราว์เซอร์ควรต้องมีระบบป้องกันป๊อบอัพ ไวรัส รวมทั้งภัยคุกคามด้านข้อมูลต่างๆ นอกจากนั้นควรที่จะสามารถลบข้อมูลส่วนตัวได้ เพื่อที่คุณจะได้มั่นใจเวลาท่องโลกอินเตอร์เน็ตในขณะที่กำลังออนไลน์อยู่

6.3 ตรวจสอบว่าการเชื่อมต่ออินเทอร์เน็ตของคุณมีความปลอดภัย

1) เปลี่ยนรหัสผ่าน (และชื่อผู้ใช้) ใหม่เสมอเมื่อเริ่มใช้งานอุปกรณ์ ไม่ควรใช้ค่าดังเดิมจากจากผู้ผลิต
2) เข้ารหัสข้อมูลด้วย WPA2 เพื่อป้องกันการถูกขโมยข้อมูล
3) ไม่ควรใช้ SSID เดิมที่ตั้งมาจากผู้ผลิต เพราะแฮกเกอร์อาจจะประเมินได้ว่าเป็น Wi-Fi Router ที่ไม่ได้ตั้งค่าความปลอดภัย ทำให้ตกเป็นเป้าหมายในการโจมตีได้
4) เปิดใช้งาน MAC Address Filtering เพื่อให้มั่นใจว่าเฉพาะอุปกรณ์ของเราเท่านั้นที่เชื่อมต่ออยู่
5) ยกเลิกการบรอดแคสต์ SSID เนื่องจากไม่จำเป็นต้องให้คนอื่นเข้าถึงอุปกรณ์ของเราได้ง่ายๆ
6) ปิดการเชื่อมต่อ Wi-Fi สาธารณะโดยอัตโนมัติ เสี่ยงข้อมูลสำคัญรั่วไหลสู่ภายนอก
7) เปิดใช้ฟีเจอร์ Firewall และติดตั้งซอฟต์แวร์ป้องกันไวรัสสำหรับปกป้องอุปกรณ์ในระบบ Wi Fi
8) ตั้งค่า Static IP ให้กับอุปกรณ์ภายใน เพื่อกำหนดขอบเขตการใช้งานและความปลอดภัยให้รัดกุม

6.4 ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

1) ติดตั้งโปรแกรมป้องกันไวรัส
2) อัพเดตข้อมูลไวรัส
3) ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่างๆ
4) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น แผ่นซีดี flash drive เป็นต้น
5) สแกนหาไวรัสสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
6) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย เช่น .pif เป็นต้น
7) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา
8) ใช้ความระมัดระวังในการเปิด E-mail
9) อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

10) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มาหรือมีไฟล์นามสกุลแปลกแนบมา

11) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

12) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่าง ๆ เช่น Line ,We chat ,Facebook, twister เป็นต้น

13) ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา

14) ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่น่าเชื่อถือ

15) ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

7. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

7.1 การจัดเก็บข้อมูล กำหนดให้มีการเข้ารหัสข้อมูลที่สำคัญก่อนการจัดเก็บ เช่นการเข้ารหัสด้วย SHA-256

7.2 การเรียกใช้ข้อมูล กำหนดให้การเข้าถึงข้อมูล หรือเรียกข้อมูลต้องเรียกผ่าน API ที่มีการใส่ token

7.3 การเชื่อมต่อข้อมูลกับเครือข่ายอินเตอร์เน็ต ต้องมีการเข้ารหัสด้วยเทคโนโลยี SSL (Secure Socket Layer) TLS (Transport Layer Security)

8. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

8.1 ควบคุมการเข้าถึงสถานที่

8.1.1 การอนุญาตให้เข้า-ออกสถานที่จัดเก็บ ติดตั้ง อุปกรณ์สารสนเทศ

8.1.2 การกำหนดสิทธิ์ในการเข้า-ออกสถานที่จัดเก็บ ติดตั้ง อุปกรณ์สารสนเทศ

8.1.3 การแบ่งแยกพื้นที่ทำงานให้ชัดเจน

8.1.4 ทบทวนมาตรการการเข้าถึงสถานที่จัดเก็บ ติดตั้ง อุปกรณ์สารสนเทศ

8.2 จัดให้มีระบบป้องกันความเสียหายอันเกิดจากอุบัติเหตุหรือภัยธรรมชาติ

8.2.1 ระบบป้องกันอัคคีภัย

- ถังดับเพลิงบรรจุสารดับเพลิง
- สารที่ใช้ในการดับเพลิง
- อุปกรณ์ตรวจจับควันไฟ
- อุปกรณ์สั่งฉีดสารดับเพลิงแบบอัตโนมัต

8.2.2 ระบบป้องกันอุทกภัย

- สร้างอาคารหรือห้องปฏิบัติการทางคอมพิวเตอร์ไว้ที่สูง

8.2.3 ระบบป้องกันภัยอันเกิดจากระบบไฟฟ้า

- ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลระบบคอมพิวเตอร์
- ติดตั้งเครื่องกำเนิดไฟฟ้า เพื่อใช้ในกรณีไฟฟ้าดับเป็นเวลานานซึ่งกิจการไม่สามารถดำเนินการได้ส่งผลกระทบต่อผู้ปฏิบัติงานและลูกค้า

9. การปกป้องข้อมูลส่วนบุคคลของลูกค้า (Data Privacy)

9.1 การเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

9.2 เก็บข้อมูลจากเจ้าของข้อมูลส่วนบุคคลเท่าที่จำเป็นต้องใช้งาน

9.3 ปรับปรุงให้ข้อมูลส่วนบุคคลถูกต้องและเป็นปัจจุบันอยู่เสมอ

9.4 ใช้ข้อมูลส่วนบุคคลตรงตามวัตถุประสงค์ที่ขอ และหากจะส่งต่อผู้อื่นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน

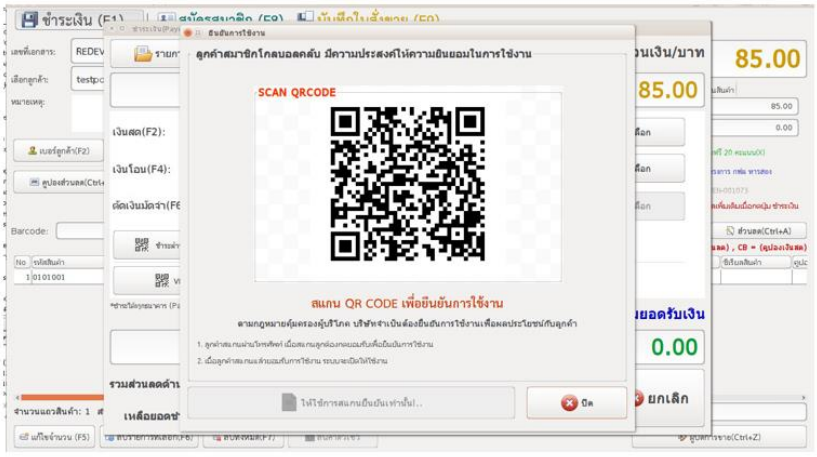
9.5 กำหนดระยะเวลาการเก็บข้อมูลตามวัตถุประสงค์การใช้งาน

9.6 มีมาตรการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย เช่นการเข้ารหัสข้อมูลที่สำคัญ

9.7 มีช่องทางให้เจ้าของข้อมูลส่วนบุคคลขอลบข้อมูลส่วนบุคคลที่จัดเก็บได้

9.8 มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล หรือ Data Protection Officers (DPO)

การขอความยินยอมจากลูกค้าช่องทางหน้าร้าน



การขอความยินยอมจากลูกค้าช่องทางออนไลน์

10. ออกแบบและพัฒนาโปรแกรม (System Development)

10.1 Coding คือ การเขียนชุดคำสั่งโปรแกรมคอมพิวเตอร์ ให้ทำงานตามที่กำหนด โดยการใช้ภาษาคอมพิวเตอร์ เช่น C++, C#, PHP, Java, Python, Dart

10.2 Test คือ การทดสอบโปรแกรมว่ากระบวนการทำงานถูกต้อง ตามที่ต้องการหรือไม่

10.3 Deploy คือ กระบวนการ Publish โปรแกรมที่ทำงานถูกต้อง ขึ้นสู่ Sandbox / Production เพื่อใช้งานจริง

10.4 Front-End คือ ส่วนสำหรับติดต่อกับผู้ใช้งาน (User Interface) ที่ User สามารถเห็นและใช้งานได้

10.5 Backup คือ การสำรองข้อมูล เพื่อป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูล อันเนื่องมาจากปัจจัยที่ไม่อาจควบคุมได้ เช่น Hdd พัง / มีการลบข้อมูลจากผู้ไม่หวังดี โดยบริษัทได้ทำการ Backup แบ่งเป็น

- Daily (Backup ทุกวันหลังปิดระบบ)
- Yearly (Backup ประจำปี ทุกๆวันสิ้นปี)

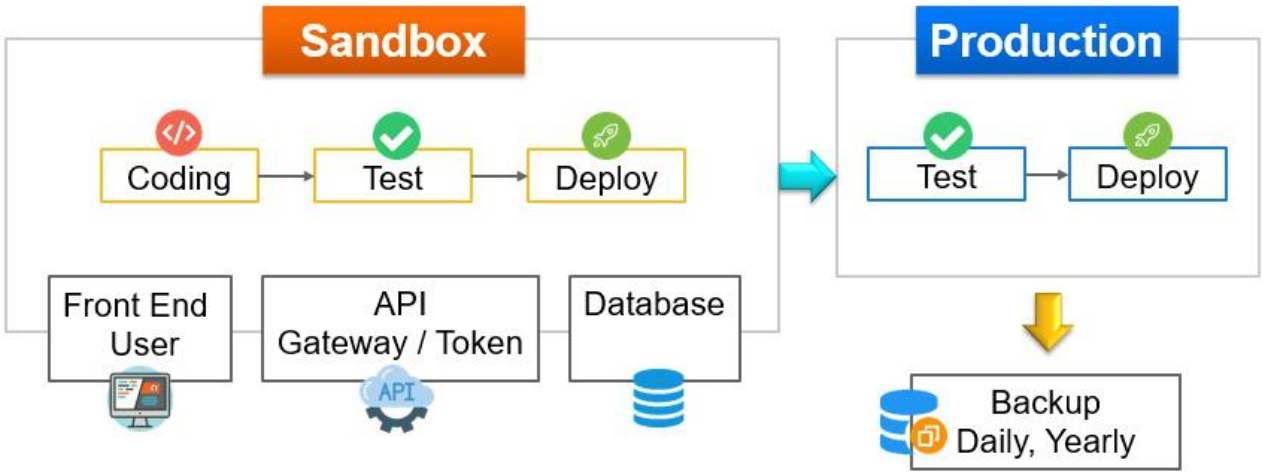
10.6 ข้อบังคับในการพัฒนาและการทดสอบระบบ

บริษัทได้จัดตั้ง sandbox (พื้นที่จำลองการพัฒนาและทดสอบระบบ) อันประกอบด้วย

- Server API Gateway
- Database Server

10.7 ให้ทีมพัฒนาทุกคน พัฒนาโปรแกรมบน sandbox เท่านั้น

Flow การออกแบบและพัฒนาโปรแกรม (System Development)



11. การใช้งานคลาวด์และรักษาความปลอดภัยในคลาวด์ (Cloud Security)

11.1 การใช้การรับรองความถูกต้อง (Authentication) และการตรวจสอบความปลอดภัย (Security Auditing):

- ใช้ระบบการรับรองความถูกต้อง (Authentication) ผู้ใช้งานเข้าถึงคลาวด์เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ตรวจสอบความปลอดภัยอย่างสม่ำเสมอ ตรวจสอบกิจกรรมที่เกิดขึ้นในระบบคลาวด์ ตรวจหาความผิดปกติที่อาจเกิดขึ้น

11.2 การจัดการสิทธิ์และการเข้าถึงข้อมูล

- กำหนดสิทธิ์การเข้าถึงข้อมูลระดับผู้ใช้งานแต่ละระดับในคลาวด์
- การเข้ารหัสข้อมูล (Encryption) เพื่อปกป้องข้อมูลที่เก็บอยู่ในคลาวด์ และใช้การเข้ารหัสสำหรับการสื่อสารระหว่างคลาวด์กับผู้ใช้งาน

11.3 การจัดการความเสี่ยงและการสังเกตุ (Risk Management and Monitoring)

- ประเมินและจัดการความเสี่ยงที่เกี่ยวข้องกับคลาวด์อย่างสม่ำเสมอ
- วางแผนการจัดการความเสี่ยงตรวจจับการบุกรุก (Intrusion Detection Systems) เพื่อตรวจสอบการโจมตีและความผิดปกติในคลาวด์

11.4 การปฏิบัติตามหลักการความปลอดภัย

- อัพเดตและรักษาความปลอดภัยของระบบคลาวด์อย่างสม่ำเสมอ
- ปรับปรุงและการอัพเกรดระบบปฏิบัติการและซอฟต์แวร์ที่ใช้งานในคลาวด์
- สร้างแผนการสำรองข้อมูล (Backup) เพื่อให้มั่นใจว่าข้อมูลสำคัญที่เก็บในคลาวด์ไม่สูญหาย

11.5 การฝึกอบรมและการแสดงความรับผิดชอบ

- ฝึกอบรมผู้ใช้งานเกี่ยวกับการรักษาความปลอดภัยในคลาวด์
- กำหนดบทบาทและความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับคลาวด์ให้ชัดเจน

12. **ลักษณะการกระทำความผิดทางไซเบอร์ภายในองค์กร**

12.1 ใช้รหัสผ่าน (Password) หรือการระบุตัวผู้ใช้อื่นๆ หรือรหัสผ่านแบบใช้ครั้งเดียว (OTP: One Time Password) ของบุคคลอื่นเข้าสู่ระบบคอมพิวเตอร์ของบริษัท การอ่าน คัดลอก อนุมัติ แก้ไข เปลี่ยนแปลง ลบ ไม่ว่าจะเพื่อประโยชน์ส่วนตนหรือของผู้อื่นโดยประมาทเลินเล่อ ใช้รหัสผ่าน (Password) หรือรหัสผู้ใช้อื่นหรือรหัสผ่านแบบใช้ครั้งเดียว (OTP: One Time Password) หรือจงใจให้ผู้อื่นใช้รหัสผ่านนั้น หรือรหัสผู้ใช้และสิทธิ์ในการใช้งานระบบคอมพิวเตอร์ของตนเอง

12.2 เปิดเผยข้อมูลธุรกิจหรือความรู้ของบริษัทที่เป็นความลับหรือถูกปกปิดแก่ผู้อื่นโดยไม่ได้รับอนุญาตจากบริษัท เจตนาขโมยหรือใช้ข้อมูลของบริษัทเพื่อเปิดเผย จำหน่าย แจกจ่ายแก่ผู้อื่นเพื่อประโยชน์ส่วนตัว อันก่อให้เกิดความเสียหายแก่บริษัทฯ

12.3 ลักลอบ ปลอมแปลงรหัสผ่าน (Password) หรือข้อมูลประจำตัวของผู้ใช้รายอื่นเพื่อจงใจเข้าสู่ระบบคอมพิวเตอร์ เพื่อกระทำการทุจริตต่อทรัพย์สินของบริษัทหรือของลูกค้าหรือทำให้เสื่อมเสียชื่อเสียง

12.4 ทำการคัดลอกหรือมีไว้ในครอบครองซึ่งไม่สมควรหรือผิดกฎหมาย เช่น ข้อความ รูปภาพลามกอนาจาร เป็นต้น หรือสิ่งอื่นใดอันเป็นการดูหมิ่นสถาบันชาติ ศาสนา และพระมหากษัตริย์ หรือยุยง ปลุกปั่นให้เกิดความแตกแยกในหมู่ประชาชนหรือพนักงานหรือ สร้างความเสียหายให้กับบริษัทฯ

12.5 การขโมย ลักลอบ ดักฟัง กำหนดเส้นทางหรือถอดรหัสข้อมูลอิเล็กทรอนิกส์ โดยใช้เครื่องมือหรือเทคโนโลยีอื่นใดเพื่อให้ได้มาซึ่งข้อมูลหรือความลับของบุคคลอื่นหรือของบริษัทโดยจงใจให้เกิดความเสียหายแก่บุคคลอื่นหรือบริษัทฯ

12.6 ประมาท เลินเล่อ ไม่ระมัดระวัง จนเป็นเหตุให้บุคคลอื่นสามารถลักลอบหรือนำข้อมูลของบริษัทไปเปิดเผย จำหน่าย จ่ายแจก พยายามเข้าถึงระบบที่ไม่มีสิทธิ์ หรือไม่ได้รับอนุญาตให้ใช้งานจงใจ หรือเจตนาก่อกวนหรือทำลายข้อมูลสารสนเทศ ระบบคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อสร้างความเสียหายต่อบริษัท

12.7 ติดตั้งหรือใช้งานซอฟต์แวร์ประเภท Hacking Tools หรือซอฟต์แวร์อื่นใดที่เกี่ยวข้องกับการตรวจสอบและเข้าถึงข้อมูลสำคัญของบริษัท ยกเว้นบุคคลหรือหน่วยงานที่รับผิดชอบด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยเฉพาะ

12.8 ทำการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่นใดเข้ากับระบบคอมพิวเตอร์หรือเครือข่ายของบริษัทโดยไม่ได้รับอนุญาตจากหน่วยงานที่รับผิดชอบทำการกำหนดและติดตั้ง หรือเปลี่ยนแปลง IP Address ด้วยตนเองโดยไม่ได้รับอนุญาตจากหน่วยงานที่รับผิดชอบ ทำการแก้ไข ดัดแปลง หรือเคลื่อนย้ายชิ้นส่วนองค์ประกอบระบบคอมพิวเตอร์โดยพลการหรือนำชิ้นส่วนอุปกรณ์คอมพิวเตอร์อื่นใดไม่ใช่ทรัพย์สินของบริษัทมาต่อหรือติดตั้งเพิ่มเติมกับทรัพย์สินของบริษัทโดยไม่ได้รับอนุญาต

12.9 ส่งข้อความหรือข้อมูลที่ไม่เหมาะสมโดยใช้ระบบ E-mail หรือใช้เครื่องมือสื่อสารของบริษัท เช่น หมิ่นประมาท คุกคาม ข่มขู่กรรโชก ใส่ร้าย ดูหมิ่นหรือส่งจดหมายลูกโซ่ เป็นต้น ใช้ Internet หรือระบบ Intranet หรือ E-mail ในเรื่องที่ไม่เกี่ยวข้องกับธุรกิจของบริษัท ใช้คอมพิวเตอร์และอุปกรณ์อื่นที่เป็นทรัพย์สินของบริษัทเพื่อความบันเทิงหรือประโยชน์ส่วนตน

12.10 ใช้ Software ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายหรือที่บริษัท ไม่ได้อนุญาตให้ใช้หรือที่อาจก่อให้เกิดความเสียหายต่อบริษัท

12.11 ให้ความช่วยเหลือ หรือร่วมมือกับบุคคลภายนอกเพื่อให้เข้าถึงระบบคอมพิวเตอร์หรือระบบข้อมูลสารสนเทศของบริษัท กระทำการคัดลอก หรือทำลายข้อมูลสารสนเทศหรือระบบคอมพิวเตอร์ของบริษัท

13. บทลงโทษสำหรับการกระทำความผิดทางไซเบอร์ภายในองค์กร

- ตักเตือนด้วยวาจา
- ตักเตือนเป็นลายลักษณ์อักษร
- พักงานชั่วคราวโดยไม่ได้รับค่าจ้าง
- ปลดออก
- ไล่ออก
- การดำเนินทางกฎหมายอาญาหรือแพ่ง

กรณีการลงโทษพนักงาน บริษัทไม่จำเป็นต้องปฏิบัติตามลำดับดังกล่าวข้างต้น บริษัทอาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

14. มาตรการรักษาความปลอดภัยทางไซเบอร์ การตอบสนองต่อภัยคุกคามทางไซเบอร์

นอกจากมาตรการต่าง ๆ ที่กล่าวมาแล้วข้างต้น พนักงานของบริษัทสามารถสอบถามรายงานความผิดปกติและแจ้งความเสียหายที่เกิดขึ้นจากการโจมตีใด ๆ ที่เกี่ยวข้องกับ Cyber Security ผ่านระบบการให้บริการ “IT Service center” ซึ่งอาจจะเกิดขึ้นได้ในการปฏิบัติงาน โดยแจ้งผ่านทาเมลล์cybersecurity@globalhouse.co.th จะมีเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศรับเรื่องไปดำเนินการตามกระบวนการและขั้นตอนการดำเนินงานที่ออกแบบไว้โดยเร็วที่สุด (Incident report and escalation process) ทั้งนี้ การสื่อสารและรายงานให้ผู้ที่เกี่ยวข้องรับไปดำเนินการ ตั้งแต่ระดับเจ้าหน้าที่ปฏิบัติการ ถึง ผู้บริหารระดับสูงที่เกี่ยวข้อง รวมทั้งมีการติดตามผลจนกว่าจะแก้ไขประเด็นปัญหาจบสิ้น

รายงานการฝ่าฝืน/ละเมิด

	2565
จำนวนเหตุการณ์การละเมิดความปลอดภัยของข้อมูล	0
จำนวนของลูกค้าและพนักงานที่ได้รับผลกระทบจากการละเมิด	0

ฉบับแก้ไขปรับปรุงครั้งที่ 1/2566 ลงวันที่ 6 มิถุนายน 2566

(นายวิทูร สุริยวนากุล)
ประธานเจ้าหน้าที่บริหาร
บริษัท สยามโกลบอลเฮ้าส์ จำกัด (มหาชน)