SUPALAI

นโยบายการใช้งานระบบสารสนเทศอย่างเหมาะสม

Acceptable Use Policy (AUP)

รหัสเอกสาร SPL-DT-PC-2604

Version: 00

ประวัติการปรับปรุงเอกสาร

(DOCUMENT VERSION HISTORY)

แก้ไขครั้งที่	วันที่บังคับใช้	รายละเอียดการแก้ไข
00	08 มิ.ย. 2569	เอกสารเผยแพร่ฉบับแรก

การอนุมัติเอกสาร

ผู้จัดทำ	ผู้ทบทวน	ผู้อนุมัติ
เฉลิมพล ลีลาชุติพงศ์	*มงคล นิตะโคตร*	*ไตรเตชะ ตั้งมติธรรม*
คุณเฉลิมพล ลีลาชุติพงศ์	คุณมงคล นิตะโคตร	คุณไตรเตชะ ตั้งมติธรรม
ผู้จัดการแผนก Digital Infrastructure & Cybersecurity Office (ประธาน ISMR)	ผู้อำนวยการ ฝ่ายดิจิทัลเทคโนโลยี (รองประธาน ISMS Management)	กรรมการผู้จัดการ (ประธาน ISMS Management)
08 / มิ.ย. / 2569	08 / มิ.ย. / 2569	08 / มิ.ย. / 2569

สารบัญ

1. หลักการและเหตุผล 5

2. วัตถุประสงค์ 5

3. ขอบเขต/การใช้บังคับ 6

4. คำจำกัดความ 6

5. นโยบายการใช้งานระบบสารสนเทศอย่างเหมาะสมและปลอดภัย 7

5.1 ข้อกำหนดทั่วไปสำหรับการใช้งานทรัพย์สิน (General Requirements for Asset Usage) 7

5.2 การอนุญาตให้ใช้ทรัพย์สิน (Acceptable Use for Assets) 8

5.3 การใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์ (Use of Computer Equipment Assets) 8

5.4 การใช้งานทรัพย์สินด้านซอฟต์แวร์ (Use of Software Assets) 9

5.5 การใช้งานอินเทอร์เน็ต (Internet Usage) 10

5.6 การใช้งานอีเมล (Email Usage) 11

5.7 การใช้งานข้อมูล (Data Use) 12

5.8 การใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร (Use of Telephone, Facsimile, Printer, and Photocopier) 13

5.9 การรักษาความลับของสถานที่ตั้งและพื้นที่สำคัญด้านเทคโนโลยีสารสนเทศ (Confidentiality of IT Facility Locations and Critical Areas) 14

5.10 การใช้งานพื้นที่จัดเก็บข้อมูลบนคลาวด์ (Cloud Storage Usage) 14

5.11 การใช้งานปัญญาประดิษฐ์และปัญญาประดิษฐ์เชิงสร้างสรรค์อย่างปลอดภัย (Safe Use of Artificial Intelligence and Generative AI) 15

5.12 การกระทำอื่นๆ ที่ถือเป็นข้อห้ามของบริษัท (Other Prohibited Activities) 16

6. การดำเนินการกรณีไม่ปฏิบัติตามนโยบายและแนวปฏิบัติ (Non-Compliance Actions) 17

1. หลักการและเหตุผล

บริษัทฯ ตระหนักถึงความสำคัญของการใช้งานระบบสารสนเทศ เครือข่าย อินเทอร์เน็ต อุปกรณ์คอมพิวเตอร์ และทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนสำคัญในการสนับสนุนการดำเนินธุรกิจ การให้บริการลูกค้า และการบริหารจัดการภายในองค์กรให้มีประสิทธิภาพ อย่างไรก็ตาม การใช้งานทรัพยากรดังกล่าวโดยไม่มีแนวทางหรือข้อกำหนดที่ชัดเจน อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การใช้งานระบบผิดวัตถุประสงค์ การรั่วไหลของข้อมูล การติดมัลแวร์ รวมถึงการกระทำที่อาจขัดต่อกฎหมาย ระเบียบ หรือข้อกำหนดที่เกี่ยวข้อง เพื่อให้การใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัทฯ เป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับหลักการด้านความมั่นคงปลอดภัยสารสนเทศ บริษัทฯ จึงได้จัดทำนโยบายการใช้งานที่ยอมรับได้ หรือ Acceptable Use Policy: AUP เพื่อกำหนดแนวทาง ข้อจำกัด หน้าที่ และความรับผิดชอบของผู้ใช้งานในการเข้าถึงและใช้งานระบบสารสนเทศ เครือข่าย อินเทอร์เน็ต อุปกรณ์ และข้อมูลของบริษัทฯ

นโยบายฉบับนี้จัดทำขึ้นภายใต้กรอบของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือ Information Security Management System: ISMS และสอดคล้องกับข้อกำหนด ISO/IEC 27001:2022 ข้อ 5.2 นโยบายความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) โดยบริษัทฯ ได้กำหนดนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศไว้ดังนี้ "บริษัท ศุภาลัย จำกัด (มหาชน) มุ่งมั่นบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบ เพื่อปกป้องข้อมูลและทรัพยากรด้านเทคโนโลยีขององค์กรให้ปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง พร้อมทั้งดำเนินการปรับปรุงอย่างต่อเนื่อง เพื่อสนับสนุนการดำเนินงานและการเติบโตขององค์กรอย่างมั่นคง"

ดังนั้น นโยบายการใช้งานที่ยอมรับได้จึงเป็นหนึ่งในกลไกสำคัญในการสนับสนุนการนำนโยบาย ISMS ไปสู่การปฏิบัติจริง โดยช่วยกำหนดพฤติกรรมการใช้งานที่เหมาะสม ลดความเสี่ยงจากการใช้งานระบบสารสนเทศ และส่งเสริมให้ผู้ใช้งานทุกคนมีความตระหนักและรับผิดชอบต่อการรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพยากรด้านเทคโนโลยีของบริษัทฯ

2. วัตถุประสงค์

1) เพื่อกำหนดหลักเกณฑ์และแนวปฏิบัติในการใช้งานระบบสารสนเทศ เครือข่าย อินเทอร์เน็ต อุปกรณ์คอมพิวเตอร์ และทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัทฯ ให้เป็นไปอย่างเหมาะสมและปลอดภัย
2) เพื่อป้องกันการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศในลักษณะที่ไม่เหมาะสม ผิดวัตถุประสงค์ หรืออาจก่อให้เกิดความเสียหายต่อบริษัทฯ ผู้ใช้งาน ลูกค้า คู่ค้า หรือบุคคลที่เกี่ยวข้อง
3) เพื่อสนับสนุนการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบสารสนเทศของบริษัทฯ
4) เพื่อสร้างความตระหนักรู้ หน้าที่ และความรับผิดชอบของผู้ใช้งานในการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัทฯ
5) เพื่อให้การใช้งานระบบสารสนเทศเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ สัญญา และข้อกำหนดที่เกี่ยวข้อง รวมถึงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

3. ขอบเขต/การใช้บังคับ

นโยบายฉบับนี้มีผลบังคับใช้กับพนักงานทุกคนของบริษัทฯ รวมถึงผู้ใช้งาน ผู้ดูแลระบบ ผู้ให้บริการภายนอก คู่ค้า ที่ปรึกษา ผู้รับจ้าง และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง ใช้งาน หรือเชื่อมต่อกับระบบสารสนเทศ ข้อมูล เครือข่าย อุปกรณ์ หรือทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัทฯ

4. คำจำกัดความ

No.	คำศัพท์	คำจำกัดความ
1.	บริษัท	บริษัท ศุภาลัย จำกัด (มหาชน) และบริษัทย่อย
2.	บริษัทย่อย	บริษัท ศุภาลัย จำกัด (มหาชน) มีอำนาจควบคุมได้
3.	ผู้ใช้งาน (User)	บุคคลที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบสารสนเทศ ข้อมูล เครือข่าย อุปกรณ์ หรือทรัพย์สินสารสนเทศของบริษัทฯ เช่น กรรมการ ผู้บริหาร พนักงาน ผู้รับจ้าง คู่ค้า ที่ปรึกษา และบุคคลภายนอกที่ได้รับอนุญาต
4.	ทรัพย์สินสารสนเทศ (Information Asset)	ข้อมูล ระบบสารสนเทศ ซอฟต์แวร์ อุปกรณ์ เครือข่าย บัญชีผู้ใช้งาน เอกสาร หรือทรัพยากรด้านเทคโนโลยีสารสนเทศที่มีคุณค่าต่อบริษัทฯ และต้องได้รับการคุ้มครอง
5.	ระบบสารสนเทศ (Information System)	ระบบ แอปพลิเคชัน ฐานข้อมูล เว็บไซต์ หรือบริการดิจิทัลที่บริษัทฯ ใช้ในการจัดเก็บ ประมวลผล รับส่ง หรือให้บริการข้อมูล
6.	ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลธรรมดาที่สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
7.	ข้อมูลลับ (Confidential Information)	ข้อมูลที่มีความสำคัญต่อบริษัทฯ ลูกค้า คู่ค้า หรือบุคคลที่เกี่ยวข้อง ซึ่งหากถูกเปิดเผย เข้าถึง แก้ไข หรือใช้งานโดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายต่อบริษัทฯ หรือผู้เกี่ยวข้อง
8.	การจำแนกประเภทข้อมูล (Data Classification)	การกำหนดระดับความสำคัญของข้อมูล เพื่อใช้ในการควบคุมการเข้าถึง การจัดเก็บ การรับส่ง การใช้งาน และการทำลายข้อมูลให้เหมาะสมกับระดับความเสี่ยง
9.	บัญชีผู้ใช้งาน (User Account)	ชื่อบัญชีหรือรหัสประจำตัวที่บริษัทฯ กำหนดให้แก่ผู้ใช้งาน เพื่อใช้ในการเข้าสู่ระบบสารสนเทศ เครือข่าย หรือบริการต่าง ๆ ของบริษัทฯ
10.	รหัสผ่าน (Password)	ข้อมูลลับที่ใช้ร่วมกับบัญชีผู้ใช้งานหรือวิธีการพิสูจน์ตัวตนอื่น เพื่อยืนยันตัวตนของผู้ใช้งานก่อนเข้าถึงระบบหรือข้อมูล
11.	สิทธิ์การเข้าถึง (Access Right)	สิทธิ์ที่กำหนดให้ผู้ใช้งานสามารถเข้าถึง ใช้งาน แก้ไข ลบ หรือจัดการระบบ ข้อมูล หรือทรัพย์สินสารสนเทศตามบทบาทหน้าที่ที่ได้รับอนุมัติ
12.	การพิสูจน์ตัวตน (Authentication)	กระบวนการตรวจสอบและยืนยันตัวตนของผู้ใช้งานก่อนอนุญาตให้เข้าถึงระบบ ข้อมูล หรือทรัพย์สินสารสนเทศ
13.	หลักสิทธิ์เท่าที่จำเป็น (Least Privilege)	หลักการกำหนดสิทธิ์ให้ผู้ใช้งานเข้าถึงระบบหรือข้อมูลเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานตามบทบาทหน้าที่เท่านั้น
14.	ความจำเป็นในการรับรู้และใช้งานข้อมูล (Need-to-Know / Need-to-Use)	หลักการที่กำหนดให้ผู้ใช้งานเข้าถึงหรือใช้ข้อมูลเฉพาะเมื่อมีความจำเป็นต่อการปฏิบัติงานเท่านั้น

No.	คำศัพท์	คำจำกัดความ
15.	อุปกรณ์ปลายทาง (Endpoint Device)	อุปกรณ์ที่ใช้เชื่อมต่อหรือเข้าถึงระบบของบริษัทฯ เช่น คอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา แท็บเล็ต โทรศัพท์มือถือ หรืออุปกรณ์อื่นที่เกี่ยวข้อง
16.	อุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD)	อุปกรณ์ที่เป็นของผู้ใช้งาน เช่น คอมพิวเตอร์พกพา โทรศัพท์มือถือ หรือแท็บเล็ต ที่นำมาใช้เชื่อมต่อหรือเข้าถึงระบบ ข้อมูล หรือเครือข่ายของบริษัทฯ
17.	ปัญญาประดิษฐ์ (Artificial Intelligence :AI)	เทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อให้คอมพิวเตอร์มีคุณสมบัติหรือพฤติกรรมใกล้เคียงมนุษย์ เช่น การเรียนรู้ การรับรู้และตอบสนองต่อสภาพแวดล้อม การให้เหตุผล และการแก้ไขปัญหา เป็นต้น ตามวัตถุประสงค์ที่มนุษย์กำหนด
18.	ข้อมูลของบริษัทฯ (Company Data)	ข้อมูลทุกประเภทที่บริษัทฯ เป็นเจ้าของหรือมีสิทธิครอบครอง รวมถึงข้อมูลที่เกิดจากการดำเนินธุรกิจ ไม่ว่าจะอยู่ในรูปแบบเอกสาร อิเล็กทรอนิกส์ เสียง ภาพ หรือรูปแบบอื่นใด
19.	มัลแวร์ (Malware)	ซอฟต์แวร์หรือโปรแกรมประสงค์ร้ายที่ถูกสร้างขึ้นเพื่อรบกวน ทำลาย เข้าถึง ขโมย หรือทำให้ระบบ ข้อมูล หรืออุปกรณ์เสียหาย
20.	ฟิชชิ่ง (Phishing)	การหลอกลวงผ่านอีเมล เว็บไซต์ ข้อความ หรือช่องทางออนไลน์ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลบัญชี หรือข้อมูลส่วนบุคคล
21.	พื้นที่ควบคุม (Controlled Area)	พื้นที่ที่มีระบบ ข้อมูล หรืออุปกรณ์สำคัญของบริษัทฯ เช่น Data Center หรือห้องเซิร์ฟเวอร์ ซึ่งต้องมีการควบคุมการเข้าออกและการเข้าถึงอย่างเหมาะสม

5. นโยบายการใช้งานระบบสารสนเทศอย่างเหมาะสมและปลอดภัย

5.1 ข้อกำหนดทั่วไปสำหรับการใช้งานทรัพย์สิน (General Requirements for Asset Usage)

บริษัท ศุภาลัย จำกัด (มหาชน) (“บริษัทฯ”) กำหนดให้ผู้ใช้งานทุกคนที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานทรัพย์สินสารสนเทศของบริษัทฯ (Information Assets) ไม่ว่าจะเป็นกรรมการ ผู้บริหาร พนักงาน ผู้รับจ้าง นักศึกษาฝึกงาน หรือบุคคลภายนอกที่ได้รับสิทธิ์การเข้าถึง ต้องปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด เพื่อให้การใช้งานทรัพย์สินสารสนเทศเป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับวัตถุประสงค์ทางธุรกิจของบริษัทฯผู้ใช้งานทุกคนต้องยึดถือหลักการพื้นฐานในการใช้งานทรัพย์สินสารสนเทศ ดังนี้

1) การใช้งานเพื่อวัตถุประสงค์ทางธุรกิจ (Business Purpose) ทรัพย์สินสารสนเทศของบริษัทฯ จัดให้มีขึ้นเพื่อสนับสนุนการดำเนินงานและการปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมาย ผู้ใช้งานต้องใช้ทรัพย์สินดังกล่าวเพื่อประโยชน์ในการปฏิบัติงานของบริษัทฯ เป็นหลัก และต้องไม่ใช้งานในลักษณะที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือนโยบายของบริษัทฯ
2) ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (Asset Accountability) ผู้ใช้งานที่ได้รับมอบหมายให้ใช้งานหรือครอบครองทรัพย์สินสารสนเทศของบริษัทฯ มีหน้าที่ดูแลรักษา ป้องกันความเสียหาย การสูญหาย การถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือการนำไปใช้งานโดยไม่เหมาะสม ตลอดระยะเวลาที่ทรัพย์สินดังกล่าวอยู่ในความรับผิดชอบของตน
3) การใช้สิทธิ์เท่าที่จำเป็น (Least Privilege) ผู้ใช้งานจะได้รับสิทธิ์การเข้าถึงระบบ ข้อมูล หรือทรัพย์สินสารสนเทศเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานตามบทบาทหน้าที่เท่านั้น และต้องไม่พยายามเข้าถึง ขยายสิทธิ์ เปลี่ยนแปลงสิทธิ์ หรือใช้งานสิทธิ์ของผู้อื่นโดยไม่ได้รับอนุญาต

4) การรักษาความลับของข้อมูล (Confidentiality) ข้อมูล เอกสาร ระบบ และทรัพย์สินสารสนเทศที่ผู้ใช้งานสามารถเข้าถึงได้จากการปฏิบัติงาน ถือเป็นทรัพย์สินของบริษัทฯ ที่ต้องได้รับการคุ้มครองตามระดับความสำคัญและการจำแนกประเภทข้อมูล (Data Classification) ที่บริษัทฯ กำหนด ผู้ใช้งานต้องไม่เปิดเผย คัดลอก ส่งต่อ หรือเผยแพร่ข้อมูลให้แก่บุคคลที่ไม่มีสิทธิ์รับทราบ เว้นแต่ได้รับอนุญาตอย่างถูกต้อง
5) การตรวจสอบและติดตามการใช้งาน (Monitoring and Audit) บริษัทฯ สงวนสิทธิ์ในการตรวจสอบ ติดตาม และบันทึกการใช้งานทรัพย์สินสารสนเทศ ระบบ เครือข่าย อุปกรณ์ และข้อมูลของบริษัทฯ ตามความเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยสารสนเทศ ป้องกันการใช้งานที่ไม่เหมาะสม และสนับสนุนการปฏิบัติตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

ผู้ใช้งานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามนโยบายฉบับนี้ รวมถึงนโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอื่น ๆ ที่บริษัทฯ กำหนดอย่างต่อเนื่องตลอดระยะเวลาที่มีความสัมพันธ์หรือได้รับสิทธิ์การเข้าถึงทรัพย์สินสารสนเทศของบริษัทฯ

5.2 การอนุญาตให้ใช้ทรัพย์สิน (Acceptable Use for Assets)

บริษัทฯ อนุญาตให้ผู้ใช้งานเข้าถึงและใช้ทรัพย์สินสารสนเทศของบริษัทฯ (Information Assets) ภายใต้เงื่อนไข ขอบเขต และสิทธิ์ที่ได้รับอนุมัติเท่านั้น เพื่อให้การใช้งานเป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับวัตถุประสงค์ทางธุรกิจ โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) การใช้งานที่ได้รับอนุญาต (Permitted Use) ผู้ใช้งานสามารถใช้ระบบ อุปกรณ์ เครือข่าย ข้อมูล และบริการดิจิทัลของบริษัทฯ เพื่อปฏิบัติงานตามหน้าที่ รวมถึงการสื่อสารทางธุรกิจผ่านช่องทางที่บริษัทฯ จัดหาให้หรืออนุมัติ ทั้งนี้ การใช้งานส่วนตัวทำได้เฉพาะในปริมาณเล็กน้อย ไม่กระทบต่องาน ไม่ก่อให้เกิดความเสี่ยง และไม่ขัดต่อนโยบายหรือกฎหมาย
2) การอนุมัติสิทธิ์การเข้าถึง (Access Authorization) ผู้ใช้งานจะได้รับสิทธิ์เข้าถึงทรัพย์สินสารสนเทศเมื่อมีความจำเป็นทางธุรกิจ ได้รับอนุมัติจากผู้มีอำนาจ และผ่านการยืนยันตัวตนอย่างถูกต้อง โดยต้องดำเนินการผ่านระบบหรือช่องทางที่บริษัทฯ กำหนด เช่น Active Directory
3) เงื่อนไขก่อนเริ่มใช้งาน (Pre-use Requirements) ก่อนใช้งาน ผู้ใช้งานต้องรับทราบและยอมรับนโยบายฉบับนี้ รวมถึงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง และเข้ารับการอบรมหรือการสื่อสารตามที่บริษัทฯ กำหนด
4) การถอนหรือเปลี่ยนแปลงสิทธิ์ (Access Revocation or Modification) บริษัทฯ จะถอนหรือเปลี่ยนแปลงสิทธิ์เมื่อสิ้นสุดการจ้างงาน เปลี่ยนบทบาทหน้าที่ หมดความจำเป็นในการใช้งาน มีการฝ่าฝืนนโยบาย หรือมีเหตุจำเป็นด้านความมั่นคงปลอดภัยสารสนเทศ

5.3 การใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์ (Use of Computer Equipment Assets)

อุปกรณ์คอมพิวเตอร์ เช่น คอมพิวเตอร์ตั้งโต๊ะ (Desktop) คอมพิวเตอร์พกพา (Laptop) แท็บเล็ต โทรศัพท์มือถือที่บริษัทฯ จัดให้ และอุปกรณ์ปลายทางอื่น ๆ (Endpoint Devices) ถือเป็นทรัพย์สินของบริษัทฯ และอยู่ภายใต้การบริหารจัดการของฝ่าย Digital Technology โดยผู้ใช้งานต้องดูแล ใช้งาน และป้องกันอุปกรณ์ดังกล่าวให้ปลอดภัย เหมาะสม และเป็นไปตามนโยบายของบริษัทฯ โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) การดูแลและรักษาความปลอดภัยของอุปกรณ์ (Device Protection) ผู้ใช้งานต้องดูแลอุปกรณ์ที่ได้รับมอบหมายให้อยู่ในสภาพสมบูรณ์ ปลอดภัยจากความเสียหาย การสูญหาย หรือการถูกใช้งานโดยไม่ได้รับอนุญาต และต้องล็อกหน้าจอทุกครั้งเมื่อออกจากพื้นที่ทำงาน รวมถึงตั้งค่าให้อุปกรณ์ล็อกอัตโนมัติเมื่อไม่มีการใช้งานตามระยะเวลาที่บริษัทฯ กำหนด
2) ผู้ใช้งานต้องไม่ติดตั้งซอฟต์แวร์ แอปพลิเคชัน หรือโปรแกรมใด ๆ บนอุปกรณ์ของบริษัทฯ โดยไม่ได้รับอนุมัติจากฝ่าย Digital Technology ผ่านระบบหรือช่องทางที่กำหนด รวมถึงต้องไม่ดัดแปลง แก้ไข หรือเปลี่ยนแปลงการตั้งค่าระบบปฏิบัติการ BIOS/UEFI การตั้งค่าความปลอดภัย หรือค่าระบบอื่นใดที่บริษัทฯ กำหนดไว้ เว้นแต่ได้รับอนุมัติอย่างเป็นทางการ
3) การใช้งานอุปกรณ์จัดเก็บข้อมูลภายนอก (External Storage Devices) ห้ามเชื่อมต่อหรือใช้งานอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น USB Drive, External Hard Disk หรือ Memory Card กับอุปกรณ์คอมพิวเตอร์ของบริษัทฯ เว้นแต่เป็นอุปกรณ์ที่ได้รับอนุมัติจาก DICO หรือหน่วยงานที่บริษัทฯ กำหนด เพื่อป้องกันความเสี่ยงจากมัลแวร์และการรั่วไหลของข้อมูล
4) การนำอุปกรณ์ออกนอกสถานที่ (Off-site Use) กรณีที่ผู้ใช้งานนำอุปกรณ์คอมพิวเตอร์ของบริษัทฯ ไปใช้งานภายนอกสถานที่ เช่น การทำงานจากที่บ้าน (Work from Home) หรือการเดินทางเพื่อธุรกิจ ผู้ใช้งานต้องดูแลรักษาอุปกรณ์ให้อยู่ในสภาพปลอดภัย ป้องกันการสูญหาย การถูกโจรกรรม การเข้าถึงโดยไม่ได้รับอนุญาต และการเปิดเผยข้อมูลของบริษัทฯ โดยต้องใช้งานอุปกรณ์ตามมาตรการรักษาความมั่นคงปลอดภัยที่บริษัทฯ กำหนด
5) การใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) อุปกรณ์ส่วนตัวของผู้ใช้งานที่ต้องการเชื่อมต่อกับเครือข่าย หรือเข้าถึงระบบและข้อมูลของบริษัทฯ ต้องได้รับการพิจารณาและอนุมัติจากฝ่าย Digital Technology หรือหน่วยงานที่บริษัทฯ กำหนด และต้องเป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยของบริษัทฯ
6) การรายงานเหตุผิดปกติของอุปกรณ์ (Incident Reporting) กรณีอุปกรณ์สูญหาย ถูกโจรกรรม เสียหาย หรือพบเหตุผิดปกติที่อาจกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ผู้ใช้งานต้องแจ้งหัวหน้างานและฝ่าย Digital Technology โดยเร็วตามขั้นตอนที่บริษัทฯ กำหนด

5.4 การใช้งานทรัพย์สินด้านซอฟต์แวร์ (Use of Software Assets)

บริษัทฯ กำหนดให้มีการบริหารจัดการซอฟต์แวร์ที่ได้รับอนุญาต (Approved Software List) และการใช้งานซอฟต์แวร์ที่มีสัญญาอนุญาตการใช้งาน (Software License) อย่างถูกต้องตามกฎหมาย เพื่อป้องกันความเสี่ยงด้านลิขสิทธิ์ ความมั่นคงปลอดภัยสารสนเทศ และการใช้งานซอฟต์แวร์ที่ไม่เหมาะสม โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) การใช้งานซอฟต์แวร์ที่ได้รับอนุญาต (Approved Software Use) ผู้ใช้งานต้องใช้งานเฉพาะซอฟต์แวร์ที่ได้รับอนุมัติจากบริษัทฯ และมีสัญญาอนุญาตการใช้งานที่ถูกต้องเท่านั้น ห้ามติดตั้งหรือใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ (Pirated Software) หรือซอฟต์แวร์ที่ไม่ได้รับอนุมัติ

2) การขอใช้งานซอฟต์แวร์เพิ่มเติม (Software Request) กรณีผู้ใช้งานมีความจำเป็นต้องใช้งานซอฟต์แวร์เพิ่มเติมเพื่อสนับสนุนการปฏิบัติงาน ผู้ใช้งานต้องแจ้งหัวหน้างานเพื่อพิจารณาความจำเป็นทางธุรกิจ และยื่นคำร้องผ่านระบบหรือช่องทางที่ฝ่าย Digital Technology กำหนด โดยต้องได้รับอนุมัติจากฝ่าย Digital Technology ก่อนดำเนินการติดตั้งหรือใช้งานซอฟต์แวร์ดังกล่าว
3) การคุ้มครองสิทธิ์การใช้งานซอฟต์แวร์ (Software License Compliance) ห้ามคัดลอก ถ่ายโอน แจกจ่าย หรือนำซอฟต์แวร์ที่บริษัทฯ จัดหาให้ไปใช้งานนอกขอบเขตที่ได้รับอนุญาต หรือมอบให้บุคคลภายนอกใช้งาน เว้นแต่เป็นไปตามเงื่อนไขของสัญญาอนุญาตและได้รับอนุมัติจากบริษัทฯ
4) การห้ามใช้ซอฟต์แวร์ที่มีความเสี่ยง (Prohibited or High-Risk Software) ห้ามติดตั้งหรือใช้งานซอฟต์แวร์ที่อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัย เช่น Remote Access Tool ที่ไม่ได้รับอนุมัติ โปรแกรม Peer-to-Peer (P2P) ซอฟต์แวร์เจาะระบบ หรือเครื่องมือทดสอบช่องโหว่ เว้นแต่เป็นส่วนหนึ่งของงานที่ได้รับมอบหมายและได้รับอนุมัติอย่างเป็นทางการ
5) การตรวจสอบซอฟต์แวร์ (Software Review and Monitoring) บริษัทฯ สงวนสิทธิ์ในการตรวจสอบซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ของบริษัทฯ เป็นระยะ และอาจถอนการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุมัติหรือมีความเสี่ยง โดยไม่จำเป็นต้องแจ้งล่วงหน้า

5.5 การใช้งานอินเทอร์เน็ต (Internet Usage)

บริษัทฯ จัดให้มีการเชื่อมต่ออินเทอร์เน็ตเพื่อสนับสนุนการปฏิบัติงานทางธุรกิจ โดยการใช้งานอินเทอร์เน็ตต้องอยู่ภายใต้มาตรการควบคุม ตรวจสอบ และรักษาความมั่นคงปลอดภัยเครือข่ายของบริษัทฯ เช่น Firewall และ Web Content Filtering เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ การใช้งานที่ไม่เหมาะสม และการละเมิดกฎหมาย โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) การใช้งานเพื่อวัตถุประสงค์ทางธุรกิจ (Business Use) ผู้ใช้งานต้องใช้อินเทอร์เน็ตเพื่อสนับสนุนการปฏิบัติงานเป็นหลัก โดยการใช้งานส่วนตัวในปริมาณเหมาะสมสามารถทำได้เฉพาะกรณีที่ไม่กระทบต่อการทำงาน ไม่ก่อให้เกิดความเสี่ยง และไม่ขัดต่อนโยบายหรือกฎหมายที่เกี่ยวข้อง
2) การเข้าถึงเว็บไซต์ที่ไม่เหมาะสม (Prohibited Websites) ห้ามเข้าถึงเว็บไซต์หรือเนื้อหาที่เกี่ยวข้องกับสิ่งผิดกฎหมาย การพนัน สื่อลามกอนาจาร ความรุนแรง การก่อการร้าย การละเมิดลิขสิทธิ์ หรือเนื้อหาใด ๆ ที่ขัดต่อกฎหมาย ศีลธรรมอันดี หรือนโยบายของบริษัทฯ
3) การดาวน์โหลดและแชร์ข้อมูล (Download and File Sharing) ห้ามดาวน์โหลดซอฟต์แวร์ สื่อ หรือไฟล์จากอินเทอร์เน็ตโดยไม่ได้รับอนุมัติจากฝ่าย Digital Technology เว้นแต่เป็นซอฟต์แวร์หรือแหล่งดาวน์โหลดที่ได้รับอนุมัติ รวมถึงห้ามใช้เครือข่ายของบริษัทฯ เพื่อแชร์หรือดาวน์โหลดข้อมูลที่ละเมิดลิขสิทธิ์ผ่านบริการ P2P, Torrent หรือช่องทางอื่นใด
4) การใช้ VPN และการหลบเลี่ยงระบบควบคุม (VPN and Filtering Bypass) ห้ามใช้ VPN ส่วนตัว (Personal VPN) เครื่องมือ Proxy หรือเครื่องมือใด ๆ เพื่อหลบเลี่ยงระบบกรองและควบคุมการเข้าถึงอินเทอร์เน็ตของบริษัทฯ เว้นแต่เป็น VPN หรือช่องทางการเชื่อมต่อที่บริษัทฯ จัดหาให้หรืออนุมัติอย่างเป็นทางการ

5) การระมัดระวังภัยคุกคามทางอินเทอร์เน็ต (Internet Threat Awareness) ผู้ใช้งานต้องระมัดระวังการเข้าถึงเว็บไซต์ ลิงก์ หรือไฟล์ที่น่าสงสัย โดยเฉพาะลิงก์จากอีเมลหรือข้อความที่ไม่ได้คาดหมาย หากพบเว็บไซต์ฟิชชิ่ง (Phishing) เนื้อหาที่น่าสงสัย หรือเหตุการณ์ที่อาจกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ต้องแจ้งหัวหน้างานและฝ่าย Digital Technology หรือหน่วยงานที่รับผิดชอบโดยเร็ว
6) การขอยกเว้นการเข้าถึงเว็บไซต์ (Website Access Exception) กรณีมีความจำเป็นทางธุรกิจในการเข้าถึงเว็บไซต์ที่ถูกจำกัดหรือบล็อก ผู้ใช้งานต้องแจ้งหัวหน้างานเพื่อพิจารณาความจำเป็น และให้หัวหน้างานยื่นคำร้องผ่านระบบหรือช่องทางที่บริษัทฯ กำหนด พร้อมระบุเหตุผลประกอบการขอใช้งาน โดยต้องได้รับอนุมัติก่อนเข้าใช้งานเว็บไซต์ดังกล่าว

5.6 การใช้งานอีเมล (Email Usage)

บริษัทฯ จัดให้มีบัญชีอีเมลองค์กรผ่านระบบ Google Workspace เพื่อใช้ในการสื่อสารและสนับสนุนการดำเนินธุรกิจ โดยบัญชีอีเมล ข้อความ ไฟล์แนบ และข้อมูลที่รับส่งหรือจัดเก็บผ่านระบบอีเมลของบริษัทฯ ถือเป็นทรัพย์สินสารสนเทศของบริษัทฯ (Information Asset) และอาจได้รับการตรวจสอบตามความจำเป็นภายใต้ขอบเขตที่กฎหมาย ระเบียบ และนโยบายของบริษัทฯ กำหนด โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) การใช้งานอีเมลองค์กร (Corporate Email Use) ผู้ใช้งานต้องใช้อีเมลองค์กร เพื่อการปฏิบัติงานและการสื่อสารทางธุรกิจเป็นหลัก โดยต้องใช้บัญชีอีเมลที่บริษัทฯ อนุญาตเท่านั้น ห้ามใช้อีเมลส่วนตัวในการรับส่งข้อมูลของบริษัทฯ โดยเฉพาะข้อมูลลับ ข้อมูลภายใน ข้อมูลส่วนบุคคล หรือข้อมูลสำคัญตามที่กำหนดไว้ในนโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย
2) การดูแลบัญชีอีเมลและการพิสูจน์ตัวตน (Account and Authentication) ผู้ใช้งานต้องดูแลรักษาบัญชีอีเมลของตนเองให้ปลอดภัย ไม่เปิดเผยรหัสผ่านหรือยินยอมให้บุคคลอื่นใช้งานบัญชีของตน และต้องใช้งานรหัสผ่านหรือวิธีการพิสูจน์ตัวตนที่บริษัทฯ กำหนด เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การแอบอ้างตัวตน หรือการนำบัญชีไปใช้ในทางที่ไม่เหมาะสม
3) การใช้งานบัญชีอีเมลกลาง (Shared Email Account) บัญชีอีเมลกลางหรือบัญชีที่มีวัตถุประสงค์เฉพาะ สามารถจัดให้มีขึ้นเพื่อสนับสนุนการปฏิบัติงานของหน่วยงาน โดยต้องกำหนดเจ้าของบัญชีหรือผู้รับผิดชอบหลัก (Account Owner) อย่างชัดเจน และต้องมีการควบคุมสิทธิ์การเข้าถึงและการใช้งานอย่างเหมาะสม
4) การรับส่งข้อมูลและไฟล์แนบ (Email and Attachment Handling) ผู้ใช้งานต้องตรวจสอบผู้รับ เนื้อหา และไฟล์แนบให้ถูกต้องก่อนส่งอีเมลทุกครั้ง โดยเฉพาะกรณีที่มีข้อมูลลับ ข้อมูลภายใน หรือข้อมูลส่วนบุคคล ห้ามคัดลอก ส่งต่อ หรือเผยแพร่ข้อมูลดังกล่าวให้แก่บุคคลที่ไม่มีสิทธิ์รับทราบ เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้มีอำนาจที่เกี่ยวข้อง และต้องใช้วิธีการป้องกันข้อมูลตามระดับความสำคัญของข้อมูล

5) มารยาทและความเหมาะสมในการใช้อีเมล (Email Etiquette) ผู้ใช้งานต้องจัดทำเนื้อหาอีเมลด้วยความสุภาพ ถูกต้อง และเหมาะสม เนื่องจากอีเมลที่ส่งจากบัญชีของบริษัทฯ อาจถือเป็นการสื่อสารในนามของบริษัทฯ และอาจส่งผลต่อภาพลักษณ์ ความน่าเชื่อถือ หรือความรับผิดชอบของบริษัทฯ ทั้งนี้ ผู้ใช้งานไม่ควรใช้คำสั่งตอบกลับถึงทุกคน (Reply All) หรือส่งต่ออีเมลโดยไม่จำเป็น ทั้งนี้ ควรดำเนินการเฉพาะกรณีที่เกี่ยวข้องและจำเป็นต่อการปฏิบัติงานเท่านั้น
6) ข้อห้ามในการใช้งานอีเมล (Prohibited Email Use) ห้ามใช้อีเมลของบริษัทฯ เพื่อกระทำการที่ผิดกฎหมาย ขัดต่อศีลธรรมอันดี ละเมิดลิขสิทธิ์ ส่งอีเมลขยะ (Spam Mail) อีเมลลูกโซ่ (Chain Mail) อีเมลหลอกลวง (Phishing Email) หรือส่งต่อเนื้อหาที่หยาบคาย ลามก อนาจาร หมิ่นประมาท เลือกปฏิบัติ ข่มขู่ หรือก่อให้เกิดความเสียหายต่อบริษัทฯ บุคคลอื่น หรือหน่วยงานที่เกี่ยวข้อง
7) การระมัดระวังภัยคุกคามทางอีเมล (Email Threat Awareness) ผู้ใช้งานต้องใช้ความระมัดระวังเมื่อได้รับอีเมลจากผู้ส่งที่ไม่รู้จัก อีเมลที่มีลิงก์หรือไฟล์แนบที่ไม่คาดหมาย หรืออีเมลที่มีลักษณะน่าสงสัยว่าเป็นฟิชชิ่ง มัลแวร์ หรือการหลอกลวง หากพบเหตุผิดปกติ ห้ามคลิกลิงก์ เปิดไฟล์แนบ หรือส่งต่ออีเมลดังกล่าว และต้องแจ้งหัวหน้างานและฝ่าย Digital Technology หรือหน่วยงานที่รับผิดชอบตามช่องทางที่บริษัทฯ กำหนดโดยเร็ว
8) การจัดการพื้นที่และการปิดบัญชีอีเมล (Mailbox and Account Management) ผู้ใช้งานต้องบริหารจัดการกล่องจดหมายของตนให้อยู่ภายใต้ข้อกำหนดของบริษัทฯ และจัดเก็บเฉพาะอีเมลที่จำเป็นต่อการปฏิบัติงานหรือจำเป็นต้องเก็บรักษาตามกฎหมาย ระเบียบ หรือข้อกำหนดที่เกี่ยวข้อง ทั้งนี้ บัญชีอีเมลองค์กรจะถูกระงับหรือปิดการใช้งานเมื่อผู้ใช้งานสิ้นสุดความสัมพันธ์กับบริษัทฯ หรือเมื่อหมดความจำเป็นในการใช้งาน และข้อมูลในบัญชีดังกล่าวจะได้รับการจัดการตามนโยบายของบริษัทฯ

5.7 การใช้งานข้อมูล (Data Use)

ข้อมูลของบริษัทฯ ไม่ว่าจะอยู่ในรูปแบบดิจิทัล เอกสารกระดาษ หรือรูปแบบอื่นใด ถือเป็นทรัพย์สินสารสนเทศที่มีคุณค่าของบริษัทฯ และต้องได้รับการใช้งาน จัดเก็บ ส่งต่อ และทำลายอย่างเหมาะสมตามระดับการจำแนกประเภทข้อมูลที่บริษัทฯ กำหนด โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) การเข้าถึงและใช้งานข้อมูล (Data Access and Use) ผู้ใช้งานต้องเข้าถึงและใช้งานข้อมูลเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานตามบทบาทหน้าที่ของตน โดยยึดหลักความจำเป็นในการรับรู้และใช้งานข้อมูล (Need-to-Know / Need-to-Use)
2) การจัดเก็บและโอนย้ายข้อมูล (Data Storage and Transfer) ผู้ใช้งานต้องจัดเก็บข้อมูลของบริษัทฯ ไว้ในระบบหรือแหล่งจัดเก็บข้อมูลที่บริษัทฯ กำหนดหรืออนุมัติเท่านั้น หรือระบบจัดเก็บข้อมูลที่ได้รับอนุญาต ห้ามคัดลอก โอนย้าย หรือจัดเก็บข้อมูลลับบนอุปกรณ์ส่วนตัว บริการ Cloud ส่วนตัว หรือสื่อบันทึกข้อมูลที่ไม่ได้รับอนุมัติ
3) การใช้ข้อมูลส่วนบุคคล (Personal Data Use) ข้อมูลส่วนบุคคล (Personal Data) ต้องได้รับการเก็บ ใช้ เปิดเผย หรือประมวลผลตามวัตถุประสงค์ที่ชอบด้วยกฎหมาย และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงนโยบายและแนวปฏิบัติที่บริษัทฯ กำหนด

4) **การเปิดเผยหรือแบ่งปันข้อมูล (Data Disclosure and Sharing)** ห้ามเปิดเผย ส่งต่อ หรือแบ่งปันข้อมูลของบริษัทฯ ให้แก่บุคคลภายนอก คู่ค้า หรือหน่วยงานอื่นที่ไม่มีสิทธิ์รับทราบ เว้นแต่ได้รับอนุญาตอย่างเป็นทางการ และมีมาตรการคุ้มครองข้อมูลที่เหมาะสม เช่น ข้อตกลงการรักษาความลับ (Non-Disclosure Agreement: NDA) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) หรือข้อกำหนดอื่นที่บริษัทฯ กำหนด
5) การสำรองและป้องกันข้อมูล (Data Backup and Protection) ผู้ใช้งานต้องหลีกเลี่ยงการจัดเก็บข้อมูลสำคัญไว้เฉพาะบนอุปกรณ์ส่วนบุคคลหรืออุปกรณ์ Local โดยไม่มีการสำรองข้อมูล และต้องปฏิบัติตามแนวทางการสำรองข้อมูลและการป้องกันข้อมูลที่บริษัทฯ กำหนด
6) การทำลายข้อมูล (Data Disposal) เมื่อข้อมูลหรือเอกสารไม่มีความจำเป็นต้องใช้งานอีกต่อไป ผู้ใช้งานต้องดำเนินการทำลายหรือส่งทำลายตามระดับการจำแนกประเภทข้อมูลและขั้นตอนที่บริษัทฯ กำหนด เช่น การใช้เครื่องทำลายเอกสาร (Shredder) สำหรับเอกสารที่มีข้อมูลลับ หรือการลบข้อมูลอิเล็กทรอนิกส์ด้วยวิธีที่เหมาะสม

5.8 การใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร (Use of Telephone, Facsimile, Printer, and Photocopier)

อุปกรณ์สื่อสารและอุปกรณ์สำนักงาน เช่น โทรศัพท์องค์กร โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร ถือเป็นทรัพย์สินของบริษัทฯ ที่จัดให้มีขึ้นเพื่อสนับสนุนการปฏิบัติงานและการดำเนินธุรกิจ โดยผู้ใช้งานต้องใช้งานอย่างเหมาะสม ระมัดระวัง และคำนึงถึงการรักษาความลับของข้อมูล โดยมีนโยบายและแนวปฏิบัติดังนี้

1) การใช้งานโทรศัพท์องค์กร (Corporate Telephone Use) ผู้ใช้งานต้องใช้โทรศัพท์องค์กรเพื่อวัตถุประสงค์ทางธุรกิจเป็นหลัก และต้องระมัดระวังการสนทนาข้อมูลลับหรือข้อมูลสำคัญในพื้นที่สาธารณะ รวมถึงต้องระวังการเปิดเผยข้อมูลแก่ผู้โทรที่ไม่สามารถยืนยันตัวตนได้ หรือมีลักษณะต้องสงสัยว่าเป็นการหลอกลวงทางสังคม (Social Engineering)
2) การใช้งานโทรสาร (Facsimile Use) การส่งเอกสารที่มีข้อมูลลับหรือข้อมูลสำคัญผ่านโทรสาร ต้องตรวจสอบความถูกต้องของหมายเลขปลายทางและผู้รับก่อนส่งทุกครั้ง หากมีช่องทางที่ปลอดภัยกว่า ควรเลือกใช้ช่องทางดังกล่าวแทนการส่งโทรสาร
3) การใช้งานเครื่องพิมพ์และเครื่องถ่ายเอกสาร (Printer and Photocopier Use) ผู้ใช้งานต้องรับเอกสารที่พิมพ์หรือถ่ายสำเนาออกจากเครื่องโดยเร็ว โดยเฉพาะเอกสารที่มีข้อมูลลับ ข้อมูลภายใน หรือข้อมูลส่วนบุคคล และห้ามทิ้งเอกสารสำคัญไว้บนถาดรับเอกสารหรือบริเวณเครื่องพิมพ์/เครื่องถ่ายเอกสาร
4) การจัดการเอกสารที่ไม่ใช้งานแล้ว (Document Disposal) เอกสารที่มีข้อมูลสำคัญ ข้อมูลลับ หรือข้อมูลส่วนบุคคล ซึ่งไม่มีความจำเป็นต้องใช้งานแล้ว ต้องนำไปทำลายด้วยวิธีที่เหมาะสม เช่น เครื่องทำลายเอกสาร (Shredder) และห้ามทิ้งในถังขยะทั่วไป
5) การใช้งานอย่างเหมาะสม (Appropriate Use) ห้ามใช้อุปกรณ์สื่อสารและอุปกรณ์สำนักงานของบริษัทฯ เพื่อวัตถุประสงค์ส่วนตัวในปริมาณมาก หรือในลักษณะที่ก่อให้เกิดความสิ้นเปลือง เสียหาย หรือกระทบต่อการใช้งานของบริษัทฯ

5.9 การรักษาความลับของสถานที่ตั้งและพื้นที่สำคัญด้านเทคโนโลยีสารสนเทศ (Confidentiality of IT Facility Locations and Critical Areas)

พื้นที่ที่เกี่ยวข้องกับระบบสารสนเทศสำคัญของบริษัทฯ เช่น ศูนย์ข้อมูล (Data Center) ห้องเซิร์ฟเวอร์ และพื้นที่ที่ใช้จัดเก็บหรือให้บริการระบบสำคัญ ถือเป็นพื้นที่ควบคุม (Controlled Area) ที่ต้องได้รับการป้องกันทั้งด้านกายภาพและด้านข้อมูล เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล และความเสี่ยงต่อความต่อเนื่องในการให้บริการระบบสารสนเทศ โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) ห้ามเปิดเผยข้อมูลเกี่ยวกับที่ตั้ง ผังพื้นที่ (Layout) โครงสร้างพื้นฐาน (Infrastructure) รายละเอียดระบบ หรือข้อมูลอื่นใดที่เกี่ยวข้องกับพื้นที่สำคัญด้านเทคโนโลยีสารสนเทศแก่บุคคลที่ไม่มีความจำเป็นต้องทราบ รวมถึงห้ามเผยแพร่ข้อมูลดังกล่าวผ่านสื่อสังคมออนไลน์หรือช่องทางสาธารณะอื่นใด
2) การเข้าถึงพื้นที่ควบคุมต้องได้รับอนุมัติจากผู้มีอำนาจหรือหน่วยงานที่รับผิดชอบ และต้องมีการบันทึกการเข้า-ออกทุกครั้ง กรณีบุคคลภายนอกเข้าพื้นที่ ต้องมีผู้รับผิดชอบของบริษัทฯ ดูแลตลอดเวลาที่อยู่ในพื้นที่ควบคุม
3) ห้ามถ่ายภาพ บันทึกวิดีโอ หรือบันทึกข้อมูลภายในพื้นที่ควบคุมโดยไม่ได้รับอนุญาตจากฝ่าย Digital Technology หรือผู้มีอำนาจที่เกี่ยวข้อง
4) การรายงานเหตุผิดปกติ (Suspicious Activity Reporting) ผู้ใช้งานต้องการรายงานเหตุผิดปกติทันที (Suspicious Activity Reporting) เมื่อพบเห็นบุคคลที่ไม่ได้รับอนุญาตในพื้นที่ควบคุม การพยายามเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต หรือพฤติกรรมที่น่าสงสัยที่อาจกระทบต่อความมั่นคงปลอดภัยของพื้นที่สำคัญด้านเทคโนโลยีสารสนเทศ ต่อฝ่าย Digital Technology หรือหน่วยงานที่บริษัทฯ กำหนด
5) เอกสาร แผนผัง รายละเอียดโครงสร้างพื้นฐาน และข้อมูลที่เกี่ยวข้องกับ Data Center ห้องเซิร์ฟเวอร์ หรือระบบสารสนเทศสำคัญ ต้องได้รับการจำแนกประเภทข้อมูลในระดับที่เหมาะสม และจัดเก็บในระบบหรือพื้นที่ที่มีการควบคุมสิทธิ์การเข้าถึง

5.10 การใช้งานพื้นที่จัดเก็บข้อมูลบนคลาวด์ (Cloud Storage Usage)

บริษัทฯ อนุญาตให้ใช้งานบริการจัดเก็บข้อมูลบนคลาวด์เฉพาะบริการที่บริษัทฯ จัดหาให้หรือได้รับอนุมัติจากบริษัทฯ เท่านั้น เช่น Google Drive ผ่านระบบ Google Workspace ของบริษัทฯ เพื่อให้การจัดเก็บ รับส่ง และแบ่งปันข้อมูลเป็นไปอย่างปลอดภัยและเหมาะสม โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) การใช้บริการคลาวด์ที่ได้รับอนุมัติ (Approved Cloud Storage Use) ผู้ใช้งานต้องจัดเก็บหรือถ่ายโอนข้อมูลของบริษัทฯ ผ่านบริการคลาวด์ที่บริษัทฯ อนุมัติเท่านั้น ห้ามใช้บริการคลาวด์ส่วนตัวหรือบริการที่ไม่ได้รับอนุมัติ เช่น คลาวด์บัญชีส่วนตัว, Dropbox, iCloud, WeTransfer หรือบริการอื่นใด ในการจัดเก็บหรือรับส่งข้อมูลของบริษัทฯ
2) การแชร์ข้อมูลบนคลาวด์ (Cloud Data Sharing) การแชร์ไฟล์หรือโฟลเดอร์กับบุคคลภายนอกต้องดำเนินการเฉพาะกรณีที่มีความจำเป็นทางธุรกิจ ได้รับอนุมัติจากผู้บังคับบัญชาหรือผู้มีอำนาจ และต้องกำหนดสิทธิ์การเข้าถึงให้เหมาะสม เช่น จำกัดเฉพาะผู้รับที่เกี่ยวข้อง กำหนดวันหมดอายุของลิงก์ หรือใช้มาตรการป้องกันเพิ่มเติมตามความเหมาะสม

3) การจัดเก็บข้อมูลลับบนคลาวด์ (Confidential Data on Cloud) ผู้ใช้งานต้องไม่อัปโหลดหรือจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงบนระบบคลาวด์โดยไม่มีมาตรการป้องกันที่เหมาะสม เช่น การจำกัดสิทธิ์การเข้าถึง การเข้ารหัสข้อมูล (Encryption) หรือมาตรการอื่นตามที่บริษัทฯ กำหนด
4) การตรวจสอบและควบคุมการใช้งาน (Cloud Usage Monitoring) บริษัทฯ สงวนสิทธิ์ในการตรวจสอบ ลบ ระงับ หรือจำกัดการเข้าถึงข้อมูลที่จัดเก็บบนระบบคลาวด์ของบริษัทฯ หากพบว่ามีการใช้งานที่ไม่เหมาะสม ฝ่าฝืนนโยบาย หรือก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

5.11 การใช้งานปัญญาประดิษฐ์และปัญญาประดิษฐ์เชิงสร้างสรรค์อย่างปลอดภัย (Safe Use of Artificial Intelligence and Generative AI)

บริษัทฯ ตระหนักถึงประโยชน์และความเสี่ยงจากการใช้งานปัญญาประดิษฐ์ (Artificial Intelligence: AI) และปัญญาประดิษฐ์เชิงสร้างสรรค์ (Generative AI) เช่น ChatGPT, Copilot, Gemini หรือเครื่องมือ AI อื่น ๆ จึงกำหนดแนวปฏิบัติเพื่อให้การใช้งานเป็นไปอย่างปลอดภัย รับผิดชอบ และสอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ รวมถึงข้อกำหนดที่เกี่ยวข้องในนโยบายเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย โดยมีนโยบายและแนวปฏิบัติ ดังนี้

1) ผู้ใช้งานต้องใช้เครื่องมือ AI ที่บริษัทฯ อนุมัติหรือกำหนดไว้เท่านั้น กรณีมีความจำเป็นต้องใช้เครื่องมือ AI ที่ยังไม่อยู่ในรายการเครื่องมือที่ได้รับอนุมัติ (Approved AI Tools List) ผู้ใช้งานต้องยื่นขออนุมัติจากผู้อำนวยการฝ่าย Digital Technology หรือผู้มีอำนาจที่บริษัทฯ กำหนดก่อนใช้งาน
2) ห้ามป้อน อัปโหลด หรือเปิดเผยข้อมูลที่เป็นความลับ ข้อมูลความลับสูงสุด ข้อมูลทางการเงิน ข้อมูลลูกค้า ข้อมูลโครงการที่ยังไม่เปิดเผย ข้อมูลส่วนบุคคล (Personal Data) หรือข้อมูลสำคัญของบริษัทฯ เข้าสู่เครื่องมือ AI ที่ให้บริการโดยบุคคลภายนอก เว้นแต่ได้รับอนุมัติและมีมาตรการคุ้มครองข้อมูลที่เหมาะสม
3) ผู้ใช้งานต้องตรวจสอบความถูกต้อง ความครบถ้วน ความเหมาะสม (AI Output Verification) และความน่าเชื่อถือของผลลัพธ์ที่ได้จาก AI ก่อนนำไปใช้งาน อ้างอิง เผยแพร่ หรือประกอบการตัดสินใจทางธุรกิจ ทั้งนี้ ผู้ใช้งานยังคงเป็นผู้รับผิดชอบต่อการนำผลลัพธ์ดังกล่าวไปใช้
4) การนำ AI ไปใช้ในกระบวนการทางธุรกิจที่สำคัญ (AI Use in Critical Processes) หรือกระบวนการที่อาจส่งผลกระทบต่อข้อมูลสำคัญ ลูกค้า การเงิน กฎหมาย การตัดสินใจเชิงธุรกิจ หรือชื่อเสียงของบริษัทฯ ต้องได้รับการพิจารณาและอนุมัติจากผู้อำนวยการฝ่าย Digital Technology หรือหน่วยงานที่บริษัทฯ กำหนดก่อนใช้งาน เพื่อประเมินความเสี่ยงและกำหนดมาตรการควบคุมที่เหมาะสม
5) ผู้ใช้งานต้องปฏิบัติตามกฎหมายลิขสิทธิ์ ทรัพย์สินทางปัญญา (Copyright and Intellectual Property) และข้อกำหนดการใช้งานของเครื่องมือ AI ที่เกี่ยวข้อง โดยต้องไม่คัดลอก เผยแพร่ หรือนำผลงานที่สร้างโดย AI ไปใช้ในลักษณะที่ละเมิดสิทธิของบุคคลอื่น หรือก่อให้เกิดความเข้าใจผิดว่าเป็นข้อมูลที่ผ่านการตรวจสอบจากบริษัทฯ แล้ว

6) การใช้งาน AI อย่างเหมาะสมและมีจริยธรรม (Responsible and Ethical AI Use) ห้ามใช้ AI เพื่อสร้าง เผยแพร่ หรือสนับสนุนเนื้อหาที่ผิดกฎหมาย หลอกลวง ปลอมแปลงตัวตน ละเมิดสิทธิของผู้อื่น สร้างความเสียหายต่อบริษัทฯ หรือบุคคลอื่น หรือขัดต่อจริยธรรม ความรับผิดชอบ และนโยบายของบริษัทฯ

5.12 การกระทำอื่นๆ ที่ถือเป็นข้อห้ามของบริษัท (Other Prohibited Activities)

นอกเหนือจากข้อห้ามและแนวปฏิบัติที่ระบุไว้ในแต่ละหัวข้อของนโยบายฉบับนี้ บริษัทฯ กำหนดให้การกระทำต่อไปนี้เป็นการใช้งานที่ไม่เหมาะสมและถือเป็นการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ โดยมีข้อห้าม ดังนี้

1) ห้ามผู้ใช้งานพยายามเข้าถึง แก้ไข ลบ ทำลาย หรือรบกวนการทำงานของข้อมูล ระบบสารสนเทศ เครือข่าย หรืออุปกรณ์ของบริษัทฯ โดยไม่ได้รับอนุญาต รวมถึงห้ามเจาะระบบ (Hacking) ทดสอบช่องโหว่ (Vulnerability Scanning) ดักจับข้อมูล (Packet Sniffing) ติดตั้งหรือเผยแพร่มัลแวร์ ไวรัส สปายแวร์ หรือซอฟต์แวร์อันตรายใด ๆ เว้นแต่เป็นการดำเนินงานที่ได้รับมอบหมายและอนุมัติอย่างเป็นทางการ
2) ห้ามผู้ใช้งานเปิดเผย แบ่งปัน หรือส่งต่อบัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลสำหรับการพิสูจน์ตัวตนให้แก่ผู้อื่น รวมถึงห้ามใช้บัญชีของผู้อื่น หรือแอบอ้างสิทธิ์การเข้าถึงระบบ ข้อมูล หรือทรัพย์สินสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาต
3) ห้ามขโมย คัดลอก โอนย้าย เปิดเผย เผยแพร่ หรือนำข้อมูลทางธุรกิจ ข้อมูลลูกค้า ข้อมูลส่วนบุคคล ทรัพย์สินทางปัญญา หรือทรัพย์สินสารสนเทศของบริษัทฯ ออกนอกองค์กร หรือมอบให้แก่คู่แข่ง บุคคลภายนอก หรือสาธารณะโดยไม่ได้รับอนุญาต รวมถึงห้ามนำข้อมูลดังกล่าวไปใช้เพื่อประโยชน์ส่วนตัวหรือประโยชน์ของบุคคลอื่น
4) ห้ามใช้ระบบสารสนเทศ อีเมล เครือข่าย หรือช่องทางสื่อสารของบริษัทฯ เพื่อสร้าง ส่งต่อ เผยแพร่ หรือสนับสนุนเนื้อหาที่ผิดกฎหมาย หมิ่นประมาท เลือกปฏิบัติ คุกคาม ลามกอนาจาร หลอกลวง ข่มขู่ หรือก่อให้เกิดความเดือดร้อน เสียหาย หรือกระทบต่อชื่อเสียงของบริษัทฯ บุคคลอื่น หรือหน่วยงานที่เกี่ยวข้อง
5) ห้ามใช้ทรัพยากร ระบบสารสนเทศ เครือข่าย หรืออุปกรณ์ของบริษัทฯ เพื่อดำเนินกิจกรรมที่ผิดกฎหมาย หรือขัดต่อกฎระเบียบและนโยบายของบริษัทฯ รวมถึงการกระทำที่อาจเป็นการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กฎหมายลิขสิทธิ์ และกฎหมายอื่นที่เกี่ยวข้อง
6) ห้ามใช้ทรัพยากรคอมพิวเตอร์ เครือข่าย หรืออุปกรณ์ของบริษัทฯ เพื่อการขุดสกุลเงินดิจิทัล (Cryptocurrency Mining) การให้บริการส่วนตัว การประมวลผลที่ไม่เกี่ยวข้องกับงาน หรือกิจกรรมใด ๆ ที่ใช้ทรัพยากรของบริษัทฯ อย่างผิดปกติ สิ้นเปลือง หรือส่งผลกระทบต่อประสิทธิภาพ ความมั่นคงปลอดภัย หรือความพร้อมใช้งานของระบบ
7) ห้ามกระทำการใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อชื่อเสียง ทรัพย์สิน ข้อมูล ระบบสารสนเทศ ความมั่นคงปลอดภัย การดำเนินธุรกิจ หรือผลประโยชน์โดยชอบของบริษัทฯ ไม่ว่าทางตรงหรือทางอ้อม

6. การดำเนินการกรณีไม่ปฏิบัติตามนโยบายและแนวปฏิบัติ (Non-Compliance Actions)

ผู้ใดฝ่าฝืน ไม่ปฏิบัติตาม หรือปฏิบัติไม่สอดคล้องกับนโยบายการใช้งานที่ยอมรับได้ฉบับนี้ ไม่ว่าทั้งโดยเจตนาหรือประมาทเลินเล่อ อาจได้รับการพิจารณาดำเนินการทางวินัยตามระเบียบ ข้อบังคับ และแนวปฏิบัติของบริษัทฯ ตามระดับความร้ายแรงของการกระทำ ทั้งนี้ หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อข้อมูล ระบบสารสนเทศ ชื่อเสียง หรือผลประโยชน์ของบริษัทฯ ลูกค้า หรือผู้มีส่วนได้เสีย บริษัทฯ อาจพิจารณาดำเนินการตามกฎหมายที่เกี่ยวข้อง รวมถึงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม พ.ศ. 2560 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) กฎหมายหลักทรัพย์และตลาดหลักทรัพย์ภายใต้การกำกับดูแลของ ก.ล.ต. และ ตลท. ตลอดจนกฎหมายอื่นที่เกี่ยวข้อง และอาจเรียกร้องค่าเสียหายตามสมควรอีกด้วย