

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

กลุ่มบริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน)



เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของบริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน) และบริษัทย่อย รวมเรียกว่า ("กลุ่มบริษัท") ที่พนักงานของกลุ่มบริษัท ใช้ในการทำงานผ่านระบบสารสนเทศและระบบเครือข่ายร่วมกัน มีความสะดวกรวดเร็วในการทำงานใช้ในการค้นหาข้อมูลและติดต่อสื่อสารทั้งภายในและภายนอกองค์กร เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท

บริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน) จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเกิดประโยชน์สูงสุด

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากทุกหน่วยงานและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ให้บริการ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทในการดูแล รักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศต่อไป

วัตถุประสงค์

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

นโยบายที่เป็นสาระสำคัญแบ่งออกเป็นหมวดดังนี้

1. ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
 - 1.1 จัดทำเอกสารนโยบายระบบการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
 - 1.2 ทบทวนการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
 - 1.3 การบริหารจัดการการปฏิบัติงานจากภายนอก

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
กลุ่มบริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน)



- 1.4 การบริหารจัดการระบบเครือข่าย
- 1.5 การบริหารจัดการระบบเครือข่ายไร้สาย
- 1.6 การบริหารจัดการอินเทอร์เน็ตสำหรับผู้มาติดต่อ
- 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 กำหนดรายชื่อผู้ถือครอง
 - 4.3 เก็บข้อมูลผู้ถือครองบนระบบบริหารจัดการสินทรัพย์
 - 4.4 การขอใช้งานคอมพิวเตอร์ หรืออุปกรณ์อื่นๆ
 - 4.5 กำหนดสิทธิผู้ถือครองในการใช้งานคอมพิวเตอร์ และการติดตั้งซอฟต์แวร์
 - 4.6 หน้าที่ความรับผิดชอบผู้ถือครอง
5. แนวทางปฏิบัติเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่บริษัทหรือพนักงานจัดหา / พัฒนา / การบำรุงรักษา
6. แนวทางปฏิบัติเกี่ยวกับคลาวด์
 - 6.1 การขออนุญาตใช้คลาวด์
 - 6.2 การกำหนดบทบาทและความรับผิดชอบ
 - 6.3 การควบคุมสิทธิ์การเข้าถึง
 - 6.4 การควบคุมการใช้คลาวด์ที่เป็นบัญชีเฉพาะบุคคล

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
กลุ่มบริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน)



- 6.5 ความปลอดภัยของระบบเครือข่ายและการเชื่อมต่อกับระบบคลาวด์
- 6.6 การจัดเก็บและคุ้มครองข้อมูล
- 6.7 การบริหาร Patch และช่องโหว่
- 6.8 การบริหารการเปลี่ยนแปลง
- 6.9 การบริหารผู้ให้บริการภายนอก
- 6.10 การตรวจสอบและประเมินผู้ให้บริการ
- 7. การใช้ทรัพยากรระบบสารสนเทศ
 - 7.1 การไม่อนุญาตให้มีการใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศในทางที่ผิดกฎหมาย
 - 7.2 การไม่ฝ่าฝืนระบบความปลอดภัย
 - 7.3 การไม่ใช้อีเมลหรือข้อความอื่น ๆ ในทางที่ผิด

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

หมวดที่ 1 ความมั่นคงและความปลอดภัยระบบเทคโนโลยีสารสนเทศ

- 1.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการเผยแพร่ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศที่ผ่านการอนุมัติตามมติที่ประชุมคณะกรรมการบริษัท เพื่อให้ผู้ใช้งานทั้งภายในองค์กร หน่วยงานภายนอก และผู้ที่เกี่ยวข้องในขอบเขตรับทราบและถือปฏิบัติ
- 1.2 การทบทวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้หรืออย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อกลุ่มบริษัท
- 1.3 กำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities) ผู้บริหารระดับสูงสุดต้องแต่งตั้งผู้รับผิดชอบ และมอบหมายหน้าที่ ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ
- 1.4 การปฏิบัติงานจากภายนอกองค์กร เพื่อเข้ามาใช้งานทรัพยากรภายในองค์กร อุปกรณ์ที่เชื่อมต่อเข้ามาต้องเป็นทรัพย์สินขององค์กรและได้รับการอนุมัติจากทางฝ่ายเทคโนโลยีสารสนเทศ
- 1.5 การปฏิบัติงานจากภายนอกองค์กร ผู้ใช้จะต้องดำเนินการแจ้งคำขอ Username และ Password เป็นลายลักษณ์อักษรให้กับทางฝ่ายเทคโนโลยีสารสนเทศ และต้องใช้งานผ่านช่องทางที่จัดเตรียมไว้ให้ และต้องมีการตรวจสอบยืนยันตัวตนก่อนการใช้งาน ไม่ควรเก็บข้อมูลที่เป็นความลับไว้ที่อุปกรณ์ส่วนตัว หรือหากจำเป็นต้องใช้งานเมื่อใช้เสร็จ ควรดำเนินการลบข้อมูลนั้นทิ้งไป

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กลุ่มบริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน)



- 1.6 เพื่อเป็นการป้องกันการเข้าถึงระบบเครือข่าย (LAN) จะต้องเป็นอุปกรณ์ที่ได้รับการขึ้นทะเบียนทรัพย์สิน และต้องได้รับการอนุมัติการใช้งานจากฝ่ายเทคโนโลยีสารสนเทศ มีการยืนยันตัวตนก่อนการใช้งานโดยใช้ Username และ Password ของ Domain ก่อนเข้าใช้งาน เพื่อความปลอดภัยและป้องกันทางฝ่ายเทคโนโลยีสารสนเทศไม่อนุญาตให้นำเครื่องส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายได้
- 1.7 เพื่อเป็นการป้องกันการเชื่อมต่อกับระบบเครือข่ายไร้สาย พนักงานต้องนำอุปกรณ์มาลงทะเบียนและขออนุมัติกับฝ่ายเทคโนโลยีสารสนเทศ หากผู้ติดต่อกับกลุ่มบริษัทมีความจำเป็นต้องขออนุมัติใช้งาน สามารถติดต่อลงทะเบียนได้ที่ประชาสัมพันธ์เพื่อรับ Username และ Password สำหรับการใช้งานระบบเครือข่ายไร้สาย (WiFi)
- 1.8 เพื่อเป็นการป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นการเปิดเผยหรือการขโมยข้อมูล กำหนดให้พนักงานของกลุ่มบริษัทมีหน้าที่รับผิดชอบในการตั้งและเปลี่ยนรหัสผ่านในการเข้าสู่ระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท ไม่เปิดหน้าจอคอมพิวเตอร์ค้างไว้ โดยไม่มีการป้องกันผู้อื่นเข้ามาใช้งานแทน ตลอดจนดูแลทรัพย์สินในระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทไว้ในที่ปลอดภัย เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์หวังดีนำสินทรัพย์ไปใช้ในทางที่เกิดความเสียหายต่อกลุ่มบริษัทได้
- 1.9 เพื่อเป็นการควบคุมการเข้าออกห้อง Datacenter โดยมีจุดประสงค์เพื่อควบคุมรักษาความปลอดภัยของระบบงาน ระบบเครือข่าย และข้อมูลของกลุ่มบริษัท โดยกำหนดให้มีการจำกัดการเข้าห้อง Datacenter ซึ่งในกรณีผู้ที่ไม่มีความจำเป็นต้องเข้าพื้นที่จะต้องลงบันทึกเวลาเข้าออกในสมุดบันทึกพร้อมระบุเหตุผล และต้องมีเจ้าหน้าที่เทคโนโลยีสารสนเทศคอยดูแลควบคุมการเข้าพื้นที่
- 1.10 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
- 1.11 พนักงานมีหน้าที่ต้องรับผิดชอบดำเนินการให้เป็นไปตามนโยบายที่กำหนดขึ้นนี้อย่างเคร่งครัดผู้ที่ฝ่าฝืนไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าข้อหนึ่งข้อใด หรือละเมิดลิขสิทธิ์ในการใช้โปรแกรม คอมพิวเตอร์ของกลุ่มบริษัท เพื่อผลประโยชน์ของตนเอง หรือบุคคลอื่นนอกเหนือจากภาระหน้าที่รับผิดชอบของตน หรือเพื่อผลประโยชน์ของกลุ่มบริษัท ถือเป็นความผิดวินัยพนักงาน

หมวดที่ 2 ควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

- 2.1 เพื่อให้การบริหารจัดการบัญชีผู้ใช้เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ผู้บังคับบัญชาและเจ้าหน้าที่บุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้
 - การว่าจ้างงาน
 - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
 - การลาออก หรือสิ้นสุดการเป็นผู้บริหาร พนักงาน ลูกจ้าง หรือถึงแก่กรรม
 - โยกย้ายหน่วยงานหรือโครงการ รวมไปถึงเปลี่ยนหน้าที่ความรับผิดชอบ

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

กลุ่มบริษัท สโตนเฮ็นจ์ อินเทอร์เน็ต จำกัด (มหาชน)



- การพักผ่อน การลงโทษทางวินัย การระงับการปฏิบัติหน้าที่ หรือตามที่ผู้บังคับบัญชาท่านนั้นร้องขอ
- 2.2 ผู้บังคับบัญชาของแต่ละฝ่ายต้องเป็นผู้กำหนดสิทธิในการเข้าถึงข้อมูลเป็นลายลักษณ์อักษร
- 2.3 เจ้าของระบบ (Owner System) จะต้องเป็นผู้พิจารณาสิทธิการเข้าถึงระบบต่างๆ ด้วยตนเอง

หมวดที่ 3 การสำรองข้อมูล การฟื้นฟูระบบข้อมูล และการเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉิน

- 3.1 เพื่อป้องกันการหยุดชะงักในการดำเนินงานของกลุ่มบริษัท ฝ่ายเทคโนโลยีสารสนเทศต้องมีการ จัดทำแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ กำหนดให้มีการทบทวน ตรวจสอบ และทบทวนแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินอย่างน้อยปีละ 1 ครั้ง
- 3.2 เพื่อเป็นการเตรียมความพร้อมการรองรับสถานการณ์ฉุกเฉิน กำหนดให้ฝ่ายเทคโนโลยีสารสนเทศต้อง ดำเนินการติดตั้งห้อง Datacenter สำรอง หรือ มีการใช้บริการคลาวด์หรือศูนย์ข้อมูลภายนอก เพื่อใช้ในการ จัดทำแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan) ทั้งนี้ เพื่อให้ระบบและข้อมูลที่มีความสำคัญ สามารถดำเนินงานได้อย่างต่อเนื่อง
- 3.3 ในกรณีที่บริษัทมีการใช้บริการสำรองและกู้คืนข้อมูลจากผู้ให้บริการภายนอก (Third-Party Providers) บริษัท จะต้องกำหนดหลักเกณฑ์ในการพิจารณาคัดเลือกผู้ให้บริการ เช่น ต้องมีมาตรฐานสากลรองรับ ต้องมี ข้อตกลงระดับการให้บริการ (SLA) ที่ชัดเจนและเหมาะสม ต้องมีการรักษาความปลอดภัยของข้อมูลที่ยอมรับ ได้และสอดคล้องกับกฎหมายที่เกี่ยวข้อง เป็นต้น
- 3.4 จัดทำระบบสำรองข้อมูลที่สำคัญในระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท เพื่อให้สามารถบริการได้อย่าง ต่อเนื่อง มีความเสถียรภาพ มีความปลอดภัย มีการตรวจสอบและดูแลระบบสำรองข้อมูลให้อยู่ในสภาพที่พร้อม นำมาใช้งานได้อยู่เสมอ มีการกำหนดเจ้าหน้าที่ผู้รับผิดชอบในการตรวจสอบและดูแลระบบสำรองข้อมูล
- 3.5 ให้ฝ่ายเทคโนโลยีสารสนเทศหรือให้ตกลงกับเจ้าของข้อมูล กำหนดระยะเวลาในการสำรองข้อมูลและ ระยะเวลาในการจัดเก็บข้อมูล
- 3.6 ผู้ดูแลระบบสำรองข้อมูลของกลุ่มบริษัทมีหน้าที่รับผิดชอบในการไม่สำรองข้อมูลส่วนตัว หรือข้อมูลที่ไม่ เกี่ยวข้องกับการปฏิบัติงานของกลุ่มบริษัทลงในระบบสำรองข้อมูลของกลุ่มบริษัทตลอดจนการเก็บรักษาข้อมูล ของกลุ่มบริษัทไว้ในที่ที่กำหนดไว้อย่างปลอดภัย เพื่อให้ระบบสำรองข้อมูลสามารถกู้คืนข้อมูลของกลุ่มบริษัท กลับมาได้ และป้องกันไม่ให้ผู้ไม่ประสงค์ดีนำข้อมูลดังกล่าวไปใช้ในทางที่ทำให้เกิดความเสียหายต่อกลุ่ม บริษัท

หมวดที่ 4 การบริหารจัดการคอมพิวเตอร์และการติดตั้งซอฟต์แวร์

- 4.1 ฝ่ายเทคโนโลยีสารสนเทศจะต้องบันทึกรายละเอียดข้อมูลของทรัพย์สินในระบบบริหารจัดการสินทรัพย์ทั้ง เข้า/ซื้อ

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กลุ่มบริษัท สโตนเฮ็นจ์ อินเทอร์เน็ต จำกัด (มหาชน)



- 4.2 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการบันทึกรายชื่อผู้ถือครองทรัพย์สินนั้นๆ บนระบบบริหารจัดการสินทรัพย์ให้ตรงตามข้อมูลปัจจุบันเสมอ และมีการเก็บข้อมูลผู้ถือครอง
- 4.3 การขอใช้งานคอมพิวเตอร์ หรืออุปกรณ์อื่นๆ ผู้ใช้งานต้องทำเรื่องแจ้งเป็นลายลักษณ์อักษรและต้องลงนามในเอกสารใบยืมวัสดุอุปกรณ์สำนักงาน
- 4.4 การควบคุมการติดตั้งระบบปฏิบัติการ และการติดตั้งซอฟต์แวร์จะต้องได้รับการอนุญาตการติดตั้งจากฝ่ายเทคโนโลยีสารสนเทศก่อนทุกครั้งและต้องเป็นซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์
- 4.5 ผู้ถือครองอุปกรณ์ของกลุ่มบริษัทมีหน้าที่รับผิดชอบอุปกรณ์ที่ยืมเหมือนเป็นอุปกรณ์ของตนเองให้สามารถใช้งานได้ดียุ่เสมอ หากมีการเปลี่ยนอุปกรณ์ผู้ถือครองมีหน้าที่ดำเนินการโอนย้าย ข้อมูลในอุปกรณ์นั้นด้วยตนเอง เมื่อผู้ถือครองใช้อุปกรณ์เสร็จเรียบร้อย ต้องนำมาคืนที่ฝ่ายเทคโนโลยีสารสนเทศ

หมวดที่ 5 แนวทางปฏิบัติเกี่ยวกับโปรแกรมคอมพิวเตอร์ที่บริษัทหรือพนักงานจัดหา / พัฒนา / การบำรุงรักษา

- 5.1 การพัฒนาโปรแกรมหรือระบบเพื่อนำมาใช้งานภายในกลุ่มบริษัท จะต้องได้รับการพิจารณาเห็นชอบเป็นลายลักษณ์อักษรจากผู้บริหาร หรือผู้มีอำนาจที่ได้รับมอบหมายจากกลุ่มบริษัท
- 5.2 การพัฒนาโปรแกรมหรือระบบที่พนักงานได้ร่วมกันพัฒนาขึ้นในฐานะพนักงานของกลุ่มบริษัทให้ลิขสิทธิ์ในการพัฒนานั้นเป็นของกลุ่มบริษัท

หมวดที่ 6 แนวทางปฏิบัติเกี่ยวกับคลาวด์

ขอบเขตและคำจำกัดความ การใช้บริการ Cloud และ Private Cloud หมายถึง การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศที่บริษัทจัดหาเช่า หรือรับบริการจากผู้ให้บริการภายนอก สำหรับการจัดเก็บ ประมวลผล รับส่ง หรือให้บริการข้อมูลและระบบสารสนเทศของกลุ่มบริษัท ซึ่งรวมถึงแต่ไม่จำกัดเพียง Virtual Machine, Server, Storage, Database, Application, Active Directory, File Server, Backup, Disaster Recovery, Network, Firewall และระบบรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง ข้อมูล ระบบงาน การตั้งค่าระบบ และทรัพยากรที่ติดตั้งหรือจัดเก็บอยู่บน Cloud หรือ Private Cloud ให้ถือเป็นทรัพย์สินสารสนเทศของกลุ่มบริษัท แม้ว่าทรัพยากรดังกล่าวจะติดตั้งหรือจัดเก็บอยู่ ณ ศูนย์ข้อมูลของผู้ให้บริการภายนอกก็ตาม

- 6.1 บริษัทต้องจัดให้มีขั้นตอนการขออนุมัติใช้บริการคลาวด์ และ/หรือ ไพรวาท คลาวด์ (Private Cloud) สำหรับการจัดตั้งระบบใหม่ การสร้าง Virtual Machine ใหม่ การเพิ่มหรือลดทรัพยากรของระบบ การเพิ่มพื้นที่จัดเก็บข้อมูล การเชื่อมต่อบนระบบ หรือการนำระบบงานของบริษัทขึ้นใช้งานบนคลาวด์ ต้องได้รับการพิจารณาและอนุมัติจากฝ่ายงานที่บริษัทได้กำหนดไว้ก่อนดำเนินการทุกครั้ง บริษัทไม่อนุญาตให้พนักงานหรือฝ่ายงานใดสมัคร จัดหาเช่า หรือนำบริการคลาวด์มาใช้งานกับข้อมูลหรือระบบงานของบริษัท ยกเว้นแต่จะได้รับอนุญาตจากผู้มีอำนาจ

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
กลุ่มบริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน)



- 6.2 บริษัทต้องมีการกำหนดบทบาทและความรับผิดชอบในการให้บริการคลาวด์อย่างชัดเจน โดยต้องมีการระบุเจ้าของระบบ เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ประสานงาน
- 6.3 บริษัทต้องมีการควบคุมสิทธิการเข้าถึงการเข้าถึงระบบคลาวด์ และ/หรือ ไฟร์วอลล์ คลาวด์ ต้องเป็นไปตามหลักความจำเป็นในการใช้งาน และให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติหน้าที่เท่านั้นบัญชีผู้ใช้งานและบัญชีผู้ดูแลระบบต้องเป็นบัญชีเฉพาะบุคคล สามารถตรวจสอบย้อนกลับได้ และห้ามใช้บัญชีร่วมกัน เว้นแต่มีเหตุผลจำเป็นทางเทคนิค ได้รับอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศ และต้องมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
- 6.4 บริษัทต้องจัดให้มีการควบคุมการใช้ระบบคลาวด์ที่เป็นบัญชีเฉพาะบุคคล (บัญชีส่วนตัว) และผู้ใช้งานต้องปฏิบัติตามแนวทางปฏิบัติที่บริษัทได้กำหนดไว้ โดยครอบคลุมในเรื่องต่อไปนี้
- 6.4.1 การขอสิทธิในการเชื่อมต่อบัญชีคลาวด์ส่วนบุคคลกับระบบเครือข่ายภายใน
 - 6.4.2 การจัดเก็บข้อมูล การแชร์ข้อมูล การลบ และแก้ไขข้อมูล บนคลาวด์ส่วนบุคคล
 - 6.4.3 การตรวจสอบข้อมูลบนคลาวด์ส่วนบุคคล
 - 6.4.4 ความรับผิดชอบของกลุ่มบริษัทต่อข้อมูลบนคลาวด์ส่วนบุคคล
- 6.5 การเชื่อมต่อระบบเครือข่ายภายในเข้ากับระบบคลาวด์ ต้องผ่านช่องทางที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดไว้เท่านั้น (เช่น Private Link, MPLS, VPN)
- 6.6 การจัดเก็บข้อมูลบนคลาวด์ ต้องสอดคล้องกับนโยบายจำแนกข้อมูล กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) และข้อตกลงของคู่ค้า ข้อมูลที่เป็นความลับ (เช่น ข้อมูลลูกค้า, โครงการ, การเงิน, กฎหมาย) ต้องได้รับการควบคุมสิทธิ์และมีมาตรการรักษาความปลอดภัยตามระดับความสำคัญ ห้ามจัดเก็บข้อมูลส่วนตัวที่ไม่เกี่ยวข้องกับการทำงานหรือข้อมูลที่ผิดกฎหมาย บนระบบคลาวด์ที่บริษัทให้บริการอย่างเด็ดขาด และข้อมูลลับ/ข้อมูลสำคัญต้องจัดเก็บในพื้นที่ที่ปลอดภัยเท่านั้น
- 6.7 บริษัทต้องจัดให้มีการตรวจสอบช่องโหว่ ประเมินความเสี่ยง และอัปเดต Security Patch / Version ของระบบปฏิบัติการ ซอฟต์แวร์ และเฟิร์มแวร์อย่างสม่ำเสมอ โดยช่องโหว่ที่วิกฤตและรุนแรงสูงต้องแก้ไขภายในเวลาที่กำหนด หากระบบหมดอายุการสนับสนุนจากผู้ผลิต บริษัทต้องดำเนินการปรับปรุง เปลี่ยนทดแทนหรือยกเลิกใช้งาน นอกจากนี้บนเครื่องแม่ข่าย (Server และ VM) จะ ต้องติดตั้งและเปิดใช้งานเครื่องมือความปลอดภัย เช่น Antivirus, EDR ตามมาตรฐานที่กำหนด
- 6.8 การเปลี่ยนแปลงระบบคลาวด์ที่ส่งผลกระทบต่อบริการ ความปลอดภัย หรือข้อมูล ต้องผ่านกระบวนการบริหารการเปลี่ยนแปลง (Change Management) ก่อนดำเนินการทุกครั้ง โดยต้องประเมินผลกระทบ ความเสี่ยง กำหนดช่วงเวลา แผนทดสอบ แผนสำรองข้อมูล และแผนย้อนกลับ (Rollback Plan) ในกรณีที่ทำไม่สำเร็จ สำหรับการเปลี่ยนแปลงฉุกเฉินสามารถทำได้ตามความจำเป็น แต่ต้องจัดทำบันทึกและรายงานให้ผู้มีอำนาจรับทราบภายหลัง

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กลุ่มบริษัท สโตนเฮ็นจ์ อินเทอร์เน็ต จำกัด (มหาชน)



6.9 ในการใช้บริการคลาวด์ของผู้ให้บริการภายนอก บริษัทต้องกำหนดวิธีการประเมินศักยภาพ ความน่าเชื่อถือ ความปลอดภัย ที่ตั้งศูนย์ข้อมูล ความพร้อมในการกู้คืนระบบ และการปฏิบัติตามกฎหมาย และในสัญญาการให้บริการหรือข้อตกลง (SLA) ต้องครอบคลุมขอบเขตความรับผิดชอบของแต่ละฝ่าย และข้อตกลงระดับการให้บริการ (SLA) ที่ชัดเจน

6.10 บริษัทต้องจัดให้มีการตรวจสอบและประเมินผู้ให้บริการ โดยพิจารณาจากผลการให้บริการตาม SLA เหตุการณ์ขัดข้อง เหตุการณ์ด้านความมั่นคงปลอดภัย การสนับสนุนทางเทคนิค และผลการทดสอบการสำรองหรือกู้คืนข้อมูล

อนึ่ง การใช้บริการคลาวด์และไพรเวท คลาวด์ ในที่นี้ให้หมายถึง การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศที่บริษัทจัดหา เช่า หรือรับบริการจากผู้ให้บริการภายนอก สำหรับการจัดเก็บ ประมวลผล รับส่ง หรือให้บริการข้อมูลและระบบสารสนเทศของกลุ่มบริษัท ซึ่งรวมถึง Virtual Machine, Server, Storage, Database, Application, Active Directory, File Server, Backup, Disaster Recovery, Network, Firewall และระบบรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง ข้อมูลระบบงาน การตั้งค่าระบบ และทรัพยากรที่ติดตั้งหรือจัดเก็บอยู่บนคลาวด์ หรือ ไพรเวท คลาวด์ ให้ถือเป็นทรัพย์สินสารสนเทศของกลุ่มบริษัท แม้ว่าทรัพยากรดังกล่าวจะติดตั้งหรือจัดเก็บอยู่ ณ ศูนย์ข้อมูลของผู้ให้บริการภายนอกก็ตาม

หมวดที่ 7 การใช้ทรัพยากรระบบสารสนเทศ

7.1 กลุ่มบริษัท ต้องไม่ใช้หรือสนับสนุน ส่งเสริม อนุญาต อำนาจความสะดวก หรือแนะนำให้พนักงานและ/หรือผู้อื่นใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทในทางที่ผิดกฎหมาย ทำให้เกิดอันตราย ฉ้อโกง ละเมิด หรือล่วงละเมิด หรือเพื่อส่ง จัดเก็บ แสดง แจกจ่ายหรือทำการอื่นใด อันมีเนื้อหาที่เป็นการผิดกฎหมาย เป็นอันตราย ฉ้อโกง ละเมิด หรือไม่เหมาะสม เป็นกิจกรรมหรือเนื้อหาที่ต้องห้าม

7.2 พนักงานต้องไม่ฝ่าฝืนระบบความปลอดภัยหรือความสมบูรณ์ของเครือข่าย คอมพิวเตอร์ หรือระบบการสื่อสาร แอปพลิเคชัน ซอฟต์แวร์ ข้อมูล หรือเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ (แต่ละประเภท เรียกว่า "ระบบ") ได้แก่ การเข้าถึงเครือข่ายหรือระบบใด ๆ โดยไม่ได้รับอนุญาตหรือผิดกฎหมาย การติดตามหรือการดักฟังข้อมูลหรือการรับส่งข้อมูลของระบบ การปลอมแปลงแหล่งกำเนิดของข้อมูลที่มีการสื่อสารผ่านเครือข่าย อินเทอร์เน็ต หรือในหัวของอีเมล

7.3 กลุ่มบริษัทจะต้องไม่แจกจ่าย เผยแพร่ ส่ง หรืออำนวยความสะดวกในการส่งอีเมลหรือข้อความจำนวนมากที่ไม่ได้ร้องขอหรือข้อความการส่งเสริมการขาย การโฆษณา หรือการชักชวน (เช่น "Spam" หรือ "สแปม") รวมถึงการโฆษณาเชิงพาณิชย์และการประกาศข้อมูล ตลอดจนจะต้องไม่แก้ไขหรือปิดบังส่วนหัวของอีเมลหรือสวมรอยเป็นผู้ส่งโดยไม่ได้รับอนุญาตโดยชัดแจ้งจากผู้ส่ง หรือการส่งอีเมลที่ขัดขวางการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นในลักษณะที่ก่อให้เกิดความรำคาญแก่ผู้รับตามที่กฎหมายห้าม

นโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
กลุ่มบริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน)



หมายเหตุ กำหนดให้แนวปฏิบัติหรือระเบียบต่าง ๆ ที่เกี่ยวข้องหรือเกี่ยวเนื่องกับนโยบายรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ ถือเป็นส่วนหนึ่งของนโยบายฉบับนี้

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้รับการปรับปรุงและอนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 4/2568-69 เมื่อวันที่ 11 สิงหาคม 2569 โดยมีผลบังคับใช้ตั้งแต่วันที่ 12 สิงหาคม 2569 จึงประกาศมาเพื่อทราบและให้ถือปฏิบัติต่อไป

นายจุมพล สำเภาพล

ประธานกรรมการ

บริษัท สโตนเฮนจ์ อินเตอร์ จำกัด (มหาชน)