# นโยบายและแนวปฏิบัติการรักษาความปลอดภัย และคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ และการสื่อสาร


**บริษัท ศิครินทร์ จำกัด (มหาชน)**

**นโยบายและแนวปฏิบัติปฏิบัติการรักษาความปลอดภัยและคุมความเสี่ยง**
**ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร**
**บริษัท ศิครินทร์ จำกัด (มหาชน)**

บริษัท ศิครินทร์ จำกัด (มหาชน) ("ศิครินทร์") ตระหนักดีว่าระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology – ICT) เป็นโครงสร้างพื้นฐานสำคัญที่สนับสนุนการดำเนินธุรกิจหลักขององค์กร ทั้งในด้านการบริหารจัดการ การให้บริการทางการแพทย์ และการสื่อสารกับผู้มีส่วนได้เสียทุกกลุ่ม ความมั่นคงปลอดภัยของระบบสารสนเทศจึงเป็นหัวใจสำคัญในการรักษาความเชื่อมั่นของผู้รับบริการ ผู้ถือหุ้น คู่ค้า หน่วยงานกำกับดูแล และสังคมโดยรวม

ศิครินทร์มีความมุ่งมั่นที่จะบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพ ปลอดภัย และสามารถรับมือกับความเสี่ยงในทุกมิติ โดยคำนึงถึงความพร้อมด้านความปลอดภัยของข้อมูล ความต่อเนื่องในการให้บริการ การป้องกันการโจมตีทางไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล

นโยบายและแนวปฏิบัตินี้ได้กำหนดหลักเกณฑ์ กระบวนการ และบทบาทความรับผิดชอบของทุกภาคส่วนในองค์กร ตั้งแต่คณะกรรมการบริษัท ผู้บริหารระดับสูง คณะกรรมการความยั่งยืน จนถึงพนักงานทุกระดับ เพื่อให้การดำเนินการด้านเทคโนโลยีสารสนเทศของศิครินทร์เป็นไปอย่างปลอดภัย สอดคล้องกับกฎหมายที่เกี่ยวข้อง และสามารถรองรับภัยคุกคามทางไซเบอร์ที่ซับซ้อนในยุคดิจิทัลได้อย่างมีประสิทธิภาพ

**ขอบเขตของนโยบาย**

นโยบายนี้ครอบคลุมถึงการบริหารจัดการความปลอดภัยและความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งหมดของศิครินทร์ รวมถึงข้อมูล ทรัพยากร ระบบ และเครือข่ายที่เกี่ยวข้อง

**วัตถุประสงค์**

- เพื่อกำหนดแนวทางในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- เพื่อป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศ
- เพื่อสร้างความมั่นใจว่าการดำเนินงานของศิครินทร์เป็นไปตามมาตรฐานและกฎหมายที่เกี่ยวข้อง

**หน้าที่ความรับผิดชอบ**

**คณะกรรมการบริษัท**

- กำหนดวิสัยทัศน์ ทิศทาง และกรอบนโยบายด้านความปลอดภัยไซเบอร์และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์หลักของศิครินทร์
- พิจารณาและอนุมัตินโยบาย พร้อมทั้งกำกับติดตามการดำเนินการตามนโยบายให้เป็นไปอย่างมีประสิทธิภาพ
- กำกับดูแลให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างรอบด้าน ครอบคลุมทั้งเชิงเทคนิคและเชิงกลยุทธ์
- ส่งเสริมให้ศิครินทร์ปฏิบัติตามข้อกำหนดด้านกฎหมาย มาตรฐานสากล และแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

**ผู้บริหาร**

- รับผิดชอบการขับเคลื่อนการนำนโยบายไปสู่การปฏิบัติอย่างเป็นรูปธรรมในระดับหน่วยงานต่าง ๆ
- จัดสรรทรัพยากร ระบบ และบุคลากรที่เหมาะสมเพื่อสนับสนุนการบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ติดตามและประเมินประสิทธิผลของมาตรการควบคุมความเสี่ยง รวมถึงจัดทำรายงานเสนอคณะกรรมการอย่างสม่ำเสมอ
- ส่งเสริมการสร้างวัฒนธรรมองค์กรที่ตระหนักรู้ถึงความปลอดภัยไซเบอร์ในทุกระดับขององค์กร

**หน่วยงานที่เกี่ยวข้อง**

- ดำเนินการตามมาตรการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศที่กำหนดไว้ในนโยบายและแนวทางปฏิบัติ
- พัฒนาและปรับปรุงระบบงาน กระบวนการ และเทคโนโลยีเพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูลและระบบ
- ประสานงานในการตรวจสอบ วิเคราะห์ และจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น
- จัดทำรายงานเกี่ยวกับเหตุการณ์และความเสี่ยงทางเทคโนโลยีสารสนเทศ เสนอแก่ผู้บริหารเพื่อการพิจารณาและแก้ไข
- ให้การฝึกอบรมและสร้างความตระหนักแก่พนักงานในประเด็นด้านความมั่นคงปลอดภัยไซเบอร์และการใช้เทคโนโลยีอย่างปลอดภัย

**พนักงาน**

- ปฏิบัติตามนโยบายและแนวปฏิบัติด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ศิครินทร์กำหนดไว้อย่างเคร่งครัด
- ใช้งานระบบสารสนเทศ อุปกรณ์ และเทคโนโลยีต่าง ๆ อย่างระมัดระวัง ไม่ละเมิดกฎระเบียบหรือสร้างความเสี่ยงต่อระบบ
- เข้าร่วมการฝึกอบรม และพัฒนาความรู้เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ที่ศิครินทร์จัดให้
- รายงานเหตุการณ์ผิดปกติหรือภัยคุกคามที่อาจส่งผลกระทบต่อความปลอดภัยของระบบแก่หน่วยงานที่เกี่ยวข้องทันที

**แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ**

จุดมุ่งหมายเพื่อทำให้แน่ใจว่าองค์กรสามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุนและสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีมาใช้ได้อย่างมีประสิทธิภาพ การบริหารงานด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากรและข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายขององค์กรและการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่าเทคโนโลยีที่ศิครินทร์นำมาใช้สามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจและสร้างศักยภาพในการแข่งขันรวมทั้งเพิ่มมูลค่าให้กับองค์กร โดยศิครินทร์ต้องพิจารณาดำเนินการดังต่อไปนี้

**1. นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy)**

1.1. คณะกรรมการบริษัทและผู้บริหารระดับสูงมีหน้าที่ดูแลให้มีการกำหนดนโยบายการรักษาความปลอดภัย ของระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร รวมทั้งทำหน้าที่ในการพิจารณาอนุมัตินโยบายดังกล่าว ทั้งนี้ ศิครินทร์ต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและให้สามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานธุรกิจภายในศิครินทร์ เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้

1.2. จัดให้มีการประเมินประสิทธิภาพของนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยของศิครินทร์ ทั้งนี้การประเมินประสิทธิภาพศิครินทร์สามารถกระทำได้โดยหน่วยงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศของศิครินทร์ (IT Audit) หรือผู้ตรวจสอบภายนอก เพื่อปรับปรุงแก้ไขข้อบกพร่องของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของศิครินทร์

1.3. ในกรณีที่ศิครินทร์มีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการจากภายนอก (Outsource) ศิครินทร์ต้องจัดให้มีนโยบายเพื่อรองรับการใช้บริการดังกล่าว ซึ่งต้องครอบคลุมถึงวิธีการคัดเลือกและพิจารณาคุณสมบัติของผู้ให้บริการและมีข้อกำาหนดเกี่ยวกับการใช้บริการเพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม รวมถึงข้อกำหนดเกี่ยวกับการรักษาความลับของข้อมูล และไม่เปิดเผยข้อมูลที่มีความสำคัญ

1.4. ศิครินทร์ต้องมีมาตรการเพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้ให้บริการจากภายนอกให้เป็นไปตามข้อตกลงที่กำหนดไว้ โดยสามารถตรวจสอบกระบวนการปฏิบัติงานรวมทั้งมีแผนรองรับใน กรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ

**2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)**

ต้องสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงรวมของศิครินทร์ (Enterprise Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้

2.1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2.2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)

2.3. การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยงและผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

2.4. การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

2.5. การกำหนดตัวชี้วัดระดับความเสี่ยง (IT Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบเพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

**3. แนวทางควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ**

3.1. การรักษาความถูกต้องปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ อย่างน้อยต้อง ครอบคลุมในเรื่องดังต่อไปนี้

1) กำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเพื่อให้การปฏิบัติงาน เป็นไปอย่างถูกต้องและปลอดภัยเป็นลายลักษณ์อักษรเพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศ

2) การรับ - ส่งข้อมูลสารสนเทศ (Information Transfer) ทั้งภายในและภายนอกองค์กร ต้องรักษาความปลอดภัยของข้อมูลที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์โดยมีการป้องกันการเปลี่ยนแปลงแก้ไข หรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดี (Malware) ที่ถูกส่งผ่านช่องทางการสื่อสาร มีการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (Attachment Files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร โดยการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ

3) ศิครินทร์ต้องมีมาตรการป้องกันและตรวจสอบภัยคุกคามจากโปรแกรมที่ไม่ประสงค์ดี (Malware) โดยติดตั้ง โปรแกรมป้องกัน Malware ให้ครอบคลุมทั้งเครื่องประมวลผลและเครื่องคอมพิวเตอร์พร้อมทั้งปรับปรุงโปรแกรมป้องกัน ให้เป็นปัจจุบัน และสามารถแก้ไขระบบเทคโนโลยีสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติ นอกจากนี้ ศิครินทร์ต้องมีระบบหรือกระบวนการในการป้องกันเพื่อลดความเสี่ยงจากการทำ website เลียนแบบ (Phishing)

4) ศิครินทร์ต้องกำหนดให้มีการสำรองข้อมูลที่สำคัญทางธุรกิจ ระบบปฏิบัติการ โปรแกรมประยุกต์ ระบบงานคอมพิวเตอร์อย่างครบถ้วน และกำหนดเป้าหมายในการกู้คืนข้อมูล (Recovery Point Objective: RPO) เช่น ประเภทของข้อมูลและชุดข้อมูลล่าสุดที่จะกู้คืนได้ โดยศิครินทร์ต้องจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่เพื่อความปลอดภัย ในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหายและต้องทำการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ศิครินทร์ต้องมีการป้องกันความเสียหายของข้อมูลที่ทำการสำรองไว้ด้วย

5)

<u>การสำรองข้อมูล ศิครินทร์ต้องกำหนดวิธีปฏิบัติอย่างน้อยดังนี้</u>

- ☐ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
- ☐ประเภทสื่อที่ใช้ในการบันทึกข้อมูล (Media)
- ☐จำนวนที่ต้องสำรอง (Copy)
- ☐ขั้นตอนและวิธีการสำรองข้อมูล
- ☐สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล
- ☐กระบวนการกู้คืนข้อมูลในกรณีที่ข้อมูลสูญหาย

6) จัดเก็บและบันทึกหลักฐาน (Logs) ต่าง ๆ ของการเข้าใช้งานระบบเทคโนโลยีสารสนเทศให้ครบถ้วนและเพียงพอสำหรับการตรวจสอบ โดยอย่างน้อยต้องครอบคลุมการเข้าถึงและใช้งานระบบสารสนเทศ (Application Log) การใช้งานแฟ้มข้อมูลและการใช้อินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายในของศิครินทร์

7) ควบคุมและจำกัดสิทธิการติดตั้งซอฟท์แวร์บนระบบงาน เพื่อให้ระบบปฏิบัติงานมีความถูกต้องครบถ้วน และน่าเชื่อถือ รวมถึงทำการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอกก่อนทำการติดตั้งบนระบบงานของศิครินทร์ เพื่อตรวจหาช่องโหว่ที่อาจเกิดขึ้น (Technical Vulnerability Management) ของซอฟต์แวร์ที่จะติดตั้งใหม่อย่างเหมาะสม ในกรณีที่มีการติดตั้ง Feature เพิ่มเติมบนระบบงานเก่าศิครินทร์ต้องพิจารณาทำการทดสอบหาก feature ใหม่มีผลกระทบต่อระบบงานที่ใช้อยู่แล้ว

3.2. การควบคุมการเข้าถึงระบบสารสนเทศและข้อมูล (Access Control) เพื่อป้องกันการถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

1) การควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ โดยศิครินทร์ต้องกำหนดสิทธิในการเข้าถึงระบบและข้อมูลให้เหมาะสมตามความจำเป็นและหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการรั่วไหลของข้อมูลและแก้ไขฐานข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้ผู้ใช้งานต้องยืนยันตัวบุคคลโดยกำหนด Username และ Password เพื่อเข้าถึงข้อมูลได้ตามสิทธิที่กำหนด และบันทึกการเข้าถึงระบบโดยบัญชีผู้ใช้ทุกประเภท

2) การกำหนดมาตรการเพื่อสร้างความปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศ โดยศิครินทร์ต้องจัดพื้นที่ในการจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญ เช่น ห้องเซิร์ฟเวอร์ ศูนย์คอมพิวเตอร์ เป็นต้น ให้มีความปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว โดยต้องคำนึงถึงความปลอดภัยจากภัยธรรมชาติ และภัยคุกคามจากมนุษย์ และมีความมิดชิดรวมทั้งป้องกันมิให้มีการเปิดเผยข้อมูลและรายละเอียดของ พื้นที่หวงห้ามต่อสาธารณะ ศิครินทร์ต้องกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง และระบบการควบคุมการเข้าออกอย่างรัดกุม และศิครินทร์ต้องบันทึกข้อมูลการเข้า-ออกห้องเซิร์ฟเวอร์หรือ ศูนย์คอมพิวเตอร์ รวมถึงต้องจัดให้มีการรักษาความมั่นคงปลอดภัย เช่น มีระบบกล้องวงจรปิด เครื่องสแกนลายนิ้วมือ อุปกรณ์เตือนไฟไหม้ ถังดับเพลิงหรือระบบดับเพลิงแบบอัตโนมัติ ระบบไฟฟ้าสำรอง

3.3. การรักษาความปลอดภัยของข้อมูล (Data Security)

ศิครินทร์ต้องมีกระบวนการในการรักษาความปลอดภัยของข้อมูลที่เพียงพอแก่การป้องกันไม่ให้บุคคลที่ไม่มีอำนาจเกี่ยวข้องเข้าถึง หรือสามารถเปลี่ยนแปลงแก้ไขข้อมูล หรือนำข้อมูลไปใช้ประโยชน์ในทางที่ผิดกฎหมาย

1) ศิครินทร์ต้องทำการระบุว่าข้อมูลอะไรบ้างที่เป็นข้อมูลที่สำคัญหรือเป็นข้อมูลความลับของศิครินทร์ และทำการจัดประเภทข้อมูลตามระดับชั้นความลับและความสำคัญ เพื่อให้ข้อมูลที่สำคัญได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับ

2) กำหนดสิทธิ์ในการเข้าถึงข้อมูลที่สำคัญหรือข้อมูลความลับเพื่อป้องกันการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

3) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ศิครินทร์ต้องทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลให้สอดคล้องและเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้น

4) การจัดเก็บข้อมูลสำคัญหรือข้อมูลที่มีชั้นความลับ ศิครินทร์ต้องรักษาความปลอดภัยของข้อมูลโดยการเข้ารหัสข้อมูล ที่สามารถป้องกันการนำข้อมูลสำคัญไปใช้ประโยชน์ในทางที่ผิดในกรณีข้อมูลรั่วไหล และ สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่มีความสำคัญ

3.4. การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ ศิครินทร์ต้องทำการประเมินช่องโหว่ กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง

3.5. การรักษาความพร้อมใช้งานของระบบสารสนเทศ และการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ

1) ศิครินทร์ต้องมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management) โดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

- กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident Response Plan) อย่างเป็นลายลักษณ์อักษร
- ประเมินเหตุการณ์หรือจุดอ่อนของการรักษาความปลอดภัยระบบสารสนเทศ เพื่อพิจารณาระดับความรุนแรงของเหตุการณ์และผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
- จัดให้มีบุคคลหรือหน่วยงาน เพื่อทำหน้าที่รายงานเหตุการณ์ที่เกิดขึ้นดังนี้

| **รายงานทันทีเมื่อเกิดเหตุ** | **ระหว่างดำเนินการแก้ไข** | **แก้ไขปัญหาได้ และเหตุยุติ** |
|---|---|---|
| 1. วันเวลาที่เกิดเหตุการณ์<br>2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ ที่เกิดขึ้น<br>3. ผลกระทบที่คาดว่าจะเกิดขึ้น<br>4. ชื่อผู้ติดต่อ / ประสานงานของ ศิครินทร์เพื่อให้ข้อมูล | 1. วันเวลาที่เกิดเหตุการณ์<br>2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ ที่เกิดขึ้น<br>3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้นกับลูกค้าและศิครินทร์<br>4. การดำเนินการแก้ไขปัญหาและระยะเวลาในการแก้ไข<br>5. ความคืบหน้าในการแก้ไขปัญหา | 1. วันเวลาที่เกิดเหตุการณ์<br>2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น<br>3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้นกับลูกค้าและศิครินทร์<br>4. การดำเนินการแก้ไขปัญหา<br>5. ผลการแก้ไขปัญหาและระยะเวลาในการแก้ไข<br>6. แนวทางป้องกันในอนาคตและการเก็บรวบรวมหลักฐานเพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป |
| รายงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์และตรวจสอบยืนยันในเบื้องต้นแล้ว | รายงานภายใน 2 วันทำการถัดไปหลังทราบเหตุการณ์และตรวจสอบยืนยันแล้ว | รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จภายใน 15 วัน |

2) ศิครินทร์ต้องกำหนดให้มีการบริหารความต่อเนื่องทางธุรกิจในด้านระบบสารสนเทศ (Information Security of Business Continuity Management)

- จัดลำดับความสำคัญในการกู้คืนระบบงานให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น รวมถึงความสัมพันธ์ของแต่ละระบบงาน และการกำหนดระยะเวลาในการกลับคืนสภาพการดำเนินงานตามปกติของระบบงาน
- ขั้นตอนการแก้ไขปัญหาหรือตอบสนองต่อเหตุการณ์ในแต่ละสถานการณ์ที่เกิดขึ้น
- บุคคลที่ทำหน้าที่รับผิดชอบและมีอำนาจตัดสินใจรวมถึงกำหนดเจ้าหน้าที่ผู้รับผิดชอบที่สามารถปฏิบัติงานได้ในแต่ละสถานการณ์รวมทั้งมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
- ระบุทรัพยากรที่จำเป็นสำหรับระบบงานที่สำคัญที่จำเป็นต้องใช้ เช่น ข้อมูลรายละเอียดของศูนย์คอมพิวเตอร์สำรอง สถานที่ตั้ง แผนที่ เครื่องรุ่นคอมพิวเตอร์ ระบบที่ใช้ในการปฏิบัติงาน ข้อมูลและบันทึกต่าง ๆ โดยต้องมีระบบสารสนเทศที่อยู่ในสภาพพร้อมใช้งาน
- ศิครินทร์ต้องมีการสื่อสารแผน IT Continuity Plan ให้แก่เจ้าหน้าที่ที่เกี่ยวข้องเพื่อรับทราบและสร้างความเข้าใจที่ตรงกัน เพื่อให้สามารถนำไปปฏิบัติได้อย่างถูกต้องเมื่อเกิดเหตุการณ์

- ทดสอบการปฏิบัติตามแผน IT Continuity Plan อย่างน้อยปีละ 1 ครั้ง โดยต้องกำหนดให้มีการทดสอบในลักษณะสถานการณ์ที่สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการดำเนินธุรกิจของศิครินทร์และ เป็นสถานการณ์ที่มีความเป็นไปได้และสอดคล้องกับสถานการณ์ในปัจจุบันของศิครินทร์

นโยบายการป้องกันความขัดแย้งทางผลประโยชน์ฉบับนี้ เป็นฉบับปรับปรุงครั้งที่ 3 มีผลบังคับใช้ตั้งแต่วันที่ 16 มกราคม 2568 เป็นต้นไป โดยมติของคณะกรรมการบริษัทในการประชุม ครั้งที่ 1/2568 เมื่อวันที่ 15 มกราคม 2568

.....

นายเสนีย์ จิตตเกษม

ประธานกรรมการบริษัท