นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

Information Technology Security Policy

บริษัท สโตนเฮ้นจ์ อินเตอร์ จำกัด (มหาชน)

ฉบับปรับปรุง ประจำปี 2567-68

บริษัท สโตนเฮ้นจ์ อินเตอร์ จำกัด (มหาชน)

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของบริษัท สโตนเฮ้นจ์ อินเตอร์ จำกัด (มหาชน) และบริษัทย่อย รวมเรียกว่า (“กลุ่มบริษัท”) ที่พนักงานของกลุ่มบริษัทใช้ในการทำงานผ่านระบบสารสนเทศและระบบเครือข่ายร่วมกัน มีความสะดวกรวดเร็วในการทำงาน ใช้ในการค้นหาข้อมูลและติดต่อสื่อสารทั้งภายในและภายนอกองค์กร เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท

บริษัท สโตนเฮ้นจ์ อินเตอร์ จำกัด (มหาชน) จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเกิดประโยชน์สูงสุด

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จากทุกหน่วยงานและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการหวังเป็นอย่างยิ่งว่า นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทในการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศต่อไป

นโยบายฉบับนี้ได้รับการทบทวนและอนุมัติจากที่ประชุมคณะกรรมการบริษัทครั้งที่ 5/2566-67 เมื่อวันที่ 13 สิงหาคม 2567 และมีผลบังคับใช้ตั้งแต่วันที่ 14 สิงหาคม 2567

วัตถุประสงค์

1. เพื่อกำหนดทิศทางและสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ โดยให้ สอดคล้องตามภารกิจขององค์กร และไม่ขัดต่อกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง
2. เพื่อเผยแพร่ให้พนักงานทุกคนของกลุ่มบริษัทรับทราบ พร้อมถือปฏิบัติตามอย่างเคร่งครัด และใช้งานระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท ได้อย่างมีประสิทธิภาพและประสิทธิผลสูงสุด
3. เพื่อกำหนดกรอบการบริหาร การให้บริการ มาตรฐาน แนวทางปฏิบัติให้แก่ผู้บริหาร พนักงานผู้ใช้งาน ผู้ดูแลระบบ รวมถึงบุคคลภายนอกที่ปฏิบัติงานให้กับกลุ่มบริษัท

นโยบายที่เป็นสาระสำคัญแบ่งออกเป็นหมวดดังนี้

1. **ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ**
   - 1.1 จัดทำเอกสารนโยบายระบบการรักษาความมั่นคงปลอดภัระบบเทคโนโลยีสารสนเทศ
   - 1.2 ทบทวนการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
   - 1.3 การบริหารจัดการการปฏิบัติงานจากภายนอก
   - 1.4 การบริหารจัดการระบบเครือข่าย
   - 1.5 การบริหารจัดการระบบเครือข่ายไร้สาย
   - 1.6 การบริหารจัดการอินเตอร์เน็ตสำหรับผู้มาติดต่อ
   - 1.7 การควบคุมการเข้าออกห้อง Datacenter
   - 1.8 การรักษาความปลอดภัยห้อง Datacenter
   - 1.9 จัดอบรมให้ความรู้ความเข้าใจในหน้าที่ความรับผิดชอบของผู้ใช้งานเกี่ยวกับการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท
2. **การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ**
   - 2.1 การบริหารจัดการสิทธิของผู้ใช้งานในการเข้าถึงข้อมูล
   - 2.2 การบริหารจัดการบัญชีรายชื่อผู้เข้าใช้งาน
   - 2.3 หน้าที่ความรับผิดชอบ
3. **การสำรองข้อมูล การฟื้นฟูระบบข้อมูล และการเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉิน**
   - 3.1 จัดทำระบบสำรองข้อมูลในระบบเทคโนโลยีสารสนเทศ
   - 3.2 จัดทำแผนและระบบสำรองกรณีเกิดสถานการณ์ฉุกเฉิน
   - 3.3 กำหนดระยะเวลาในการสำรองข้อมูล และการตรวจสอบ
   - 3.4 ทดสอบระบบสำรองข้อมูล
   - 3.5 หน้าที่ความรับผิดชอบของผู้ดูแลระบบการสำรองข้อมูล
4. **การบริหารจัดการคอมพิวเตอร์ และการติดตั้งซอฟต์แวร์**
   - 4.1 การจัดการลงทะเบียนสินทรัพย์ ทั้งเช่า และซื้อ
   - 4.2 กำหนดผู้รายชื่อผู้ถือครอง
   - 4.3 เก็บข้อมูลผู้ถือครองบนระบบบริหารจัดการสินทรัพย์
   - 4.4 การขอใช้งานคอมพิวเตอร์ หรืออุปกรณ์อื่นๆ
   - 4.5 กำหนดสิทธิผู้ถือครองในการใช้งานคอมพิวเตอร์ และการติดตั้งซอฟท์แวร์
   - 4.6 หน้าที่ความรับผิดชอบผู้ถือครอง
5. **แนวทางปฏิบัติเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่บริษัทหรือพนักงานจัดหา / พัฒนา / การบำรุงรักษา**
6. **แนวทางปฏิบัติเกี่ยวกับคลาวด์**
   - 6.1 การขออนุญาตใช้คลาว์ด
   - 6.2 หน้าที่รับผิดชอบของผู้ใช้งาน

7. **การใช้ทรัพยากรระบบสารสนเทศ**

7.1 การไม่อนุญาตให้มีการใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศในทางที่ผิดกฎหมาย

7.2 การไม่ฝ่าฝืนระบบความปลอดภัย

7.3 การไม่ใช้อีเมล์หรือข้อความอื่น ๆ ในทางที่ผิด

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

หมวดที่ 1 ความมั่นคงและความปลอดภัยระบบเทคโนโลยีสารสนเทศ

1.1. ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการเผยแพร่ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศที่ผ่านการอนุมัติตามมติที่ประชุมคณะกรรมการบริษัท เพื่อให้ผู้ใช้งานทั้งภายในองค์กร หน่วยงานภายนอก และผู้ที่เกี่ยวข้องในขอบเขตรับทราบและถือปฏิบัติ

1.2. การทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการตรวจสอบ ทบทวน และ ประเมินนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อกลุ่มบริษัท

1.3. กำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities) ผู้บริหารระดับสูงสุดต้องแต่งตั้งผู้รับผิดชอบ และ มอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

1.4. การปฏิบัติงานจากภายนอกองค์กร เพื่อเข้ามาใช้งานทรัพยากรภายในองค์กร อุปกรณ์ที่เชื่อมต่อเข้ามาต้องเป็นทรัพย์สินขององค์กรและได้รับการอนุมัติจากทางฝ่ายเทคโนโลยีสารสนเทศ

1.5. การปฏิบัติงานจากภายนอกองค์กร ผู้ใช้จะต้องดำเนินการแจ้งคำขอ Username และ Password เป็นลายลักษณ์อักษรให้กับทางฝ่ายเทคโนโลยีสารสนเทศ และต้องใช้งานผ่านช่องทางที่จัดเตรียมไว้ให้ และต้องมีการตรวจสอบยืนยันตัวตนก่อนการใช้งาน ไม่ควรเก็บข้อมูลที่เป็นความลับไว้ที่อุปกรณ์ส่วนตัว หรือหากจำเป็นต้องใช้งานเมื่อใช้เสร็จ ควรดำเนินการลบข้อมูลนั้นทิ้งไป

1.6. เพื่อเป็นการป้องกันการเข้าถึงระบบเครือข่าย (LAN) จะต้องเป็นอุปกรณ์ที่ได้รับการขึ้นทะเบียนทรัพย์สิน และต้องได้รับการอนุมัติการใช้งานจากฝ่ายเทคโนโลยีสารสนเทศ มีการยืนยันตัวตนก่อนการใช้งานโดยใส่ Username และ Password ของ Domain ก่อนเข้าใช้งาน เพื่อความปลอดภัยและป้องกันทางฝ่ายเทคโนโลยีสารสนเทศไม่อนุญาตให้นำเครื่องส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายได้

1.7. เพื่อเป็นการป้องกันการเชื่อมต่อกับระบบเครือข่ายไร้สาย พนักงานต้องนำอุปกรณ์มาลงทะเบียนและขออนุมัติกับฝ่ายเทคโนโลยีสารสนเทศ หากผู้ติดต่องานกับกลุ่มบริษัทมีความจำเป็นต้องขออนุมัติใช้งานสามารถติดต่อลงทะเบียนได้ที่ประชาสัมพันธ์เพื่อรับ Username และ Password สำหรับการใช้งานระบบเครือข่ายไร้สาย (Wi-Fi)

1.8. เพื่อเป็นการป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นการเปิดเผยหรือการขโมยข้อมูล กำหนดให้พนักงานของกลุ่มบริษัทมีหน้าที่รับผิดชอบในการตั้งและเปลี่ยนรหัสผ่านในการเข้าสู่ระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท ไม่เปิดหน้าจอคอมพิวเตอร์ค้างไว้ โดยไม่มีการป้องกันผู้อื่นเข้ามาใช้งานแทน ตลอดจนดูแลทรัพย์สินในระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทไว้ในที่ปลอดภัย เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์หวังดีนำสินทรัพย์ไปใช้ในทางที่ให้เกิดความเสียหายต่อกลุ่มบริษัทได้

1.9. เพื่อเป็นการควบคุมการเข้าออกห้อง Datacenter โดยมีจุดประสงค์เพื่อควบคุมรักษาความปลอดภัยของระบบงาน ระบบเครือข่าย และข้อมูลของกลุ่มบริษัทโดยกำหนดให้มีการจำกัดการเข้าห้อง Datacenter ซึ่งในกรณีผู้ที่ไม่มีหน้าที่เกี่ยวข้องจำเป็นต้องเข้าพื้นที่จะต้องลงบันทึกเวลาเข้าออกในสมุดบันทึกพร้อมระบุเหตุผล และต้องมีเจ้าหน้าที่เทคโนโลยีสารสนเทศคอยดูแลควบคุมการเข้าพื้นที่

1.10. การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

1.11. พนักงานมีหน้าที่ต้องรับผิดชอบดำเนินการให้เป็นไปตามนโยบายที่กำหนดขึ้นนี้อย่างเคร่งครัด ผู้ที่ฝ่าฝืนไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าข้อหนึ่งข้อใด หรือละเมิดลิขสิทธิ์ในการใช้โปรแกรมคอมพิวเตอร์ของกลุ่มบริษัท เพื่อผลประโยชน์ของตนเอง หรือบุคคลอื่นนอกเหนือจากภาระหน้าที่รับผิดชอบของตน หรือเพื่อผลประโยชน์ของกลุ่มบริษัท ถือเป็นความผิดวินัยพนักงาน

หมวดที่ 2 ควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.1 เพื่อให้การบริหารจัดการบัญชีผู้ใช้เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ผู้บังคับบัญชาและเจ้าหน้าที่บุคคลต้องแจ้งให้ ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออก หรือสิ้นสุดการเป็นผู้บริหาร พนักงาน ลูกจ้าง หรือถึงแก่กรรม
- โยกย้ายหน่วยงานหรือโครงการ รวมไปถึงเปลี่ยนหน้าที่ความรับผิดชอบ
- การพักงาน การลงโทษทางวินัย การระงับการปฏิบัติหน้าที่ หรือตามที่ผู้บังคับบัญชาท่านนั้นร้องขอ

2.2 ผู้บังคับบัญชาของแต่ละฝ่ายต้องเป็นผู้กำหนดสิทธิ์ในการเข้าถึงข้อมูลเป็นลายลักษณ์อักษร

2.3 เจ้าของระบบ (Owner System) จะต้องเป็นผู้พิจารณาสิทธิการเข้าถึงระบบต่างๆ ด้วยตนเอง

หมวดที่ 3 การสำรองข้อมูล การฟื้นฟูระบบข้อมูล และการเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉิน

3.1. เพื่อป้องกันการหยุดชะงักในการดำเนินงานของกลุ่มบริษัท ฝ่ายเทคโนโลยีสารสนเทศต้องมีการจัดทำแผนรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ กำหนดให้มีการทบทวน ตรวจสอบ และทบทวนแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

3.2. เพื่อเป็นการเตรียมความพร้อมการรองรับสถานการณ์ฉุกเฉิน กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการติดตั้งห้อง Datacenter สำรอง (Disaster Recovery Site) เพื่อให้ระบบที่มีความสำคัญสามารถดำเนินงานได้อย่างต่อเนื่อง

3.3. จัดทำระบบสำรองข้อมูลที่สำคัญในระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท เพื่อให้สามารถบริการได้อย่างต่อเนื่อง มีความเสถียรภาพ มีความปลอดภัย มีการตรวจสอบและดูแลระบบสำรองให้อยู่ในสภาพที่พร้อมนำมาใช้งานได้อยู่เสมอ มีการกำหนดเจ้าหน้าที่ผู้รับผิดชอบในการตรวจสอบและดูแลระบบสำรองข้อมูล

3.4. ให้ฝ่ายเทคโนโลยีสารสนเทศหรือให้ตกลงกับเจ้าของข้อมูล กำหนดระยะเวลาในการสำรองข้อมูล และระยะเวลาในการจัดเก็บข้อมูล

3.5. ผู้ดูแลระบบสำรองข้อมูลของกลุ่มบริษัทมีหน้าที่รับผิดชอบในการไม่สำรองข้อมูลส่วนตัว หรือข้อมูลที่ไม่เกี่ยวข้องกับการปฏิบัติงานของกลุ่มบริษัทลงในระบบสำรองข้อมูลของกลุ่มบริษัท ตลอดจนการเก็บรักษาข้อมูลของกลุ่ม

บริษัทไว้ในที่ที่กำหนดไว้อย่างปลอดภัย เพื่อให้ระบบสำรองข้อมูลสามารถกู้คืนข้อมูลของกลุ่มบริษัทกลับมาได้ และป้องกันไม่ให้ผู้ไม่ประสงค์ดีนำข้อมูลดังกล่าวไปใช้ในทางที่ทำให้เกิดความเสียหายต่อกลุ่มบริษัท

หมวดที่ 4 การบริหารจัดการคอมพิวเตอร์ และการติดตั้งซอฟท์แวร์

4.1. ฝ่ายเทคโนโลยีสารสนเทศจะต้องรายละเอียดข้อมูลของทรัพย์สินบนระบบบริหารจัดการสินทรัพย์ทั้งเช่า/ซื้อ

4.2. ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการบันทึกรายชื่อผู้ถือครองทรัพย์สินนั้นๆ บนระบบบริหารจัดการสินทรัพย์ให้ตรงตามข้อมูลปัจจุบันเสมอ และมีการเก็บข้อมูลผู้ถือครอง

4.3. การขอใช้งานคอมพิวเตอร์ หรืออุปกรณ์อื่นๆ ผู้ใช้งานต้องทำเรื่องแจ้งเป็นลายลักอักษรและต้องลงนามในเอกสารใบยืมวัสดุอุปกรณ์สำนักงาน

4.4. การควบคุมการติดตั้งระบบปฏิบัติการ และการติดตั้งซอฟท์แวร์จะต้องได้รับการอนุญาต การติดตั้งจากฝ่ายเทคโนโลยีสารสนเทศก่อนทุกครั้งและต้องเป็นซอฟท์แวร์ที่ไม่ละเมิดลิขสิทธิ์

4.5. ผู้ถือครองอุปกรณ์ของกลุ่มบริษัทมีหน้าที่รับผิดชอบอุปกรณ์ที่ยืมเหมือนเป็นอุปกรณ์ของตนเองให้สามารถใช้งานได้ดีอยู่เสมอ หากมีการเปลี่ยนอุปกรณ์ผู้ถือครองมีหน้าที่ดำเนินการโอนย้ายข้อมูลในอุปกรณ์นั้นด้วยตนเอง เมื่อผู้ถือครองใช้อุปกรณ์เสร็จเรียบร้อย ต้องนำมาคืนที่ฝ่ายเทคโนโลยีสารสนเทศ

หมวดที่ 5 แนวทางปฏิบัติเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่บริษัทหรือพนักงานจัดหา / พัฒนา / การบำรุงรักษา

5.1. การพัฒนาโปรแกรมหรือระบบเพื่อนำมาใช้งานในภายในกลุ่มบริษัท จะต้องได้รับการพิจารณาเห็นชอบเป็นลายลักษณ์อักษรจากผู้บริหาร หรือผู้มีอำนาจที่ได้รับมอบหมายจากกลุ่มบริษัท

5.2. การพัฒนาโปรแกรมหรือระบบที่พนักงานได้ร่วมกันพัฒนาขึ้นในฐานะพนักงานของกลุ่มบริษัท ให้ลิขสิทธิ์ในการพัฒนานั้นเป็นของกลุ่มบริษัท

หมวดที่ 6 แนวทางปฏิบัติเกี่ยวกับคลาวด์

6.1. การใช้บริการคลาวด์จะต้องได้รับการอนุญาตอย่างเป็นทางการจากฝ่ายเทคโนโลยีสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้ตรวจสอบรับรองว่าการให้บริการของผู้ให้บริการคลาวด์มีคุณสมบัติด้านความปลอดภัย

6.2. พนักงานผู้ใช้งานคลาวด์จะต้องมีความระมัดระวัง

หมวดที่ 7 การใช้ทรัพยากรระบบสารสนเทศ

7.1 กล่มบริษัท ต้องไม่ใช้หรือสนับสนุน ส่งเสริม อนุญาต อำนวยความสะดวก หรือแนะนำให้พนักงาน และ/หรือผู้อื่นใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทในทางที่ผิดกฎหมาย ทำให้เกิดอันตราย ฉ้อโกง ละเมิด หรือล่วงละเมิด หรือเพื่อส่ง จัดเก็บ แสดง แจกจ่ายหรือทำการอื่นใดอันมีเนื้อหาที่เป็นการผิดกฎหมาย เป็นอันตราย ฉ้อโกง ละเมิด หรือไม่เหมาะสม เป็นกิจกรรมหรือเนื้อหาที่ ต้องห้าม

7.2 พนักงานต้องไม่ฝ่าฝืนระบบความปลอดภัยหรือความสมบูรณ์ของเครือข่าย คอมพิวเตอร์ หรือระบบการสื่อสาร แอปพลิเคชันซอฟต์แวร์ข้อมูล หรือเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ (แต่ละประเภท เรียกว่า **"ระบบ"**) ได้แก่ การเข้าถึงเครือข่ายหรือระบบใด ๆ โดยไม่ได้รับอนุญาตหรือผิดกฎหมาย การติดตามหรือการดักฟังข้อมูลหรือการรับส่งข้อมูลของระบบ การปลอมแปลงแหล่งกำเนิดของข้อมูลที่มีการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต หรือในหัวของอีเมล์

7.3 กลุ่มบริษัทจะต้องไม่แจกจ่าย เผยแพร่ ส่ง หรืออำนวยความสะดวกในการส่งอีเมลหรือข้อความจำนวนมากที่ไม่ได้ร้องขอหรือข้อความการส่งเสริมการขาย การโฆษณา หรือการชักชวน (เช่น “Spam” หรือ “สแปม”) รวมถึง การโฆษณาเชิงพาณิชย์และการประกาศข้อมูล ตลอดจนจะไม่แก้ไขหรือปิดบังส่วนหัวของอีเมล หรือสวมรอยเป็นผู้ส่งโดยไม่ได้รับอนุญาตโดยชัดแจ้งจากผู้ส่ง หรือการส่งอีเมลที่ขัดขวางการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นในลักษณะที่ก่อให้เกิดความรำคาญแก่ผู้รับตามที่กฎหมายห้าม

หมายเหตุ กำหนดให้แนวปฏิบัติหรือระเบียบต่างๆ ที่เกี่ยวข้องหรือเกี่ยวเนื่องกับนโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายฉบับนี้

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ได้รับการปรับปรุงและอนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2566-67 เมื่อวันที่ 13 สิงหาคม 2567 จึงประกาศมาเพื่อทราบและให้ถือปฏิบัติต่อไป

นายจุมพล สำเภาพล
ประธานกรรมการ
บริษัท สโตนเฮ้นจ์ อินเตอร์ จำกัด (มหาชน)