นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

บริษัท ไฮบริด เอ็นเนอร์จี จำกัดและบริษัทย่อย

ได้รับอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2567 ซึ่งประชุมเมื่อวันที่ 30 มกราคม 2567

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

บทนำ

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทและบริษัทย่อยฉบับนี้จัดทำโดยอ้างอิงจากระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 : 2013 จัดทำขึ้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท มีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัย ถูกต้องเชื่อถือได้ สามารถดำเนินงานอย่างต่อเนื่องและสามารถป้องกันรักษาสารสนเทศที่เป็นความลับของบริษัท ทั้งที่เป็นข้อมูลของบริษัทและข้อมูลส่วนบุคคลอื่น ๆ

วัตถุประสงค์

1. เพื่อให้เกิดความเชื่อมั่นและมั่นคงปลอดภัยในการใช้งานสารสนเทศของบริษัทและบริษัทย่อย ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลและวัตถุประสงค์ที่กำหนดไว้
2. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติให้ผู้ใช้งานและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท
3. เพื่อป้องกันไม่ให้ระบบสารสนเทศของบริษัทถูกบุกรุก เปลี่ยนแปลง ขโมย ทำลาย หรือการกระทำอื่นๆ ที่อาจสร้างความเสียหายต่อบริษัท
4. เพื่อสร้างความมั่นใจให้กับบุคคลภายนอกที่เป็นคู่ค้าหรือผู้มีส่วนได้เสียต่างๆ ว่าข้อมูลส่วนบุคคลจะได้รับการปกป้องตามมาตรฐานความปลอดภัยของบริษัท
5. เพื่อเผยแพร่ให้ผู้ใช้งานและบุคคลภายนอกซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศได้รับทราบและถือปฏิบัติอย่างเคร่งครัด

ขอบเขต

ได้รับอนุญาตให้ใช้ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพาหรืออุปกรณ์สื่อสารโทรคมนาคมเพื่อเข้าถึงสารสนเทศของบริษัท

ส่วนที่ 1 การจัดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อกำหนดบทบาทและหน้ามี่รับผิดชอบของผู้ที่เกี่ยวข้องในการกำกับดูแลและปฏิบัติตามหน้าที่รักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวปฏิบัติ ได้แก่

1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร

1.2 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย

ส่วนที่ 2 การสร้างความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

เพื่อให้ผู้ใช้งานเข้าใจหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมต่อบทบาทหน้าที่ของตนเองที่ได้รับ และปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง เพื่อป้องกันผลประโยชน์ของบริษัทซึ่งเป็นส่วนหนึ่งของการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน โดยมีแนวปฏิบัติ ได้แก่

2.1 ความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนเข้าทำงาน

2.2 ความมั่นคงปลอดภัยในระหว่างการจ้างงาน

2.3 การสิ้นสุดหรือเปลี่ยนการจ้างงาน

ส่วนที่ 3 การบริหารจัดการทรัพย์สินสารสนเทศ

เพื่อให้มีการระบุทรัพย์สินสารสนเทศของบริษัทและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินสารสนเทศอย่างเหมาะสม รวมทั้งข้อมูลได้รับระดับการป้องกันที่เหมาะสมสอดคล้องกับความสำคัญของข้อมูลนั้นที่มีต่อบริษัท ป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูลที่จัดเก็บอยู่ในสื่อบันทึกข้อมูล โดยมีแนวปฏิบัติ ได้แก่

3.1 หน้าที่รับผิดชอบต่อทรัพย์สินสารสนเทศ

3.2 การคืนทรัพย์สินสารสนเทศ

3.3 การจัดชั้นความลับของข้อมูล

3.4 การถือครองทรัพย์สินสารสนเทศ

3.5 การจัดการสื่อบันทึกข้อมูล

ส่วนที่ 4 การควบคุมการเข้าถึง

เพื่อกำหนดมาตรฐานการควบคุมบุคคลที่ไม่ได้รับอนุญาตในการเข้าถึงระบบสารสนเทศของบริษัทและสามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัทได้อย่างถูกต้อง และควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ได้แก่

4.1 การควบคุมการเข้าถึง

4.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

4.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน

4.4 การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์

ส่วนที่ 5 การเข้ารหัสข้อมูล

เพื่อให้มีการใช้ การเข้ารหัสข้อมูล สำหรับรับหรือส่งและจัดเก็บข้อมูลที่เป็นความลับ และป้องกันการปลอมแปลงหรือยืนยันความถูกต้องของข้อมูล โดยมีแนวปฏิบัติ ได้แก่ การควบคุมการเข้ารหัสข้อมูลที่มีชั้นความลับ

ส่วนที่ 6 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต สร้างความเสียหายและการแทรกแซงการทำงานที่มีผลต่อข้อมูลและอุปกรณ์ประมวลผลสารสนเทศของบริษัทและป้องกันการสูญหายและสร้างความเสียหาย การขโมยหรือภาวะเป็นอันตรายต่อทรัพย์สินสารสนเทศและป้องกันการหยุดชะงักต่อการดำเนินงานของบริษัท โดยมีแนวปฏิบัติ ได้แก่

6.1 ความมั่นคงปลอดภัยของพื้นที่ปฏิบัติงาน

6.2 ความมั่นคงปลอดภัยของอุปกรณ์ทรัพย์สินสารสนเทศ

ส่วนที่ 7 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี ป้องกันการสูญหายของข้อมูลรวมทั้งมีการบันทึกเหตุการณ์และการจัดทำหลักฐานป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค เพื่อให้ทราบถึงระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศและระดับความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวปฏิบัติ ได้แก่

7.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร

7.2 การสำรองข้อมูล

7.3 การกู้คืนระบบ

7.4 การบริหารและจัดการด้านความมั่นคงปลอดภัยเครือข่าย

7.5 การควบคุมกิจกรรมในการตรวจสอบระบบสารสนเทศ

ส่วนที่ 8 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ มีการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีการถ่ายโอนกับหน่วยงานภายในบริษัท และถ่ายโอนกับหน่วยงานภายนอก ป้องกันการสูญหายหรือสูญเสียข้อมูล/ระบบต่าง ๆ ที่ทำการสำรองข้อมูลไว้ ป้องกันข้อมูลความลับของบริษัทตกไปสู่บุคคลภายนอก โดยเฉพาะบริษัทคู่แข่ง ซึ่งอาจก่อให้เกิดความเสียหายต่อธุรกิจได้ในวงกว้างและรุนแรง โดยมีแนวปฏิบัติ ได้แก่

8.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร

8.2 การถ่ายโอนข้อมูลสารสนเทศ

ส่วนที่ 9 การจัดหา การพัฒนา และการบำรุงรักษาระบบ

เพื่อให้ความมั่นคงปลอดภัยด้านสารสนเทศเป็นข้อกำหนดสำคัญในการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ และให้มีการทดสอบระบบสารสนเทศตามข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวปฏิบัติ ได้แก่

9.1 ความต้องการด้านความมั่นคงปลอดภัยระบบสารสนเทศ

9.2 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ

9.3 ระเบียบกระบวนการในการควบคุมการพัฒนาเปลี่ยนแปลงแก้ไขซอฟต์แวร์

ส่วนที่ 10 ความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอก

เพื่อให้มีการป้องกันทรัพย์สินสารสนเทศของบริษัท ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก และกำหนดแนวทางการคัดเลือกผู้ให้บริการภายนอกอย่างเหมาะสม โดยมีแนวปฏิบัติ ได้แก่

10.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร

10.2 การคัดเลือกผู้ให้บริการภายนอก

ส่วนที่ 11 การบริหารจัดการสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยด้านสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยด้านสารสนเทศให้ได้รับทราบ โดยมีแนวปฏิบัติ ได้แก่ การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

ส่วนที่ 12 การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือบริษัทเพื่อให้มีความต่อเนื่อง

เพื่อป้องกันการหยุดชะงักในการดำเนินงานของบริษัทที่เป็นผลมาจากภัยพิบัติ และเพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ โดยมีแนวปฏิบัติ ได้แก่

12.1 การบริหารจัดการความต่อเนื่องของความมั่นคงปลอดภัยด้านสารสนเทศ

12.2 การประเมินความเสี่ยง

ส่วนที่ 13 การปฏิบัติตามข้อกำหนด

เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีการปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท โดยมีแนวปฏิบัติ ได้แก่

13.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท

13.2 การทบทวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

13.3 การกำกับดูแลการปฏิบัติงานให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

ผู้รับผิดชอบ

1. ผู้อำนวยการสายสนับสนุนบริหาร (Chief Administrative Officer : CAO)
2. ผู้จัดการแผนกเทคโนโลยีสารสนเทศ

วันที่มีผลบังคับใช้

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ฉบับนี้ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัทครั้งที่ 1/2567 เมื่อวันที่ 30 มกราคม 2567 และให้ยกเลิกฉบับเดิมที่ลงวันที่ 31 สิงหาคม 2564 โดยให้ถือปฏิบัติตามฉบับนี้แทน โดยมีผลบังคับใช้ตั้งแต่วันที่ 30 มกราคม 2567 เป็นต้นไป

ประกาศ ณ วันที่ 30 มกราคม 2567

(นายสุรพล สติมานนท์)

ประธานกรรมการบริษัท