นโยบายคุ้มครองข้อมูลส่วนบุคคล

(Data protection Policy)

บริษัท ที คิว อาร์ จำกัด (มหาชน)

TQR Public Company Limited
46/7 Rungrojthanakul Building (Building A), 8th floor, Ratchadapisek Road, Huaykwang, Bangkok 10310
46/7 อาคารรุ่งโรจน์ธนกุล (อาคาร A) ชั้น 8 ถนนรัชดาภิเษก แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
T : 66(0) 2150 8560
F : 66(0) 2150 8563

ประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	วันที่มีผลบังคับใช้	รายละเอียดการแก้ไขปรับปรุง	ผู้จัดทำ

สารบัญ

นโยบายคุ้มครองข้อมูลส่วนบุคคลของ บริษัท ที คิว อาร์ จำกัด (มหาชน)

บริษัท ที คิว อาร์ จำกัด (มหาชน) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการรับผิดชอบต่อสังคมและเป็นรากฐานในการสร้างความสัมพันธ์ทางธุรกิจที่น่าเชื่อถือกับลูกค้า บริษัท จึงยึดมั่นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎเกณฑ์ของราชการอื่น ๆ ที่เกี่ยวข้อง อันเป็นสิทธิขั้นพื้นฐานในความเป็นส่วนตัวของบุคคลโดยเจ้าของข้อมูลส่วนบุคคลย่อมมีความประสงค์ที่จะให้ข้อมูลของตนได้รับการดูแลให้มีความมั่นคงปลอดภัย ซึ่งในนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ประกอบด้วยนโยบายดังต่อไปนี้

1. นโยบายการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล (Personal Data Classification policy)
2. นโยบายการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)
3. นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)
4. นโยบายการส่งหรือโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก (Third Parties Policy)
5. นโยบายการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศอื่น (Cross Border data Transfer Policy)
6. การคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)
7. นโยบายหรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing)

คำนิยาม

ในนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ คำหรือข้อความสามารถนิยามได้ดังนี้

คำศัพท์	คำนิยาม
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และที่จะมีการแก้ไขเพิ่มเติม รวมถึงกฎ ระเบียบ และคำสั่งที่เกี่ยวข้อง
การจัดทำข้อมูลนิรนาม (Anonymization)	ข้อมูลส่วนบุคคลที่ผ่านกระบวนการทำให้ไม่สามารถระบุตัวบุคคลได้กลายเป็นข้อมูลนิรนาม (Anonymous Data) เช่น Masking (การปิดทับข้อมูล) Hash Function (การเปลี่ยนข้อมูลโดยการใช้ฟังก์ชันแฮชทางคณิตศาสตร์)
การแฝงข้อมูล (Pseudonymization)	การแฝงข้อมูลไม่ใช่กระบวนการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ ข้อมูลที่ได้ยังคงเป็นข้อมูลส่วนบุคคลตามความหมายนี้ แต่เป็นการลดหรือจำกัดความสามารถในการเชื่อมโยงข้อมูลส่วนบุคคลกับชุดข้อมูลดั้งต้น ซึ่งถือเป็นมาตรการเพื่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลแบบหนึ่ง โดยอาจใช้วิธีเปลี่ยนข้อมูลที่ระบุตัวบุคคล (Identifier) ด้วยข้อมูลอื่น หรือเลขที่กำหนดใหม่ขึ้นมาได้
การประมวลผลข้อมูล	การดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้างเก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อม ใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย
การลบ/ทำลายข้อมูล	การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกจากระบบหรือถูกทำลายอย่างถาวร ไม่อาจกู้คืนหรือนำชิ้นส่วนมาปะติดปะต่อกลับคืนมาได้ ไม่ว่าจะโดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล

คำศัพท์	คำนิยาม
การเข้าถึง	สิทธิในการอ่าน/ดู บันทึก คัดลอก เก็บสำรอง จัดเก็บ สืบค้น ดาวน์โหลด หรือแก้ไข (อัพเดท แทรก/เพิ่ม ลบ) ข้อมูล รวมถึงการจัดการสิทธิการเข้าถึงนั้น ๆ
การบันทึก	ข้อมูลหรือสารสนเทศในรูปแบบเฉพาะ ซึ่งถูกสร้างขึ้นหรือได้มาจากกิจกรรมบุคคล หรือกิจกรรมองค์กร และได้สำรอง (เก็บรักษา) ไว้เป็นหลักฐานของกิจกรรมนั้น ๆ เพื่อใช้อ้างอิงในอนาคต
ข้อมูล	ข้อมูลทุกรูปแบบทั้งแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ ซึ่งได้รับจากหรือครอบครองโดย เจ้าของข้อมูล พันธมิตรของบริษัท หรือบุคคลภายนอก
ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามมาตรา 6 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่นชื่อ นามสกุล อีเมล์ รูป ลายนิ้วมือ รหัสประชาชน สามารถระบุตัวบุคคลได้ในทางตรง หรือ การเก็บ Location หรือ Cookie เป็นการเก็บข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้ในทางอ้อม นอกจากนี้ ข้อมูลที่โดยพื้นฐานแล้วไม่สามารถนำไประบุตัวบุคคลได้แต่เมื่อนำไปใช้ร่วมกับข้อมูลอื่นแล้วก่อให้เกิดชุดข้อมูลที่สามารถระบุข้อมูลส่วนบุคคลได้ เก็บข้อมูลเหล่านั้นไว้ ก็เป็นการเก็บข้อมูลส่วนบุคคล เช่น ที่อยู่ เพศและอายุ เมื่อนำมารวมกันสามารถนำไประบุตัวบุคคลได้ก็จะเกิดเป็นข้อมูลส่วนบุคคล
ข้อมูลส่วนบุคคลอ่อนไหว	ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพหรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	เจ้าหน้าที่ซึ่งได้รับการแต่งตั้งโดยผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้ทำหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
เจ้าของข้อมูลส่วนบุคคล	บุคคลซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคลนั้น ๆ ไม่ว่าโดยทางตรงหรือทางอ้อม “บุคคล” ในที่นี้หมายถึง บุคคลธรรมดาที่มีชีวิตอยู่ ไม่รวมถึง “นิติบุคคล” ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท, สมาคม, มูลนิธิ หรือองค์กรอื่นใด
เจ้าของสารสนเทศ	ผู้ซึ่งมีความรับผิดชอบต่อข้อมูลสารสนเทศนั้นโดยตรง ซึ่งอาจได้รับข้อมูลนั้นมาโดยตรงจากเจ้าของข้อมูลหรือเป็นผู้สร้างข้อมูลนั้น ๆ ขึ้นมาเอง โดยที่เจ้าของสารสนเทศจะมีหน้าที่ในการกำหนดระดับชั้นของข้อมูล และระดับความเสี่ยงของข้อมูลส่วนบุคคลชุดต่าง ๆ
บุคคลภายนอก	บุคคลธรรมดาหรือนิติบุคคล สำนักงานราชการ หน่วยงานราชการ หรือบุคคลอื่นที่มิใช่เจ้าของข้อมูล มิใช่บริษัท มิใช่ผู้ประมวลผลข้อมูล และมิใช่บุคคลผู้ได้รับอำนาจจากบริษัท หรือ ผู้ประมวลผลข้อมูลโดยตรงให้ประมวลผลข้อมูลของเจ้าของข้อมูล
ผู้ควบคุมข้อมูลส่วนบุคคล	บริษัทซึ่งมีอำนาจตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคลนั้น ๆ ซึ่งเป็นบริษัทที่ได้ข้อมูลส่วนบุคคลจากพนักงาน ลูกจ้าง หรือผู้สมัครงาน หรือต้องทำหรือปฏิบัติตามสัญญากับบุคคลดังกล่าว
ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล

คำศัพท์	คำนิยาม
	ส่วนบุคคลตามคำสั่งหรือในนามผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ให้บริการภายนอก	ผู้ประมวลผลข้อมูลส่วนบุคคล ที่เป็นบุคคลธรรมดาหรือนิติบุคคล ซึ่งไม่ใช่พนักงานหรือหน่วยงานของบริษัท ทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท
สื่อบันทึกข้อมูล	สื่อที่ใช้บันทึกข้อมูล หรือจัดเก็บข้อมูลซึ่งมีหลายรูปแบบ เช่น เอกสารกระดาษ Hard Disk, Flash Drive, เทปข้อมูล, ดิสก์, ซีดี, ดีวีดี เป็นต้น

1. นโยบายการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล (Personal Data Classification policy)

บริษัท มีการกำหนดชั้นความลับของสารสนเทศไว้ 4 ระดับ ได้แก่ ข้อมูลทั่วไป (Public Data) ข้อมูลใช้ภายใน (Internal Use Only Data) ข้อมูลความลับ (Confidential Data) ข้อมูลความลับที่สุด (Top Secret Data) โดยมีการกำหนดแนวทางในการดำเนินการในหัวข้อขั้นตอนการปฏิบัติงานสำหรับการแบ่งชั้นของข้อมูลส่วนบุคคล (Personal Data Classification Procedure) ผู้ที่เกี่ยวข้องจะต้องปฏิบัติตามโดยเคร่งครัด หากกลุ่มของสารสนเทศประกอบไปด้วยสารสนเทศหลายระดับชั้นความลับ ให้เจ้าของสารสนเทศกำหนดระดับชั้นความลับของสารสนเทศนั้นตามระดับชั้นความลับของสารสนเทศระดับสูงสุดของกลุ่มสารสนเทศ

- เจ้าของสารสนเทศมีหน้าที่กำหนดและทบทวนระดับชั้นความลับของข้อมูลส่วนบุคคล ที่อยู่ภายใต้ความรับผิดชอบในของตนอย่างสม่ำเสมอ รวมทั้งจัดให้มีการควบคุมที่เหมาะสมกับระดับชั้นความลับของข้อมูล
- เจ้าของสารสนเทศควรเก็บข้อมูลส่วนบุคคลเป็นความลับและเปิดเผยต่อบุคคลที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมายและกฎเกณฑ์ที่บังคับใช้เท่านั้น
- หน่วยงานที่เกี่ยวข้อง ต้องร่วมดำเนินการให้มีมาตรการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็น และได้รับอนุญาตให้เข้าถึงข้อมูลที่ถูกต้องในเวลาที่เหมาะสมเท่านั้น
- การขอสิทธิเพื่อเข้าถึงข้อมูลส่วนบุคคลนอกเหนือจากสิทธิที่กำหนดไว้จะต้องผ่านการพิจารณาจากเจ้าของสารสนเทศ
- การดำเนินการทางเทคนิคในการให้สิทธิเข้าถึงข้อมูลต้องเป็นไปตามมาตรการการรักษาความมั่นคงปลอดภัยสารสนเทศที่บริษัท กำหนด
- ในการเก็บรักษาข้อมูลส่วนบุคคลต้องเก็บรักษาตามระยะเวลาเท่าที่จำเป็นเท่านั้น เพื่อให้เป็นไปตามวัตถุประสงค์ในการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้เมื่อไม่ได้ใช้ข้อมูลส่วนบุคคลนั้นตามวัตถุประสงค์
- หากมีการว่าจ้างผู้ให้บริการภายนอกที่ต้องมีการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องมีการปฏิบัติตามแนวทางการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing for Personal Data Processing) ซึ่งต้องมีการจัดระดับชั้นความลับของข้อมูลส่วนบุคคลโดยเจ้าของสารสนเทศที่ได้ทำการว่าจ้างผู้ให้บริการภายนอกนั้นๆ

1.1 แนวทางปฏิบัติในการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล (Personal Data Classification Procedure)

เจ้าของสารสนเทศมีหน้าที่กำหนดและสอบทานระดับชั้นความลับของข้อมูลส่วนบุคคลที่อยู่ภายใต้ความรับผิดชอบของหน่วยงานตนเองอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับระดับความสำคัญของสารสนเทศที่อาจมีการเปลี่ยนแปลงตามระยะเวลา รวมทั้งจัดให้มีการควบคุมที่เหมาะสมกับระดับชั้นความลับของข้อมูลดังกล่าว โดยเจ้าของ

สารสนเทศอาจมอบหมายกิจกรรมการควบคุมข้างต้นให้กับผู้ดูแลสารสนเทศ และอาจขอการสนับสนุนและความช่วยเหลือทางด้านเทคนิคจากหน่วยงานเทคโนโลยีสารสนเทศ อย่างไรก็ดีเจ้าของสารสนเทศยังเป็นผู้รับผิดชอบที่แท้จริงในการจัดระดับชั้นความลับและการควบคุมความมั่นคงปลอดภัยของสารสนเทศที่ตนเป็นผู้รับผิดชอบ

นอกจากนี้ ข้อมูลส่วนบุคคลจะต้องได้รับการเก็บรักษาตามระยะเวลาเท่าที่จำเป็นเท่านั้น เพื่อให้เป็นไปตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลดังกล่าว และจะต้องดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ตามแนวทางการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal) หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

ดังนั้น นอกเหนือจากข้อบังคับในการเก็บรักษาข้อมูล หน่วยงานที่เกี่ยวข้องต้องพิจารณาว่ามีข้อกำหนดทางกฎหมาย หรือความจำเป็นใด ๆ ในการจัดเก็บข้อมูลส่วนบุคคลตามระยะเวลาที่ระบุไว้ในแนวทางการจัดเก็บข้อมูลส่วนบุคคล (Data Retention) หรือไม่ ในกรณีที่ไม่สามารถกำหนดระดับชั้นความลับของสารสนเทศบางประเภทตามคำนิยามหรือตัวอย่างที่ได้กล่าวไว้ข้างต้น ให้เจ้าของสารสนเทศเป็นผู้ตัดสินใจในการกำหนดระดับชั้นความลับของสารสนเทศดังกล่าว เมื่อกลุ่มของสารสนเทศประกอบด้วยสารสนเทศหลายระดับชั้นความลับ ให้เจ้าของสารสนเทศกำหนดระดับชั้นความลับของสารสนเทศนั้นตามระดับชั้นความลับของสารสนเทศระดับสูงสุดของกลุ่ม โดยการแบ่งระดับชั้นความลับของข้อมูลสามารถแบ่งออกได้เป็น 4 ระดับ ดังต่อไปนี้

ระดับชั้นความลับ	คำนิยามระดับชั้นความลับข้อมูลสารสนเทศ
ความลับที่สุด (Top Secret)	เป็นข้อมูลที่มีการประเมินแล้วว่า หากมีการเปิดเผยโดยไม่ได้รับอนุญาตจะสามารถสร้างความเสียหายทั้งในรูปการเงินและที่ไม่ใช่การเงินต่อบริษัท อย่างร้ายแรง ข้อมูลที่จัดอยู่ในกลุ่มนี้จะต้องได้รับการดูแลเป็นพิเศษ ทั้งจากผู้เป็นเจ้าของสารสนเทศ และผู้ที่จำเป็นต้องใช้ตามหน้าที่ของงานที่รับผิดชอบ ทุกคนที่สามารถเข้าถึงข้อมูลเหล่านี้จำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA) หรือในกรณีที่เป็นบริษัทในเครือ อาจจัดทำเป็นข้อตกลงไม่เปิดเผยข้อมูล (NDA) หรือ ข้อตกลงในการรักษาความลับระหว่างหน่วยงาน ซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายทั้งสองฝ่าย ตัวอย่างข้อมูลความลับที่สุด เช่น แผนกลยุทธ์ทางธุรกิจ (ก่อนประกาศอย่างเป็นทางการ)
ความลับ (Confidential)	ข้อมูลซึ่งหากเปิดเผยโดยไม่ได้รับอนุญาต จะเป็นการฝ่าฝืนกฎ ข้อบังคับของ บริษัท ก่อให้เกิดผลกระทบด้านชื่อเสียง การเงิน เสียเปรียบในการแข่งขันทางการค้าต่อบริษัท ผู้ที่สามารถเข้าถึงข้อมูลประเภทนี้ได้จึงถูกจำกัดเพียงพนักงานเป็นรายบุคคล กลุ่มพนักงานหรือบุคคลที่สาม ที่มีความสัมพันธ์กันตามสัญญา โดยกลุ่มคนที่ระบุจำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA) ในนามรายบุคคล หรือบริษัทต้นสังกัด หรือในกรณีที่เป็นบริษัทในเครือ อาจจัดทำเป็นข้อตกลงไม่เปิดเผยข้อมูล (NDA) หรือ ข้อตกลงในการรักษาความลับระหว่างหน่วยงาน ซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายทั้งสองฝ่าย ตัวอย่างข้อมูลความลับ เช่น รหัสผ่าน คีย์การเข้ารหัส ข้อมูลทางการเงิน ข้อมูลงบประมาณ ข้อมูลลูกค้า ข้อมูลที่เกี่ยวข้องกับระบบความปลอดภัย ข้อมูลจำลองลายนิ้วมือ ข้อมูลเงินเดือน ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ข้อมูลพันธุกรรม ข้อมูลสุขภาพ เป็นต้น

ระดับชั้นความลับ	คำนิยามระดับชั้นความลับข้อมูลสารสนเทศ
ใช้ภายใน (Internal Use Only)	ข้อมูลที่เปิดเผยได้เฉพาะภายในบริษัท และบุคคลภายนอกที่มีความสัมพันธ์ทางการค้าซึ่งได้รับสิทธิเท่านั้น ไม่เหมาะที่จะเปิดเผยต่อสาธารณชนเป็นการทั่วไป ตัวอย่างข้อมูลใช้ภายใน เช่น เอกสารภายใน E-mail ภายในบริษัท นโยบาย และมาตรฐาน ของบริษัท สมุดรายชื่อโทรศัพท์
ทั่วไป (Public)	ข้อมูลสารสนเทศที่ไม่ได้กระทบอย่างมีนัยสำคัญต่อการดำเนินงาน และผู้บริหารอนุมัติให้เปิดเผยต่อสาธารณะได้ อย่างไรก็ดีข้อมูลสารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกันหรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้กับลูกค้ารวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท ตัวอย่างข้อมูลทั่วไป เช่น แผ่นพับประชาสัมพันธ์ด้านการตลาด ข่าวประชาสัมพันธ์ ข่าวประกาศผู้ถือหุ้น

1.2 แนวทางในการควบคุมและป้องกันสารสนเทศ

การควบคุมและป้องกันสารสนเทศครอบคลุมในด้านการจัดทำ การจัดเก็บ การจัดพิมพ์และการทำสำเนา การจัดส่ง การทำลายและการนำกลับมาใช้ใหม่ของสารสนเทศทั้งในรูปแบบของเอกสารและอิเล็กทรอนิกส์ โดยมีรายละเอียดการควบคุมที่จำเป็น ดังต่อไปนี้

การประมวลผลตามประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use Only)	ความลับ (Confidential)	ความลับที่สุด (Top Secret)
การจัดทำข้อมูล				
การทำเครื่องหมายหรือสัญลักษณ์แสดงชั้นความลับเอกสารฉบับพิมพ์ (Hard Copy) และอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ควรระบุคำว่า “ข้อมูลใช้ภายใน” หรือ “INTERNAL USE ONLY” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน ● กรณีที่เป็นเทป backup จะไม่ทำเครื่องหมายสัญลักษณ์เพื่อป้องกันข้อผิดพลาดทางเทคนิค ● กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ข้อมูลใช้ภายใน [ชื่อบริษัท] ” หรือ “[ชื่อบริษัท] INTERNAL USE ONLY” หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น	ระบุคำว่า “ลับ” หรือ “CONFIDENTIAL” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน กรณีทำได้ควรระบุทุกหน้า ● กรณีที่เป็นเทป backup จะไม่ทำเครื่องหมายสัญลักษณ์ เพื่อป้องกันข้อผิดพลาดทางเทคนิค ● กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ลับ [ชื่อบริษัท] ” หรือ “[ชื่อบริษัท] CONFIDENTIAL” หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น	ระบุคำว่า “ลับที่สุด” หรือ “TOP SECRET”ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน กรณีทำได้ควรระบุทุกหน้าและควรระบุชื่อหน่วยงานเจ้าของเรื่อง เลขที่ชุดของจำนวนชุดทั้งหมดและเลขที่หน้าของจำนวนหน้าทั้งหมดด้วย ● กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ลับที่สุด [ชื่อบริษัท]” หรือ “[ชื่อบริษัท] TOP SECRET” หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น

การประมวลผลตามประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use Only)	ความลับ (Confidential)	ความลับที่สุด (Top Secret)
การพิมพ์ออกทางเครื่องพิมพ์ (Printer) เอกสารฉบับพิมพ์	ไม่มีข้อบังคับพิเศษ	เมื่อสั่งพิมพ์เอกสารไปแล้วจะต้อง เก็บทันทีเมื่อพิมพ์เสร็จโดยไม่ปล่อย เอกสารวางทิ้งไว้	• ตรวจสอบเครื่องพิมพ์ปลายทางให้แน่ใจทุกครั้งก่อนที่จะพิมพ์เอกสารว่าเป็นเครื่องพิมพ์ที่ต้องการจะส่งข้อมูลไป • เมื่อสั่งพิมพ์เอกสารไปแล้วจะต้องเก็บทันทีเมื่อพิมพ์เสร็จโดยไม่ปล่อยเอกสารวางทิ้งไว้ • หากมีการพิมพ์ไปที่เครื่องพิมพ์ซึ่งเชื่อมต่อกับระบบเครือข่าย ที่มีการใช้งานโดยผู้ใช้หลายคนผู้สั่งพิมพ์ต้องเป็นผู้ไปรับเอกสารด้วยตนเองโดยรอเอกสารตั้งแต่เริ่มพิมพ์จนกระทั่งเอกสารพิมพ์เสร็จ • ห้ามพิมพ์เอกสารภายนอกบริษัท เช่น โรงแรม ศูนย์ประชุม สนามบิน เป็นต้น เนื่องจากเครื่องพิมพ์อาจบันทึกสำเนาข้อมูลที่สั่งพิมพ์ไว้	• ตรวจสอบเครื่องพิมพ์ปลายทางให้แน่ใจทุกครั้งก่อนที่จะพิมพ์เอกสารว่าเป็นเครื่องพิมพ์ที่ต้องการจะส่งข้อมูลไป • เมื่อสั่งพิมพ์เอกสารไปแล้วจะต้องเก็บทันทีเมื่อพิมพ์เสร็จโดยไม่ปล่อยเอกสารวางทิ้งไว้ • หากมีการพิมพ์ไปที่เครื่องพิมพ์ซึ่งเชื่อมต่อกับระบบเครือข่าย ที่มีการใช้งานโดยผู้ใช้หลายคนผู้สั่งพิมพ์ต้องเป็นผู้ไปรับเอกสารด้วยตนเองโดยรอเอกสารตั้งแต่เริ่มพิมพ์จนกระทั่งเอกสารพิมพ์เสร็จ • ห้ามพิมพ์เอกสารภายนอกบริษัท เช่น โรงแรม ศูนย์ประชุม สนามบิน เป็นต้นเนื่องจากเครื่องพิมพ์อาจบันทึกสำเนาข้อมูลที่สั่งพิมพ์ไว้
การจัดเก็บข้อมูล				
เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	เก็บไว้ในที่เหมาะสมกับ การปฏิบัติงานและมีการจัดเก็บอย่างเป็นระบบ	เก็บไว้ในที่มิดชิดและสามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น การเก็บในตู้ใส่กุญแจเมื่อไม่ได้ใช้งาน หรือการเก็บในตู้นิรภัย	เก็บไว้ในที่มิดชิดและสามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น การเก็บในตู้ใส่กุญแจเมื่อไม่ได้ใช้งาน หรือการเก็บในตู้นิรภัย
การจัดเก็บข้อมูลในเครื่อง คอมพิวเตอร์ หรือเครื่อง	ไม่มีข้อบังคับพิเศษ	ไม่จำเป็นต้องเข้ารหัส (Unencrypted) แต่ต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่มี	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่

การประมวลผลตามประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use Only)	ความลับ (Confidential)	ความลับที่สุด (Top Secret)
แม่ข่าย (ข้อมูลอิเล็กทรอนิกส์)		และกำหนดสิทธิในการเข้าถึง	มาตรการในการควบคุม และกำหนดสิทธิในการเข้าถึง	มีมาตรการในการควบคุม และกำหนดสิทธิในการเข้าถึง
การจัด เก็บข้อมูลใน Cloud (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	มีมาตรการในการควบคุม และกำหนดสิทธิในการเข้าถึง	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และกำหนดสิทธิในการเข้าถึง	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และกำหนดสิทธิในการเข้าถึง
การจัดเก็บข้อมูลในโทรศัพท์เคลื่อนที่(ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	มีการตั้งค่าการพิสูจน์ตัวตนก่อนการเข้าถึง เช่น pin-code หรือรหัสผ่านเพื่อป้องกันการเข้าถึงข้อมูล กรณีโทรศัพท์สูญหายหรือถูกขโมย	มีการตั้งค่าการพิสูจน์ตัวตนก่อนการเข้าถึง เช่น pin-code หรือรหัสผ่านเพื่อป้องกันการเข้าถึงข้อมูล กรณีโทรศัพท์สูญหายหรือถูกขโมย	มีการตั้งค่าการพิสูจน์ตัวตนก่อนการเข้าถึง เช่น pin-code หรือรหัสผ่านเพื่อป้องกันการเข้าถึงข้อมูล กรณีโทรศัพท์สูญหายหรือถูกขโมย
การจัดเก็บข้อมูลบนสื่อบันทึกข้อมูล (Media) เช่น USB, Memory Stick, SD Card, CD, DVD, External Hard Disk (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	มีการเข้ารหัส (Encrypted) แฟ้มข้อมูลหรือสื่อบันทึกข้อมูล เช่น ● Zip file ด้วย AES-256 ● BitLocker ● Utility ที่เจ้าของผลิตภัณฑ์มีให้	มีการเข้ารหัส (Encrypted) แฟ้มข้อมูลหรือสื่อบันทึกข้อมูล เช่น ● Zip file ด้วย AES-256 ● BitLocker ● Utility ที่เจ้าของผลิตภัณฑ์มีให้
การจัดเก็บสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	เก็บไว้ในที่เหมาะสมกับการปฏิบัติงานและมีการจัดเก็บอย่างเป็นระบบ	เก็บไว้ในที่มิดชิดและสามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น การเก็บในตู้ ใส่กุญแจเมื่อไม่ได้ใช้งาน หรือการเก็บในตู้นิรภัย	เก็บไว้ในที่มิดชิดและสามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น การเก็บในตู้ ใส่กุญแจเมื่อไม่ได้ใช้งาน หรือการเก็บในตู้นิรภัย
การจัดเก็บข้อมูล (เมื่อนำข้อมูลออกนอกสถานที่)				
เมื่อนำข้อมูลไปด้วยระหว่างการเดินทาง เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	ข้อมูลจะต้องอยู่ภายใต้การดูแลตลอดเวลา หรือเก็บในที่ที่สามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น ใส่ซองปิดผนึกไว้ในห้องโรงแรมที่มีการใส่กุญแจ หรือเก็บในตู้นิรภัย	ข้อมูลจะต้องอยู่ภายใต้การดูแลตลอดเวลา หรือเก็บในที่ที่สามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น ใส่ซองปิดผนึกไว้ในห้องโรงแรมที่มีการใส่กุญแจ หรือเก็บในตู้นิรภัย	ข้อมูลจะต้องอยู่ภายใต้การดูแลตลอดเวลา หรือเก็บในที่ที่สามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น ใส่ซองปิดผนึกไว้ในห้องโรงแรมที่มีการใส่กุญแจ หรือเก็บในตู้นิรภัย
เมื่อนำข้อมูลไปด้วยในรถ เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	เก็บไว้ในรถที่มีการล็อคและไว้ในจุดที่ไม่สามารถมองเห็นได้จากภายนอก	เก็บไว้ในรถที่มีการล็อคและไว้ในจุดที่ไม่สามารถมองเห็นได้จากภายนอก	เก็บไว้ในรถที่มีการล็อคและไว้ในจุดที่ไม่สามารถมองเห็นได้จากภายนอก

การประมวลผลตามประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use Only)	ความลับ (Confidential)	ความลับที่สุด (Top Secret)
การส่ง/รับ และการโอนข้อมูล				
การจัดส่งผ่านทางไปรษณีย์ เอกสารฉบับพิมพ์ (Hard copy) และสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	ใส่เอกสารในซองทึบ ปิดผนึก	ใส่เอกสารในซองทึบ ปิดผนึก และประทับตราที่ระบุ Confidential	ไม่ควรส่งผ่านไปรษณีย์ หากจำเป็นจะต้องได้รับอนุญาตจากเจ้าของสารสนเทศก่อน โดยวิธีการปฏิบัติ ให้ปฏิบัติเช่นเดียวกับข้อมูลความลับ
การส่งด้วยมือ เอกสารฉบับพิมพ์ (Hard Copy) และสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	• ใส่เอกสารในซองทึบปิดผนึก และประทับตราที่ระบุ Confidential • จัดทำบันทึกการส่งและการรับไว้เป็นหลักฐาน	• ต้องทำการปิดผนึกซองเอกสารก่อนจัดส่งให้ไม่สามารถสังเกตได้จากภายนอก • ใส่เอกสารในซอง 2 ชั้น • ซองชั้นในให้ระบุระดับชั้นความลับของเอกสาร • ซองชั้นนอกห้ามระบุระดับชั้นความลับเอกสาร • จัดทำบันทึกการส่งและรับไว้เป็นหลักฐาน • จัดส่งให้บุคคลที่ได้รับมอบหมายเท่านั้น
การส่งผ่านเครื่องโทรสาร	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	• ต้องระบุชื่อรายละเอียดของผู้รับและผู้ส่งให้ชัดเจนครบถ้วน • ตรวจสอบหมายเลขปลายทางก่อนเสมอว่าเป็นหมายเลขของสถานที่ที่จะส่งไปจริง • ต้องส่งโทรสารไปยังสถานที่ปลายทางที่มีความมั่นคงปลอดภัยเพียงพอ • ผู้ส่งต้องอยู่รอจนการส่งเสร็จสิ้นแล้วจึงเก็บเอกสารกลับไปโดยไม่ลืมไว้ที่เครื่องโทรสาร • ต้องให้ผู้ได้รับอนุญาตรอรับเอกสารที่ปลายทาง	ห้ามส่งผ่านเครื่องโทรสาร

การประมวลผลตามประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use Only)	ความลับ (Confidential)	ความลับที่สุด (Top Secret)
การแลกเปลี่ยนข้อมูลทาง อิเล็กทรอนิกส์ (Email, FTP)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	ต้องแลกเปลี่ยนข้อมูลให้มีความมั่นคงปลอดภัย เช่น ต้องมีการเข้ารหัส หรือ ใส่รหัสผ่านโดยต้องไม่ส่งรหัสผ่านไปพร้อมกับข้อมูล หรือส่งรหัสผ่านคนละช่องทางกับการส่งข้อมูลครั้งนั้นเป็นต้น	ไม่ควรมีการแลกเปลี่ยนข้อมูลทาง Electronic หากจำเป็นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน โดยวิธีการปฏิบัติ ให้ปฏิบัติเช่นเดียวกับข้อมูลความลับ
การทำลายข้อมูล				
เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	ฉีกทำลาย หรือใช้เครื่องย่อยเอกสาร หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร	ใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร	ต้องส่งเอกสารคืนกลับให้เจ้าของเอกสารเพื่อทำการทำลาย หรือใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) เท่านั้นโดยต้องได้รับอนุมัติจากระดับผู้จัดการฝ่ายขึ้นไปที่เป็น เจ้าของสารสนเทศก่อนทำลาย
การทำลายข้อมูลอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ต้องดำเนินการลบข้อมูลด้วยการลบข้อมูลและ Clear ข้อมูลใน Recycle Bin หรือใช้โปรแกรมในการลบข้อมูล เช่น Eraser	ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ 3 Passes หรือ Dumping ข้อมูล **กรณีที่มีการคืนอุปกรณ์ให้กับหน่วยงานภายนอกให้ใช้ซอฟต์แวร์ Low Level Format	ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ 3 Passes หรือ Dumping ข้อมูล **กรณีที่มีการคืนอุปกรณ์ให้กับหน่วยงานภายนอกให้ใช้ซอฟต์แวร์ Low Level Format
การทำลายข้อมูลค่า Configuration และข้อมูลที่จัดเก็บบนอุปกรณ์	ไม่มีข้อบังคับพิเศษ	Reset ค่า Configuration และข้อมูลที่จัดเก็บบนอุปกรณ์เป็นค่า Factory Default	Reset ค่า Configuration และข้อมูล ที่จัดเก็บบนอุปกรณ์เป็นค่า Factory Default	Reset ค่า Configuration และข้อมูล ที่จัดเก็บบนอุปกรณ์เป็นค่า Factory Default
การทำลายสื่อบันทึกข้อมูล ชนิด CD/DVD	ไม่มีข้อบังคับพิเศษ	ทุบทำลาย หรือใช้เครื่องทำลายแผ่นบันทึกข้อมูลแบบ Strip-cut	ทุบทำลาย หรือใช้เครื่องทำลายแผ่นบันทึกข้อมูลแบบ Strip-cut	ทุบทาลาย หรือใช้เครื่องทำลายแผ่นบันทึกข้อมูลแบบ Strip-cut
การทำลายสื่อบันทึกข้อมูล ชนิด USB Flash Drive, Hard disk และ Tape	ไม่มีข้อบังคับพิเศษ	ทุบทำลาย หรือ วิธีการที่กลุ่มเทคโนโลยีสารสนเทศพิจารณาว่ามีความมั่นคงปลอดภัย	ทุบทำลาย หรือ วิธีการที่กลุ่มเทคโนโลยีสารสนเทศพิจารณาว่ามีความมั่นคงปลอดภัย	ทุบทำลาย หรือ วิธีการที่กลุ่มเทคโนโลยีสารสนเทศพิจารณาว่ามีความมั่นคงปลอดภัย
การจัดการกรณีข้อมูลสูญหาย				

การประมวลผลตามประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use Only)	ความลับ (Confidential)	ความลับที่สุด (Top Secret)
Electronic	ไม่มีข้อบังคับพิเศษ	กรณีข้อมูลส่วนบุคคลสูญหายหรือถูกขโมยให้รายงานต่อผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลทันทีที่ทราบเหตุ เพื่อดำเนินการลดความเสียหายให้มากที่สุด เท่าที่จะเป็นไปได้ เช่น การเปลี่ยนรหัสผ่าน หรือล็อคการเข้าสู่บัญชีผู้ใช้ กรณีเครื่องคอมพิวเตอร์ถูกขโมย หรือการลบข้อมูล (wipe data) ในโทรศัพท์เคลื่อนที่ กรณีโทรศัพท์เคลื่อนที่สูญหาย	กรณีข้อมูลส่วนบุคคลอ่อนไหวสูญหายหรือถูกขโมยให้รายงานต่อผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลทันทีที่ทราบเหตุ เพื่อดำเนินการลดความเสียหายให้มากที่สุด เท่าที่จะเป็นไปได้ เช่น การเปลี่ยนรหัสผ่าน หรือล็อคการเข้าสู่บัญชีผู้ใช้ กรณี เครื่องคอมพิวเตอร์ถูกขโมย หรือการลบข้อมูล (wipe data) ในโทรศัพท์เคลื่อนที่ กรณีโทรศัพท์เคลื่อนที่สูญหาย	กรณีข้อมูลสูญหายหรือถูกขโมยให้รายงานต่อผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลทันทีที่ทราบเหตุ เพื่อดำเนินการลดความเสียหายให้มากที่สุด เท่าที่จะเป็นไปได้ เช่น การเปลี่ยนรหัสผ่าน หรือล็อคการเข้าสู่บัญชีผู้ใช้ กรณี เครื่องคอมพิวเตอร์ถูกขโมย หรือการลบข้อมูล (wipe data) ในโทรศัพท์เคลื่อนที่ กรณีโทรศัพท์เคลื่อนที่สูญหาย
เอกสารฉบับพิมพ์ (Hard copy)	ไม่มีข้อบังคับพิเศษ	กรณีข้อมูลส่วนบุคคลสูญหายหรือถูกขโมยให้รายงานผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลทันทีที่ทราบเหตุ	กรณีข้อมูลส่วนบุคคลอ่อนไหวสูญหายหรือถูกขโมยให้รายงานผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลทันทีที่ทราบเหตุ	กรณีข้อมูลสูญหายหรือถูกขโมยให้รายงานผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลทันทีที่ทราบเหตุ
อื่น ๆ				
เอกสารฉบับพิมพ์ (Hard copy) และ อิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	กรณีที่ ข้อมูลข่าวสารลับใดไม่มีเครื่องหมายแสดงชั้นความลับไว้ แต่หากพนักงานรู้ หรือควรจะรู้ข้อเท็จจริงว่าข้อมูลข่าวสารนั้นได้มีการกำหนดชั้นความลับไว้แล้ว ให้ปฏิบัติกับข้อมูลนั้น ๆ เช่นเดียวกับข้อมูลที่มีเครื่องหมายแสดงชั้นความลับไว้ และให้พนักงานจัดทำหรือแจ้งหน่วยงานเจ้าของข้อมูลให้จัดทำเครื่องหมายแสดงชั้นความลับโดยเร็ว	กรณีที่ ข้อมูลข่าวสารลับใดไม่มีเครื่องหมายแสดงชั้นความลับไว้ แต่หากพนักงานรู้ หรือควรจะรู้ข้อเท็จจริงว่าข้อมูลข่าวสารนั้นได้มีการกำหนดชั้นความลับไว้แล้ว ให้ปฏิบัติกับข้อมูลนั้น ๆ เช่นเดียวกับข้อมูลที่มีเครื่องหมายแสดงชั้นความลับไว้ และให้พนักงานจัดทำหรือแจ้งหน่วยงานเจ้าของข้อมูลให้จัดทำเครื่องหมายแสดงชั้นความลับโดยเร็ว

2. นโยบายการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)

บริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล จึงกำหนดให้มีกระบวนการลบ ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลตามนโยบายในการจัดเก็บข้อมูลส่วนบุคคล หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม และสอดคล้องกับการรักษาความลับของข้อมูลส่วนบุคค เพื่อป้องกันการสูญหาย การเข้าถึง การทำลาย การใช้

การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย รวมถึงควบคุมให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามที่กำหนดในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของบริษัท

2.1 การลบ/ทำลายเอกสาร

บริษัท มีการเก็บรักษาข้อมูลส่วนบุคคลที่เป็นกระดาษซึ่งต้องมีการตรวจสอบแนวทางการทำลายด้วยวิธีที่มีความมั่นคงปลอดภัย เพื่อให้เป็นไปตามแนวทางปฏิบัติในการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล (Personal Data Classification Procedure) โดยมีรายละเอียดดังนี้

- **ทั่วไป (Public)** ฉีกทำลาย หรือใช้เครื่องย่อยเอกสาร หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร
- **ใช้ภายใน (Internal Use Only)** ฉีกทำลาย หรือใช้เครื่องย่อยเอกสาร หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร
- **ความลับ (Confidential)** ต้องใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร
- **ความลับที่สุด (Top Secret)** ต้องส่งเอกสารคืนกลับให้เจ้าของเอกสารเพื่อทำการทำลาย หรือใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) เท่านั้น

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงหรือเพิ่มเติมได้ตามที่บริษัท เห็นว่าเหมาะสม หรือเพื่อให้เป็นไปตามกฎเกณฑ์เกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลเพิ่มเติมตามที่อาจมีการแก้ไขหรือควบคุมโดยหน่วยงานที่เกี่ยวข้อง

2.2 การลบ/ทำลายด้วยวิธีอิเล็กทรอนิกส์

บริษัท มีการเก็บรักษาข้อมูลส่วนบุคคลที่เป็นอิเล็กทรอนิกส์ซึ่งต้องมีการตรวจสอบแนวทางการทำลายด้วยวิธีที่มีความมั่นคงปลอดภัย เพื่อให้เป็นไปตามแนวทางปฏิบัติในการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล (Personal Data Classification Procedure) โดยมีรายละเอียดดังนี้

- **ทั่วไป (Public)** ต้องดำเนินการลบข้อมูลด้วยการลบข้อมูลและ Clear ข้อมูลใน Recycle Bin หรือใช้โปรแกรมในการลบข้อมูล เช่น Eraser
- **ใช้ภายใน (Internal Use Only)** ต้องดำเนินการลบข้อมูลด้วยการลบข้อมูลและ Clear ข้อมูลใน Recycle Bin หรือใช้โปรแกรมในการลบข้อมูล เช่น Eraser
- **ความลับ (Confidential)** ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ 3 Passes
- **ความลับที่สุด (Top Secret)** ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ 3 Passes

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงหรือเพิ่มเติมได้ตามที่บริษัท เห็นว่าเหมาะสม หรือเพื่อให้เป็นไปตามกฎเกณฑ์เกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลเพิ่มเติมตามที่อาจมีการแก้ไขหรือควบคุมโดยหน่วยงานที่เกี่ยวข้อง

2.3 วิธีการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ในกรณีที่ไม่สามารถลบ/ทำลายข้อมูลส่วนบุคคลได้โดยตรง เนื่องจากอาจส่งผลกระทบต่อความถูกต้องในการปฏิบัติงาน เช่น อาจส่งผลให้การทำงานของฐานข้อมูลไม่ถูกต้อง หรือเป็นข้อจำกัดของระบบ บริษัท อาจใช้วิธีการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของข้อมูลส่วนบุคคลได้ ดังนี้

1. การเปลี่ยนแปลงส่วนใดส่วนหนึ่งของข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่ม หรือการทำให้เป็นข้อมูลอื่น ๆ หรือการใช้กระบวนการอื่นใดที่ได้รับการรับรองเป็นมาตรฐานในปัจจุบัน เช่น การใช้ Hash Function เพื่อเปลี่ยนข้อมูลเดิมให้ไม่สามารถที่จะให้ข้อมูลย้อนกลับมาระบุตัวตนของเจ้าของข้อมูลได้
2. การลดความชัดเจนของข้อมูล (Blurring or Noising) โดยการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลเดิมเพื่อลดความเฉพาะเจาะจงของข้อมูลลง

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงหรือเพิ่มเติมได้ตามที่บริษัท เห็นว่าเหมาะสม หรือเพื่อให้เป็นไปตามกฎเกณฑ์เกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลเพิ่มเติมตามที่อาจมีการแก้ไขหรือควบคุมโดยหน่วยงานที่เกี่ยวข้อง

2.4 กระบวนการลบข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

บริษัท จะดำเนินการลบข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ เมื่อมีกรณีดังต่อไปนี้

1. ครบกำหนดระยะเวลาการจัดเก็บตามที่กำหนดไว้นโยบายในการจัดเก็บข้อมูลส่วนบุคคล
2. ข้อมูลส่วนบุคคลนั้นไม่มีความเกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น
3. ข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย
4. เจ้าของข้อมูลส่วนบุคคลร้องขอการใช้สิทธิตามสิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคลที่มีการระบุไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อเจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม
5. เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ทั้งนี้ บริษัท สามารถปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคลได้ ตามมาตรา 33 วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

1. มีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล
2. การประมวลผลเป็นไปตามวัตถุประสงค์ในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุเพื่อประโยชน์สาธารณะหรือที่เกี่ยวกับการศึกษาวิจัย ซึ่งในกรณีดังกล่าว บริษัท จะจัดให้มีมาตรการป้องกันที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
3. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของบริษัท หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่บริษัท
4. เป็นการจำเป็นในการปฏิบัติตามกฎหมายของบริษัท เพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

5. การเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

3. นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)

3.1 สถานที่จัดเก็บข้อมูล

3.1.1 เอกสารในรูปแบบอิเล็กทรอนิกส์, จดหมายอิเล็กทรอนิกส์ (อีเมล) และ บันทึกมัลติมีเดีย (Multimedia)

เอกสารในรูปแบบอิเล็กทรอนิกส์ อีเมล และบันทึกมัลติมีเดียทั้งหมดจะต้องจัดเก็บภายในสถานที่ที่เหมาะสมเพื่อให้แน่ใจว่ามีการใช้มาตรการรักษาความปลอดภัยที่เป็นไปตามมาตรฐานที่กำหนดโดยกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึง กฎหมายอื่น แนวปฏิบัติ และคำสั่งที่เกี่ยวข้อง

3.1.2 เอกสารในรูปแบบกระดาษ

การจัดเก็บเอกสารในรูปแบบกระดาษที่จำเป็นสำหรับการดำเนินธุรกิจในแต่ละวัน ต้องเก็บไว้ในตู้เก็บเอกสารและลิ้นชักโต๊ะทำงานเมื่อไม่ได้ใช้งาน และพนักงานจะต้องล็อคกุญแจตู้เก็บเอกสารและลิ้นชักที่จัดเก็บเอกสารที่มีข้อมูลส่วนบุคคลเมื่อสิ้นวันทำการ

3.2 การปกป้องเอกสาร

บริษัท มุ่งมั่นที่จะป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยเอกสารที่มีข้อมูลส่วนบุคคลซึ่งอยู่ในการควบคุมของบริษัท โดยมิชอบหรือโดยปราศจากอำนาจ เอกสารทั้งในรูปแบบกระดาษและรูปแบบอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลจะถูกเก็บไว้ในที่ปลอดภัยจนกว่าจะถูกทำลาย บริษัท จะใช้เทคโนโลยีและกระบวนการต่าง ๆ ที่ได้รับการตรวจสอบอย่างสม่ำเสมอเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล

3.3 การทำลายเอกสาร

เมื่อพ้นกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลหรือหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลแล้ว เอกสารในรูปแบบประเภทกระดาษที่มีข้อมูลส่วนบุคคลจะถูกทำลายโดยการย่อยเอกสาร โดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว ส่วนข้อมูลส่วนบุคคลที่จัดเก็บทางอิเล็กทรอนิกส์จะถูกลบออกจากสื่อที่ใช้เก็บข้อมูล เช่น ฮาร์ดดิสก์จะถูกทำลาย หรือ ถูกลบข้อมูลโดยวิธีที่ไม่สามารถกู้คืนข้อมูลได้ โดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว

3.4 การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัท ต้องมีการกำหนดระยะเวลาการจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ในการเก็บรวบรวมสำหรับการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน โดยอาจเป็นไปตามระยะเวลาที่กำหนดตามกฎหมาย แนวปฏิบัติของธุรกิจ หรือมาตรฐานของการประมวลผล สำหรับระยะเวลาในการเก็บรักษาข้อมูลทั้งหมดสามารถตรวจสอบได้จากภาคผนวก

บริษัท ต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเป็นไปตามนโยบายในการลบหรือทำลายข้อมูลส่วนบุคคล (Personal Data Disposal Policy)

4. นโยบายการส่งหรือโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก (Third Parties Policy)

บริษัท จะเปิดเผยข้อมูลส่วนบุคคลให้แก่องค์กรหรือหน่วยงานภายนอก โดยมีแนวปฏิบัติดังนี้

1. หากจะมีการเปิดเผยข้อมูลส่วนบุคคลให้กับ คู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก จะสามารถดำเนินการได้เฉพาะในกรณีที่มีการระบุรายชื่อของ คู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก ในบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Data Inventory) เท่านั้น หากไม่มีการระบุในบันทึกรายการประมวลผลข้อมูลส่วนบุคคล จะต้องขออนุมัติจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก่อนที่จะเปิดเผยข้อมูลส่วนบุคคล โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องพิจารณาฐานในการประมวลผลข้อมูลส่วนบุคคลและเงื่อนไขให้สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. สัญญาระหว่างบริษัทและคู่ค้า พันธมิตรทางธุรกิจ และ/หรือ ผู้ให้บริการภายนอกจะต้องมีการกำหนดมาตรการเกี่ยวกับ
   - หน้าที่ในการประมวลผลข้อมูลส่วนบุคคล
   - มาตรการในการรักษาความมั่นคงปลอดภัย
   - การดำเนินกิจกรรมที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล
   - การแจ้งเตือนหากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
   - การเก็บรักษาข้อมูลส่วนบุคคลและการลบข้อมูลส่วนบุคคล
   - การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
3. กรณีส่งหรือโอนข้อมูลส่วนบุคคลไปยังนิติบุคคล จะต้องพิจารณาว่าในการส่งหรือโอนข้อมูลส่วนบุคคลนั้นมีมาตรการการรักษาความมั่นคงปลอดภัย และมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน
4. กรณีที่หน่วยงานรัฐ หรือองค์กรผู้ถืออำนาจรัฐ ร้องขอเข้าถึงข้อมูลส่วนบุคคลโดยการอ้างถึงกฎหมาย ระเบียบ หรือคำสั่งใด ๆ ที่บริษัท จะต้องปฏิบัติตาม ผู้รับผิดชอบจะสามารถให้หน่วยงานเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่มีบทบัญญัติกฎหมาย หรือคำสั่ง หรือหนังสือแจ้งอย่างเป็นทางการ อย่างใดอย่างหนึ่งเป็นอย่างน้อยตามอำนาจทางกฎหมายเท่านั้น มิเช่นนั้นบริษัท จะมีความผิดตามกฎหมายจากการให้หน่วยงานดังกล่าวเข้าถึงหรือเปิดเผยข้อมูลโดยไม่มีหน้าที่ตามกฎหมาย ยกเว้นกรณีที่เป็นการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation) ของบริษัท ที่แม้ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่บริษัทจะต้องกระทำตามหน้าที่อยู่แล้ว

5. นโยบายการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศอื่น (Cross Border data Transfer Policy)

การถ่ายโอนข้อมูลส่วนบุคคลอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล การดำเนินการถ่ายโอนข้อมูลส่วนบุคคลไปประเทศปลายทาง หรือองค์กรระหว่างประเทศจะต้องมีความมั่นคงปลอดภัย โดยบริษัท พิจารณาทางเลือกดังต่อไปนี้

1. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทาง หรือองค์กรระหว่างประเทศ โดยบริษัท จะดำเนินการส่งข้อมูลส่วนบุคคลไปยังประเทศที่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
2. มีการจัดทำข้อตกลงระหว่างกันในรูปแบบใดรูปแบบหนึ่งดังต่อไปนี้
   - นโยบายการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules) ที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองส่วนบุคคลแล้ว
   - มีการจัดทำข้อตกลงเป็นไปตามข้อสัญญามาตรฐาน (Standard Data Protection Clauses)
   - จรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ (Code of Conduct)
3. ในกรณีที่ไม่สามารถใช้ทางเลือกการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในข้อ 1 และ 2 สามารถดำเนินการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ หากเป็นกรณีดังนี้
   - เป็นการปฏิบัติตามกฎหมาย
   - ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
   - เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
   - เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
   - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
   - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
4. ในกรณีที่มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้นไม่มีมาตรฐานเพียงพอ ให้เสนอต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัยเสียก่อน

6. การคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)

บริษัท สามารถโอนข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกันได้ หากการส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าวเป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน (“สมาชิกเครือกิจการ”) ที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว โดยนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หรือ Binding Corporate Rules (BCR) จะต้อง

1. มีผลผูกพันตามกฎหมายและบังคับใช้กับและถูกบังคับใช้โดยสมาชิกเครือกิจการทุกราย รวมถึงลูกจ้างและพนักงานของเครือกิจการ (“สมาชิกเครือกิจการ”)
2. รับรองสิทธิอันสามารถบังคับใช้ได้ของเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลถูกนำมาประมวลผล
3. BCR ประกอบด้วยองค์ประกอบอย่างน้อยดังต่อไปนี้
    3.1 รายละเอียดโครงสร้างและช่องทางการติดต่อของสมาชิกเครือกิจการ
    3.2 ข้อมูลส่วนบุคคลที่จะถูกเปิดเผยหรือชุดข้อมูลส่วนบุคคลที่จะถูกเปิดเผย รวมถึงรายละเอียดประเภทของข้อมูลส่วนบุคคล, วิธีการและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล, ประเภทของเจ้าของข้อมูลส่วนบุคคล, ประเทศหรือองค์การระหว่างประเทศปลายทางซึ่งรับข้อมูลส่วนบุคคล
    3.3 ความมีผลผูกพันทางกฎหมายทั้งภายในและภายนอกกลุ่มสมาชิกเครือกิจการของ BCR
    3.4 การนำหลักการคุ้มครองข้อมูลทั่วไปมาปรับใช้ เช่น การจำกัดวัตถุประสงค์ (Purpose Limitation), การใช้ข้อมูลอย่างน้อยที่สุด (Data Minimization), การจำกัดระยะเวลาในการจัดเก็บข้อมูล (Limited Storage Periods), คุณภาพของข้อมูล (Data Quality), การคุ้มครองข้อมูลผ่านการออกแบบและโดยปริยาย (Data Protection by Design and by Default), ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis for Processing), การประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 ของพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Processing of Special Categories of Personal Data), มาตรการในการรับประกันความปลอดภัยของข้อมูล และเงื่อนไขในการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอกที่ไม่ใช่สมาชิกเครือกิจการ (Requirements in Respect of Onward Transfers to Bodies not Bound by the Binding Corporate Rules)
    3.5 สิทธิของเจ้าของข้อมูลส่วนบุคคลอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล และช่องทางในการใช้สิทธินั้น รวมถึงสิทธิที่จะร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และการฟ้องร้องคดีต่อศาลที่มีอำนาจ สิทธิในการได้รับการเยียวยา และสิทธิในการได้รับค่าเสียหายอันเกิดจากการละเมิด BCR
    3.6 ความยินยอมรับผิดโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นสมาชิกเครือกิจการซึ่งตั้งอยู่ในประเทศไทย ในกรณีที่เกิดเหตุละเมิด BCR โดยสมาชิกเครือกิจการซึ่งไม่ได้ตั้งอยู่ในประเทศไทย ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ต้องรับผิดบางส่วนหรือทั้งหมด หากพิสูจน์ได้ว่าสมาชิกเครือกิจการมิได้มีส่วนรับผิดชอบกับเหตุการณ์ที่ก่อให้เกิดความเสียหาย
    3.7 การแจ้งเนื้อหาของ BCR (โดยเฉพาะข้อ 3.4 - ข้อ 3.6) ให้แก่เจ้าของข้อมูลส่วนบุคคลรับทราบเพิ่มเติมจากการแจ้งรายละเอียดตามมาตรา 23 และมาตรา 25 ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
    3.8 หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer (DPO) ที่ได้รับมอบหมายตามมาตรา 41 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือบุคคล/นิติบุคคลที่ได้รับมอบหมายให้ตรวจสอบการดำเนินการตาม BCR ของสมาชิกเครือกิจการ, การฝึกอบรม, การรับเรื่องร้องเรียน
    3.9 กระบวนการรับเรื่องร้องเรียน

3.10 กลไกภายในกลุ่มสมาชิกเครือกิจการสำหรับการรับประกันการดำเนินการตาม BCR ซึ่งต้องมีองค์ประกอบอย่างน้อยดังนี้ การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Audit) และวิธีการในการรับประกันการดำเนินการเชิงแก้ไขเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยบุคคลที่ได้รับมอบหมายตามข้อ 3.8 (DPO) และคณะกรรมการกลุ่มสมาชิกเครือกิจการจะต้องรับทราบผลการตรวจสอบข้างต้น รวมถึงจัดเตรียมให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบผลการตรวจสอบข้างต้นได้

3.11 กลไกการรายงานและบันทึกการเปลี่ยนแปลงเนื้อหาของ BCR และการรายงานการเปลี่ยนแปลงดังกล่าวไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3.12 กลไกการให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการรับประกันการดำเนินการตาม BCR ของสมาชิกเครือกิจการ เช่น การจัดเตรียมผลการตรวจสอบให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

3.13 กลไกในการรายงานไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งข้อบังคับทางกฎหมายที่สมาชิกเครือกิจการที่ตั้งอยู่ในประเทศปลายทางต้องปฏิบัติตามอันอาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อหลักประกันที่ได้ให้ไว้ตาม BCR

3.14 จัดการฝึกอบรมการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม ให้แก่พนักงานหรือบุคคลที่เข้าถึงข้อมูลส่วนบุคคลเป็นประจำหรือตลอดเวลา

4. นอกเหนือจาก BCR แล้ว บริษัท อาจยอมรับให้มาตรการคุ้มครองที่เหมาะสมอื่น ๆ ที่สามารถบังคับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจมีการกำหนดขึ้น ได้แก่ ข้อสัญญามาตรฐาน หรือจรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ หรือคำรับรอง ซึ่งเป็นเงื่อนไขที่ทำให้บริษัท สามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางได้ แม้ว่าประเทศปลายทางนั้นจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยอาจเลือกใช้แนวทางตามข้อ 4.1 ถึงข้อ 4.3 ดังต่อไปนี้

4.1 ข้อสัญญามาตรฐาน (Standard Data Protection Clauses)

บริษัท นำข้อสัญญามาตรฐาน (Standard Contractual Clauses) มาใช้เพื่อให้ข้อมูลส่วนบุคคลถูกถ่ายโอนอย่างที่ควรจะเป็น เพื่อให้การให้บริการ รวมถึงการรักษามาตรฐานและการปรับปรุงบริการให้เป็นไปโดยถูกต้องตามกฎหมาย อย่างไรก็ตามข้อสัญญาคุ้มครองข้อมูลส่วนบุคคลจะต้องมีการกำหนดหน้าที่ทางสัญญาเกี่ยวกับการส่งข้อมูลส่วนบุคคลไปยังต่างประเทศตลอดจนการโอนย้ายข้อมูลส่วนบุคคล ซึ่งเจ้าข้อมูลส่วนบุคคลสามารถใช้สิทธิของตนเองในการส่งหรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศได้

4.2 จรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ (Code of Conduct)

บริษัท จะนำส่งหรือโอนข้อมูลส่วนบุคคลเมื่อผู้รับโอนได้ลงนามในข้อปฏิบัติซึ่งได้รับการอนุมัติจากเจ้าพนักงาน โดยข้อปฏิบัติที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศจะต้องมีรายละเอียดของมาตรการที่เหมาะสมในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งถูกนำไปประมวลผล ตลอดจนโอนข้อมูลส่วนบุคคล ทั้งนี้ข้อปฏิบัติดังกล่าวจะต้องมีผลบังคับได้ต่อเจ้าข้อมูลส่วนบุคคลโดยตรง บริษัท จะนำจรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ ที่ยึดมั่นในเจตนารมณ์ของการดำเนินธุรกิจอันตั้งอยู่บนพื้นฐานของการบริหารจัดการตามหลักการกำกับดูแลกิจการที่ดี โดยยึดมั่นต่อคุณธรรมและจริยธรรมใน

การดำเนินธุรกิจ มีความโปร่งใส ตรวจสอบได้ และตระหนักถึงความรับผิดชอบต่อผู้มีส่วนได้เสียทุกฝ่าย เพื่อให้เกิดการป้องกันข้อมูลส่วนบุคคลอย่างเหมาะสมและเป็นไปตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

4.3 คำรับรอง (Certification Mechanism)

บริษัท จะใช้คำรับรองที่ได้รับการยอมรับโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งประกอบกับคำมั่นสัญญาที่มีผลบังคับผูกพันผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศ ที่จะปรับใช้มาตรการที่เหมาะสมเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล เพื่อแสดงให้เห็นว่ามีการป้องกันที่เหมาะสมในการถ่ายโอนข้อมูลส่วนบุคคลในระดับสากล

7. นโยบายหรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing)

แนวปฏิบัติการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

1. หน่วยงานที่มีการเปิดเผยข้อมูลส่วนบุคคลให้กับ คู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก จะต้องมีการทำสัญญาระหว่างบริษัท และคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก รายนั้น โดยสัญญาจะต้องเป็นไปตามรูปแบบที่ - *หน่วยงานที่รับผิดชอบ* - กำหนดไว้
2. เนื้อหาของสัญญาระหว่างบริษัท และคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก จะต้องมีการกำหนดมาตรการเกี่ยวกับ
    - หน้าที่ในการประมวลผลข้อมูล โดยต้องมีข้อความเกี่ยวกับ
        - คำสั่งในการประมวลผลข้อมูลส่วนบุคคล และไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งเป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลส่วนบุคคล
        - การให้การรับรองจากผู้ประมวลผลข้อมูลส่วนบุคคลว่าคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
        - ผู้ประมวลผลข้อมูลส่วนบุคคลมีการจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลให้กับบุคคลที่ได้รับมอบหมาย โดยมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายในวัตถุประสงค์ของสัญญา
        - ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ประมวลผล รวมถึงมีมาตรการที่ทำให้มั่นใจว่าบุคคลที่ได้รับสิทธิเข้าถึงข้อมูลส่วนบุคคลได้ให้คำมั่นสัญญาหรือมีหน้าที่ตามสัญญาในการรักษาความลับของข้อมูลส่วนบุคคล
        - ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดข้อมูลที่จำเป็นต่อการแสดงให้เป็นที่พอใจถึงการปฏิบัติตามหน้าที่ตามสัญญารวมถึงยินยอมและให้ความร่วมมือในการตรวจสอบและสอบสวนโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ตรวจสอบซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมอบหมาย
    - มาตรการในการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อความเกี่ยวกับ
        - ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดหามาตรการการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อเป็นการรักษาความลับ ความถูกต้อง และความพร้อมใช้

ของข้อมูลส่วนบุคคล โดยต้องมีมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องเข้าถึงควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วยการดำเนินการดังนี้

- การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
- การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
- การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- หน้าที่ในการดำเนินกิจกรรมที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล
  - หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการสนับสนุนการผู้ควบคุมข้อมูลส่วนบุคคลในเรื่องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
  - การแจ้งต่อผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- การแจ้งเตือนหากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับ
  - การแจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้า หากทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- การเก็บรักษาข้อมูลส่วนบุคคล และการลบข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับ
  - หน้าที่และระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็น เพื่อการปฏิบัติหน้าที่ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
  - วิธีในการลบ ทำลาย ส่งคืน หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
  - การเก็บข้อมูลส่วนบุคคลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยต้องมีข้อความเกี่ยวกับ
  - การไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เว้นแต่จะได้รับอนุมัติจากบริษัท

- การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ จะต้องเป็นไปตามเงื่อนไขที่กำหนดในกฎหมายคุ้มครองข้อมูลส่วนบุคคล และประกาศที่เกี่ยวข้อง

ภาคผนวก ก. ตัวอย่างการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use Only)
ข้อมูลที่ใช้ในการพิสูจน์หรือยืนยันตัวตน	รหัสผ่าน	✓	
	คีย์การเข้ารหัสข้อมูล (Encryption keys)	✓	
	ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า (Face recognition) ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ	✓	
	บันทึกกิจกรรมการเข้าถึงระบบ (Authentication logs)	✓	
ข้อมูลบัตรอิเล็กทรอนิกส์ (เช่น บัตรเดบิต บัตรเครดิต เป็นต้น)	ชื่อผู้ถือบัตรอิเล็กทรอนิกส์	✓	
	เลขบัตรอิเล็กทรอนิกส์	✓	
	PIN, PIN block	✓	
	CVV, CVV2, CVC2, CID	✓	
	ข้อมูลบัตรบนแถบแม่เหล็ก	✓	
ข้อมูลที่สามารถระบุตัวบุคคลได้ (Personally Identifiable Information (PII))	ชื่อ นามสกุล		✓
	เลขบัตรประชาชน		✓
	เลขหนังสือเดินทาง		✓
	เลขบัตรประกันสังคม		✓
	เลขใบอนุญาตขับขี่		✓
	เลขประจำตัวผู้เสียภาษี		✓
	รหัสพนักงาน		✓
	เลขบัญชีธนาคาร		✓
	เลขที่กรมธรรม์		✓
	วันเดือนปีเกิด		✓
	อายุ		✓
	เพศ		✓
	ที่อยู่		✓

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use Only)
	เบอร์โทรศัพท์		✓
	อีเมล		✓
	ข้อมูลเงินเดือน	✓	
	ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID		✓
	ข้อมูลชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม	✓	
	ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน		✓
	ข้อมูลการจ้างงาน		✓
	ประวัติการทำงาน		✓
	ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง		✓
	ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file		✓
ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว	ความเชื่อในลัทธิ ศาสนาหรือปรัชญา	✓	
	ความคิดเห็นทางการเมือง	✓	
	เชื้อชาติ เผ่าพันธุ์	✓	
	ข้อมูลพันธุกรรม	✓	
	ประวัติอาชญากรรม	✓	
	พฤติกรรมทางเพศ	✓	
	ข้อมูลประวัติทางการแพทย์ สุขภาพ หมู่เลือด ความพิการ หรือข้อมูลสุขภาพจิต	✓	
	ข้อมูลสหภาพแรงงาน	✓	

ภาคผนวก ข. ตัวอย่างการจัดเก็บข้อมูลส่วนบุคคล (Personal Data Retention)

ลำดับ	แผนก	ฟังก์ชันงาน	วัตถุประสงค์	เงื่อนไขระยะเวลาการจัดเก็บ	ระยะเวลาการจัดเก็บ	กิจกรรมที่ต้องดำเนินการ	เหตุผลในการจัดเก็บ และ/หรือ หน่วยงานที่เกี่ยวข้อง
1.	การเงินและบัญชี	บันทึกการรับเงินและการจ่ายเงิน	เพื่อจัดทำบันทึกการรับเงินและการจ่ายเงินภายในบริษัท	เมื่อมีการรับและจ่ายเงินสิ้นสุด	5 ปี	ทบทวนเหตุผลในการจัดเก็บต่อไป	แตกต่างกันไปตามวัตถุประสงค์ของกิจกรรม
2.	การเงินและบัญชี	การยื่นภาษี	เพื่อยื่นเอกสารแก่กรมสรรพากร	เมื่อปิดบัญชีหรือจนกว่าจะมีการส่งมอบบัญชี ตามมาตรา 17 พ.ร.บ.การบัญชี	5-7 ปี	ทบทวนเหตุผลในการจัดเก็บต่อไป	พ.ร.บ.การบัญชี พ.ศ. 2543 มาตรา 14
3.	การเงินและบัญชี	ทำเอกสารทางการเงิน	เพื่อจ่ายเงินให้แก่ลูกค้า/ ผู้จัดจำหน่าย	เมื่อกระบวนการจ่ายเงินสิ้นสุด	5 ปี	ทบทวนเหตุผลในการจัดเก็บต่อไป	แตกต่างกันไปตามวัตถุประสงค์ของกิจกรรม
4.	ทรัพยากรบุคคล	รับสมัครงาน	เพื่อเก็บผู้สมัครงานที่ไม่รับการเลือกจากบริษัท	สิ้นสุดขั้นตอนการพิจารณารับสมัครงาน	2 ปี	ทบทวนเหตุผลในการจัดเก็บต่อไป	เพื่อพิจารณาการสมัครงานครั้งต่อไป
5.	ทรัพยากรบุคคล	จ้างแรงงาน	เพื่อทำสัญญาจ้างแรงงาน	สิ้นสุดสัญญาจ้าง	12 ปี (อายุความ 10 ปี + ระยะเวลาตั้งต้นคดี 2 ปี)	ทบทวนเหตุผลในการจัดเก็บต่อไป	พ.ร.บ.คุ้มครองแรงงาน พ.ศ. 2541 ม. 115
6.	ทรัพยากรบุคคล	การยื่นประกันสังคม	เพื่อส่งให้ต่อประกันสังคม	สิ้นสุดสัญญาจ้าง	12 ปี (อายุความ 10 ปี + ระยะเวลาตั้งต้นคดี 2 ปี)	ทบทวนเหตุผลในการจัดเก็บต่อไป	ตามระยะเวลาสัญญาจ้างแรงงาน
7.	เทคโนโลยีสารสนเทศ	ดูแลระบบ	เพื่อเก็บ log ข้อมูล	เมื่อบรรลุวัตถุประสงค์ในการเก็บรวบรวมข้อมูล	120 วัน	ลบ/ทำลาย	พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550