สารบัญและประวัติการแก้ไข

หน้า	รายละเอียด	ปรับปรุงครั้งที่	อ้างอิง
1	หน้าปก	00	-
2	วัตถุประสงค์	00	-
	ขั้นตอนการปฏิบัติงาน	00	-

ผู้จัดทำ	ผู้สอบทาน	ผู้อนุมัติ
.....	.....	.....
(นายอิทธิฤทธิ์ โฆษิอาภานันท์)	(นายวุฒิชัย สุริยวรวงศ์)	(ดร.สันติสุข โฆษิอาภานันท์)
ผู้ช่วยผู้จัดการแผนกเทคโนโลยีสารสนเทศ	ผู้จัดการทั่วไป	กรรมการผู้จัดการ
07/07/2569	07/07/2569	07/07/2569

นโยบายเทคโนโลยีสารสนเทศ
(Information Technology Policy)

หมวดที่ 1 บททั่วไปและกรอบการกำกับดูแล

1.1 วัตถุประสงค์

นโยบายฉบับนี้กำหนดหลักการและเจตจำนงของกลุ่มบริษัทโซนิคในการบริหารจัดการและใช้งานเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยน่าเชื่อถือเป็นไปตามกฎหมายและสนับสนุนการดำเนินธุรกิจอย่างต่อเนื่อง โดยครอบคลุมการคุ้มครองข้อมูล การเข้าถึงระบบ การดูแลโครงสร้างพื้นฐาน การบริหารการเปลี่ยนแปลง และ เหตุการณ์ การใช้งานทรัพยากรและสินทรัพย์ การใช้ปัญญาประดิษฐ์ และการบริหารผู้ให้บริการภายนอกและ การจัดซื้อจัดจ้าง

1.2 ขอบเขตการบังคับใช้

นโยบายฉบับนี้บังคับใช้ร่วมกันทั้งบริษัทในกลุ่มโซนิคทั้งหมด ได้แก่ บริษัท โซนิค อินเตอร์เฟรท จำกัด (มหาชน) และ บริษัท แกรนด์ลิงค์ ลอจิสติคส์ จำกัด และ บริษัท โซนิค ออโตโลจิส จำกัด และบังคับใช้กับพนักงานทุกระดับ กรรมการ ผู้รับเหมา ที่ปรึกษา ผู้ให้บริการภายนอก และบุคคลภายนอกทุกรายที่ได้รับสิทธิ์เข้าถึงระบบ ข้อมูล หรือทรัพยากรสารสนเทศของกลุ่มบริษัทครอบคลุมข้อมูลทุกรูปแบบ อุปกรณ์และระบบสารสนเทศทั้งหมดที่กลุ่มบริษัทเป็นเจ้าของหรือใช้งาน ทั้งภายในองค์กร ระบบคลาวด์ และอุปกรณ์ส่วนบุคคลที่นำมาใช้ในเครือข่ายบริษัท (BYOD)

1.3 หลักการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ

การบริหารจัดการเทคโนโลยีสารสนเทศทั้งหมดของกลุ่มบริษัทยึดหลักการพื้นฐานต่อไปนี้

- รักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล (Confidentiality, Integrity, Availability)
- ให้สิทธิ์เท่าที่จำเป็น (Least Privilege) และจำกัดการเข้าถึงข้อมูลเท่าที่จำเป็นต่อหน้าที่ (Need-to-Know)
- แยกหน้าที่การอนุมัติ การปฏิบัติ และการตรวจสอบออกจากกัน (Segregation of Duties)
- ป้องกันแบบหลายชั้น (Defense in Depth) และปฏิเสธการเข้าถึงเป็นค่าตั้งต้น (Default Deny)
- ตรวจสอบทุกการเข้าถึงโดยไม่เชื่อถือโดยปริยาย (Zero Trust)
- เก็บและใช้ข้อมูลเท่าที่จำเป็น (Data Minimisation) และออกแบบเพื่อความเป็นส่วนตัวและความปลอดภัยตั้งแต่ต้น (Privacy & Security by Design)
- ให้มนุษย์กำกับดูแลการตัดสินใจที่สำคัญเสมอ (Human Oversight)
- ปฏิบัติตามกฎหมาย มาตรฐาน และจริยธรรมที่เกี่ยวข้อง (Compliance)

1.4 ลักษณะของเอกสาร

นโยบายฉบับนี้เป็นกรอบและหลักการที่ผู้บริหารของกลุ่มบริษัทโซนิคกำหนดให้บุคลากรและผู้เกี่ยวข้องทุกฝ่ายต้องปฏิบัติตาม ส่วนวิธีปฏิบัติ ขั้นตอน เกณฑ์เชิงตัวเลข กรอบเวลา และเครื่องมือ ให้ฝ่ายเทคโนโลยีสารสนเทศ ร่วมกับหน่วยงานที่เกี่ยวข้อง จัดทำเป็นระเบียบปฏิบัติและแบบฟอร์มแยกต่างหาก เพื่อสนับสนุนการปฏิบัติตามนโยบาย โดยให้ผู้จัดการแผนก IT เป็นผู้รับผิดชอบในการอนุมัติและทบทวนระเบียบปฏิบัติดังกล่าว

หมวดที่ 2 การคุ้มครองข้อมูลและความเป็นส่วนตัว

2.1 การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

กลุ่มบริษัทเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคล และต้องประมวลผลข้อมูลส่วนบุคคล ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และกฎหมายที่เกี่ยวข้อง โดยยึดหลักการต่อไปนี้

- กลุ่มบริษัทต้องประมวลผลข้อมูลส่วนบุคคลโดยมีฐานทางกฎหมายรองรับ และเพื่อวัตถุประสงค์ที่ชัดเจน และชอบด้วยกฎหมาย
- ผู้ประมวลผลต้องเก็บรวบรวมและใช้ข้อมูลเท่าที่จำเป็น ให้ถูกต้องเป็นปัจจุบัน และเก็บรักษาเฉพาะระยะเวลาที่จำเป็น
- ฝ่าย IT ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยสอดคล้องกับระดับความเสี่ยงที่ประเมิน
- ผู้ประมวลผลต้องแจ้งวัตถุประสงค์และให้ความโปร่งใสในการประมวลผลข้อมูลต่อเจ้าของข้อมูล
- กลุ่มบริษัทต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ให้กำกับดูแลการปฏิบัติตามกฎหมาย
- พนักงานที่เกี่ยวข้องต้องผ่านการอบรม และต้องรักษาความลับของข้อมูลส่วนบุคคลแม้พ้นสภาพการจ้างแล้ว
- ผู้ประมวลผลต้องจัดให้การส่งหรือโอนข้อมูลไปต่างประเทศมีมาตรการคุ้มครองตามที่กฎหมายกำหนด

2.2 สิทธิของเจ้าของข้อมูลและการรับมือเหตุละเมิดข้อมูล

กลุ่มบริษัทต้องเคารพและอำนวยความสะดวกให้เจ้าของข้อมูลใช้สิทธิตามกฎหมาย ได้แก่ สิทธิได้รับแจ้ง เข้าถึง แก้ไข ลบ ระงับการใช้ คัดค้าน โอนย้ายข้อมูล และถอนความยินยอม DPO ต้องดำเนินการตามคำร้องภายในกรอบเวลาที่กฎหมายกำหนด

กรณีเกิดหรือสงสัยว่าเกิดเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach) ผู้พบเหตุต้องรายงานต่อ DPO และฝ่าย IT โดยทันที จากนั้น DPO และฝ่าย IT ต้องควบคุมความเสียหาย ตรวจสอบสาเหตุ แจ้งหน่วยงานกำกับดูแลและเจ้าของข้อมูลที่ได้รับผลกระทบภายในกรอบเวลาที่กฎหมายกำหนด ฟื้นฟูระบบ และบันทึกเหตุการณ์ในทะเบียนการละเมิดข้อมูล (Data Breach Register)

2.3 การจัดชั้นข้อมูล (Data Classification)

ข้อมูลของกลุ่มบริษัทต้องได้รับการจัดชั้นตามระดับความลับและผลกระทบหากรั่วไหล
เพื่อกำหนดมาตรการคุ้มครองให้สมเหตุสมผลกับความสำคัญของข้อมูล โดยแบ่งเป็น 4 ระดับ

ระดับชั้นข้อมูล	ความหมายโดยสังเขป
Public	ข้อมูลที่เปิดเผยต่อสาธารณะได้
Internal	ข้อมูลภายในสำหรับใช้ในการปฏิบัติงาน
Confidential	ข้อมูลลับที่หากรั่วไหลจะกระทบต่อกลุ่มบริษัท
Restricted	ข้อมูลลับมาก/อ่อนไหว ที่หากรั่วไหลจะกระทบรุนแรง

- เจ้าของข้อมูล (Data Owner) ต้องเป็นผู้กำหนดระดับชั้นและอนุมัติสิทธิ์การเข้าถึง
- ผู้สร้างหรือครอบครองข้อมูลต้องทำเครื่องหมายระบุระดับชั้นสำหรับข้อมูล Confidential และ Restricted ทุกครั้ง

- ฝ่าย IT ต้องกำหนดมาตรการจัดเก็บ ส่งต่อ เข้ารหัส และควบคุมการเข้าถึงให้เข้มงวดตามระดับชั้นข้อมูล
- ผู้ทำลายข้อมูลต้องใช้วิธีที่ปลอดภัยตามระดับชั้น และต้องจัดทำหลักฐานการทำลาย

2.4 การเฝ้าระวังด้วยกล้องโทรทัศน์วงจรปิด (CCTV)

- ฝ่าย IT และฝ่ายรักษาความปลอดภัยต้องติดตั้งกล้องเฉพาะพื้นที่ที่มีเหตุผลอันชอบธรรม และห้ามติดตั้งในพื้นที่ที่ละเมิดความเป็นส่วนตัว
- ผู้ดูแลกล้องต้องติดป้ายแจ้งการใช้กล้องวงจรปิดพร้อมช่องทางติดต่อ DPO ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด
- ผู้ดูแลกล้องต้องจำกัดสิทธิ์การเข้าถึงภาพ บันทึกการเข้าถึง และเก็บรักษาภาพตามระยะเวลาที่กฎหมายกำหนด

หมวดที่ 3 การควบคุมการเข้าถึงและการพิสูจน์ตัวตน

3.1 การบริหารบัญชีและสิทธิ์การเข้าถึง

- ฝ่าย IT ต้องสร้าง เปลี่ยนแปลง หรือยกเลิกบัญชีเฉพาะเมื่อได้รับอนุมัติเป็นลายลักษณ์อักษร และต้องเก็บหลักฐานทุกครั้ง
- ฝ่าย IT ต้องให้สิทธิ์ตามหลัก Least Privilege และ Need-to-Know และต้องกำหนดสิทธิ์ตามบทบาทหน้าที่ (RBAC)
- ผู้ใช้ต้องไม่ใช้บัญชีร่วมกัน (Shared Account) เว้นแต่ได้รับอนุมัติเป็นกรณีพิเศษและมีการบันทึกการใช้งาน
- ฝ่าย IT ต้องเพิกถอนหรือระงับสิทธิ์โดยทันทีเมื่อพนักงานพ้นสภาพ เปลี่ยนหน้าที่ หรือหมดความจำเป็น
- ฝ่าย IT ต้องทบทวนสิทธิ์การเข้าถึงเป็นรอบ โดยเฉพาะบัญชีสิทธิ์สูงและบัญชีบุคคลภายนอก

3.2 การพิสูจน์ตัวตน (Authentication)

- ผู้ใช้ต้องตั้งรหัสผ่านหรือข้อมูลยืนยันตัวตนให้เข้มแข็งตามมาตรฐานที่ฝ่าย IT กำหนด
- ฝ่าย IT ต้องบังคับใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) สำหรับการเข้าถึงที่มีความเสี่ยงสูง เช่น การเข้าถึงจากภายนอก บัญชีสิทธิ์สูง ระบบคลาวด์ และระบบที่เก็บข้อมูลสำคัญ
- ผู้ใช้ต้องไม่ใช้รหัสผ่านซ้ำกับระบบภายนอก ห้ามเปิดเผยหรือแบ่งปันรหัสผ่าน และต้องใช้เครื่องมือจัดเก็บรหัสผ่านที่ฝ่าย IT อนุมัติ
- กรณีระบบไม่รองรับ MFA ฝ่าย IT ต้องจัดให้มีมาตรการชดเชย (Compensating Controls) บันทึกในทะเบียนข้อยกเว้นและต้องมีแผนปรับปรุง

3.3 การจัดการสิทธิ์ระดับสูง (Privileged Access)

- ผู้ดูแลระบบต้องไม่ใช้บัญชีผู้ดูแลระบบ (Administrator/Root) ในงานประจำวัน ให้ยกระดับสิทธิ์เฉพาะเมื่อจำเป็น
- ฝ่าย IT ต้องบันทึกการใช้งานสิทธิ์ระดับสูง (Logging) ทุกครั้ง
- ฝ่าย IT ต้องใช้หลักการให้สิทธิ์เฉพาะช่วงเวลาที่จำเป็น (Just-in-Time) และต้องพิจารณาใช้ระบบควบคุมสิทธิ์สูง (PAM) สำหรับระบบที่จำเป็น

3.4 การเข้าถึงจากภายนอก (Remote Access)

- ผู้ใช้ต้องเข้าถึงระบบจากภายนอกผ่านช่องทางที่ฝ่าย IT รับรองเท่านั้น (เช่น VPN หรือ Bastion Host) และต้องเปิด MFA
- ผู้ขอต้องยื่นคำขอโดยระบุเหตุผล ขอบเขต และระยะเวลา และฝ่าย IT ต้องกำหนดวันหมดอายุของสิทธิ์
- ฝ่าย IT ต้องบันทึกการเข้าถึง และผู้ใช้ต้องใช้อุปกรณ์ที่มีการป้องกันตามมาตรฐานที่ฝ่าย IT กำหนด

หมวดที่ 4 ความมั่นคงปลอดภัยของระบบและโครงสร้างพื้นฐาน

4.1 การป้องกันมัลแวร์และอุปกรณ์ปลายทาง

- ผู้ใช้ต้องติดตั้งซอฟต์แวร์ป้องกันมัลแวร์/EDR ที่ฝ่าย IT รับรอง บนอุปกรณ์ทุกเครื่องที่เชื่อมต่อเครือข่ายบริษัท
- ผู้ใช้ต้องอัปเดตระบบและซอฟต์แวร์ความปลอดภัยตามที่ฝ่าย IT กำหนด และห้ามปิดการอัปเดตหรือการป้องกันโดยไม่ได้รับอนุญาต
- ผู้ใช้ต้องระมัดระวังอีเมลและลิงก์ที่น่าสงสัย และต้องรายงานเหตุที่สงสัยว่าถูกโจมตีต่อฝ่าย IT โดยทันที

4.2 ความปลอดภัยเครือข่าย

- ฝ่าย IT ต้องจัดแบ่งเครือข่ายเป็นส่วน (Network Segmentation) เพื่อจำกัดผลกระทบเมื่อเกิดเหตุ
- ฝ่าย IT ต้องตั้งค่าอุปกรณ์ควบคุมเครือข่าย (Firewall/UTM) ให้ปฏิเสธการเข้าถึงเป็นค่าตั้งต้น (Default Deny) และต้องเปิดใช้ฟังก์ชันป้องกันภัยตามมาตรฐาน
- ฝ่าย IT ต้องกำหนดให้เครือข่ายไร้สายมีการยืนยันตัวตนและการเข้ารหัสตามมาตรฐาน และต้องแยกเครือข่ายผู้มาติดต่อออกจากเครือข่ายภายใน
- ฝ่าย IT ต้องส่งการเปลี่ยนแปลงกฎเครือข่ายเข้ากระบวนการบริหารการเปลี่ยนแปลง (หมวดที่ 5) และต้องบันทึกและทบทวนเป็นรอบ

4.3 การบริหารจัดการเซิร์ฟเวอร์และโครงสร้างพื้นฐาน

- ฝ่าย IT ต้องตั้งค่าเซิร์ฟเวอร์และระบบทุกประเภทให้ปลอดภัย และต้องเปลี่ยนค่าตั้งต้นก่อนใช้งานจริง
- ฝ่าย IT ต้องติดตั้งแพตช์และอัปเดตความปลอดภัยตามระดับความเร่งด่วนของช่องโหว่ โดยต้องทดสอบก่อนและต้องมีแผนย้อนกลับ
- ฝ่าย IT ต้องจำกัดการเข้าถึงและแก้ไขระบบและฐานข้อมูลที่ใช้งานจริง (Production) เฉพาะผู้ได้รับอนุมัติและต้องผ่านกระบวนการตามหมวดที่ 5
- ฝ่าย IT ต้องควบคุมความปลอดภัยและการบริหารทรัพยากรของระบบเสมือน (Virtualization) และคอนเทนเนอร์ตามมาตรฐาน
- ฝ่าย IT ต้องได้รับอนุมัติก่อนเลิกใช้งานระบบ ต้องสำรองข้อมูลที่จำเป็น และต้องลบข้อมูลอย่างปลอดภัยก่อนจำหน่ายหรือทำลาย

4.4 การสำรองและกู้คืนข้อมูล

- ฝ่าย IT ต้องสำรองข้อมูลและระบบสำคัญตามหลัก 3-2-1 (สำเนาหลายชุด สื่อหลายประเภท เก็บนอกสถานที่ 1 ชุด)

- ฝ่าย IT ต้องเข้ารหัสข้อมูลสำรอง และต้องจัดให้มีมาตรการป้องกันการถูกเข้ารหัสเรียกค่าไถ่ (เช่น Immutable/Air-Gap Storage)
- เจ้าของระบบและฝ่าย IT ต้องกำหนดเป้าหมายการกู้คืน (RTO/RPO) ให้สอดคล้องกับความสำคัญทางธุรกิจของระบบ
- ฝ่าย IT ต้องทดสอบการกู้คืนข้อมูลเป็นรอบ และต้องบันทึกผล เพื่อยืนยันว่ากู้คืนได้จริง

4.5 การบันทึกและเฝ้าระวังเหตุการณ์ (Logging & Monitoring)

- ฝ่าย IT ต้องกำหนดให้ระบบสำคัญบันทึกเหตุการณ์ (Log) การเข้าถึงและการเปลี่ยนแปลง และส่งเข้าระบบจัดเก็บ Log
- ฝ่าย IT ต้องป้องกัน Log จากการแก้ไข/ลบ และต้องเก็บรักษาตามระยะเวลาที่กฎหมายกำหนด
- ฝ่าย IT ต้องเฝ้าระวังและแจ้งเตือนเหตุการณ์สำคัญ กรณีเกินขีดความสามารถของทีม ต้องใช้บริการภายนอก (Managed Service) แทนการละเลย

4.6 ความปลอดภัยทางกายภาพและสภาพแวดล้อม

- ฝ่าย IT ต้องควบคุมการเข้าถึงห้องศูนย์ข้อมูล/ห้องเครือข่าย ให้ได้รับอนุมัติ มีการบันทึกการเข้า-ออก และควบคุมบุคคลภายนอก
- ฝ่าย IT ต้องจัดให้พื้นที่สำคัญมีมาตรการป้องกันทางกายภาพ เช่น ระบบดับเพลิง ไฟสำรอง การควบคุมสภาพแวดล้อม และการป้องกันการลักลอบตามเข้า (Tailgating)

4.7 ความต่อเนื่องทางธุรกิจและการกู้คืนระบบ (BCP/DR)

- ฝ่าย IT ต้องจัดทำการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) เพื่อจัดลำดับความสำคัญของระบบและกำหนดเป้าหมาย RTO/RPO ให้สอดคล้องกับธุรกิจ
- ฝ่าย IT ต้องจัดทำและทบทวนแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบ (BCP/DR) สำหรับระบบสำคัญโดยอ้างอิงเป้าหมาย RTO/RPO ในข้อ 4.4
- ฝ่าย IT ต้องจัดให้มีสำเนาข้อมูลสำรองและขั้นตอนกู้คืน ณ สถานที่สำรอง และต้องฝึกซ้อมกู้คืนระบบเป็นระยะเพื่อยืนยันว่าระบบสำคัญกลับมาทำงานได้ภายในเป้าหมาย

4.8 การเข้ารหัสข้อมูลและการบริหารกุญแจเข้ารหัส (Cryptography & Key Management)

- ฝ่าย IT ต้องกำหนดมาตรฐานการเข้ารหัสข้อมูล (Encryption Standard) ที่ใช้ทั่วทั้งกลุ่มบริษัท โดยอ้างอิงอัลกอริทึมที่เป็นที่ยอมรับในปัจจุบันและมีความแข็งแรงเพียงพอ และต้องทบทวนมาตรฐานดังกล่าวเป็นระยะให้ทันต่อภัยคุกคาม
- ฝ่าย IT ต้องเข้ารหัสข้อมูลที่จัดชั้น Confidential และ Restricted ทั้งขณะจัดเก็บ (Data at Rest) และขณะส่งผ่านเครือข่าย (Data in Transit)
- ฝ่าย IT ต้องบริหารวงจรชีวิตของกุญแจเข้ารหัส (Key Management) ครอบคลุมการสร้าง จัดเก็บ ใช้งาน หมุนเวียน (Rotation) เพิกถอน และทำลายกุญแจ โดยจำกัดสิทธิ์การเข้าถึงกุญแจเฉพาะผู้ที่ได้รับอนุมัติ

- ฝ่าย IT ต้องไม่จัดเก็บกุญแจเข้ารหัสรวมไว้กับข้อมูลที่ถูกเข้ารหัส และต้องพิจารณาใช้อุปกรณ์หรือบริการบริหารกุญแจโดยเฉพาะ (HSM/KMS) สำหรับระบบที่มีความเสี่ยงสูง
- ผู้พัฒนาระบบต้องไม่ฝังกุญแจเข้ารหัสหรือข้อมูลลับ (Credentials) ไว้ในซอร์สโค้ดหรือไฟล์ตั้งค่าที่ไม่มีการควบคุมการเข้าถึง

4.9 ความปลอดภัยของบริการคลาวด์ (Cloud Security)

- ฝ่าย IT ต้องนำหลักการบริหารผู้ให้บริการภายนอกในหมวดที่ 8 และหลักการคุ้มครองข้อมูลข้ามพรมแดนในหมวดที่ 2 มาใช้กับบริการคลาวด์ทุกประเภท และต้องกำหนดมาตรการเพิ่มเติมเฉพาะสำหรับบริการคลาวด์ดังนี้
- ฝ่าย IT ต้องกำหนดขอบเขตความรับผิดชอบระหว่างกลุ่มบริษัทและผู้ให้บริการคลาวด์ให้ชัดเจนตามรูปแบบบริการ (IaaS/PaaS/SaaS) (Shared Responsibility Model) และต้องสื่อสารให้ผู้เกี่ยวข้องทราบ
- ฝ่าย IT ต้องควบคุมการตั้งค่าบริการคลาวด์ให้ปลอดภัยตามมาตรฐาน (Secure Configuration) และต้องตรวจสอบการตั้งค่าที่เปิดเผยต่อสาธารณะโดยไม่ได้ตั้งใจ (Misconfiguration) เป็นระยะ
- ฝ่าย IT ต้องจัดให้มีแผนสำรองข้อมูลและแผนถอนตัวออกจากผู้ให้บริการ (Exit Strategy) สำหรับบริการคลาวด์ที่จัดเก็บข้อมูลหรือระบบสำคัญ เพื่อป้องกันการผูกติดกับผู้ให้บริการรายเดียว (Vendor Lock-in)

หมวดที่ 5 การบริหารการเปลี่ยนแปลงและการจัดการเหตุการณ์

5.1 การบริหารการเปลี่ยนแปลง (Change Management)

ฝ่าย IT ต้องส่งการเปลี่ยนแปลงระบบที่ใช้งานจริง (Production) เข้ากระบวนการประเมินผลกระทบ การอนุมัติ การทดสอบ และการบันทึก เพื่อลดความเสี่ยงต่อความพร้อมใช้งานและความมั่นคงปลอดภัย
โดยจำแนกประเภทการเปลี่ยนแปลงและระดับการอนุมัติตามความเสี่ยง

- ฝ่าย IT ต้องกำหนดการเปลี่ยนแปลงมาตรฐาน (Standard) ที่ความเสี่ยงต่ำ ให้อนุมัติล่วงหน้าเป็นรายการ
- การเปลี่ยนแปลงปกติ (Normal) ต้องผ่านการพิจารณาของผู้บริหาร
- การเปลี่ยนแปลงฉุกเฉิน (Emergency) ผู้จัดการ IT ต้องอนุมัติเร่งด่วนได้ และต้องรายงานย้อนหลัง
- ผู้ขอเปลี่ยนแปลงต้องจัดทำแผนทดสอบและแผนย้อนกลับ (Rollback) และฝ่าย IT ต้องดำเนินการในช่วงเวลาที่กำหนด
- ผู้ใช้และฝ่าย IT ต้องไม่เปลี่ยนแปลงระบบที่ใช้งานจริงโดยไม่ผ่านกระบวนการที่กำหนด (Unauthorized Change)

5.2 การจัดการเหตุการณ์ (Incident Management)

- พนักงานทุกคนต้องรายงานเหตุการณ์ผิดปกติด้านสารสนเทศต่อฝ่าย IT โดยทันที ตามช่องทางที่ฝ่าย IT กำหนด
- ฝ่าย IT ต้องจัดระดับความรุนแรงของเหตุการณ์ตามผลกระทบ และต้องตอบสนองตามลำดับความสำคัญ

ฝ่าย IT ต้องดำเนินการตามวงจรจัดการเหตุการณ์ ดังนี้

1. ตรวจพบ (Detect)
2. ประเมินเบื้องต้น (Triage)
3. จำกัดขอบเขต (Contain)
4. ขจัดต้นเหตุ (Eradicate)
5. กู้คืนระบบ (Recover)
6. ทบทวนหลังเหตุการณ์ (Post-Incident Review)

- ผู้จัดการ IT ต้องจัดให้มีทีมตอบสนองเหตุการณ์ (IRT) และแนวทางการสื่อสารที่ชัดเจน โดยการให้ข่าวต่อสาธารณะต้องผ่านผู้รับผิดชอบด้านการสื่อสารเท่านั้น
- เหตุการณ์ที่เป็นการละเมิดข้อมูลส่วนบุคคลต้องดำเนินการตามหลักการในหมวดที่ 2
- ฝ่าย IT ต้องจัดการฝึกซ้อมรับมือเหตุการณ์และปรับปรุงแนวทางปฏิบัติเป็นระยะ

หมวดที่ 6 การใช้งานที่เหมาะสมและการบริหารสินทรัพย์

6.1 การใช้งานทรัพยากรสารสนเทศอย่างเหมาะสม (Acceptable Use)

- ผู้ใช้ต้องใช้ทรัพยากรสารสนเทศเพื่อวัตถุประสงค์ทางธุรกิจเป็นหลัก และต้องดูแลรักษาให้อยู่ในสภาพที่ใช้งานได้
- ผู้ใช้ต้องไม่ใช้งานที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ ขัดต่อศีลธรรม หรือหลบเลี่ยงระบบความปลอดภัยของบริษัท
- ผู้ใช้ต้องไม่นำข้อมูลบริษัทออกผ่านช่องทางส่วนบุคคล เช่น อีเมลหรือที่เก็บข้อมูลบนคลาวด์ส่วนตัวที่ไม่ได้รับอนุมัติ
- ผู้ใช้ต้องใช้อีเมล อินเทอร์เน็ต สื่อบันทึกพกพา อุปกรณ์ส่วนบุคคล (BYOD) และเครือข่ายไร้สาย ตามมาตรฐานที่ฝ่าย IT กำหนด
- กลุ่มบริษัทสงวนสิทธิ์ในการตรวจสอบและบันทึกการใช้งานเพื่อความมั่นคงปลอดภัยและการกำกับดูแลภายใต้ขอบเขตที่กฎหมายอนุญาต
- พนักงานต้องลงนามรับทราบและปฏิบัติตามนโยบาย และต้องเข้ารับการอบรมตามที่กำหนด

6.2 การบริหารสินทรัพย์สารสนเทศ (IT Asset Management)

- ฝ่าย IT ต้องลงทะเบียนสินทรัพย์สารสนเทศทุกรายการในทะเบียนสินทรัพย์ พร้อมระบุผู้รับผิดชอบและสถานะ
- ฝ่าย IT และผู้รับมอบต้องบริหารสินทรัพย์ตลอดวงจรชีวิต ตั้งแต่จัดหา รับมอบ ใช้งาน บำรุงรักษา จนถึงเลิกใช้ พร้อมหลักฐานการรับมอบและส่งคืน
- ผู้ใช้ต้องใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องเท่านั้น และฝ่าย IT ต้องบริหารลิขสิทธิ์ให้สอดคล้องกับที่ครอบครอง
- ผู้ใช้ต้องเปิดการเข้ารหัสและการลบข้อมูลระยะไกลบนอุปกรณ์เคลื่อนที่ของบริษัท และต้องรายงานฝ่าย IT ทันทีเมื่อสูญหาย
- ฝ่าย IT ต้องทำลายข้อมูลในสินทรัพย์ที่เลิกใช้อย่างปลอดภัยตามระดับชั้นข้อมูล และต้องจัดทำหลักฐานการทำลาย
- ฝ่าย IT ต้องตรวจนับสินทรัพย์เป็นรอบ และต้องรายงานผลต่อผู้บริหาร

หมวดที่ 7 การใช้งานปัญญาประดิษฐ์อย่างรับผิดชอบ

7.1 หลักการใช้งานปัญญาประดิษฐ์ (AI)

กลุ่มบริษัทส่งเสริมการใช้เครื่องมือปัญญาประดิษฐ์อย่างมีประสิทธิภาพ มีจริยธรรม และปลอดภัย ภายใต้หลักการต่อไปนี้

- ผู้ใช้ต้องให้มนุษย์ตรวจสอบผลลัพธ์ของ AI ก่อนนำไปใช้เสมอ (Human-in-the-Loop)
- ผู้ใช้ต้องไม่ป้อนข้อมูลส่วนบุคคลและข้อมูลลับลงในเครื่องมือ AI สาธารณะ (Data Protection)
- ผู้ใช้ต้องเปิดเผยการใช้ AI ในเนื้อหาที่สื่อสารภายนอก เมื่อเหมาะสม (Transparency)
- ผู้ใช้ต้องรับผิดชอบต่อผลลัพธ์ของ AI ที่นำไปใช้ (Accountability)
- ผู้ใช้ต้องปฏิบัติตามกฎหมาย ลิขสิทธิ์ และมาตรฐานจริยธรรม (Compliance)

7.2 การจัดประเภทเครื่องมือ AI และการควบคุมข้อมูล

- ฝ่าย IT ต้องจัดประเภทเครื่องมือ AI ตามคุณลักษณะและเงื่อนไขบริการ (ไม่ใช่ตามชื่อผู้ให้บริการ) เป็นระดับ อนุมัติให้ใช้ (Approved) ใช้ได้แบบจำกัด (Restricted) และห้ามใช้ (Prohibited)
- ผู้ขอต้องส่งเครื่องมือ AI ใหม่เข้าประเมินความเสี่ยงและต้องได้รับอนุมัติจากฝ่าย IT ก่อนนำมาใช้
- ผู้ใช้ต้องใช้ข้อมูลอ่อนไหวกับ AI ระดับองค์กรที่มีสัญญาคุ้มครองข้อมูลเท่านั้น และต้องปกปิดข้อมูล (Masking) ก่อนป้อน
- ผู้ใช้ต้องไม่ใช้เครื่องมือ AI ที่ไม่ผ่านการอนุมัติของฝ่าย IT (Shadow AI)

7.3 ความรับผิดชอบและภัยคุกคามด้าน AI

- ผู้ใช้ต้องตรวจสอบความถูกต้อง (ระวัง Hallucination) อคติ (Bias) และลิขสิทธิ์ของผลลัพธ์ก่อนนำไปใช้
- ผู้ใช้ต้องระวังภัยคุกคามเฉพาะของ AI เช่น การแทรกคำสั่ง (Prompt Injection) การรั่วไหลข้อมูลและการปลอมแปลงด้วย AI (Deepfake)
- ผู้ใช้ต้องไม่ใช้ AI ตัดสินใจที่กระทบสิทธิ์ของบุคคลโดยปราศจากการกำกับดูแลของมนุษย์

หมวดที่ 8 ผู้ให้บริการภายนอกและการจัดซื้อจัดจ้าง

8.1 การบริหารผู้ให้บริการภายนอก (Vendor & Third-Party)

- ฝ่ายจัดซื้อและฝ่าย IT ต้องจัดประเภทผู้ให้บริการตามระดับความเสี่ยง และต้องประเมินความน่าเชื่อถือ ความมั่นคงปลอดภัย และความเป็นส่วนตัวก่อนใช้บริการ
- ฝ่ายกฎหมายต้องตรวจสอบให้มีสัญญาที่จำเป็น เช่น สัญญาไม่เปิดเผยข้อมูล (NDA) สัญญาประมวลผลข้อมูลส่วนบุคคล (DPA) ข้อตกลงระดับบริการ (SLA) และสิทธิ์ตรวจสอบ (Right to Audit) ตามระดับความเสี่ยง
- ฝ่าย IT ต้องให้สิทธิ์ผู้ให้บริการตามหลัก Least Privilege กำหนดระยะเวลา เปิด MFA และต้องบันทึกการเข้าถึง
- ผู้ให้บริการต้องรายงานเหตุการณ์ความปลอดภัยและการละเมิดข้อมูลตามกรอบเวลาในสัญญา
- ฝ่าย IT ต้องทบทวนและตรวจสอบผู้ให้บริการเป็นรอบ และเมื่อสิ้นสุดสัญญาต้องถอนสิทธิ์ เรียกคืนและลบข้อมูลของบริษัท
- ฝ่ายกฎหมายและ DPO ต้องตรวจสอบให้การส่งข้อมูลไปต่างประเทศ และผู้ให้บริการที่กฎหมายกำหนดเป็นการเฉพาะ (เช่น VANS สำหรับพิธีการศุลกากร และผู้ให้บริการ GPS) มีมาตรการคุ้มครองและการรับรองตามที่กฎหมายกำหนด

8.2 การจัดซื้อจัดจ้างด้านสารสนเทศ (IT Procurement)

- ผู้ขอจัดซื้อและฝ่ายจัดซื้อต้องพิจารณาความคุ้มค่า (ทั้งต้นทุนตลอดอายุการใช้งาน) ความสอดคล้องกับสถาปัตยกรรม IT และความโปร่งใส
- ฝ่าย IT ละ DPO ต้องประเมินความมั่นคงปลอดภัย และความเป็นส่วนตัวของทุกการจัดซื้อจัดจ้าง ด้านสารสนเทศก่อนอนุมัติ
- ผู้อนุมัติต้องอนุมัติตามลำดับชั้นวงเงินและระเบียบการจัดซื้อของบริษัท
- การจัดซื้อจัดจ้างฉุกเฉิน ผู้จัดการ IT ต้องอนุมัติเฉพาะในกรณีจำเป็น และต้องรายงานย้อนหลัง

หมวดที่ 9 บทบาท การกำกับดูแล และการบังคับใช้

9.1 บทบาทและความรับผิดชอบ

บทบาท	ความรับผิดชอบโดยสังเขป
คณะกรรมการ / ผู้บริหารระดับสูง	อนุมัตินโยบาย กำกับดูแลภาพรวม และสนับสนุนทรัพยากร
ผู้จัดการแผนก IT	บังคับใช้ ติดตาม และทบทวนนโยบาย รวมถึงกำกับมาตรการทางเทคนิค
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	กำกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
ผู้ดูแลระบบ/เครือข่าย/ฐานข้อมูล	ดำเนินมาตรการทางเทคนิค เฝ้าระวัง และจัดการเหตุการณ์
เจ้าของข้อมูล/เจ้าของสินทรัพย์ (Owner)	กำหนดระดับชั้นข้อมูล อนุมัติสิทธิ์ และดูแลสินทรัพย์ในความรับผิดชอบ
ฝ่ายทรัพยากรบุคคล / จัดซื้อ / กฎหมาย	สนับสนุนกระบวนการบุคคล การจัดซื้อ และสัญญาตามนโยบาย
พนักงานทุกคนและผู้ให้บริการภายนอก	ปฏิบัติตามนโยบายและรายงานเหตุการณ์ผิดปกติ

การมอบหมายบทบาทและความรับผิดชอบโดยละเอียด ให้ผู้จัดการ IT กำหนดและประกาศเป็นระเบียบปฏิบัติแยกต่างหาก

9.2 การปฏิบัติตามและบทลงโทษ

ผู้ฝ่าฝืนนโยบายฉบับนี้จะได้รับโทษทางวินัยตามระเบียบของบริษัท และอาจมีความรับผิดทางแพ่ง ทางอาญา หรือทางปกครองตามกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กลุ่มบริษัทสงวนสิทธิ์ในการเพิกถอนสิทธิ์การเข้าถึงระบบทันที เมื่อพบความเสี่ยงร้ายแรง

9.3 การขอยกเว้นนโยบาย (Exception)

- ผู้ขอยกเว้นข้อกำหนดในนโยบายต้องยื่นคำขอเป็นลายลักษณ์อักษร ระบุเหตุผล ขอบเขต ระยะเวลา และมาตรการชดเชยความเสี่ยง
- ผู้จัดการ IT ต้องเป็นผู้พิจารณาอนุมัติยกเว้น กรณีกระทบข้อมูลส่วนบุคคลต้องร่วมกับ DPO และกรณีกระทบระดับสูงต้องร่วมกับผู้บริหาร
- ฝ่าย IT ต้องบันทึกข้อยกเว้นทุกกรณีในทะเบียนข้อยกเว้น กำหนดอายุข้อยกเว้นไม่เกิน 12 เดือน และต้องทบทวนข้อยกเว้นทุก 6 เดือนจนกว่าจะปิดได้

9.4 การติดตาม วัดผล และทบทวนโดยผู้บริหาร

- ฝ่าย IT ต้องติดตามและรายงานตัวชี้วัดการปฏิบัติตามนโยบายต่อผู้บริหารอย่างน้อยไตรมาสละครั้ง ตัวอย่างตัวชี้วัด เช่น อัตราพนักงานลงนามรับทราบนโยบาย อัตราการปิดเหตุการณ์ตามกรอบเวลา อัตราความสำเร็จของการสำรองข้อมูล ความครบถ้วนของการทบทวนสิทธิ์ และจำนวนข้อยกเว้นที่คงค้าง
- ผู้บริหารต้องทบทวนผลการปฏิบัติตามนโยบายและความเสี่ยงสำคัญอย่างน้อยปีละ 1 ครั้ง และต้องสั่งการแก้ไขช่องว่างที่พบ

9.5 การรับทราบนโยบายและการอบรม

- พนักงานทุกคนต้องลงนามรับทราบและยินยอมปฏิบัติตามนโยบายนี้ในวันเริ่มงาน
- ฝ่าย IT ต้องเก็บหลักฐานการลงนามและการอบรมไว้เป็นระยะเวลาที่กฎหมายหรือระเบียบกำหนด
- ผู้รับเหมา ที่ปรึกษา และผู้ให้บริการภายนอกต้องรับทราบข้อกำหนดที่เกี่ยวข้องก่อนได้รับสิทธิ์เข้าถึงระบบ

9.6 การทบทวนและการอนุมัตินโยบาย

- ผู้บริหารระดับสูงต้องอนุมัตินโยบายฉบับนี้ และให้ฝ่าย IT เป็นผู้รับผิดชอบทบทวน
- ฝ่าย IT ต้องทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี หรือความเสี่ยงที่มีนัยสำคัญ
- ฝ่าย IT ต้องจัดเก็บนโยบายในระบบเอกสารกลาง ควบคุมเวอร์ชัน เผยแพร่ให้พนักงานเข้าถึงได้ และกำหนดชั้นความลับที่สมเหตุสมผล

วันที่มีผลใช้บังคับ เริ่มบังคับใช้ตั้งแต่วันที่ 7 กรกฎาคม 2569