นโยบายการจัดการระบบดิจิทัล

(Digital Management Policy)

1 October 2024

Document Version 002

DEESTONE

บริษัท ดีสโตน คอร์ปอเรชั่น จำกัด (มหาชน)
84 หมู่ที่ 7 ซอยเพชรเกษม 122 ถนนเพชรเกษม ตำบลอ้อมน้อย อำเภอกระทุ่มแบน จังหวัดสมุทรสาคร 74130
DEESTONE CORPORATION PUBLIC COMPANY LIMITED
84 Soi Petchkasem 122, Moo7, Petchkasem Rd., Ommoi, Krathumban,
Samutsakorn, 74130 Thailand
Tel : (+662) 420-0038, 023-4756 Fax : (+662) 420-0572, 023-4724
E-mail : deestone@deestone.com, Website : www.deestone.com

Document Revision Control

Version	Date (DD-MM-YYYY)	Type (A/M/D)	Description
001	01-10-2022	A	เอกสารเริ่มต้น Digital Management Policy
002	01-10-2024	A / M / D	เพิ่มหมายเหตุ ขอยกเลิกการประกาศของเอกสารนโยบาย แก้ไขคำนิยาม ภาคผนวก ก เพิ่มกลุ่มมาตรฐานสากล NIST Cybersecurity Framework เพิ่มกลุ่มมาตรฐานภายในประเทศ พระราชบัญญัติสิทธิบัตร พระราชบัญญัติเครื่องหมายการค้า พระราชบัญญัติความลับทางการค้า พระราชบัญญัติคุ้มครองสิ่งบ่งชี้ทางภูมิศาสตร์

** Noted **

Type: A = Add, M = Modify, D = Delete

DEESTONE
บริษัท ดีสโตน คอร์ปอเรชั่น จำกัด (มหาชน)
84 หมู่ที่ 7 ซอยเพชรเกษม 122 ถนนเพชรเกษม ตำบลอ้อมน้อย อำเภอกระทุ่มแบน จังหวัดสมุทรสาคร 74130
DEESTONE CORPORATION PUBLIC COMPANY LIMITED
84 Soi Petchkasem 122, Moo7, Petchkasem Rd., Ommoi, Krathumban,
Samutsakorn, 74130 Thailand
Tel : (+662) 420-0038, 023-4756 Fax : (+662) 420-0572, 023-4724
E-mail : deestone@deestone.com, Website : www.deestone.com

สารบัญ

บริษัท ดีสโตน คอร์ปอเรชั่น จำกัด (มหาชน)
84 หมู่ที่ 7 ซอยเพชรเกษม 122 ถนนเพชรเกษม ตำบลอ้อมน้อย อำเภอกระทุ่มแบน จังหวัดสมุทรสาคร 74130
DEESTONE CORPORATION PUBLIC COMPANY LIMITED
84 Soi Petchkasem 122, Moo7, Petchkasem Rd., Omnoi, Krathumban,
Samutsakorn, 74130 Thailand
Tel : (+662) 420-0038, 023-4756 Fax : (+662) 420-0572, 023-4724
E-mail : deestone@deestone.com, Website : www.deestone.com

นโยบายการจัดการระบบดิจิทัล

(Digital Management Policy)

หลักการและเหตุผล

บริษัทฯ ตระหนักถึงความสำคัญในการใช้เทคโนโลยีดิจิทัลเป็นส่วนหนึ่งของการดำเนินธุรกิจ ไม่ว่าจะเป็นการเพิ่มขีดความสามารถในการแข่งขัน การพัฒนานวัตกรรมและการปรับปรุงประสิทธิภาพการทำงานได้อย่างต่อเนื่อง บริษัทฯ จึงกำหนดกรอบการกำกับดูแลและจัดการระบบดิจิทัล รวมถึงการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลขึ้น เพื่อเป็นแนวทางในการทำงานของทุกหน่วยงานที่เกี่ยวข้อง และเกิดความสอดคล้องกับแนวทางการปฏิบัติใน*การรักษาความมั่นคงปลอดภัย*ของระบบสารสนเทศของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ตลอดจนกฎหมายอื่นๆ และมาตรฐานสากลที่เกี่ยวข้องตามที่ระบุไว้ในภาคผนวก ข โดยนำมาปรับใช้ให้เหมาะสมกับบริบทการดำเนินธุรกิจของบริษัทฯ

ขอบเขตการบังคับใช้

นโยบายฉบับนี้ กำหนดให้มีการวางนโยบายในด้านต่างๆ เพื่อให้ครอบคลุมการดำเนินการด้านดิจิทัล และสอดคล้องกับนโยบายอื่นๆของบริษัทฯ ดังนี้

- นโยบายการบริหารทรัพย์สินดิจิทัล (Digital Asset Policy)
- นโยบายการบริการดิจิทัล (Digital Service Policy)
- นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy)

1. นโยบายการบริหารทรัพย์สินดิจิทัล (Digital Asset Policy)

เพื่อให้มีการบริหาร*ทรัพย์สินดิจิทัล* เป็นไปอย่างมีประสิทธิภาพ และมีความสอดคล้องกับแผนกลยุทธ์ของบริษัทฯ ได้อย่างตรงตามเป้าหมายตามที่กำหนดไว้ จึงมีแนวทางการบริหารทรัพย์สินดิจิทัล ไว้ดังนี้

1.1. การจัดการวงจรชีวิตของทรัพย์สินดิจิทัล กล่าวถึงการบริหารทรัพย์สินทั้งที่จับต้องได้ และจับต้องไม่ได้ให้เกิดประโยชน์ต่อการดำเนินธุรกิจของบริษัทฯ

1.1.1. ขั้นตอนพื้นฐานของการจัดการวงจรชีวิตของทรัพย์สินแต่ละกลุ่ม ควรมีอย่างน้อย 3 ขั้นตอนคือ การลงทะเบียน การเปลี่ยนแปลง และการกำจัด ทั้งนี้อาจเพิ่มเติมขั้นตอนให้เหมาะสมกับทรัพย์สินแต่ละชนิดได้

1.1.2. การกำหนด*การควบคุมภายใน* ให้ใช้หลักการวิเคราะห์ต้นทุนและผลประโยชน์ (Cost benefit Analysis) ในการสรุปการควบคุมภายในที่เลือกใช้ เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่กำหนด

1.2. การจัดการผลประโยชน์ (Benefit) และการใช้สิทธิการรับประกันของทรัพย์สินดิจิทัล

1.2.1. ผลประโยชน์ต่างๆทั้งที่มีตัวตนและไม่มีตัวตน ถือเป็นทรัพย์สินของบริษัทฯ ต้องมีการบันทึกทุกขั้นตอนตั้งแต่การบันทึก การปรับปรุง การแลกเปลี่ยน การใช้สิทธิ จนถึงการยกเลิก โดยคำนึงถึงผลกระทบที่จะได้รับทั้งทางเทคนิค และ ทางการจัดการ

1.2.2. สิทธิการรับประกัน จะต้องจัดการให้เกิดประโยชน์สูงสุด และไม่ส่งผลกระทบหรือลดทอนความสามารถในการดำเนินการของบริษัทฯ

1.2.3. ข้อมูลที่ใช้ในการจัดการผลประโยชน์และการใช้สิทธิการรับประกัน จะต้องจัดเก็บไว้อย่างครบถ้วน ถูกต้องและเป็นปัจจุบันเสมอ โดยสามารถติดตามตรวจสอบ และ แจ้งเตือนได้อย่างทันท่วงที

1.3. การปรับปรุง และ การแลกเปลี่ยนสิทธิ์ด้านดิจิทัล จะต้องมีการประเมินผลได้ ผลเสีย จากกิจกรรมเหล่านี้อย่างรอบด้าน เพื่อให้บริษัทฯ ได้ใช้ประโยชน์จาก*สิทธิ์*ที่มีอยู่ให้เกิดประโยชน์สูงสุด โดยพิจารณาเปรียบเทียบจากทางเลือกต่างๆ ที่เป็นไปได้ตามวัตถุประสงค์การใช้งาน

2. นโยบายการบริการดิจิทัล (Digital Service Policy)

2.1. การรักษาความต่อเนื่องของบริการ (Service Continuity)

2.1.1. ความต่อเนื่องของ*บริการ*ดิจิทัลจะต้องเป็นไปตามแผนงานการกู้คืนระบบ (Disaster Recovery Plan: DRP) และสามารถให้บริการได้ตามเป้าหมายค่าของข้อมูลล่าสุด *(Recovery Point Objective: RPO)* และเป้าหมายช่วงเวลาที่กู้คืนบริการ *(Recovery Time Objective: RTO)*

2.1.2. การปรับปรุงบริการดิจิทัล ต้องมาจากการปรับปรุงแผนงานการกู้คืนระบบ การปรับปรุงคุณภาพการบริการและการปรับเปลี่ยนบริการผ่านการพัฒนานวัตกรรม ทั้งนี้จะต้องไม่ส่งผลกระทบต่อความต่อเนื่องในการให้บริการ

2.2. การพัฒนานวัตกรรมและการส่งเสริมคุณค่าการบริการดิจิทัล (Service Innovation & Value Proposition) จัดให้มีการจัดเก็บข้อมูลที่จำเป็นต่อการวิเคราะห์และประเมินคุณค่าของการบริการอย่างสม่ำเสมอ เพื่อส่งเสริมให้เกิดนวัตกรรมการบริการ ประยุกต์ใช้เทคโนโลยีสมัยใหม่และปรับปรุงประสิทธิภาพการบริการในทุกกระบวนการดิจิทัลให้มีประสิทธิผลสูงสุด รวมทั้งผลักดันให้เกิดการพัฒนาองค์ความรู้และเพิ่มศักยภาพในการแข่งขันของบริษัทฯ ให้เกิดความได้เปรียบในการแข่งขันสูงขึ้น และสอดคล้องกับแผนงานธุรกิจของบริษัทฯ

2.3. การรับรองคุณภาพและปรับปรุงประสิทธิผลของบริการดิจิทัล (Service Quality Assurance & Efficiency Improvement) จะต้องเป็นส่วนหนึ่งของการจัดการบริการดิจิทัล โดยมีเป้าหมายที่จะปรับปรุงบริการให้มีประสิทธิภาพอยู่ในระดับเดิมหรือสูงขึ้น และสามารถให้บริการตามเป้าหมายที่กำหนดไว้ในข้อตกลงการให้บริการ

(Service level agreement: SLA) และ ข้อตกลงระดับปฏิบัติการ (Operational Level Agreement: OLAs) ของทรัพย์สินดิจิทัลทั้งหมดที่เกี่ยวข้องกับบริการ นั้นๆ

2.3.1. บริการดิจิทัลที่กำหนดขึ้นต้องสามารถทำงานได้โดยอิสระจากบริการ ดิจิทัลอื่นในในแง่ของกระบวนการทำงาน และข้อมูลที่จำเป็นในการใช้งาน และเป็นบริการที่สามารถขยายความสามารถในการทำงานได้ในเวลาอันสั้นทั้งในแง่ของความรวดเร็วในการตอบสนองการใช้งานและความสามารถในการใช้งานได้สะดวกขึ้น

2.3.2. การกำหนดดัชนีชี้วัดความสำเร็จ (Key Performance Indicator: KPI) ของบริการดิจิทัล ต้องสอดรับกับข้อตกลงการให้บริการ และข้อตกลงระดับปฏิบัติการที่กำหนดไว้ของบริการดิจิทัล

2.3.3. การเฝ้าระวังและติดตาม*คุณภาพบริการดิจิทัล*ให้สำรวจความคิดเห็น อาทิเช่น ข้อเสนอแนะ ข้อแนะนำคำติชม คำวิจารณ์ ที่เกี่ยวข้องกับบริการต่างๆของบริษัทฯ จาก*พนักงาน*ทั้งในนามส่วนตัวหรือในนามของบริษัทฯ และผู้ใช้บริการ ผ่านช่องทางการร้องขอบริการดิจิทัล หรือช่องทางดิจิทัลอื่นๆ ไม่ว่าจะเป็นสื่อสังคมออนไลน์ หรือดิจิทัลแพลตฟอร์มที่เกี่ยวข้อง อย่างสม่ำเสมออย่างน้อยเป็นรายไตรมาส

3. นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy)

3.1. การรักษาความปลอดภัยด้านกายภาพและข้อมูล

3.1.1. สถานที่ของบริษัทฯ หรือ*ผู้ให้บริการภายนอก*ในการปฏิบัติการโดยตรงกับบริษัทฯ องค์ประกอบด้านกายภาพต่างๆของเทคโนโลยีดิจิทัล จะต้องมีระดับความเสี่ยงจากสาธารณภัยธรรมชาติ และสาธารณภัยที่เกิดจากมนุษย์ตามเกณฑ์ความเสี่ยงที่ยอมรับได้ของบริษัทฯ (Risk Appetite)

3.1.2. การจัดการข้อมูลทั้งในรูปแบบเอกสารและดิจิทัล ต้องครอบคลุมทั้งวงจรชีวิตของข้อมูล รวมถึงการจัดการคุณภาพข้อมูล และการรักษาความปลอดภัยข้อมูล โดยจัดให้มีการควบคุมระดับการเข้าถึงระบบเทคโนโลยีดิจิทัลตามหน้าที่และความรับผิดชอบ

3.2. การรักษาความปลอดภัยระบบงาน (Application & System Security) กำหนดให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีดิจิทัล และการป้องกันภัยคุกคามต่อระบบสารสนเทศ ให้ใช้การควบคุมการเข้าถึงแบบเปลี่ยนแปลงนโยบายได้ (Dynamic Policy Based Access Control) และ กำหนดแนวทางการรักษาความปลอดภัยของเทคโนโลยีดิจิทัล (CIA) ให้รองรับกรอบการดำเนินการที่วางไว้ และสามารถป้องกันภัยคุกคามทางไซเบอร์จากเครือข่ายการเชื่อมโยงบริการต่างๆที่ใช้ในการดำเนินธุรกิจอันส่งผลกระทบต่อการดำเนินการทางธุรกิจของบริษัทฯ

3.3. การรักษาประโยชน์จากลิขสิทธิ์ และสิทธิ (Licensing & Right Protection)

3.3.1. ต้องกำหนดหลักเกณฑ์ ตรวจสอบสิทธิ์ของ*ผู้ใช้งาน*เรื่องการใช้ หรือติดตั้งโปรแกรมที่เครื่องคอมพิวเตอร์แบบถูกลิขสิทธิ์ เนื่องจากจะได้รับบริการปรับปรุง พัฒนาและแก้ไขข้อผิดพลาดเพื่อความปลอดภัยสารสนเทศ

3.3.2. การตรวจสอบและติดตามการนำเนื้อหาของบริษัทฯ ไปเผยแพร่ ทำซ้ำ ดัดแปลง หรือคัดลอกผ่านช่องทางดิจิทัลแพลตฟอร์มหรือสื่อสังคมออนไลน์ต่างๆ โดยมิได้ขออนุญาตต้องมีการรายงานหรือข้อความแจ้งเตือนผู้เกี่ยวข้องของบริษัทฯ

3.3.3. บริษัทฯ จะมีสิทธิเหนือทรัพย์สินทางปัญญาใดๆ (ไม่ว่าจะเป็นลิขสิทธิ์ สิทธิบัตร หรือสิทธิในทรัพย์สินทางปัญญาใดๆ) ที่พนักงานได้ประพันธ์ สร้างขึ้น หรือได้จัดทำขึ้นในระหว่างที่พนักงานถูกจ้างภายใต้สัญญาจ้างงาน และมีความเกี่ยวข้องกับธุรกิจของบริษัทฯ หรือมีความเกี่ยวข้องกับการวิจัยและพัฒนาของบริษัทฯ หรือได้พัฒนาขึ้นหรือได้มีการใช้อุปกรณ์ สิ่งของ สถานที่ หรือข้อมูลความลับของบริษัทฯ

3.4. การจัดการบริการภายนอก (External/Outsourcing Services) การบริการภายนอกบริษัทฯ ต้องมีประสิทธิภาพมากกว่าการบริการภายใน หรือจะทำการจัดหาบริการภายนอกได้ก็ต่อเมื่อบริษัทฯ ไม่มีศักยภาพในการบริการนั้นๆ ทั้งนี้ต้องจัดทำสัญญาการใช้บริการจาก*บุคคลภายนอก*หรือผู้ให้บริการภายนอกด้านเทคโนโลยีดิจิทัลที่มีการจัดทำข้อตกลงการให้บริการเป็นลายลักษณ์อักษร และต้องระบุ บทบาท หน้าที่ ความรับผิดชอบ เงื่อนไขการให้บริการและความรับผิดชอบต่อความเสียหายใดๆในกรณีที่ผู้ให้บริการภายนอกไม่ปฏิบัติตาม

หมายเหตุ ขอยกเลิกการประกาศของเอกสารนโยบายดังต่อไปนี้

1. นโยบายการจัดการระบบดิจิทัล พ.ศ.2565

บริษัท ดีสโตน คอร์ปอเรชั่น จำกัด (มหาชน)
84 หมู่ที่ 7 ซอยเพชรเกษม 122 ถนนเพชรเกษม ตำบลอ้อมน้อย อำเภอกระทุ่มแบน จังหวัดสมุทรสาคร 74130
DEESTONE CORPORATION PUBLIC COMPANY LIMITED
84 Soi Petchkasem 122, Moo7, Petchkasem Rd., Ommoi, Krathumban,
Samutsakorn, 74130 Thailand
Tel : (+662) 420-0038, 023-4756 Fax : (+662) 420-0572, 023-4724
E-mail : deestone@deestone.com, Website : www.deestone.com

เนื่องจากบริษัท ดีสโตนคอร์ปอเรชั่น จำกัด มหาชน ได้มีการปรับปรุงระเบียบการปฏิบัติงาน เรื่อง นโยบายด้านการจัดการระบบดิจิทัล เพื่อให้ครอบคลุมการดำเนินการด้านดิจิทัล และสอดคล้องกับนโยบายอื่นๆของบริษัทฯ

ทั้งนี้ให้มีผลโดยให้มีผลบังคับใช้ บริษัทดีสโตนคอร์ปอเรชั่น จำกัด มหาชน และ*บริษัทในเครือ* ตั้งแต่วันที่ 1 ตุลาคม 2567 เป็นต้นไป

(นางสาวกรวิกา วงศาริยวานิช)
รองประธานเจ้าหน้าที่บริหาร
บริษัท ดีสโตน คอร์ปอเรชั่น จำกัด (มหาชน)

ภาคผนวก

ภาคผนวก ก คำนิยาม

บริษัทฯ	บริษัท ดีสโตน คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ
บริษัทในเครือ	บริษัทย่อยและบริษัทร่วมที่อยู่ภายใต้การควบคุมและกำกับดูแลของบริษัทที่มีอยู่ในปัจจุบันและที่จะตั้งขึ้นในอนาคต
ผู้ใช้งาน	พนักงานของบริษัท รวม ไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ และมีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท
พนักงาน	พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงานพนักงานประจำ พนักงานสัญญจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท
ผู้ให้บริการภายนอก	บุคคลจากภายนอกบริษัทฯซึ่งประกอบธุรกิจ ว่าจ้างเพื่อใช้บริการที่เกี่ยวข้องกับระบบสารสนเทศ
ทรัพย์สินดิจิทัล	1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ระบบเครือข่ายคอมพิวเตอร์ 2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิมเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใดๆ 3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลในระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลส่วนบุคคล (PDPA) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดการพัฒนา หรือสิทธิ์ในการใช้จากเจ้าของผลิตภัณฑ์
คุณภาพบริการดิจิทัล	มาตรฐานและความสามารถในการตอบสนองความต้องการของผู้ใช้งานบริการต่างๆ ที่ดำเนินการผ่านช่องทางดิจิทัล รวมถึงคุณภาพข้อมูล ถือเป็นส่วนหนึ่งของคุณภาพการบริการ
การรักษาความมั่นคงปลอดภัย	กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัทได้รับความเสียหาย

บุคคลภายนอก	บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น ● บริษัทคู่ค้า (Business Partner) ● ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource) ● ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier) ● ผู้ให้บริการต่างๆ (Service Provider) ● ที่ปรึกษา (Consultant)
บริการ	บริการดิจิทัลที่สนับสนุนการดำเนินงานทางธุรกิจ โดยครอบคลุมทุกองค์ประกอบของเทคโนโลยีดิจิทัล ไม่ว่าจะเป็นด้าน ซอฟต์แวร์หรือฮาร์ดแวร์ รวมถึงทั้งบริการจากภายในและภายนอกบริษัทฯ
Recovery Point Objective (RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย ซึ่งบริษัทฯ ยอมรับได้
Recovery Time Objective (RTO)	ระยะเวลาสูงสุดที่จะกู้ข้อมูลได้หลังจากเกิด incident ซึ่งบริษัทฯ ต้องยอมรับได้
การควบคุมภายใน	กระบวนการปฏิบัติงานที่ถูกกำหนดร่วมกันโดย คณะกรรมการ ผู้บริหารตลอดจนพนักงานขององค์กรทุกระดับชั้นเพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่า วิธีการหรือการปฏิบัติงานตามที่กำหนดไว้จะทำให้บรรลุวัตถุประสงค์ของการควบคุม
ลิขสิทธิ์	ผลงานหรืองานสร้างสรรค์ต่างๆที่บริษัทฯ จัดทำขึ้น โดยรวมถึงผลงานของพนักงานที่เกิดขึ้นจากการทำงานในฐานะพนักงานหรือลูกจ้าง

ภาคผนวก ข มาตรฐานต่างๆ ที่ใช้อ้างอิง

กลุ่มมาตรฐานสากล

ISO IEC 27000:2018	มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ
ISO/IEC 20000	มาตรฐานของการบริหารบริการด้านไอที
ISO 22301	ระบบการบริหารความต่อเนื่องทางธุรกิจ
CSA-STAR	มาตรฐานความปลอดภัยสำหรับระบบคลาวด์
ISO 16175-2:2020	แนวทางและข้อกำหนดการทำงานสำหรับระบบการจัดการบันทึกดิจิทัล
NIST Cybersecurity Framework	กรอบงานที่ใช้ในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

กลุ่มมาตรฐานภายในประเทศ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562
พระราชบัญญัติคุ้มครองสิ่งบ่งชี้ทางภูมิศาสตร์ พ.ศ.2546
พระราชบัญญัติความลับทางการค้า พ.ศ.2545
พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 5) พ.ศ.2565
พระราชบัญญัติลิขสิทธิ์ พ.ศ.2537
พระราชบัญญัติเครื่องหมายการค้า (ฉบับที่ 3) พ.ศ.2534
พระราชบัญญัติเครื่องหมายการค้า พ.ศ.2534
พระราชบัญญัติสิทธิบัตร พ.ศ.2522

กลุ่มนโยบายภายในของบริษัทฯ

นโยบายการคุ้มครองข้อมูลส่วนบุคคล ฉบับวันที่ 22 กันยายน 2564
นโยบายการบริหารความเสี่ยง ฉบับวันที่ 22 กันยายน 2564