บริษัท ปูนซีเมนต์เอเชีย จำกัด (มหาชน)
Asia Cement
Public Company Limited

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

ขอบเขต:	บริษัท ปูนซีเมนต์เอเชีย จำกัด (มหาชน) และทุกบริษัทในเครือ
ผู้เขียน:	ฝ่ายกฎหมายและกำกับการปฏิบัติตามกฎระเบียบ
ผู้อนุมัติ:	นายซาลวาโตเร พาลาซโซ และนายนภดล รมยะรูป / กรรมการผู้จัดการ
จัดทำเมื่อ:	30 ตุลาคม 2569
เวอร์ชั่น:	2.0

สารบัญ

1. บทนำ 1
2. วัตถุประสงค์และความมุ่งมั่นของบริษัท 1
3. คำนิยาม 1
4. โครงสร้างการกำกับดูแลและผู้รับผิดชอบ 2
5. ข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวม และกลุ่มเจ้าของข้อมูล 3
6. ฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล 4
7. การขอความยินยอม (Consent Management) 5
8. สิทธิของเจ้าของข้อมูลส่วนบุคคล 5
9. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention) 6
10. มาตรการรักษาความมั่นคงปลอดภัย (Security Measures) 6
11. การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Response) 6
12. การประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment / DPIA) 6
13. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer) 7
14. การทบทวนนโยบาย (Policy Review) 7
15. ช่องทางติดต่อเรื่องการคุ้มครองข้อมูลส่วนบุคคล 7
16. ประวัติการแก้ไข (Version History) 7

1. บทนำ

นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ("นโยบาย") ใช้บังคับกับบริษัท ปูนซีเมนต์เอเซีย จำกัด (มหาชน) และบริษัทในเครือ ได้แก่ บริษัท เอเซีย ผลิตภัณฑ์ซีเมนต์ จำกัด บริษัท ชลประทานซีเมนต์ จำกัด (มหาชน) บริษัท เอเซีย ซีเมนต์ เอ็นเนอจี คอนเซอร์เวชั่น จำกัด และบริษัท ชลประทานคอนกรีต จำกัด (รวมเรียกว่า "บริษัท") โดยกำหนดหลักการ แนวปฏิบัติ และความรับผิดชอบในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของพนักงาน ผู้สมัครงาน ลูกค้า คู่ค้า ผู้รับเหมา ผู้มาติดต่อ และบุคคลที่เกี่ยวข้อง ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง ทั้งนี้ รายละเอียดการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลที่ต้องแจ้งให้เจ้าของข้อมูลทราบ ให้เป็นไปตามประกาศความเป็นส่วนตัว (Privacy Notice) ที่บริษัทจัดทำแยกต่างหาก

2. วัตถุประสงค์และความมุ่งมั่นของบริษัท

2.1 เหตุผลและความจำเป็น

ความก้าวหน้าทางเทคโนโลยีทำให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลทำได้โดยง่าย และหากเกิดการละเมิดย่อมสร้างความเสียหายแก่เจ้าของข้อมูล บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจึงกำหนดนโยบายนี้เพื่อให้การดำเนินงานของบริษัทสอดคล้องกับกฎหมาย และคุ้มครองสิทธิของเจ้าของข้อมูลอย่างเหมาะสม

2.2 หลักการพื้นฐาน 7 ประการ

บริษัทและพนักงานทุกคนต้องยึดถือหลักการพื้นฐานดังต่อไปนี้ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

(1) หลักความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส (Lawfulness, Fairness and Transparency) - เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลโดยมีฐานกฎหมายรองรับ ด้วยวิธีที่เป็นธรรม และแจ้งให้เจ้าของข้อมูลทราบอย่างชัดเจน

(2) การจำกัดวัตถุประสงค์ (Purpose Limitation) - ใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น

(3) การเก็บรวบรวมข้อมูลเท่าที่จำเป็น (Data Minimization) – เก็บรวบรวมเฉพาะข้อมูลที่จำเป็นต่อวัตถุประสงค์

(4) ความถูกต้องของข้อมูล (Accuracy) - ดูแลให้ข้อมูลถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด

(5) การจำกัดระยะเวลาเก็บรักษา (Storage Limitation) - เก็บข้อมูลไม่นานเกินความจำเป็น

(6) ความมั่นคงปลอดภัยของข้อมูล (Security) - จัดให้มีมาตรการป้องกันข้อมูลที่เหมาะสม

(7) ความรับผิดชอบตรวจสอบได้ (Accountability) – บริษัทต้องสามารถแสดงให้เห็นว่าได้ปฏิบัติตามหลักการข้างต้น

3. คำนิยาม

"การประมวลผลข้อมูลส่วนบุคคล" หมายถึง การดำเนินการใดๆ กับข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการเก็บรวบรวม บันทึก จัดระบบ จัดเก็บ ปรับเปลี่ยน แก้ไข ค้นคืน ใช้ เปิดเผย ส่งต่อ เผยแพร่ จัดเรียง รวม จำกัด ลบ หรือทำลายข้อมูลส่วนบุคคล

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน เบอร์โทรศัพท์ อีเมล ที่อยู่ ที่อยู่ IP ภาพถ่ายหรือวิดีโอที่ระบุตัวบุคคลได้ (เช่น ภาพจากกล้องวงจรปิด) ข้อมูลตำแหน่งที่ตั้ง (GPS) และคุกกี้ (Cookies) ที่สามารถระบุตัวบุคคลได้

"ข้อมูลอ่อนไหว" หมายถึง ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในลักษณะเดียวกัน ตัวอย่างในบริบทของบริษัท ได้แก่ ผลตรวจสุขภาพ เวชระเบียน ข้อมูลลายนิ้วมือหรือภาพสแกนใบหน้าที่ใช้เข้าออกพื้นที่สถานประกอบกิจการ ประวัติอาชญากรรมจากการตรวจสอบประวัติก่อนเข้าทำงาน (Background Check) และข้อมูลสหภาพแรงงาน

"ผู้ควบคุมข้อมูลส่วนบุคคล" หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

"ผู้ประมวลผลข้อมูลส่วนบุคคล" หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

"เจ้าของข้อมูลส่วนบุคคล" หมายถึง บุคคลธรรมดาซึ่งเป็นผู้ที่ข้อมูลส่วนบุคคลนั้นระบุถึง เช่น พนักงาน ผู้สมัครงาน ลูกค้า คู่ค้า ผู้รับเหมา ผู้มาติดต่อ และผู้เข้าร่วมกิจกรรมของบริษัท

"ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล" (Privacy Lead) หมายถึง ผู้ที่บริษัทแต่งตั้งให้ทำหน้าที่ดูแลให้คำปรึกษา และประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร ตามที่กำหนดไว้ในข้อ 4 ของนโยบายนี้

"เหตุการละเมิดข้อมูลส่วนบุคคล" หมายถึง เหตุการณ์ที่ข้อมูลส่วนบุคคลสูญหาย ถูกเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยโดยปราศจากอำนาจหรือโดยมิชอบ

4. โครงสร้างการกำกับดูแลและผู้รับผิดชอบ

4.1 ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Lead)

บริษัทแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล โดยมีหน้าที่ดังนี้

(1) ให้คำแนะนำแก่ฝ่ายต่างๆ เกี่ยวกับการปฏิบัติตามนโยบายนี้และกฎหมายที่เกี่ยวข้อง

(2) ตรวจสอบและติดตามการปฏิบัติตามนโยบายและกระบวนการภายในที่เกี่ยวข้อง

(3) ประสานงานกรณีมีปัญหาหรือข้อสงสัยเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(4) เป็นผู้ประสานงานหลักในกรณีเกิดเหตุการละเมิดข้อมูลส่วนบุคคลหรือมีข้อร้องเรียน

(5) ทบทวนและปรับปรุงนโยบายและเอกสารที่เกี่ยวข้องเป็นระยะ

4.2 ผู้รับผิดชอบข้อมูลส่วนบุคคลประจำหน่วยงาน

ผู้รับผิดชอบข้อมูลส่วนบุคคลประจำหน่วยงานมีหน้าที่กำกับดูแลให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในความรับผิดชอบของหน่วยงานเป็นไปตามนโยบายฉบับนี้ รวมทั้งประสานงานกับผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลตามความเหมาะสม

4.3 หน้าที่ของพนักงาน

พนักงานทุกคนต้องปฏิบัติตามนโยบายนี้ เข้าถึงและใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อการปฏิบัติงาน และรายงานเหตุการละเมิดหรือข้อสงสัยเกี่ยวกับความปลอดภัยของข้อมูลต่อผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลหรือผู้บังคับบัญชาทันที ทั้งนี้ การไม่ปฏิบัติตามนโยบายนี้อาจถูกพิจารณาโทษทางวินัยตามข้อบังคับเกี่ยวกับการทำงานของบริษัท

5. ข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวม และกลุ่มเจ้าของข้อมูล

บริษัทเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของกลุ่มเจ้าของข้อมูลหลักดังต่อไปนี้ โดยรายละเอียดของแต่ละกลุ่มให้เป็นไปตามประกาศความเป็นส่วนตัวที่เกี่ยวข้อง

5.1 กลุ่มพนักงานและผู้สมัครงาน

หมวดข้อมูล	ตัวอย่างข้อมูล
ข้อมูลที่เปิดเผยเป็นการภายใน	ชื่อ-นามสกุล, เลขประจำตัวพนักงาน, แผนก, ตำแหน่ง, สถานภาพการจ้างงาน, อีเมลบริษัท, เบอร์โทรศัพท์มือถือที่ใช้ในการทำงาน
ข้อมูลพื้นฐาน	ชื่อ, ที่อยู่, อายุ, วันเดือนปีเกิด, เพศ, หมายเลขโทรศัพท์, อีเมล, ภาพถ่ายหน้าตรง, สัญชาติ, สถานภาพการสมรส, สถานภาพทางทหาร (สำหรับผู้ชาย)
ข้อมูลการจ่ายค่าตอบแทน	การกำหนดรายได้รายปีและรายเดือน, เงินเดือนและโบนัส, บัญชีธนาคาร, หมายเลขเช็ค, บัตรเดบิต/เครดิต, ประวัติธุรกรรมทางการเงิน, ภาษีหัก ณ ที่จ่าย
ข้อมูลทรัพยากรบุคคล	ผลการประเมินการปฏิบัติงาน, ประวัติการศึกษา, คุณสมบัติ/ใบอนุญาต, วีซ่าและใบอนุญาตทำงานสำหรับชาวต่างชาติ, ประสบการณ์ทำงาน, การลงโทษทางวินัย/คำชม, ประวัติการอบรม, สิทธิประโยชน์และสวัสดิการ, ข้อมูลประกันสังคม, กองทุนสำรองเลี้ยงชีพ, ภาษีเงินได้บุคคลธรรมดา
ข้อมูลครอบครัวและญาติ	โครงสร้างครอบครัว, ผู้อยู่ในความอุปการะ, รายละเอียดผู้ติดต่อกรณีฉุกเฉิน

ข้อมูลอ่อนไหว (Sensitive Data) ของกลุ่มนี้ ได้แก่ เชื้อชาติ ศาสนา ภาวะสุขภาพ เวชระเบียน ความบกพร่องทางร่างกายหรือจิตใจ ผลการตรวจสุขภาพ ประวัติอาชญากรรมจากการตรวจสอบประวัติก่อนเข้าทำงาน และข้อมูลชีวภาพ (Biometric) เช่น ลายนิ้วมือหรือภาพสแกนใบหน้าที่ใช้สำหรับการเข้าออกพื้นที่สถานประกอบกิจการ ซึ่งการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลประเภทนี้ต้องเป็นไปตามข้อ 6.2

5.2 กลุ่มลูกค้า คู่ค้า และผู้รับเหมา

ข้อมูลติดต่อ (ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล) ข้อมูลบัญชีและธุรกรรมทางการเงิน ข้อมูลใบเสนอราคาและสัญญา และข้อมูลของกรรมการหรือตัวแทนของลูกค้า/คู่ค้าที่เป็นนิติบุคคล

5.3 กลุ่มผู้มาติดต่อ (Visitor)

ภาพจากกล้องวงจรปิด (CCTV) และข้อมูลจากการลงทะเบียนหรือแลกบัตรประจำตัวก่อนเข้าพื้นที่ (รายละเอียดตามประกาศความเป็นส่วนตัวสำหรับการใช้กล้องโทรทัศน์วงจรปิด (CCTV) ของบริษัท)

5.4 กลุ่มผู้ใช้เว็บไซต์และผู้เข้าร่วมกิจกรรมทางการตลาด

ข้อมูลการเข้าชมเว็บไซต์ คุกกี้ (Cookies) และภาพถ่ายหรือวิดีโอที่บันทึกในงานกิจกรรมหรือการสื่อสารทางการตลาดของบริษัท

5.5 กลุ่มกรรมการ ผู้ถือหุ้น และตัวแทนนิติบุคคล

เนื่องจากบริษัทเป็นบริษัทมหาชน บริษัทอาจเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของกรรมการ ผู้ถือหุ้น และตัวแทนของลูกค้าหรือคู่ค้าที่เป็นนิติบุคคล เพื่อการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับบริษัทมหาชนและการกำกับดูแลกิจการ

6. ฐานทางกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล

6.1 หลักการทั่วไป

บริษัทจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเมื่อมีฐานทางกฎหมายรองรับ โดยจะระบุฐานที่เหมาะสมสำหรับแต่ละกิจกรรมก่อนดำเนินการ ฐานทางกฎหมายที่บริษัทอาจใช้ ได้แก่

(1) ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)

เมื่อบริษัทมีภาระผูกพันตามกฎหมายที่ต้องปฏิบัติ เช่น กฎหมายแรงงาน กฎหมายภาษี หรือกฎหมายที่เกี่ยวข้องกับบริษัทมหาชน

(2) ฐานประโยชน์สำคัญต่อชีวิต (Vital Interests)

เมื่อจำเป็นต้องป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลที่อาจเกิดขึ้น

(3) ฐานสัญญา (Contract)

เมื่อเจ้าของข้อมูลเป็นคู่สัญญากับบริษัท หรือเพื่อดำเนินการตามคำขอของเจ้าของข้อมูลก่อนเข้าทำสัญญา เช่น การจ้างงาน หรือสัญญาซื้อขาย

(4) ฐานภารกิจเพื่อประโยชน์สาธารณะ (Public Interest)

เมื่อจำเป็นต้องปฏิบัติภารกิจเพื่อประโยชน์สาธารณะ หรือใช้อำนาจรัฐที่ได้รับมอบให้แก่บริษัท

(5) ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)

เมื่อจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัทหรือบุคคลอื่น ซึ่งไม่ขัดกับสิทธิขั้นพื้นฐานของเจ้าของข้อมูล เช่น การใช้กล้องวงจรปิดเพื่อรักษาความปลอดภัย

(6) ฐานการจัดทำเอกสารประวัติศาสตร์ วิจัยและสถิติ (Research/Statistics)

เมื่อจำเป็นเพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือเพื่อการศึกษาวิจัยหรือการจัดทำสถิติ

(7) ฐานความยินยอม (Consent)

เมื่อเจ้าของข้อมูลให้ความยินยอมให้บริษัทเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่แจ้งไว้ เช่น การส่งข้อมูลข่าวสารทางการตลาด หรือการใช้ภาพถ่ายเพื่อการประชาสัมพันธ์

6.2 ฐานทางกฎหมายสำหรับข้อมูลอ่อนไหว

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลอ่อนไหวต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล เว้นแต่เข้าข้อยกเว้นตามกฎหมาย เช่น เพื่อป้องกันอันตรายต่อชีวิตเมื่อเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ เพื่อการใช้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมายด้านเวชศาสตร์ สาธารณสุข หรือการคุ้มครองแรงงาน ทั้งนี้ บริษัทจะจำกัดการเข้าถึงข้อมูลอ่อนไหวเฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง และจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามข้อ 10

7. การขอความยินยอม (Consent Management)

7.1 หลักเกณฑ์การขอความยินยอมที่ถูกต้อง

ในกรณีที่บริษัทอาศัยความยินยอมเป็นฐานในการประมวลผลข้อมูลส่วนบุคคล บริษัทจะขอความยินยอมโดยชัดแจ้ง แจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างชัดเจน แยกจากข้อความอื่น และใช้ภาษาที่เข้าใจง่าย ทั้งนี้ บริษัทจะไม่กำหนดให้เจ้าของข้อมูลต้องให้ความยินยอมเกินกว่าที่จำเป็นต่อวัตถุประสงค์หรือการให้บริการนั้น

7.2 การถอนความยินยอม

เจ้าของข้อมูลส่วนบุคคลมีสิทธิถอนความยินยอมได้ตลอดเวลา ด้วยวิธีการเดียวกับหรือใกล้เคียงกับการให้ความยินยอม เว้นแต่มีข้อจำกัดตามกฎหมายหรือสัญญา ทั้งนี้ บริษัทจะแจ้งผลกระทบจากการถอนความยินยอมให้เจ้าของข้อมูลทราบ (หากมี) ก่อนดำเนินการตามคำขอ

7.3 กรณีผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ

การขอความยินยอมให้ดำเนินการดังนี้

(1) ผู้เยาว์: ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองตามเงื่อนไขที่กฎหมายกำหนด

(2) คนไร้ความสามารถ: ขอความยินยอมจากผู้อนุบาล

(3) คนเสมือนไร้ความสามารถ: ขอความยินยอมจากผู้พิทักษ์

8. สิทธิของเจ้าของข้อมูลส่วนบุคคล

บริษัทเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย และจะพิจารณาดำเนินการตามคำขอใช้สิทธิที่ยื่นผ่านช่องทางตามข้อ 15 โดยเจ้าของข้อมูลหรือผู้มีอำนาจกระทำการแทนตามข้อ 7.3 อาจใช้สิทธิดังต่อไปนี้

(1) สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่ไม่ได้ให้ความยินยอม

(2) สิทธิขอรับหรือโอนข้อมูลส่วนบุคคล (Data Portability) ในกรณีที่ข้อมูลอยู่ในรูปแบบที่อ่านหรือใช้งานได้โดยระบบอัตโนมัติ

(3) สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(4) สิทธิขอให้ลบหรือทำลายข้อมูล หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้

(5) สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล

(6) สิทธิขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด

(7) สิทธิถอนความยินยอม

(8) สิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ ในกรณีที่บริษัทหรือผู้ประมวลผลข้อมูลของบริษัทฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

9. ระยะเวลาการเก็บรักษาข้อมูล (Data Retention)

บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลไว้เท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือตามระยะเวลาที่กฎหมายกำหนด โดยทั่วไปข้อมูลส่วนบุคคลจะถูกเก็บรักษาไว้ไม่เกิน 10 ปี เว้นแต่กฎหมายกำหนดหรืออนุญาตให้เก็บรักษาไว้เป็นระยะเวลานานกว่า เมื่อพ้นระยะเวลาการเก็บรักษาหรือหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล บริษัทจะดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ตามความเหมาะสม ทั้งนี้ บริษัทอาจเก็บรักษาข้อมูลไว้ต่อไปได้หากมีเหตุอันชอบด้วยกฎหมาย

10. มาตรการรักษาความมั่นคงปลอดภัย (Security Measures)

บริษัทจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การแก้ไขเปลี่ยนแปลง หรือการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ และทบทวนหรือปรับปรุงมาตรการดังกล่าวตามความจำเป็นหรือเมื่อเทคโนโลยีหรือความเสี่ยงที่เกี่ยวข้องเปลี่ยนแปลงไป ในกรณีที่บริษัทให้ผู้ให้บริการภายนอกประมวลผลข้อมูลส่วนบุคคลแทนบริษัท บริษัทจะกำหนดหน้าที่ในการรักษาความลับและความมั่นคงปลอดภัยของข้อมูลไว้ในสัญญาหรือข้อตกลงกับผู้ให้บริการดังกล่าว

11. การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล (Data Breach Response)

บริษัทกำหนดให้มีการรายงานและบริหารจัดการเหตุการละเมิดข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อจำกัดผลกระทบและป้องกันการเกิดซ้ำ โดยเหตุการละเมิดอาจรวมถึงการส่งข้อมูลไปยังผู้รับที่ไม่ถูกต้อง การสูญหายของเอกสารหรืออุปกรณ์ การโจมตีทางไซเบอร์ การรั่วไหลของข้อมูลจากผู้ให้บริการภายนอก การนำข้อมูลออกไปโดยไม่ได้รับอนุญาต หรือการกำหนดสิทธิการเข้าถึงข้อมูลที่ไม่เหมาะสม

ผู้พบเหตุต้องแจ้งเหตุผ่านช่องทางที่บริษัทกำหนดโดยทันที เพื่อให้มีการประเมินความเสี่ยง ควบคุมและแก้ไขความเสียหาย บันทึกเหตุการณ์ และทบทวนมาตรการป้องกัน หากเหตุการละเมิดมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล บริษัทจะแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุ และหากมีความเสี่ยงสูง บริษัทจะแจ้งเหตุพร้อมแนวทางการเยียวยาให้เจ้าของข้อมูลทราบโดยไม่ชักช้าด้วย

12. การประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment / DPIA)

กิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล เช่น กิจกรรมที่เกี่ยวข้องกับข้อมูลชีวภาพ การติดตามพฤติกรรมหรือตำแหน่งที่ตั้ง การใช้ระบบปัญญาประดิษฐ์ (AI) หรือกิจกรรมอื่นที่มีความเสี่ยงในทำนองเดียวกัน ต้องได้รับการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล

(Data Protection Impact Assessment / DPIA) ก่อนเริ่มดำเนินการ โดยผู้รับผิดชอบข้อมูลส่วนบุคคลประจำหน่วยงาน เป็นผู้จัดทำและเสนอให้ผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลพิจารณา

13. การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross-Border Data Transfer)

บริษัทจะส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ เมื่อประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หรือบริษัทได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมตามที่กฎหมายกำหนด หรือเป็นกรณีที่เข้าข้อยกเว้นตามกฎหมาย เช่น ได้รับความยินยอมจากเจ้าของข้อมูล เป็นการปฏิบัติตามกฎหมายหรือสัญญา เพื่อประโยชน์ของเจ้าของข้อมูล เพื่อป้องกันอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ หรือเพื่อประโยชน์สาธารณะที่สำคัญ

14. การทบทวนนโยบาย (Policy Review)

ฝ่ายกฎหมายและกำกับการปฏิบัติตามกฎระเบียบเป็นผู้รับผิดชอบทบทวนนโยบายนี้อย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อกฎหมายที่เกี่ยวข้องหรือกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของบริษัท และเสนอการปรับปรุงต่อกรรมการผู้จัดการเพื่อพิจารณาอนุมัติ

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 30 ตุลาคม 2569 เป็นต้นไป

15. ช่องทางติดต่อเรื่องการคุ้มครองข้อมูลส่วนบุคคล

บริษัทกำหนดให้อีเมล LegalandCompliance@acc.co.th เป็นช่องทางกลางสำหรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การสอบถามข้อมูล และการแจ้งเหตุหรือข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยบริษัทจะตอบกลับคำร้องหรือข้อสอบถามภายใน 7 วันทำการ หรือไม่เกิน 14 วันทำการ แล้วแต่กรณี และจะดำเนินการตามคำขอใช้สิทธิภายในระยะเวลาที่กฎหมายกำหนด

16. ประวัติการแก้ไข (Version History)

วันที่	เวอร์ชั่น	ผู้เขียน	รายละเอียดการแก้ไข
มิถุนายน 2565	1.0	ฝ่ายกฎหมาย	จัดทำเอกสารฉบับใหม่
ตุลาคม 2569	2.0	ฝ่ายกฎหมาย	เอกสารฉบับปรับปรุง

อนุมัติโดย: กรรมการผู้จัดการ

Salvatore Palazzo

(นายซาลวาโตเร พาลาซโซ) (นายนภดล รมยะรูป)