นโยบายการรักษาความมั่นคงปลอดภัย ของระบบสารสนเทศ

บริษัทได้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ในการดำเนินธุรกิจให้สอดคล้องและเป็นไปในแนวทางเดียวกับหลักการกำกับกิจการที่ดี สำหรับบริษัทจดทะเบียน CG Code 2560 ซึ่งคณะกรรมการบริษัท มิตรสิบ ลิสซิ่ง จำกัด (มหาชน) ในการประชุมเมื่อวันที่ 24 กุมภาพันธ์ 2569 ได้มีมติอนุมัติทบทวนนโยบายดังกล่าว

ประกาศ

นโยบาย การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(Information Security Policy)

นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อกำหนดเป็นแนวทางไว้เป็นกรอบนโยบาย (Policy) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ บริษัท มิตรสิบ ลิสซิ่ง จำกัด(มหาชน) และบริษัทในเครือ ให้ระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง

1. วัตถุประสงค์

1. เพื่อกำหนด และประกาศนโยบาย แนวทางปฏิบัติ และขั้นตอนการปฏิบัติงาน ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติตามอย่างเหมาะสม

2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสนเทศ ของ บริษัท มิตรสิบ ลิสซิ่ง จำกัด(มหาชน) และบริษัทในเครือ ว่าสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)

3. เพื่อเผยแพร่ให้ผู้ใช้งาน และผู้ดูแลระบบสารสนเทศ ของ บริษัท มิตรสิบ ลิสซิ่ง จำกัด (มหาชน) และบริษัทในเครือ ได้รับทราบและถือปฏิบัติตามนโยบายและระเบียบปฏิบัติที่กำหนดอย่างเคร่งครัด เพื่อให้ระบบสารสนเทศของบริษัทมีความมั่นคงปลอดภัยและเชื่อถือได้

2. ขอบเขต/แนวทางของนโยบาย

นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของ บริษัท มิตรสิบ ลิสซิ่ง จำกัด (มหาชน) และบริษัทในเครือ ประกอบด้วยหัวข้อหลัก ดังนี้

1. การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

2. การบริหารจัดการทรัพย์สินสารสนเทศ (Information Assets Management)

ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัทจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของบริษัทเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัท และผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

3. การบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของบริษัทถือเป็นทรัพย์สินของบริษัทห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาและส่วนงานแผนกเทคโนโลยีสารสนเทศ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัท หรือข้อมูลของผู้รับบริการ ไม่ให้เกิดการสูญหาย ไม่ให้นำไปใช้ในทางที่ผิด และการเผยแพร่โดยไม่รับอนุญาต

4. การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ผู้ใช้งานต้องดูแลและรักษาระบบสารสนเทศบริษัท ห้ามกระทำการใดๆ เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัท

5. ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

บริษัทได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทอนุญาตให้ใช้งานหรือที่บริษัทมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัทห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบในการกระทำดังกล่าว

6. การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

ผู้ใช้งานต้องพึงระวังไวรัส และโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ส่วนงานแผนกเทคโนโลยีสารสนเทศ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาต่อทรัพย์สินหรือข้อมูลของบริษัท

7. การปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ผู้ใช้งานต้องปฏิบัติตามกฎหมายที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังว่า บริษัทถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดนั้นเอง

8. การจัดทำแผนรองรับเหตุสุดวิสัย (Disaster Recovery Plan)

การจัดทำแผนรองรับเหตุสุดวิสัยเพื่อป้องกันความเสียหายที่จะเกิดขึ้นต่อระบบสารสนเทศ และเตรียมการรับเหตุการณ์ฉุกเฉินที่คุกคามต่อระบบสารสนเทศของบริษัท

9. การบริหารจัดการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (Supplire Relationship)

การบริหารจัดการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ โดยกำหนดระเบียบ ข้อบังคับ หลักเกณฑ์ และแนวปฏิบัติในการดำเนินงาน เพื่อใช้ในการติดตาม ทบทวน บริหารจัดการการเปลี่ยนแปลงการให้บริการ และตรวจประเมินการส่งมอบบริการของหน่วยงานภายนอกอย่างสม่ำเสมอ และเพื่อควบคุมการเข้าถึงหรือใช้งานข้อมูลระบบสารสนเทศของบริษัท ให้เป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

10. ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

เพื่อให้มีการควบคุมเปลี่ยนแปลงแก้ไขซอฟต์แวร์ หลังการแก้ไข/เปลี่ยนแปลง จะต้องทำการทดสอบการใช้งานในพื้นที่ทดสอบ(Test) ก่อนทุกครั้งจนมั่นใจว่าสามารถใช้งานได้จริง และมีประสิทธิภาพ จึงนำขึ้นฐานจริง (Production)

11. ควบคุมการเข้า - ออก และการปฏิบัติงานในห้อง Server

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศจากการเข้าถึงโดยไม่ได้รับอนุญาต

12. การสำรองข้อมูล และกู้คืนข้อมูล

เพื่อป้องกันข้อมูลจากการสูญหาย ถูกทำลาย จากเหตุการณ์ไม่พึงประสงค์หรือเหตุการณ์ที่ไม่คาดคิด เพื่อให้ระบบสารสนเทศของบริษัทสามารถให้บริการได้อย่างต่อเนื่อง และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

13. ความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

เพื่อกลั่นกรองข้อมูลให้มีความปลอดภัยต่อระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ของบริษัท ป้องกันการบุกรุก หรือสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศ

14. ความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-Mail Policy)

ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทหรือละเมิดสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจการในการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายบริษัท

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน