นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท สตาร์เฟล็กซ์ จำกัด (มหาชน) (“บริษัท”) มีความมุ่งมั่นที่จะกำกับดูแลและสนับสนุนการพัฒนาการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างมีประสิทธิภาพ และประสิทธิผล เพื่อให้มั่นใจว่าการดำเนินธุรกิจบรรลุตามวัตถุประสงค์และเป้าหมายที่กำหนด รวมทั้งการก้าวไปอย่างมั่นคง เติบโตอย่างยั่งยืนสอดคล้องกับหลักการกำกับดูแลกิจการที่ดี เพื่อให้บรรลุวัตถุประสงค์ดังกล่าว บริษัทจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

1. **ความมั่นคงปลอดภัยสารสนเทศ**

   ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สินสารสนเทศขององค์กร มีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการ และให้ความร่วมมือในการดำเนินการตามนโยบายอย่างเคร่งครัด การฝ่าฝืนนโยบายนี้ ถือเป็นความผิดที่ร้ายแรง โดยมีบทลงโทษถึงขั้นสูงสุดตามระเบียบขององค์กร

2. **ความสอดคล้อง**

   เพื่อให้การปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศเกิดความสอดคล้องกับทิศทางในการบริหารองค์กร ผู้บริหารระดับสูงมีหน้าที่ต้องดำเนินการทบทวนความสอดคล้องของขั้นตอนปฏิบัติ โดยมีการทบทวน อย่างน้อยปีละ 1 ครั้ง

3. **การบริหารจัดการทรัพย์สินสารสนเทศ**

   เพื่อให้การใช้งานทรัพย์สินสารสนเทศของบริษัทเกิดประโยชน์สูงสุด หน่วยงานที่ใช้สารสนเทศต้องดำเนินการจัดทำบัญชีและตรวจสอบทรัพย์สินสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และปรับปรุงแก้ไขสารสนเทศนั้นๆ เมื่อมีการเปลี่ยนแปลง

4. **ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม**

   ระบบสารสนเทศถือเป็นระบบที่สำคัญในการดำเนินการของบริษัท ดังนั้นห้องที่ติดตั้งระบบสารสนเทศแม่ข่ายต้องยึดถือสภาพแวดล้อมที่ปลอดภัยเป็นหลัก ป้องกันภัยคุกคามจากภายนอก และมีการควบคุมสิทธิ์การเข้าถึงอย่างเหมาะสม รวมถึงจัดเตรียมอุปกรณ์รักษาปลอดภัยให้พร้อมใช้งานตลอดเวลา อุปกรณ์ที่ใช้ได้รับการป้องกันการล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ

5. **ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล**

   5.1 ให้กำหนดมาตรการควบคุมและป้องกันระบบสารสนเทศให้มีความปลอดภัยในการรับส่งข้อมูล ห้ามมีการเปลี่ยนแปลง ทำซ้ำ ลบทิ้ง หรือทำลายข้อมูลบริษัทฯ รวมถึงห้ามเปิดเผยข้อมูลที่อยู่ในระบบข้อมูลของบริษัทฯ โดยไม่ได้รับอนุญาตจากบริษัทฯ เพื่อปกป้องความลับทางธุรกิจ และการนำสารสนเทศไปใช้ในทางมิชอบหรือไม่ตรงกับวัตถุประสงค์ของบริษัท และต้องวางแผนในการปรับปรุงระบบเครือข่ายให้รองรับการขยายตัวในอนาคต

   5.2 กำหนดมาตรการการใช้งานคอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกลเพื่อสนับสนุนการปฏิบัติงานของพนักงานที่มีความจำเป็น โดยคำนึงถึงความปลอดภัยของสารสนเทศเป็นสำคัญ

   5.3 ผู้บริหาร พนักงานและผู้ที่เกี่ยวข้อง พึงปกป้องดูแลรักษาบัญชีชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ห้ามใช้ร่วมกับผู้อื่น ห้ามการเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้

5.4 ห้ามผู้บริหาร พนักงานและผู้ที่เกี่ยวข้อง ใช้อีเมลของบริษัท ในการส่งต่อข้อความหรือรูปภาพที่ให้ร้าย ทำให้เสื่อมเสีย หรือหยาบคาย ลามก ข่มขู่ ก่อกวน สร้างความรำคาญให้กับผู้อื่น หรือสิ่งที่ขัดต่อกฎหมาย

6 ความสัมพันธ์กับผู้ให้บริการภายนอก

เพื่อให้การให้บริการจากผู้ให้บริการภายนอกเป็นไปอย่างมีประสิทธิภาพและต่อเนื่อง ให้บริษัททำข้อตกลงกับผู้ให้บริการภายนอกให้เป็นลายลักษณ์อักษร รวมถึงจัดทำทะเบียนควบคุมสัญญาว่าจ้างให้ถูกต้องและมีการทบทวน อย่างน้อยปีละ 1 ครั้ง

7 การควบคุมการเข้าถึง

ข้อมูลสารสนเทศถือเป็นทรัพย์สินสารสนเทศของบริษัทและมีลำดับความสำคัญในการใช้งาน ผู้บริหาร พนักงาน และผู้เกี่ยวข้อง จะต้องให้การใช้งานข้อมูลสารสนเทศของบริษัทเป็นไปตามสิทธิ์ในการเข้าถึงที่กำหนดไว้และตามลำดับชั้นความลับของสารสนเทศที่มีสิทธิ์ที่เข้าถึงได้เท่านั้น โดยสิทธิ์ในการเข้าถึงนี้จะต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้ง

8 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล

เพื่อให้การใช้งานสารสนเทศเป็นไปอย่างมีประสิทธิภาพ ผู้บริหาร พนักงาน และผู้เกี่ยวข้อง พึงใช้งานสารสนเทศตามหน้าที่และความรับผิดชอบของตนเองตามโครงสร้างภายในของบริษัท และตระหนักถึงความรับผิดชอบในการใช้งานและดูแลสารสนเทศของบริษัทให้มีความถูกต้องสมบูรณ์ตามหน้าที่ของตนเอง

9 ความมั่นคงปลอดภัยในการดำเนินงาน

เพื่อป้องกันมิให้การใช้ข้อมูลสารสนเทศเกิดติดขัดในการดำเนินงาน ให้บริษัทกำหนดมาตรการสำรองข้อมูลและจัดทำแผนการทดสอบกู้คืนข้อมูล และทบทวนแผนอย่างน้อยปีละ 1 ครั้ง นอกจากนี้ บริษัทฯกำหนดมาตรการจัดเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ให้ตรงข้อกำหนดของพ.ร.บ.คอมพิวเตอร์ เพื่อให้เป็นหลักฐานแก่เจ้าพนักงานเมื่อได้รับการร้องขอ รวมถึงจัดหาวิธีการป้องกันไวรัสคอมพิวเตอร์เพื่อไม่ให้สารสนเทศของบริษัทเกิดความเสียหาย

10 การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ

เพื่อให้การดำเนินธุรกิจของบริษัทฯมีความต่อเนื่องและไม่เกิดการชะงัก ให้บริษัทกำหนดแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศเพื่อรองรับการต่อเนื่องของธุรกิจเมื่อเกิดเหตุที่ทำให้ระบบสารสนเทศหยุดชะงัก เช่น ภัยพิบัติ โรคระบาด หรือระบบสารสนเทศเสียหาย เป็นต้น และสื่อสารไปยังพนักงานทุกคนทราบถึงแผนการดำเนินการเมื่อเกิดเหตุฉุกเฉิน ผู้บริหาร พนักงาน และผู้เกี่ยวข้องมีหน้าที่ให้ความร่วมมือในการดำเนินงานตามแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการซ้อมแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศซึ่งมีกำหนดซ้อมปีละ 1 ครั้ง

11 การจัดหา การพัฒนา และการเปลี่ยนแปลงระบบ

การเปลี่ยนแปลงระบบสารสนเทศเป็นปัจจัยสำคัญในการพัฒนาสารสนเทศให้มีประสิทธิภาพมากขึ้น ให้บริษัทกำหนดมาตรการเปลี่ยนแปลงระบบสารสนเทศโดยคำนึงถึงความต้องการใช้สารสนเทศเพื่อตอบสนองต่อนโยบายของบริษัทฯและก่อให้เกิดประโยชน์สูงสุดต่อบริษัท

12 การบริหารจัดการปัญหาด้านสารสนเทศ

บริษัทตระหนักถึงความสำคัญในการแก้ปัญหาการใช้งานสารสนเทศ เพื่อให้ลดความสูญเสียทรัพย์สินสารสนเทศ และทำให้เกิดการใช้งานสารสนเทศให้ถูกต้องและเกิดประสิทธิภาพมากที่สุด ผู้บริหาร พนักงาน และผู้เกี่ยวข้องมีหน้าที่ใช้งานสารสนเทศอย่างถูกต้องและเหมาะสม และมีการแก้ไขปัญหาการใช้งานสารสนเทศอย่างเหมาะสม โดยไม่ใช้งานสารสนเทศในทางอื่นที่บริษัทมิได้กำหนดไว้

ทั้งนี้ ตั้งแต่วันที่ 25 กุมภาพันธ์ 2569 เป็นต้นไป

บริษัท สตาร์เฟล็กซ์ จำกัด (มหาชน)