Bangkok Lab and Cosmetic Public Company Limited
48/1 Moo 5, Nongshaesao Road, Tumbon Namphu, Ampur Meung,
Ratchaburi 70000, Thailand

เอกสารฝ่ายบริหารบริษัท บางกอกแล็ป แอนด์ คอสเมติค

BLCP 10-053

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

Revision No. 0 Effective date: 02/07/2025

Prepared by	Reviewed by	Approved by
เลขานุการบริษัท Date: 30/06/2025	ประธานเจ้าหน้าที่สายปฏิบัติการ Date: 01/07/2025	ประธานเจ้าหน้าที่บริหาร Date: 02/07/2025

บริษัท บางกอกแล็ป แอนด์ คอสเมติค จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้อนุมัติ ..... - เภสัชกรสุวิทย์ งามภูพันธ์ -

(ประธานคณะกรรมการบริหาร)

ตามมติที่ประชุมคณะกรรมการบริหาร ครั้งที่ 5/2568 วันที่ 20 มิถุนายน 2568

ครั้งที่ 1 ปี 2568

ORIGINAL DOCUMENT

UNCONTROLLED COPY

สารบัญ

หน้า

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

กลุ่มบริษัท บางกอกแล็ป แอนด์ คอสเมติค (“บริษัท”) ตระหนักถึงความสำคัญของสารสนเทศซึ่งนับเป็นทรัพย์สินที่มีค่าสูงสุดขององค์กร จึงได้จัดทำนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขึ้นเพื่อให้มั่นใจว่าสารสนเทศทั้งระบบมีการดูแลด้านการบริหารจัดการอย่างมีประสิทธิภาพ เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาทรัพย์สินด้านสารสนเทศจากภาวะภัยคุกคามทุกประเภทที่อาจเกิดขึ้นทั้งจากภายในและภายนอก โดยเจตนาหรือโดยรู้เท่าไม่ถึงการณ์ ซึ่งครอบคลุมด้านการรักษาความลับ ความถูกต้องครบถ้วน และสภาพความพร้อมใช้งานของสารสนเทศ จึงประกาศนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และได้มีการปรับปรุงเนื้อหานโยบายอย่างต่อเนื่อง

วัตถุประสงค์

1. เพื่อกำหนดแนวทางในการรักษาความปลอดภัยแก่ระบบสารสนเทศอย่างมีประสิทธิภาพ ตามมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ISO/IEC 27001
2. เสริมสร้างความมั่นให้กับลูกค้าของบริษัทในด้านความสามารถในการให้บริการและรักษา ความลับของข้อมูลและระบบเทคโนโลยีสารสนเทศ
3. เพื่อเป็นแนวทางกำหนดในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของบริษัท ให้สอดคล้องกับการควบคุมภายในที่ดีด้านสารสนเทศ และให้เป็นไปตามกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง รวมทั้งเพื่อป้องกันมิให้เกิดการกระทำผิดตามข้อกำหนดและกฎหมายที่เกี่ยวข้อง ต่อการใช้ระบบสารสนเทศของบริษัท

แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

หมวดที่ 1 มาตรการขององค์กร (Organizational controls)

1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ กำหนดอนุมัติโดยผู้บริหาร และสื่อสาร ให้บุคลากรหน่วยงานภายในและหน่วยงานภายนอกที่เกี่ยวข้อง ตลอดจนทบทวนตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

1.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ มีการกำหนดและแบ่งความรับผิดชอบตามผังโครงสร้างองค์กร

1.3 การแบ่งแยกหน้าที่ความรับผิดชอบ หน้าที่และส่วนของการปฏิบัติหน้าที่ดังกล่าวที่จะก่อให้เกิดการขัดต่อผลประโยชน์ของบริษัท ต้องมีการแยกส่วนของการปฏิบัติหน้าที่ดังกล่าวออกจากกัน

1.4 หน้าที่ความรับผิดชอบของผู้บริหาร ผู้บริหารต้องกำหนดให้บุคลากรทั้งหมดยึดมั่นและรักษาความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้ปฏิบัติตามตามนโยบายความมั่นคงปลอดภัยสารสนเทศ และ ระเบียบปฏิบัติหรือขั้นตอนการทำงานที่กำหนดไว้

1.5 การติดต่อกับหน่วยงานผู้มีอำนาจ บริษัทกำหนดและปรับปรุงข้อมูลสำหรับการติดต่อกับหน่วยงานผู้มีอำนาจ

1.6 การติดต่อกับกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน ต้องกำหนดข้อมูลสำหรับการติดต่อกับกลุ่มพิเศษ และกลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ

1.7 ข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย ข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศมีการเก็บรวบรวมและวิเคราะห์เพื่อจัดทำข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย

1.8 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ ความมั่นคงปลอดภัยสารสนเทศต้องมีการบูรณาการกับการบริหารจัดการโครงการ

1.9 บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่นๆ รวมถึงเจ้าของทรัพย์สิน มีการจัดทำและปรับปรุงเพื่อให้ข้อมูลมีความเป็นปัจจุบันและถูกต้อง

1.10 การใช้ทรัพย์สินอย่างเหมาะสม บริษัทกำหนดขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลและทรัพย์สินที่เกี่ยวข้อง โดยมีการจัดทำเป็นลายลักษณ์อักษร และนำไปปฏิบัติ

1.11 การคืนทรัพย์สิน บุคลากรและผู้ที่เกี่ยวข้องจากหน่วยงานภายนอกต้องคืนทรัพย์สินทั้งหมดที่ตนเองถือครองเมื่อสิ้นสุดหรือ เปลี่ยนการจ้างงาน สัญญาจ้าง

1.12 ชั้นความลับของข้อมูล ข้อมูลมีการแยกหมวดหมู่ให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท โดยพิจารณาจากความลับ ความถูกต้องครบถ้วน และความพร้อมใช้จากหน่วยงานต่างๆที่เกี่ยวข้อง

1.13 การบ่งชี้ข้อมูล บริษัทกำหนดขั้นตอนสำหรับการบ่งชี้ข้อมูลตามความเหมาะสม มีการนำไปปฏิบัติให้สอดคล้องกับการจัดชั้นความลับของข้อมูลที่ได้กำหนดไว้

1.14 การถ่ายโอนข้อมูล บริษัทกำหนดระเบียบ/ขั้นตอนปฏิบัติสำหรับการถ่ายโอนข้อมูลของเครื่องมือหรืออุปกรณ์ทุกประเภท ทั้งการถ่ายโอนข้อมูลภายในและภายนอก

1.15 การควบคุมการเข้าถึง บริษัทกำหนดเกณฑ์สำหรับการเข้าถึงข้อมูลและทรัพย์สิน ทั้งทางกายภาพ และการเข้าถึงระบบจากระยะไกล และนำสู่การปฏิบัติ

1.16 การบริหารจัดการอัตลักษณ์ (ที่ใช้ในการพิสูจน์ตัวตนเข้าระบบ) วัฏจักรทั้งวงจรชีวิตของข้อมูลอัตลักษณ์ ที่เป็นส่วนหนึ่งของการพิสูจน์ตัวตนในการเข้าถึงระบบ ต้องได้รับการบริหารจัดการตลอดวงจรชีวิตของข้อมูล

1.17 ข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน การจัดสรรและการบริหารจัดการข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตน ต้องได้รับการควบคุมอย่างเหมาะสม

1.18 สิทธิการเข้าถึงข้อมูลและทรัพย์สิน ต้องมีการดำเนินการ ทบทวน ปรับปรุง และถอดถอนให้เป็นไปตามนโยบายสำหรับควบคุมการเข้าถึงขององค์กร

1.19 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก เพื่อบริหารจัดการความเสี่ยงต่อความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอก

1.20 การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงการให้บริการของผู้ให้บริการภายนอก ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง ต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกแต่ละราย โดยขึ้นอยู่กับประเภทและความสัมพันธ์กับผู้ให้บริการภายนอกนั้น

1.21 มีการกำหนดขั้นตอนในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่การให้บริการและผลิตภัณฑ์ด้าน ICT

1.22 มีการการติดตาม การทบทวน ประเมิน และการบริหารจัดการการเปลี่ยนแปลงอย่างสม่ำเสมอในวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ และการส่งมอบบริการของผู้ให้บริการภายนอก

1.23 มีการกำหนดความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการ การบริหารจัดการและการใช้บริการ Cloud ต้องมีการกำหนดโดยให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

1.24 มีการการวางแผนและการเตรียมการสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

1.25 มีการประเมินและตัดสินใจสำหรับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

1.26 การรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ มีการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เป็นไปตามขั้นตอนปฏิบัติที่กำหนดไว้อย่างเป็นลายลักษณ์อักษร

1.27 ความรู้ที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศต้องนำมาใช้เพื่อเสริมสร้างความแข็งแกร่ง และปรับปรุงมาตรการความมั่นคงปลอดภัยสารสนเทศ

1.28 บริษัทกำหนดให้มีขั้นตอนปฏิบัติเพื่อระบุ รวบรวม และเก็บรักษาหลักฐานของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

1.29 บริษัทวางแผนเพื่อรักษาความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่เหมาะสมและเพียงพอต่อความต้องการในช่วงที่เกิดการหยุดชะงัก

1.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ ต้องได้รับการวางแผนและมีความพร้อมอยู่เสมอ โดยให้เป็นไปตามวัตถุประสงค์และความต้องการด้านความต่อเนื่องทางธุรกิจและของระบบ ICT ที่เกี่ยวข้อง

1.31 ความต้องการที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง ต้องมีการกำหนดบันทึกไว้เป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบัน

1.32 สิทธิในทรัพย์สินทางปัญญา กำหนดขั้นตอนปฏิบัติที่เหมาะสมเพื่อป้องกันสิทธิในทรัพย์สินทางปัญญา และป้องกันการละเมิดทรัพย์สินทางปัญญาทั้งของบริษัทและของผู้อื่น

1.33 การป้องกันข้อมูล ข้อมูลขององค์กรต้องได้รับการป้องกันจากการสูญหาย การทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่ออกไปโดยไม่ได้รับอนุญาต

1.34 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล ต้องระบุและดำเนินการให้สอดคล้องกับความต้องการที่เกี่ยวข้องกับการรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลตามที่กฎหมาย ระเบียบข้อบังคับ กำหนดให้ต้องปฏิบัติตาม

1.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ ต้องมีการทบทวนอย่างเป็นอิสระตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้น

1.36 การปฏิบัติตามนโยบาย กฎเกณฑ์ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องมีการทบทวนอย่างสม่ำเสมอ

1.37 ขั้นตอนปฏิบัติงานที่เป็นลายลักษณ์อักษร และต้องมีพร้อมไว้สำหรับบุคลากรที่มีความจำเป็นต้องใช้งาน

หมวดที่ 2 มาตรการด้านบุคลากร (People controls)

2.1 การคัดเลือก การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการ และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

2.2 ข้อตกลงและเงื่อนไขการจ้างงาน ต้องกล่าวถึงหน้าที่ความรับผิดชอบ ด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรและของบริษัท

2.3 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ บุคลากร ต้องได้รับการอย่างเหมาะสม

2.4 กระบวนการทางวินัย ต้องมีการกำหนดอย่างเป็นทางการและสื่อสารให้ได้รับทราบอย่างสม่ำเสมอ

2.5 ความรับผิดชอบภายหลังการสิ้นสุด หรือการเปลี่ยนแปลงการจ้างงาน ต้องมีการกำหนดบังคับให้เป็นไปตามที่กำหนดนั้น และสื่อสารไปยังบุคลากรและหน่วยงานที่เกี่ยวข้องต่างๆ

2.6 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ ต้องมีการระบุ จัดทำเป็นลายลักษณ์อักษร ทบทวนอย่างสม่ำเสมอ และมีการลงนามโดยบุคลากรและผู้ที่เกี่ยวข้องจากหน่วยงานต่างๆ

2.7 การปฏิบัติงานจากระยะไกล มาตรการความมั่นคงปลอดภัยต้องมีการปฏิบัติเมื่อบุคลากรจะปฏิบัติงานจากระยะไกลเพื่อป้องกันข้อมูลที่มีการเข้าถึง ประมวลผล หรือจัดเก็บไว้ภายนอกองค์กร

2.8 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ต้องมีกลไกสำหรับบุคลากรในการรายงานเหตุการณ์ที่สังเกตพบ หรือที่เกิดความสงสัยเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ โดยผ่านช่องทางการรายงานที่เหมาะสมและอย่างทันกาล

หมวดที่ 3 มาตรการทางกายภาพ (Physical controls)

3.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ ต้องมีการกำหนดขึ้นมาเพื่อใช้ในการป้องกันพื้นที่ที่มีข้อมูลและทรัพย์สินที่เกี่ยวข้อง

3.2 การควบคุมการเข้าออกทางกายภาพ พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการควบคุมการเข้าออกพื้นที่และควบคุมจุดที่มีการเข้าถึงอย่างเหมาะสม

3.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ ต้องมีการออกแบบและนำสู่การปฏิบัติเพื่อให้เกิดการป้องกันอย่างเป็นรูปธรรม

3.4 การเฝ้าระวังด้านความมั่นคงปลอดภัยทางกายภาพ ต้องมีการเฝ้าระวังและติดตามอย่างต่อเนื่องเพื่อป้องกันการเข้าถึงการกายภาพโดยไม่ได้รับอนุญาต

3.5 การป้องกันต่อภัยคุกคามทางกายภาพ และด้านสภาพแวดล้อม เช่น ภัยพิบัติทางธรรมชาติ ภัยคุกคามทางกายภาพทั้งที่เจตนา หรือไม่เจตนาต้องมีการออกแบบและนำสู่การปฏิบัติ

3.6 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการออกแบบและนำสู่การปฏิบัติ

3.7 โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ ต้องมีการกำหนดและบังคับใช้งานเพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร

3.8 การจัดวางและป้องกันอุปกรณ์ อุปกรณ์ต้องมีการจัดวางและป้องกันให้มีความปลอดภัย

3.9 ความมั่นคงปลอดภัยของทรัพย์สินที่มีการใช้งานนอกองค์กร ทรัพย์สินที่มีการใช้งานนอกองค์กรต้องมีการป้องกัน

3.10 สื่อบันทึกข้อมูล ต้องได้รับการบริหารจัดการตลอดวัฏจักรชีวิต โดยให้เป็นไปตามวิธีการจัดชั้นความลับและการจัดการข้อมูลและทรัพย์สินที่เกี่ยวข้อง

3.11 ระบบสาธารณูปโภคสนับสนุน ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่นๆ

3.12 ความมั่นคงปลอดภัยของสายสัญญาณ ต้องได้รับการป้องกันการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย

3.13 การบำรุงรักษาอุปกรณ์ เพื่อให้มีความพร้อมใช้งาน สามารถรักษาความถูกต้องและความลับของข้อมูล

3.14 ความมั่นคงปลอดภัยสำหรับการจำหน่ายออกหรือการทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น ต้องมีการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการจำหน่ายออกหรือก่อนการนำอุปกรณ์นั้นไปใช้งานอย่างอื่น

หมวดที่ 4 มาตรการทางเทคโนโลยี (Technological controls)

4.1 อุปกรณ์ปลายทางของผู้ใช้งาน ต้องได้รับการป้องกัน โดยทั่วไปหมายรวมถึงเครื่องคอมพิวเตอร์โน้ตบุ๊ค โทรศัพท์มือถือและอุปกรณ์ที่สามารถประมวลผลข้อมูลอื่นๆ ที่มีการใช้งานโดยผู้ใช้งานโดยทั่วไป หรือสามารถติดต่อสื่อสารข้อมูลผ่านทางเครือข่ายได้

4.2 สิทธิการเข้าถึงในระดับพิเศษ การจัดสรรและให้สิทธิการเข้าถึงในระดับพิเศษ เช่น ระดับของผู้ดูแลระบบ ระดับของผู้จัดการ ต้องมีการจำกัดและบริหารจัดการ

4.3 การจำกัดการเข้าถึงข้อมูล การควบคุมการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้อง ต้องมีการจำกัดให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับการควบคุมการเข้าถึงที่ได้กำหนดไว้

4.4 การจำกัดการเข้าถึงซอร์สโค้ด เครื่องมือที่ใช้ในการพัฒนาระบบ และซอฟต์แวร์ที่สามารถอ่านและเขียนทับข้อมูลเหล่านั้นได้ ต้องมีการบริหารจัดการอย่างเหมาะสม

4.5 การพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย เทคโนโลยีและขั้นตอนปฏิบัติสำหรับใช้ในการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย ต้องมีการนำสู่การปฏิบัติโดยขึ้นอยู่กับนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับการควบคุมการเข้าถึง

4.6 การบริหารจัดการขีดความสามารถของระบบ การใช้ทรัพยากรของระบบต้องมีการเฝ้าระวัง ติดตาม และปรับปรุงให้เป็นไปตามความต้องการทรัพยากรในปัจจุบันและที่คาดการณ์ว่าจะเกิดขึ้น

4.7 การป้องกันจากโปรแกรมไม่ประสงค์ดี ต้องมีการนำสู่การปฏิบัติ และได้รับการสนับสนุนโดยการสร้างความตระหนักให้แก่ผู้ใช้งานอย่างเหมาะสม

4.8 การบริหารจัดการช่องโหว่ทางเทคนิค ต้องมีการติดตามเพื่อให้ได้มาซึ่งข้อมูลความเสี่ยงต่อช่องโหว่ ต้องได้รับการประเมิน และมีการกำหนดมาตรการที่เหมาะสมเพื่อดำเนินการ

4.9 การบริหารจัดการการตั้งค่าระบบ การตั้งค่าด้านความมั่นคงปลอดภัย ของฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร นำสู่การปฏิบัติ ติดตาม และทบทวน เพื่อให้เป็นไปตามการตั้งค่าที่กำหนดไว้นั้น

4.10 การลบข้อมูล ข้อมูลที่มีการจัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือบนสื่อบันทึกข้อมูลอื่นๆ ต้องมีการลบทำลายเมื่อไม่มีความจำเป็นในการใช้งานอีกต่อไป

4.11 การปิดบังข้อมูล เพื่อไม่ให้ข้อมูลที่จัดเก็บไว้ในระบบถูก มองเห็น หรือถูกนำไปใช้ประโยชน์ ต้องมีการนำมาใช้งานโดยให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้อง และความต้องการทางธุรกิจ โดยต้องพิจารณากฎหมายที่เกี่ยวข้องประกอบด้วย

4.12 การป้องกันการรั่วไหลของข้อมูล ต้องมีการนำมาประยุกต์ใช้กับระบบ เครือข่าย และอุปกรณ์ต่างๆ ที่มีการประมวลผล จัดเก็บ หรือรับส่งข้อมูลสำคัญ

4.13 การสำรองข้อมูล สำเนาของข้อมูลซอฟต์แวร์ และระบบต้องมีการจัดเก็บรักษาไว้ และทดสอบอย่างสม่ำเสมอโดยให้เป็นไปตามนโยบายเฉพาะแยกตามเรื่องที่เกี่ยวข้องกับการสำรองข้อมูล

4.14 การสำรองอุปกรณ์ประมวลผลข้อมูล ต้องมีการเตรียมการสำรองไว้ให้เพียงพอเพื่อให้เป็นไปตามความต้องการด้านสภาพความพร้อมใช้ของอุปกรณ์เหล่านั้น

4.15 การบันทึกข้อมูลล็อก ต้องมีการจัดเตรียมระบบไว้ สำหรับข้อมูลล็อกเพื่อให้สามารถสร้าง จัดเก็บ ป้องกัน และนำมาวิเคราะห์ข้อมูลได้

4.16 กิจกรรมการเฝ้าระวังการทำงานของ ระบบและอุปกรณ์ ต้องมีการเฝ้าระวังการทำงานเพื่อตรวจหาพฤติกรรมที่ผิดปกติ เพื่อประเมินความเป็นไปได้ของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น

4.17 การตั้งนาฬิกาให้ถูกต้อง ต้องได้รับการตั้งค่าเวลาให้เที่ยงตรงโดยเทียบกับแหล่งเทียบเวลาที่ได้รับการรับรอง

4.18 การใช้โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิในระดับพิเศษ ซึ่งทำให้สามารถละเมิดมาตรการควบคุมของแอพพลิเคชั่นและระบบต้องมีการจำกัด และควบคุมการใช้งานอย่างเคร่งครัด

4.19 การติดตั้งซอฟต์แวร์บนระบบให้บริการ ขั้นตอนปฏิบัติและมาตรการที่จำเป็นต้องมีการนำสู่การปฏิบัติ เพื่อบริหารจัดการการติดตั้งซอฟต์แวร์บนระบบให้บริการให้มีความมั่นคงปลอดภัย เมื่อผ่านขั้นตอนการพัฒนาและได้รับการทดสอบเป็นที่เรียบร้อยแล้ว จะมีการนำไปติดตั้งบนระบบให้บริการเพื่อให้บริการแก่ผู้ใช้งาน

4.20 ความมั่นคงปลอดภัยของเครือข่าย ต้องมีการรักษาความมั่นคง ปลอดภัย และมีการควบคุมเพื่อป้องกันข้อมูลทั้งในระบบและแอพพลิเคชั่นที่มีการทำงาน ผ่านเครือข่ายและอุปกรณ์เครือข่ายขององค์กร

4.21 ความมั่นคงปลอดภัยของบริการ เครือข่าย ต้องมีการกำหนด นำสู่การปฏิบัติ ติดตาม และเฝ้าระวัง เพื่อให้เป็นไปตามกลไก ระดับการให้บริการ และความต้องการที่ได้กำหนดไว้นั้น

4.22 การแบ่งแยกเครือข่าย กลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบสารสนเทศ ต้องมีการแบ่งแยกออกจากกันในเครือข่ายขององค์กรตามความต้องการขององค์กร

4.23 การคัดกรองเว็บ การเข้าถึงเว็บไซต์ภายนอกต้องได้รับการบริหารจัดการเพื่อลดโอกาสการเข้าถึงเนื้อหาที่เป็นอันตราย

4.24 การใช้การเข้ารหัสข้อมูล กฎเกณฑ์สำหรับการใช้การเข้ารหัสข้อมูล ซึ่งรวมถึงการบริหารจัดการกุญแจสำหรับการเข้ารหัส ต้องมีการกำหนดและนำสู่การปฏิบัติ

4.25 วัฏจักรการพัฒนาระบบให้มีความมั่นคงปลอดภัย กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบให้มีความมั่นคงปลอดภัย ต้องมีการกำหนดและนำสู่การปฏิบัติ

4.26 ความต้องการด้านความมั่นคงปลอดภัยของแอพพลิเคชั่น ต้องมีการกำหนดและอนุมัติเมื่อมีการพัฒนา หรือจัดหาแอพพลิเคชั่น

4.27 สถาปัตยกรรมของระบบที่มีความมั่นคงปลอดภัยและหลักการวิศวกรรมระบบ ต้องมีการกำหนดจัดทำเป็นลายลักษณ์อักษร ปรับปรุง และนำมา ปฏิบัติต่อกิจกรรมการพัฒนาระบบสารสนเทศ

4.28 การเขียนโปรแกรมให้มีความมั่นคงปลอดภัย ต้องนำหลักการเขียนโปรแกรมให้มีความมั่นคงปลอดภัยมาปฏิบัติกับการพัฒนาซอฟแวร์

4.29 การทดสอบด้านความมั่นคงปลอดภัยในการพัฒนาและรับรองระบบ ต้องมีการกำหนดและนำสู่การปฏิบัติในวัฏจักรของการพัฒนาระบบ

4.30 การพัฒนาระบบโดยหน่วยงานภายนอก องค์กรต้องกำกับดูแล เฝ้าระวัง ติดตาม และทบทวนกิจกรรม การพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ

4.31 การแยกสภาพแวดล้อมสำหรับการ พัฒนาการทดสอบ และการให้บริการออกจากกัน ต้องมีการแยกออกจากกันและต้องมีการรักษาความมั่นคงปลอดภัย

4.32 การบริหารจัดการการเปลี่ยนแปลง ต้องมีการควบคุมผ่านขั้นตอนปฏิบัติสำหรับการบริหารจัดการการเปลี่ยนแปลง

4.33 ข้อมูลสำหรับการทดสอบ ต้องมีการคัดเลือก มีการป้องกัน และมีการบริหารจัดการอย่างเหมาะสม

4.34 การป้องกันระบบสารสนเทศในช่วงที่มีการทดสอบระบบโดยผู้ตรวจประเมิน ต้องมีการวางแผนและตกลงกันระหว่างผู้ดำเนินการทดสอบและผู้บริหารที่เกี่ยวข้อง เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นกับระบบให้บริการ เช่น ระบบเกิดการหยุดชะงักในระหว่างที่ทำการทดสอบ ข้อมูลสำคัญในระบบถูกเข้าถึงโดยไม่ได้รับอนุญาต เป็นต้น

การทบทวนนโยบาย

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศจะได้รับการทบทวนและประเมินความเพียงพอและความเหมาะสมของนโยบายเป็นประจำทุกปี

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะ บริหาร ครั้งที่ 5/2568 วันที่ 20 มิถุนายน 2568 โดยมีผลบังคับใช้ตั้งแต่วันที่ 21 มิถุนายน 2568 เป็นต้นไป

Historical of Changes

บันทึกการแก้ไขเอกสาร

Rev. No	Effective date	Description	DAR No	Prepared by	Reviewed by	Approved by
0	02/07/2025	NDR: เพื่อให้มั่นใจว่าสารสนเทศทั้งระบบมีการดูแลด้านการบริหารจัดการอย่างมีประสิทธิภาพ เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาทรัพย์สินด้านสารสนเทศจากภาวะภัยคุกคามทุกประเภท โดยนโยบายดังกล่าวมีระบุไว้ในคู่มือปฏิบัติงาน แต่เนื่องจากบริษัทฯ จะมีการขอการรับรองระบบ ISO/IEC 27001 เพื่อรองรับการดำเนินการดังกล่าว จึงนำมาจัดทำให้ชัดเจน ซึ่งได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริหาร ครั้งที่ 5/2568	ISO-DAR-BLCP-10-6647	เลขานุการบริษัท Date: 30/06/2025	ประธานเจ้าหน้าที่สายปฏิบัติการ Date: 01/07/2025	ประธานเจ้าหน้าที่บริหาร Date: 02/07/2025