

บริษัท นาทasha ครีเอชั่นส์ จำกัด กำหนดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อคุ้มครองความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล ป้องกันภัยคุกคาม และให้ระบบสำคัญสามารถกู้คืนได้ตามแผนความต่อเนื่องทางธุรกิจ

ใช้กับผู้บริหาร พนักงาน ผู้รับเหมา ผู้ให้บริการ และบุคคลที่เข้าถึงระบบหรือข้อมูลของบริษัทฯ ครอบคลุมสำนักงาน โรงงาน การทำงานนอกสถานที่ อุปกรณ์ส่วนตัวที่ได้รับอนุญาต บริการคลาวด์ และข้อมูลทุกสื่อ ทั้งข้อมูลลูกค้า คู่ค้า บุคลากร การผลิต บัญชี แบบงาน ข้อมูลชนิดและแหล่งที่มาของวัสดุ และเอกสารตรวจสอบย้อนกลับ

นโยบายนี้สนับสนุนระบบบริหารและการควบคุมหลักฐานตามมาตรฐานของสภาอัญมณีและเครื่องประดับที่มีความรับผิดชอบ (Responsible Jewellery Council: RJC) ได้แก่ มาตรฐานหลักปฏิบัติในการดำเนินธุรกิจอย่างรับผิดชอบ (Code of Practices Standard 2024: COP 2024) มาตรฐานห่วงโซ่การควบคุมและตรวจสอบย้อนกลับ (Chain of Custody Standard 2024: COC 2024) และมาตรฐานวัสดุที่ผลิตในห้องปฏิบัติการ (Laboratory Grown Materials Standard 2025: LGMS 2025) ตามกิจกรรมและขอบเขตที่เกี่ยวข้อง การกำหนดมาตรการทางเทคนิคเป็นหน้าที่ของบริษัทฯ ตามความเสี่ยงและกฎหมาย มิใช่การรับรองว่าระบบได้รับการรับรองมาตรฐานใดโดยอัตโนมัติ

กฎหมายและหลักการที่ใช้บังคับ

บริษัทฯ ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E. 2562 (2019): PDPA) และประกาศที่เกี่ยวข้อง พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และที่แก้ไขเพิ่มเติม และพระราชบัญญัติความลับทางการค้า พ.ศ. 2545 และที่แก้ไขเพิ่มเติม

การปฏิบัติต่อพนักงานให้เป็นไปตามพระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541 และที่แก้ไขเพิ่มเติม ส่วนหน้าที่เฉพาะภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้ประเมินตาม

สถานะและกิจกรรมที่กฎหมายกำหนด ห้ามถือว่าบริษัท เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศโดยไม่มีข้อเท็จจริงรองรับ ผู้รับผิดชอบต้องติดตามกฎหมายและคำสั่งที่มีผลใช้บังคับ และยกระดับมาตรการเมื่อกฎหมายกำหนดเข้มงวดกว่านโยบายนี้

ให้ติดตามกฎหมายและข้อกำหนดที่ใช้กับกิจกรรมของบริษัท กฎหมายหรือประกาศที่มีผลภายหลัง ให้ใช้ตั้งแต่วันที่กฎหมายนั้นมีผล รายการกฎหมายลำดับรองที่เกี่ยวข้องระบุไว้ท้ายเอกสาร

หมวดที่ 1: การพิสูจน์ตัวตนและการบริหารสิทธิ์

- 1.1 ผู้ใช้งานต้องใช้บัญชีเฉพาะบุคคล ห้ามเปิดเผยรหัสผ่านหรือใช้บัญชีร่วมกัน บัญชีระบบหรือบัญชีบริการ ต้องมีเจ้าของ ผู้อนุมัติ และการควบคุมที่ตรวจสอบผู้ปฏิบัติงานได้ แยกบัญชีผู้ดูแลระบบออกจากบัญชีใช้งานประจำ
- 1.2 กำหนดสิทธิ์เท่าที่จำเป็นต่อหน้าที่ โดยเจ้าของข้อมูลหรือหัวหน้างานอนุมัติเป็นหลักฐาน ทบทวนสิทธิ์อย่างน้อยทุก 6 เดือน และเมื่อเปลี่ยนหน้าที่ ระบุสิทธิ์ทันทีเมื่อพ้นสภาพหรือพบความเสี่ยง ส่วนสิทธิ์ชั่วคราว ต้องมีวันสิ้นสุด
- 1.3 เปลี่ยนรหัสผ่านเริ่มต้นก่อนใช้งาน ใช้รหัสผ่านหรือวลีรหัสผ่านที่คาดเดายากและไม่ซ้ำกับบริการอื่น ผู้ดูแลระบบต้องกำหนดความยาวขั้นต่ำ การป้องกันการเดารหัส และการกู้คืนบัญชีไว้ในมาตรฐานการตั้งค่าระบบ ใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับบัญชีผู้ดูแลระบบ บัญชีสำคัญ และการเข้าถึงจากภายนอก ระบบที่ยังไม่รองรับต้องมีมาตรการทดแทน ผู้อนุมัติ และกำหนดแก้ไข เปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่าถูกเปิดเผย
- 1.4 ล็อกหน้าจอเมื่อไม่อยู่หน้าเครื่อง และออกจากระบบเมื่อเสร็จงาน ระบบต้องบันทึกการเข้าถึงและเหตุผิดปกติตามความเสี่ยง ผู้ใช้งานต้องแจ้งเหตุบัญชีถูกใช้โดยมิชอบทันที การพิจารณาความรับผิดชอบอาศัยข้อเท็จจริง ไม่ถือว่าผู้ถือบัญชีเป็นผู้กระทำผิดโดยอัตโนมัติ

หมวดที่ 2: การบริหารทรัพยากรสารสนเทศ

- 2.1 ผู้ดูแลระบบจัดทำทะเบียนอุปกรณ์ ซอฟต์แวร์ ระบบงาน ฐานข้อมูล และผู้ให้บริการ ระบุเจ้าของ สถานที่ ระดับความสำคัญ การเชื่อมโยง และผู้รับผิดชอบ ปรับปรุงทะเบียนเมื่อมีการติดตั้ง เปลี่ยนแปลง ย้าย หรือ เลิกใช้
- 2.2 ทะเบียนทรัพยากรสารสนเทศต้องครอบคลุมเครื่องแม่ข่าย ฐานข้อมูล ระบบวางแผนทรัพยากรองค์กร (Enterprise Resource Planning: ERP) ระบบงานโรงงาน ฐานข้อมูลสำรอง ไฟล์ออกแบบด้วย คอมพิวเตอร์ (Computer-Aided Design: CAD) และอีเมล ให้ผู้ดูแลระบบควบคุมรายชื่อเครื่องแม่ข่าย และระบบจริง หน้าที่ สถานะ เจ้าของระบบ และอายุการสนับสนุนไว้ในทะเบียนภายในที่จำกัดสิทธิ์เข้าถึง พร้อมทบทวนเมื่อเปลี่ยนแปลง
- 2.3 ใช้อุปกรณ์เพื่อวัตถุประสงค์ทางธุรกิจที่ได้รับอนุญาต การนำออกนอกสถานที่ ให้ยืม ติดตั้งอุปกรณ์ส่วนตัว หรือเชื่อมต่อสื่อบันทึกภายนอกต้องผ่านการอนุมัติและมาตรการป้องกันข้อมูล ห้ามเปลี่ยนแปลง ส่วนประกอบหรือการตั้งค่าความปลอดภัยเอง
- 2.4 เมื่ออุปกรณ์สูญหายหรือเสียหาย ให้แจ้งและเก็บข้อเท็จจริงเพื่อสอบสวนอย่างเป็นธรรม การดำเนินการ ทางวินัยหรือเรียกค่าเสียหายต้องเป็นไปตามกฎหมายและข้อบังคับที่ขอบด้วยกฎหมาย ไม่กำหนดการหัก ค่าจ้างหรือความรับผิดชอบเต็มจำนวนโดยอัตโนมัติ ก่อนโอนหรือกำจัดอุปกรณ์ต้องลบข้อมูลอย่างปลอดภัย และบันทึกผล

หมวดที่ 3: การจัดการข้อมูลและหลักฐาน

- 3.1 เจ้าของข้อมูลต้องกำหนดวัตถุประสงค์ ชั้นความลับ ผู้เข้าถึง และอายุข้อมูล โดยใช้ชั้นข้อมูลสาธารณะ ข้อมูลภายใน และข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลคู่ค้า และแบบงานที่ยังไม่เผยแพร่ต้องจำกัดสิทธิ์ตาม หน้าที่ ข้อมูลส่วนบุคคลอ่อนไหวต้องมีการควบคุมเพิ่มเติม สิทธิในข้อมูลหรือทรัพย์สินทางปัญญาเป็นไป ตามกฎหมายและสัญญา การเก็บในอุปกรณ์บริษัท ไม่ทำให้สิทธิของเจ้าของเดิมโอนมายังบริษัท

- 3.2 ห้ามเข้าถึง แก้ไข ทำสำเนา ส่งต่อ หรือทำลายข้อมูลเกินสิทธิ์ ต้องรักษาความถูกต้องและความลับใช้งาน ข้อมูลส่วนบุคคลให้ปฏิบัติตามหมวดที่ 11 ถึง 13 ของนโยบายนี้ การเปิดเผยแก่ลูกค้า ผู้ตรวจประเมิน หรือหน่วยงานภายนอกต้องมีฐานกฎหมาย เปิดเผยเท่าที่จำเป็น และปกปิดข้อมูลที่ไม่เกี่ยวข้อง
- 3.3 เอกสารการรู้จักคู่ค้า (Know Your Counterparty: KYC) ข้อมูลลึกลับ ชนิดวัสดุ น้ำหนักหรือจำนวน เอกสารห่วงโซ่การควบคุมและตรวจสอบย้อนกลับ (Chain of Custody: COC) ผลทดสอบ และหลักฐานคำกล่าวอ้างต้องเชื่อมโยงกัน ตรวจสอบผู้สร้างหรือผู้แก้ไขได้ และควบคุมรุ่นเอกสาร ห้ามแก้ไขย้อนหลังโดยไม่เก็บร่องรอยและการอนุมัติ
- 3.4 เก็บหลักฐานการปฏิบัติตามมาตรฐานของสภาอณูมณีและเครื่องประดับที่มีความรับผิดชอบอย่างน้อย 5 ปี หรือนานกว่าตามกฎหมายหรือข้อผูกพันที่บังคับเก็บเฉพาะข้อมูลส่วนบุคคลที่จำเป็นต่อหลักฐานนั้น พร้อมระบุฐานกฎหมายและจุดเริ่มนับอายุในตารางอายุเอกสาร ห้ามใช้อายุ 5 ปีเป็นเหตุให้เก็บข้อมูลส่วนบุคคลทุกประเภท เมื่อครบกำหนดให้ตรวจคัด การสอบสวน และคำสั่งคงสภาพหลักฐานก่อนทำลาย พร้อมบันทึกผล

หมวดที่ 4: การสำรองข้อมูลและการกู้คืน

- 4.1 เจ้าของระบบและผู้ดูแลระบบต้องจัดทำแผนสำรองและกู้คืน ระบุความถี่ อายุสำเนา สถานที่ ผู้รับผิดชอบ และการตรวจผล ระบบธุรกรรมสำคัญต้องสำรองอย่างน้อยทุกวันทำการ หรือถี่กว่านั้นตามช่วงข้อมูลสูญหายที่ยอมรับได้ (Recovery Point Objective: RPO) และต้องมีระยะเวลากู้คืนเป้าหมาย (Recovery Time Objective: RTO) ที่สอดคล้องกับแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และได้รับอนุมัติจากผู้จัดการทั่วไปหรือคณะกรรมการที่ได้รับมอบหมาย
- 4.2 จัดให้มีสำเนาที่แยกจากระบบใช้งานจริง และมีสำเนาออกสถานที่หรือแยกจากเครือข่ายตามความเสี่ยงจำกัดสิทธิ์และเข้ารหัสข้อมูลสำคัญตามความเหมาะสม ระบบจัดเรียงดิสก์เพื่อความทนทานต่อความเสียหาย (Redundant Array of Independent Disks: RAID) เป็นมาตรการความพร้อมของอุปกรณ์ ไม่ใช่แทนการสำรองข้อมูล

- 4.3 ผู้ดูแลระบบตรวจสอบผลการสำรองอย่างน้อยทุกวันทำการและทันทีเมื่อได้รับการแจ้งเตือนความล้มเหลว บันทึกการแก้ไขและผลการสำรองใหม่ การใช้โปรแกรม COBIAN BACKUP หรือระบบอื่นต้องมีการตั้งค่าที่อนุมัติและตรวจสอบว่าสำรองข้อมูลครบ รวมทั้งธุรกรรม เอกสารห่วงโซ่การควบคุมและตรวจสอบย้อนกลับ ผลทดสอบ และค่าระบบ ต้องกำหนดอายุข้อมูลสำรองและวิธีลบข้อมูลส่วนบุคคลที่สอดคล้องกับหมวดที่ 11 และ 12
- 4.4 ทดสอบกู้คืนระบบสำคัญตามรอบที่กำหนด อย่างน้อยปีละหนึ่งครั้งและหลังการเปลี่ยนแปลงสำคัญ บันทึกผล ระยะเวลากู้คืน ความครบถ้วนของข้อมูล และข้อบกพร่อง ก่อนเปิดใช้งานต้องตรวจสอบความถูกต้องของยอดวัสดุและธุรกรรมที่เกิดระหว่างระบบหยุดทำงาน

หมวดที่ 5: ซอฟต์แวร์ ลิขสิทธิ์ และผู้ให้บริการ

- 5.1 ใช้ซอฟต์แวร์และข้อมูลตามสิทธิการใช้งานที่ถูกต้อง จัดเก็บทะเบียนใบอนุญาตและหลักฐานการจัดการ ติดตั้ง ถอดถอน หรือแก้ไขซอฟต์แวร์ต้องได้รับอนุมัติจากผู้ดูแลระบบและเจ้าของระบบตามความเหมาะสม
- 5.2 กำหนดสิทธิในโปรแกรมที่พัฒนาขึ้นตามกฎหมายและสัญญา รักษาซอร์สโค้ด เอกสาร และข้อมูลคู่ค้า ห้ามเผยแพร่หรือใช้ภายนอกเกินขอบเขตสิทธิ การประเมินการละเมิดต้องตรวจสอบข้อเท็จจริงและกระบวนการจัดหาของบริษัทฯ ร่วมด้วย
- 5.3 ผู้ให้บริการเทคโนโลยีสารสนเทศและคลาวด์ต้องผ่านการประเมินก่อนใช้บริการและเมื่อเปลี่ยนแปลงสำคัญ ข้อตกลงต้องกำหนดความลับ มาตรการรักษาความปลอดภัย การเข้าถึง การแจ้งเหตุ ความต่อเนื่อง การคืนหรือลบข้อมูล สิทธิการตรวจสอบ และการใช้ผู้รับจ้างช่วง หากประมวลผลข้อมูลส่วนบุคคลแทนบริษัทฯ ต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ตามมาตรา 40 ก่อนเริ่มดำเนินการ และตรวจเงื่อนไขการส่งข้อมูลต่างประเทศด้วย

หมวดที่ 6: การป้องกันมัลแวร์และการรับมือเหตุการณ์

- 6.1 ติดตั้งและปรับปรุงระบบป้องกันมัลแวร์บนอุปกรณ์ที่รองรับ จัดการแพตช์ ช่องโหว่ และระบบที่หมดการสนับสนุนตามระดับความเสี่ยง ซ้ายกเว้นต้องมีผู้อนุมัติ มาตรการทดแทน และวันทบทวน ห้ามผู้ใช้ปิดหรือลบเครื่องมือป้องกันโดยพลการ
- 6.2 ตรวจไฟล์และสื่อบันทึกจากภายนอกก่อนใช้งาน ฝึกอบรมเรื่องอีเมลหลอกลวง มัลแวร์เรียกค่าไถ่ และการรายงานเหตุ เมื่อพบความผิดปกติให้หยุดกิจกรรมที่เสี่ยงและแจ้งผู้ดูแลระบบหรือผู้บังคับบัญชาทันที
- 6.3 ผู้ดูแลระบบประเมินเหตุ แยกระบบที่ได้รับผลกระทบโดยคำนึงถึงความปลอดภัย เก็บบันทึกและพยานหลักฐาน หาสาเหตุ กำจัดภัย และกู้คืนโดยได้รับอนุมัติ ห้ามลบหลักฐานหรือสื่อสารข้อสรุปที่ยังไม่ยืนยัน
- 6.4 ผู้จัดการทั่วไปหรือผู้ได้รับมอบหมายประสานคณะกรรมการบริหารความต่อเนื่องทางธุรกิจและอนุมัติการสื่อสารกับผู้เกี่ยวข้อง กรณีเกี่ยวข้องกับข้อมูลส่วนบุคคลต้องดำเนินการตามหมวดที่ 13 โดยทันที การรอผลสอบสวนหรือการอนุมัติภายในต้องไม่ทำให้พันกรอบเวลาแจ้งเหตุตามกฎหมาย บันทึกการตัดสินใจ การเยียวยา และมาตรการป้องกันการเกิดซ้ำ

หมวดที่ 7: เครือข่ายและเครื่องแม่ข่าย

- 7.1 จัดเก็บเครื่องแม่ข่ายและอุปกรณ์สำคัญในพื้นที่ควบคุม มีมาตรการด้านไฟฟ้า อัคคีภัย อุณหภูมิ และการเข้าออกตามความเสี่ยง บันทึกบุคคลภายนอกและการปฏิบัติงานที่กระทบระบบ
- 7.2 จัดทำแผนผังเครือข่ายและค่าควบคุม แยกเครือข่ายผู้มาเยือนออกจากระบบธุรกิจ แยกระบบการผลิตและระบบที่มีความเสี่ยงตามความจำเป็น ใช้ระบบกรองการสื่อสารเครือข่าย (Firewall) และการตรวจจับเหตุผิดปกติ ปิดบริการที่ไม่จำเป็น ควบคุมบัญชีผู้ดูแลอุปกรณ์ และสำรองค่าระบบก่อนเปลี่ยนแปลง
- 7.3 การเข้าถึงจากภายนอกต้องได้รับอนุมัติ มีเหตุจำเป็น ระยะเวลาชัดเจน และใช้ช่องทางที่ปลอดภัย พร้อมยืนยันตัวตนและบันทึกการใช้งาน ผู้ให้บริการต้องเข้าถึงเฉพาะงานที่ได้รับมอบหมายและยกเลิกสิทธิ์เมื่อเสร็จงาน

7.4 บันทึกการเข้าถึง การเปลี่ยนแปลง และเหตุผิดปกติตามอายุที่กำหนด รักษาความถูกต้องของเวลาและป้องกันการแก้ไข ให้ผู้ดูแลระบบร่วมกับผู้ประสานงานกฎหมายประเมินหน้าที่ในฐานะผู้ให้บริการตามมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม หากเข้าข่าย ต้องเก็บข้อมูลจราจรที่กำหนดไม่น้อยกว่า 90 วันนับแต่เข้าสู่ระบบ และข้อมูลระบุตัวผู้ใช้ไม่น้อยกว่า 90 วันนับแต่สิ้นสุดบริการ รวมถึงปฏิบัติตามคำสั่งเจ้าหน้าที่ที่ชอบด้วยกฎหมาย

หมวดที่ 8: อินเทอร์เน็ตและบริการออนไลน์

- 8.1 ใช้อินเทอร์เน็ตเพื่อกิจกรรมที่ได้รับอนุญาต ห้ามกระทำความผิดกฎหมาย ละเมิดสิทธิ หรือทำให้ระบบเสี่ยงหลักเสี่ยงการดาวน์โหลดไฟล์และติดตั้งส่วนขยายที่น่าเชื่อถือ และไม่ข้ามมาตรการควบคุมของบริษัทฯ
- 8.2 ห้ามเผยแพร่ข้อมูลลับ แบบงาน ข้อมูลส่วนบุคคล หรือข้อมูลลูกค้าผ่านสื่อสังคม บริการรับฝากไฟล์ เครื่องมือปัญญาประดิษฐ์ (Artificial Intelligence: AI) หรือบริการออนไลน์ภายนอก เว้นแต่ผ่านการอนุมัติและเงื่อนไขการคุ้มครองข้อมูลแล้ว
- 8.3 การเผยแพร่ข้อมูลผลิตภัณฑ์ แหล่งที่มา ความยั่งยืน หรือสถานะการรับรองของสภาอัญมณีและเครื่องประดับที่มีความรับผิดชอบ ต้องผ่านผู้รับผิดชอบตรวจสอบหลักฐาน วัสดุที่ผลิตในห้องปฏิบัติการ (Laboratory-grown) อย่างชัดเจน และไม่กล่าวอ้างห่วงโซ่การควบคุมและตรวจสอบย้อนกลับเกินวัสดุหรือกิจกรรมที่มีสิทธิและอยู่ในขอบเขตที่ได้รับการรับรอง

หมวดที่ 9: อีเมลและการรับส่งข้อมูล

- 9.1 ให้อีเมลธุรกิจที่ได้รับอนุญาต ตรวจสอบผู้รับและเอกสารแนบก่อนส่ง ข้อมูลสำคัญต้องใช้ช่องทางเข้ารหัสหรือวิธีคุ้มครองตามระดับความลับ ห้ามส่งรหัสผ่านร่วมกับไฟล์ที่รหัสนั้นใช้เปิดผ่านช่องทางเดียวกัน
- 9.2 ห้ามเปิดเผยรหัสผ่านบัญชีอีเมล การมอบหมายให้อ่านหรือดำเนินงานแทนต้องใช้สิทธิ์ที่ระบบรองรับและได้รับอนุมัติ ห้ามยืมบัญชีหรือใช้รหัสผ่านของผู้อื่น การเปลี่ยนข้อมูลบัญชีธนาคารหรือคำสั่งจ่ายเงินต้องยืนยันผ่านช่องทางที่เชื่อถือได้อีกช่องทางหนึ่ง

- 9.3 ห้ามเปิดลิงก์หรือเอกสารแนบที่สงสัย ให้รายงานผู้ดูแลระบบทันที จัดเก็บอีเมลที่เป็นหลักฐานธุรกรรมและหลักฐานตามมาตรฐานของสภาอณูมณีนีและเครื่องประดับที่มีความรับผิดชอบตามตารางอายุเอกสาร การส่งอีเมลการตลาดต้องมีฐานกฎหมายและช่องทางปฏิเสธรับที่ใช่ง่าย เมื่อพนักงานเปลี่ยนหน้าที่หรือพ้นสภาพให้ส่งมอบงานและปิดสิทธิ์โดยไม่เปิดเผยการติดต่อส่วนตัวเกินความจำเป็น

หมวดที่ 10: การพัฒนาระบบและการควบคุมการเปลี่ยนแปลง

- 10.1 การพัฒนาหรือปรับปรุงระบบต้องมีผู้รับผิดชอบและหลักฐานครบตั้งแต่วิเคราะห์ความต้องการ ออกแบบ พัฒนา ทดสอบ อนุมัติใช้ จัดทำคู่มือ และบำรุงรักษา ประเมินความมั่นคงปลอดภัย ความเป็นส่วนตัว และผลต่อการตรวจสอบย้อนกลับตั้งแต่การออกแบบ ตั้งค่าเริ่มต้นให้เก็บและเปิดเผยข้อมูลเท่าที่จำเป็น โครงการที่ใช้ข้อมูลอ่อนไหว การเฝ้าติดตาม หรือเทคโนโลยีใหม่ต้องประเมินผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) ตามเกณฑ์ความเสี่ยงของบริษัทฯ ก่อนใช้งาน
- 10.2 แยกสภาพแวดล้อมพัฒนา ทดสอบ และใช้งานจริง ควบคุมซอร์สโค้ดและรุ่นซอฟต์แวร์ ใช้ข้อมูลจำลองหรือข้อมูลที่ทำให้ไม่สามารถระบุตัวบุคคลได้ในการทดสอบ ข้อมูลที่เพียงแทนชื่อด้วยรหัสและยังเชื่อมโยงกลับได้ยังถือเป็นข้อมูลส่วนบุคคล การใช้ข้อมูลจริงต้องมีฐานกฎหมาย เหตุจำเป็น ผู้อนุมัติ สิทธิเฉพาะ และกำหนดลบหลังทดสอบ
- 10.3 ทดสอบการทำงาน สิทธิเข้าถึง การเก็บหลักฐาน การสำรอง และการย้อนกลับก่อนนำใช้ เจ้าของระบบ อนุมัติผลทดสอบและช่วงเปลี่ยนระบบ พร้อมแผนคืนสภาพเดิม การแก้ไขฉุกเฉินต้องบันทึกเหตุและบทวนการอนุมัติภายหลังโดยเร็ว

หมวดที่ 11: การคุ้มครองข้อมูลส่วนบุคคล

- 11.1 บริษัทฯ เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) สำหรับกิจกรรมที่บริษัทฯ กำหนด วัตถุประสงค์และวิธีการประมวลผลเอง และเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

11.2 ข้อมูลส่วนบุคคลหมายถึงข้อมูลเกี่ยวกับบุคคลธรรมดาที่ระบุตัวบุคคลได้โดยตรงหรือโดยอ้อม โดยไม่รวมข้อมูลผู้ถึงแก่กรรมโดยเฉพาะ เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือบุคคลที่ข้อมูลนั้นเกี่ยวข้องกับ การประมวลผลครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผย รวมทั้งจัดเก็บ ส่งต่อ แก้ไข และทำลาย ตามกิจกรรมที่เกี่ยวข้อง

11.3 ก่อนเริ่มหรือเปลี่ยนกิจกรรม เจ้าของกระบวนการต้องจัดทำบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) ระบุวัตถุประสงค์ ฐานกฎหมาย กลุ่มเจ้าของข้อมูล ประเภทและแหล่งข้อมูล ผู้รับข้อมูล ประเทศปลายทาง ผู้ประมวลผล ระยะเวลาเก็บ มาตรการรักษาความปลอดภัย และผู้รับผิดชอบ ครอบคลุมงานบุคคล เงินเดือน คู่ค้า ลูกค้า ผู้มาติดต่อ กล้องวงจรปิด เว็บไซต์ และระบบสำรอง ให้ปรับปรุงเมื่อเปลี่ยนแปลงและทบทวนอย่างน้อยปีละครั้ง

11.4 เก็บข้อมูลเท่าที่จำเป็นต่อวัตถุประสงค์ที่ชอบด้วยกฎหมายและแจ้งไว้ ประเมินฐานกฎหมายเป็นรายกิจกรรม เช่น การปฏิบัติตามสัญญา การปฏิบัติตามกฎหมาย ประโยชน์โดยชอบด้วยกฎหมาย หรือความยินยอมตามมาตรา 19 และ 24 การอ้างประโยชน์โดยชอบด้วยกฎหมายต้องบันทึกความจำเป็น การชั่งน้ำหนักสิทธิ และมาตรการลดผลกระทบ ห้ามอ้างสัญญากับนิติบุคคลเป็นฐานสัญญาของข้อมูลผู้ติดต่อโดยอัตโนมัติ

11.5 จัดให้มีคำประกาศความเป็นส่วนตัวส่วนตัว (Privacy Notice) ที่อ่านเข้าใจได้ก่อนหรือขณะเก็บข้อมูล แจ้งวัตถุประสงค์ ความจำเป็นและผลเมื่อไม่ให้ข้อมูล ประเภทข้อมูล ระยะเวลาเก็บหรือเกณฑ์กำหนดอายุ ประเภทผู้รับข้อมูล ข้อมูลติดต่อบริษัท ผู้ประสานงานหรือเจ้าหน้าที่คุ้มครองข้อมูล และสิทธิของเจ้าของข้อมูล กรณีได้ข้อมูลจากแหล่งอื่นให้แจ้งตามมาตรา 25 ภายในกรอบเวลาที่กฎหมายกำหนด

- โดยทั่วไปไม่เกิน 30 วันนับแต่เก็บรวบรวม หรือในการติดต่อหรือเปิดเผยครั้งแรกตามกรณี เว้นแต่เข้าเงื่อนไขยกเว้นที่บันทึกเหตุผลได้
- 11.6 เมื่อใช้ฐานความยินยอม ต้องขอโดยชัดแจ้ง แยกจากเงื่อนไขอื่น ระบุวัตถุประสงค์เฉพาะ ให้ตัดสินใจโดยอิสระ และเก็บหลักฐานฉบับข้อความ วันเวลา วิธีให้ และการถอนความยินยอม ห้ามใช้การรับทราบนโยบายนี้แทนความยินยอมแบบครอบคลุม หรือบังคับยินยอมในกิจกรรมที่ไม่จำเป็นต่อการจ้างงานหรือบริการ การถอนต้องทำได้ง่ายและไม่กระทบความชอบด้วยกฎหมายของการดำเนินการก่อนถอน
- 11.7 ข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 เช่น สุขภาพ ความพิการ เชื้อชาติ ศาสนา ความเห็นทางการเมือง ประวัติอาชญากรรม ข้อมูลพันธุกรรม และข้อมูลชีวภาพที่ใช้ระบุตัวบุคคล ต้องมีความยินยอมโดยชัดแจ้งหรือข้อยกเว้นเฉพาะตามกฎหมาย จำกัดผู้เข้าถึง แยกจัดเก็บตามความเหมาะสม และไม่เก็บเกินจำเป็น การตรวจประวัติอาชญากรรมต้องปฏิบัติตามเงื่อนไขเฉพาะของมาตรา 26 และหลักเกณฑ์ที่ใช้บังคับ ห้ามถือว่าความยินยอมเพียงอย่างเดียวเพียงพอทุกกรณี
- 11.8 การใช้ลายนิ้วมือหรือใบหน้าเพื่อบันทึกเวลาหรือควบคุมการเข้าออกต้องประเมินความจำเป็นและฐานกฎหมายก่อนใช้ หากอาศัยความยินยอมต้องมีทางเลือกที่ไม่ทำให้ผู้ไม่ยินยอมเสียเปรียบอย่างไม่เป็นธรรม ข้อมูลสุขภาพให้เปิดเผยแก่ผู้มีหน้าที่เฉพาะเท่าที่จำเป็น เช่น ข้อจำกัดในการทำงาน ไม่ส่งผลตรวจฉบับเต็มให้ผู้ไม่มีหน้าที่เกี่ยวข้อง การเก็บข้อมูลผู้เยาว์หรือบุคคลที่มีข้อจำกัดความสามารถต้องตรวจผู้มีอำนาจให้ความยินยอมตามมาตรา 20
- 11.9 ระบบกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV) และบันทึกการใช้งานต้องมีวัตถุประสงค์ ฐานกฎหมาย ป้ายแจ้งหรือคำประกาศ สิทธิรูปภาพหรือค้นข้อมูล และอายุเก็บที่อนุมัติ ห้ามติดตั้งในพื้นที่ที่คาดหมายความเป็นส่วนตัวสูง เช่น ห้องน้ำหรือห้องเปลี่ยนเสื้อผ้า การบันทึกเสียงหรือวิเคราะห์ชีวมิติเป็นกิจกรรมเพิ่มเติมที่ต้องประเมินและอนุมัติแยก การตรวจอีเมลหรืออุปกรณ์พนักงานต้องมีเหตุจำเป็น ผู้อนุมัติ และบันทึกขอบเขต ห้ามตรวจติดตามโดยไร้ขอบเขต

(INFORMATION SECURITY POLICY)

- 11.10 เว็บไซต์และบริการออนไลน์ต้องแจ้งการใช้ข้อมูลและคุกกี้ตามจริง คุกกี้หรือเครื่องมือติดตามที่อาศัยความยินยอมต้องไม่เริ่มก่อนรับความยินยอม และต้องถอนหรือเปลี่ยนตัวเลือกได้ การนำข้อมูลไปใช้เพื่อการบัญชีหรือบริการภายนอกต้องประเมินวัตถุประสงค์ ฐานกฎหมาย ผู้รับข้อมูล การเก็บต่อ และการส่งต่างประเทศก่อนอนุญาต
- 11.11 ผู้ประมวลผลต้องทำตามคำสั่งที่มีหลักฐานของบริษัทฯ และข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ซึ่งต้องระบุงาน ระยะเวลา ประเภทข้อมูล ผู้มีสิทธิ์เข้าถึง มาตรการรักษาความปลอดภัย การใช้ผู้ประมวลผลช่วง การช่วยตอบสิทธิ การตรวจสอบ การแจ้งเหตุ และการคืนหรือลบเมื่อสิ้นสุดงาน กำหนดให้แจ้งเหตุแก่บริษัทฯ โดยไม่ชักช้าและภายใน 24 ชั่วโมงนับแต่ทราบเหตุเป็นเงื่อนไขสัญญาของบริษัทฯ หรือเร็วกว่านั้นตามข้อตกลง กรณีบริษัทฯ เป็นผู้ประมวลผลให้ปฏิบัติตามหน้าที่และคำสั่งที่ขอด้วยกฎหมายของลูกค้า
- 11.12 ก่อนส่งหรือเปิดให้เข้าถึงข้อมูลจากต่างประเทศ รวมถึงการใช้คลาวด์หรือการสนับสนุนระบบจากต่างประเทศ เจ้าของกระบวนการต้องระบุประเทศ ผู้รับ วัตถุประสงค์ ประเภทข้อมูล และกลไกตามมาตรา 28 หรือ 29 เช่น มาตรฐานปลายทางที่เพียงพอ ข้อยกเว้นตามกฎหมาย หรือมาตรการคุ้มครองที่เหมาะสมและบังคับสิทธิได้ ให้ผู้ประสานงานด้านข้อมูลส่วนบุคคลตรวจสอบและผู้จัดการทั่วไปอนุมัติเป็นหลักฐาน ห้ามถือว่าสัญญาบริการคลาวด์ทั่วไปทำให้โอนข้อมูลได้ทุกกรณี
- 11.13 ตารางอายุข้อมูลต้องระบุเหตุผลทางกฎหมายหรือธุรกิจ จุดเริ่มต้น ระยะเวลา ผู้อนุมัติ และวิธีลบของข้อมูลแต่ละประเภท ครอบคลุมสำเนา อีเมล ภาพจากกล้อง และข้อมูลสำรอง เมื่อสิ้นความจำเป็นหรือครบกำหนดให้ลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวบุคคลได้อย่างเหมาะสม การแทนชื่อด้วยรหัสอย่างเดียวไม่ถือเป็นการทำให้ไม่สามารถระบุตัวบุคคล หากมีคำสั่งคงสภาพหลักฐานให้แยกจำกัดการใช้และทบทวนเหตุจำเป็นเป็นระยะ ห้ามเก็บทุกประเภทไว้โดยไม่มีกำหนด

หมวดที่ 12: การรับคำขอและการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

- 12.1 เจ้าของข้อมูลมีสิทธิถอนความยินยอม ขอเข้าถึงและรับสำเนา ขอทราบแหล่งที่มาของข้อมูลที่ไม่ได้ให้ความยินยอม ขอรับหรือโอนข้อมูลในกรณีที่ถูกกฎหมายกำหนด คัดค้าน ขอให้ลบหรือทำให้ไม่สามารถระบุตัวบุคคล ขอระงับการใช้ และขอแก้ไขข้อมูล รวมทั้งร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สิทธิแต่ละประเภทมีเงื่อนไขและข้อยกเว้นตามกฎหมาย
- 12.2 ให้ฝ่ายทรัพยากรบุคคลเป็นหน่วยรับคำขอและส่งต่อผู้ประสานงานด้านข้อมูลส่วนบุคคล รับคำขอด้วยตนเอง ณ สถานที่ประกอบกิจการของบริษัทฯ และทางไปรษณีย์ถึง ผู้ประสานงานด้านข้อมูลส่วนบุคคล บริษัท นาทาชา ครีเอชันส์ จำกัด เลขที่ 322/26-29 อาคารบางกอกเจมส์แอนด์จิวเวลรี่ทาวเวอร์ ถนนสุขุมวงศ์ แขวงสีพระยา เขตบางรัก กรุงเทพมหานคร 10500 รวมถึงช่องทางอิเล็กทรอนิกส์ที่บริษัทฯ ประกาศเพิ่มเติม ผู้รับเรื่องทุกหน่วยงานต้องส่งต่อโดยไม่ชักช้า และต้องไม่ปฏิเสธรับเรื่องเพียงเพราะไม่ได้ใช้แบบฟอร์มบริษัทฯ
- 12.3 สำหรับคำขอเข้าถึง รับสำเนา หรือทราบแหล่งที่มาตามมาตรา 30 ให้บันทึกวันรับ เลขที่คำขอ ชื่อผู้ขอ ขอบเขตข้อมูล วิธีรับผล และหลักฐานยืนยันตัวตนหรือมอบอำนาจ ตรวจสอบรายละเอียดและตัวตนโดยไม่ชักช้าไม่เกิน 15 วันนับแต่รับคำขอ ใช้วิธีที่เหมาะสมกับความเสี่ยงและหลักเกณฑ์กฎหมาย โดยไม่เรียกข้อมูลเกินจำเป็น หากข้อมูลไม่ครบให้แจ้งเป็นหนังสือหรือทางอิเล็กทรอนิกส์และให้เวลาแก้ไขไม่น้อยกว่า 10 วัน เมื่อได้รับคำขอและหลักฐานครบถ้วนแล้วให้บันทึกวันรับคำขอที่สมบูรณ์ตามประกาศ พ.ศ. 2569
- 12.4 คำขอเข้าถึง รับสำเนา หรือทราบแหล่งที่มาที่ถูกต้องครบถ้วนและไม่อาจปฏิเสธตามกฎหมาย ต้องดำเนินการโดยไม่ชักช้าและไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอตามหลักเกณฑ์ประกาศ พ.ศ. 2569 หากมีข้อมูลจำนวนมากหรือเหตุจำเป็นที่เข้าเงื่อนไข อาจขยายได้อีกไม่เกิน 30 วัน โดยบันทึกเหตุผลและแจ้งผู้ขอถึงเหตุจำเป็น รายละเอียด และกำหนดเสร็จก่อนครบกำหนดเดิม ห้ามใช้เวลาตรวจตัวตนเป็นเหตุขยายเวลาโดยอัตโนมัติ

- 12.5 เจ้าของข้อมูลภายในร่วมกับผู้ดูแลระบบค้นข้อมูล ตรวจสอบสิทธิ และปกปิดข้อมูลบุคคลอื่นก่อนส่ง ให้เข้าถึงหรือรับสำเนาผ่านวิธีที่ปลอดภัย หากรับคำขอทางอิเล็กทรอนิกส์ให้ตอบทางอิเล็กทรอนิกส์เมื่อทำได้ เว้นแต่ผู้ขอเลือกวิธีอื่น บริษัทฯ กำหนดให้การดำเนินการตามคำขอเป็นบริการโดยไม่เรียกค่าธรรมเนียม การปฏิเสธทั้งหมดหรือบางส่วนต้องอาศัยเหตุที่กฎหมายอนุญาต แจ้งเหตุผลและช่องทางร้องเรียน พร้อมบันทึกการตัดสินใจ
- 12.6 คำขอลบ ทำลาย หรือทำให้ไม่สามารถระบุตัวบุคคลที่ไม่มีเหตุยกเว้น ต้องดำเนินการโดยไม่ชักช้าไม่เกิน 90 วันนับแต่รับคำขอตามประกาศ พ.ศ. 2567 ครอบคลุมสำเนาและข้อมูลสำรอง หากมีข้อจำกัดทางเทคนิคต้องจำกัดให้ไม่สามารถนำกลับมาใช้งานหรือเปิดเผยตามหลักเกณฑ์กฎหมายจนกว่าจะเสร็จ และติดตามผลจริง กรณีข้อมูลที่มีประมวลผลโดยไม่ชอบด้วยกฎหมายและต้องลบตามมาตรา 33 (4) ห้ามใช้การทำให้ไม่สามารถระบุตัวบุคคลแทนการลบหรือทำลายในกรณีที่ประกาศห้ามไว้
- 12.7 คำขออื่นให้ดำเนินการโดยไม่ชักช้าภายในกรอบเวลาตามกฎหมาย และใช้เป้าหมายภายใน 30 วันเมื่อไม่มีกำหนดเฉพาะ หากยังดำเนินการไม่แล้วเสร็จให้แจ้งความคืบหน้าและเหตุผลโดยไม่อ้างเป้าหมายภายในแทนหน้าที่ตามกฎหมาย เมื่อแก้ไข ลบ ถอนความยินยอม หรือระงับการใช้ ให้ประสานผู้ประมวลผลและผู้รับข้อมูลตามหน้าที่ที่เกี่ยวข้อง และป้องกันไม่ให้ข้อมูลที่ลบแล้วกลับเข้าสู่การใช้งานจากการกู้คืนสำรอง
- 12.8 แจ้งผลการดำเนินการหรือเหตุปฏิเสธให้ผู้ขอทราบ และเก็บคำขอ หลักฐานประกอบ ผลตรวจตัวตน การดำเนินการ การขยายเวลา และเหตุปฏิเสธสำหรับสิทธิขอเข้าถึงหรือรับสำเนาไว้นานอย่างน้อย 2 ปี ตามประกาศ พ.ศ. 2569 โดยกำหนดในตารางอายุเอกสารให้นับจากวันที่ปิดคำขอ และจำกัดสิทธิเข้าถึง การเก็บนานกว่านั้นต้องมีเหตุรองรับ ห้ามนำการขอใช้สิทธิมาเป็นเหตุให้ผู้ขอเสียประโยชน์โดยไม่ชอบ

หมวดที่ 13: การจัดการเหตุละเมิดข้อมูลส่วนบุคคล

- 13.1 เหตุละเมิดครอบคลุมการสูญหาย ถูกเข้าถึง เปิดเผย แก้ไข ทำลาย หรือไม่พร้อมใช้งานโดยปราศจากอำนาจหรือโดยมิชอบ ทั้งเอกสารและระบบอิเล็กทรอนิกส์ เช่น ส่งอีเมลผิดผู้รับ เอกสารหรืออุปกรณ์หาย ตั้งค่าสิทธิ์ผิด และถูกมัลแวร์เรียกค่าไถ่ ผู้พบเหตุหรือสงสัยเหตุให้แจ้งผู้ดูแลระบบและผู้บังคับบัญชาทันทีผ่านช่องทางติดต่อที่ใช้งานได้ หากติดต่อไม่ได้ให้แจ้งผู้จัดการทั่วไปหรือฝ่ายทรัพยากรบุคคลโดยตรง ห้ามรอให้มีข้อมูลครบ
- 13.2 ผู้รับแจ้งต้องบันทึกเวลาพบและเวลารับรู้เหตุ แหล่งแจ้ง ระบบ ประเภทข้อมูล และผู้เกี่ยวข้อง พร้อมแจ้งผู้จัดการทั่วไปและผู้ประสานงานด้านข้อมูลส่วนบุคคลทันที ผู้ดูแลระบบจำกัดความเสียหาย เก็บพยานหลักฐานอย่างตรวจสอบการรับส่งได้ และรักษาความปลอดภัยของผู้ปฏิบัติงาน ห้ามลบหลักฐานหรือสอบสวนเกินอำนาจ
- 13.3 ผู้ประสานงานด้านข้อมูลส่วนบุคคลร่วมกับเจ้าของกระบวนการและผู้ดูแลระบบตรวจสอบข้อเท็จจริงและประเมินความเสี่ยงต่อสิทธิและเสรีภาพโดยไม่ชักช้า พิจารณาประเภทและปริมาณข้อมูล ความสามารถระบุตัวบุคคล จำนวนและความเปราะบางของผู้ได้รับผลกระทบ ผลเสียที่อาจเกิด และมาตรการที่ใช้ได้จริง จัดทำผลประเมินเบื้องต้นภายใน 24 ชั่วโมงเป็นเป้าหมายภายใน ซึ่งต้องไม่ทำให้การแจ้งตามกฎหมายล่าช้า
- 13.4 กรณีบริษัท เป็นผู้ควบคุมข้อมูล ต้องแจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าและภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ เว้นแต่เหตุไม่มีความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล หากมีความเสี่ยงสูงต้องแจ้งเจ้าของข้อมูลที่ได้รับผลกระทบพร้อมแนวทางเยียวยาโดยไม่ชักช้าด้วย กรณีตัดสินใจไม่แจ้งต้องมีเหตุผลและหลักฐานประเมินรองรับ ไม่ถือว่าข้อมูลเข้ารหัสแล้วทำให้ยกเว้นได้ทุกกรณี
- 13.5 ผู้จัดการทั่วไปเป็นผู้สั่งการและมอบหมายผู้แจ้งผ่านช่องทางที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด โดยต้องมีผู้ปฏิบัติแทนที่ติดต่อได้ ข้อมูลแจ้งอย่างน้อยต้องครอบคลุมลักษณะเหตุ ประเภทและจำนวนเจ้าของข้อมูลหรือรายการเท่าที่ทราบ ผู้ประสานงาน ผลกระทบ มาตรการระงับ

(INFORMATION SECURITY POLICY)

เหตุ และการเยียวยา หากข้อมูลยังไม่ครบให้แจ้งส่วนที่มีและส่งเพิ่มเติมตามหลักเกณฑ์ หากแจ้งเกินกำหนดต้องแจ้งโดยเร็วพร้อมเหตุจำเป็นและหลักฐานตามประกาศ ห้ามถือว่าเป็นการขยายเวลาได้โดยอัตโนมัติ

- 13.6 หากบริษัท เป็นผู้ประมวลผล ต้องแจ้งผู้ควบคุมข้อมูลโดยไม่ชักช้าและภายในกรอบสัญญาที่ใช้บังคับโดยบริษัท กำหนดเป้าหมายไม่เกิน 24 ชั่วโมงนับแต่ทราบเหตุ หรือเร็วกว่านั้นตามสัญญา ประสานการแจ้งเจ้าของข้อมูลหรือหน่วยงานตามบทบาทและคำสั่งที่ขอด้วยกฎหมาย เมื่อควบคุมเหตุแล้วต้องกู้คืนอย่างปลอดภัย ทบทวนสาเหตุ เยียวยา กำหนดผู้รับผิดชอบและเส้นตายแก้ไข เก็บบันทึกเหตุการณ์และทดสอบมาตรการป้องกันซ้ำ

หมวดที่ 14: การกำกับดูแล การติดตาม และการทบทวน

- 14.1 ผู้จัดการทั่วไปเป็นผู้รับผิดชอบสูงสุด อนุมัตินโยบาย ทรัพยากร ช้อยกเว้น และผู้ปฏิบัติแทน ให้ผู้จัดการทั่วไปทำหน้าที่ผู้ประสานงานด้านข้อมูลส่วนบุคคลจนกว่าจะมอบหมายผู้เหมาะสมเป็นลายลักษณ์อักษร โดยมีฝ่ายทรัพยากรบุคคลรับเรื่องและประสานการใช้สิทธิ ผู้ดูแลระบบรับผิดชอบมาตรการทางเทคนิค เจ้าของกระบวนการรับผิดชอบวัตถุประสงค์ สถานกฎหมาย ความถูกต้องและอายุข้อมูล หัวหน้างานกำกับผู้ใช้งาน และผู้รับผิดชอบระบบมาตรฐานของสมาชิกภูมิและเครื่องประดับที่มีความรับผิดชอบดูแลหลักฐานที่เกี่ยวข้อง
- 14.2 ประเมินและบันทึกหน้าที่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ตามมาตรา 41 และประกาศที่เกี่ยวข้อง โดยเฉพาะกิจกรรมที่ต้องตรวจสอบข้อมูลหรือระบบอย่างสม่ำเสมอเนื่องจากมีข้อมูลจำนวนมาก หรือมีกิจกรรมหลักประมวลผลข้อมูลอ่อนไหว หากเข้าข่ายต้องแต่งตั้งบุคคลที่มีความรู้ ไม่มีผลประโยชน์ขัดกัน ปฏิบัติงานได้อย่างอิสระ และรายงานผู้บริหารสูงสุดได้โดยตรง พร้อมแจ้งข้อมูลติดต่อแก่เจ้าของข้อมูลและสำนักงานตามกฎหมาย การมีผู้ประสานงานทั่วไปไม่ใช่แทนหน้าที่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลเมื่อกฎหมายกำหนด

- 14.3 ให้สื่อสารนโยบายและฝึกอบรมก่อนอนุญาตให้ใช้งานระบบ และทบทวนอย่างน้อยปีละครั้งหรือเมื่อมีความเสี่ยงใหม่ ครอบคลุมรหัสผ่าน การหลอกลวง การใช้ข้อมูลส่วนบุคคล การรับคำขอ และการรายงานเหตุ จัดให้มีการซ้อมเหตุละเมิดและการกู้คืนอย่างน้อยปีละครั้งตามความเสี่ยง เก็บหลักฐานการรับทราบ ผลทดสอบ และข้อบกพร่อง
- 14.4 หน่วยงานที่เกี่ยวข้องต้องจัดให้มีทะเบียนทรัพย์สินและสิทธิ ทะเบียนกฎหมาย บันทึกกิจกรรมการประมวลผล คำประกาศความเป็นส่วนตัว หลักฐานความยินยอม ข้อตกลงผู้ประมวลผล ทะเบียนการส่งต่างประเทศ ตารางอายุข้อมูล บันทึกทำลาย บันทึกใช้สิทธิ บันทึกเหตุละเมิด และผลสำรวจกับกู้คืน โดยระบุเจ้าของเอกสารและควบคุมฉบับปัจจุบัน เอกสารสนับสนุนต้องไม่เพิ่มภาระการเก็บข้อมูลส่วนบุคคลเกินจำเป็น
- 14.5 ทบทวนสิทธิอย่างน้อยทุก 6 เดือน ตรวจสอบผลสำรวจทุกวันทำการ และติดตามข้อบกพร่องตามความรุนแรง ผู้บริหารทบทวนอย่างน้อยปีละครั้ง ครอบคลุมเหตุการณ์และการแจ้งตรงเวลา คำขอใช้สิทธิ ผลกู้คืน ช่องโหว่ ผู้ให้บริการ การฝึกอบรม ข้อร้องเรียน และความครบถ้วนของหลักฐาน พร้อมกำหนดผู้รับผิดชอบ กำหนดเสร็จ และติดตามปิดประเด็น ทบทวนนโยบายเพิ่มเติมเมื่อกฎหมาย ระบบ หรือความเสี่ยงเปลี่ยนแปลง

(INFORMATION SECURITY POLICY)

- 14.6 ซ้อยกเว้นมาตรการภายในต้องมีเหตุผล ผลประเมินความเสี่ยง มาตรการทดแทน ผู้อนุมัติ และวันสิ้นสุด ห้ามอนุมัติซ้อยกเว้นที่ขัดกฎหมายหรือทำให้ไม่สามารถปฏิบัติตามกรอบเวลาตามกฎหมาย การฝ่าฝืนต้องสอบสวนโดยเป็นกรรม ให้ผู้เกี่ยวข้องชี้แจง และพิจารณาตามข้อบังคับการทำงาน สัญญา และกฎหมาย ห้ามหักค่าจ้างหรือเรียกค่าเสียหายเต็มจำนวนโดยอัตโนมัติ และคุ้มครองผู้รายงานโดยสุจริตจากการตอบโต้

ให้ดำเนินงานตามประกาศนี้ร่วมกับระบบของบริษัท ได้แก่ ระบบสภาพภูมิณีและเครื่องประดับที่มีความรับผิดชอบต่อ (Responsible Jewellery Council: RJC) ระบบบริหารคุณภาพในกลุ่มมาตรฐาน ISO 9000 (Quality management) ระบบการจัดการสิ่งแวดล้อมในกลุ่มมาตรฐาน ISO 14000 (Environmental management) และการจัดทำบัญชี การรายงาน และการทวนสอบก๊าซเรือนกระจกในชุดมาตรฐาน ISO 14064 (Greenhouse gases) ตามส่วนที่เกี่ยวข้อง ให้ผู้รับผิดชอบระบบควบคุมเลขส่วน ฉบับปี ขอบเขต และสถานะการรับรองหรือการทวนสอบในทะเบียนมาตรฐานของบริษัท และใช้ข้อมูลจากทะเบียนที่อนุมัติในการสื่อสารหรือกล่าวอ้างต่อภายนอก

(INFORMATION SECURITY POLICY)

สำหรับข้อมูลแสดงตน เอกสารธุรกรรม และข้อมูลการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Due Diligence: CDD) ให้ใช้การแยกประเภท ระยะเวลา จุดเริ่มต้น และเงื่อนไขเก็บต่อในเอกสาร หมายเลข 6 และนโยบายการกำกับดูแลและการรายงานธุรกรรมด้านการป้องกันและปราบปรามการฟอกเงิน หมายเลข 10 โดยข้อมูลแสดงตนเก็บอย่างน้อย 5 ปีนับแต่ปิดบัญชีหรือยุติความสัมพันธ์ และข้อมูล CDD เก็บอย่างน้อย 10 ปีนับแต่ปิดบัญชีหรือยุติความสัมพันธ์ กรณีธุรกรรมเป็นครั้งคราวและคำสั่งให้เก็บต่อให้ปฏิบัติตามเอกสารหมายเลข 10 หากหลักฐานเข้าข่ายหลายประเภทให้ใช้ระยะเวลาดำเนินการที่สิ้นสุดช้าที่สุด ห้ามทำลายเมื่อยังมีหน้าที่เก็บรักษาตามกฎหมายหรือคำสั่ง

ประกาศและมีผลใช้บังคับตั้งแต่วันที่ 28 เดือน กันยายน พ.ศ. 2569

จึงประกาศให้ทราบโดยทั่วกัน



(คุณอิศรา อุณหรัมย์)

ผู้จัดการทั่วไป

เอกสารกฎหมายลำดับรองและแหล่งอ้างอิง

แหล่งกฎหมายอ้างอิงประกอบนโยบายฉบับพทพวณ ณ วันที่ 26 กันยายน พ.ศ. 2569

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 ถึง 42 และ 73
2. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
3. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565
4. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567
5. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับการเข้าถึงและการขอรับสำเนาข้อมูลส่วนบุคคลเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม พ.ศ. 2569 มีผลใช้บังคับวันที่ 14 กันยายน พ.ศ. 2569
6. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
7. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
8. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566
9. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564