บริษัท ไอ.ซี.ซี. อินเตอร์เนชั่นแนล จำกัด (มหาชน)
530 ซอยสาธุประดิษฐ์ 58 แขวงบางโพงพาง เขตยานนาวา กรุงเทพฯ 10120 โทรศัพท์: (02) 293-9000,293-9300
โทรสาร: (02) 294-3024 www.icc.co.th E-mail: webmaster@icc.co.th ทะเบียนเลขที่ 0107537001374

ประกาศ
นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

ด้วยบริษัท ไอ.ซี.ซี. อินเตอร์เนชั่นแนล จำกัด (มหาชน) ("บริษัทฯ") ได้จัดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงานของทั้งระบบ ให้การใช้บริการ และการให้บริการสามารถดำเนินการร่วมกันได้อย่างเหมาะสม สอดคล้องกับนโยบายทางธุรกิจ และป้องกันปัญหาที่อาจเกิดจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ทั้งจากผู้ใช้งาน และภัยคุกคามต่าง ๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของบริษัทฯ ได้

ดังนั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ คงไว้ซึ่งความปลอดภัย ครบถ้วนสมบูรณ์ และพร้อมใช้งาน จึงกำหนดนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเพื่อเป็นแนวทางในการปฏิบัติดังนี้

1. ขอบเขต และวัตถุประสงค์

1.1 ขอบเขต

บริษัทฯ กำหนดขอบเขตของการดำเนินงานด้านสารสนเทศเพื่อสร้างมาตรฐาน และแนวทางที่ชัดเจนในการจัดการข้อมูล และระบบสารสนเทศ ขอบเขตครอบคลุมถึงการจัดการข้อมูล ระบบเทคโนโลยี บุคลากร กระบวนการที่เกี่ยวข้องทั้งหมด ตั้งแต่การพัฒนา การใช้งาน การบำรุงรักษา ไปจนถึงการป้องกัน และจัดการความเสี่ยงมุ่งเน้นให้ระบบสารสนเทศมีความปลอดภัย เชื่อถือได้ พร้อมใช้งาน สอดคล้องกับเป้าหมายในการพัฒนาธุรกิจอย่างยั่งยืน

1.2 วัตถุประสงค์

- ปกป้องข้อมูล และระบบสารสนเทศให้มีความมั่นคงปลอดภัย
- ให้เกิดความพร้อมใช้งานอย่างต่อเนื่องสำหรับระบบสารสนเทศของบริษัทฯ
- สร้างความเชื่อมั่นให้แก่ผู้มีส่วนเกี่ยวข้อง ในการใช้บริการระบบสารสนเทศของบริษัทฯ
- รักษาระดับการให้บริการระบบสารสนเทศที่มีการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล สอดคล้องกับข้อบังคับบริษัทฯ และกฎหมายที่เกี่ยวข้อง

2. การบริหารจัดการความเสี่ยง

กำหนดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมีแผนการจัดการความเสี่ยง ซึ่งกำหนดสาเหตุ เกณฑ์ในการประเมิน การปรับปรุง พัฒนา เพื่อลด หรือกำหนดความเสี่ยงที่เหมาะสมในการพัฒนาระบบสารสนเทศให้ถูกต้อง ครบถ้วน ตรงเวลา พร้อมใช้งาน และโอกาสในการสูญเสียความลับทางสารสนเทศ ความถูกต้องครบถ้วนของข้อมูล ความพร้อมใช้งานของสินทรัพย์ระบบสารสนเทศบริษัทฯ ซึ่งมีการจัดแบ่งระดับความเสี่ยงเป็น 5 ระดับ คือ วิกฤติ สูง ปานกลาง ต่ำ และ ต่ำมาก

3. การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

บริษัทฯ ให้ความสำคัญกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อปกป้องข้อมูล และระบบจากภัยคุกคาม โดยกำหนดให้นโยบายครอบคลุมในทุกปัจจัย ดังนี้

3.1 บุคลากร

- สร้างความรู้ ทักษะ และความตระหนักด้านความมั่นคงปลอดภัยแก่ผู้ใช้งานและผู้มีส่วนได้เสีย
- กำหนดขอบเขตความรับผิดชอบ พร้อมจัดทำคู่มือ นโยบาย และแนวปฏิบัติที่เกี่ยวข้อง
- จัดการฝึกอบรม สื่อสารแนวปฏิบัติผ่านช่องทางต่าง ๆ ของบริษัทฯ
- ในกระบวนการสรรหาบุคลากร ต้องมีการตรวจสอบคุณสมบัติ ประวัติอาชญากรรม ข้อตกลงเงื่อนไขการจ้างงาน และลงนามในข้อตกลงรักษาความลับข้อมูล

3.2 กายภาพ และสภาพแวดล้อม

- กำหนดมาตรการควบคุมการเข้าถึงพื้นที่ต่าง ๆ เช่น พื้นที่ทั่วไป พื้นที่สำคัญ และศูนย์ข้อมูลของ บริษัทฯ (Data Center)
- ติดตั้งระบบรักษาความปลอดภัยที่เหมาะสม เช่น กล้องวงจรปิดและบัตรผ่าน
- การกำหนดมาตรการพิจารณาตามความสำคัญของอุปกรณ์และข้อมูล
- มีผลบังคับใช้กับผู้ใช้งาน บุคลากร และผู้ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ

3.3 การเข้าถึงและการใช้งานระบบสารสนเทศ

- การเข้าถึงระบบต้องมีการยืนยันตัวตน และกำหนดสิทธิ์การเข้าถึงอย่างเหมาะสม
- ข้อมูลสำคัญต้องถูกเข้ารหัสด้วยมาตรฐานที่ปลอดภัย ทั้งขณะจัดเก็บ และส่งผ่านเครือข่าย
- ข้อมูลที่ถูกจัดเก็บในคอมพิวเตอร์ เซิร์ฟเวอร์ หรือระบบคลาวด์ของบริษัทฯ ต้องได้รับการปกป้อง
- ควบคุมการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ตั้งแต่การลงทะเบียน การกำหนดสิทธิ์ การเพิกถอนสิทธิ์ และการทบทวนสิทธิ์
- ควบคุมการใช้งานอุปกรณ์พกพา (Mobile Device) ให้เป็นไปตามมาตรฐานความปลอดภัย
- ให้ความคุ้มครองข้อมูลส่วนบุคคลที่ไม่พึงเปิดเผยตามบทบัญญัติของกฎหมาย

3.4 การบันทึกข้อมูลเหตุการณ์ในระบบสารสนเทศ (Log) และการเฝ้าระวัง

- ติดตั้งระบบบันทึก ตรวจสอบ และติดตามการใช้งานระบบสารสนเทศ
- บันทึก และเฝ้าระวังเหตุการณ์ต่าง ๆ เช่น กิจกรรมของผู้ดูแลระบบ การใช้งานที่ผิดปกติ หรือข้อผิดพลาดของระบบ
- ข้อมูลเหตุการณ์ที่ถูกบันทึกต้องได้รับการปกป้องจากการเปลี่ยนแปลง ทำลาย หรือเข้าถึงโดยไม่ได้รับอนุญาต
- นำข้อมูลที่บันทึกมาวิเคราะห์อย่างสม่ำเสมอ เพื่อป้องกันภัยคุกคามหรือเหตุการณ์ไม่พึงประสงค์ที่อาจส่งผลกระทบต่อบริษัทฯ

4. การบริหารจัดการข้อมูล และสื่อบันทึกข้อมูล

4.1 การบริหารจัดการข้อมูล

บริษัทฯ กำหนดให้มีการจัดการข้อมูลอย่างเป็นระบบ โดยแบ่งประเภทชั้นความลับของข้อมูลทั้งในรูปแบบเอกสารกระดาษ และอิเล็กทรอนิกส์ เพื่อควบคุมการเข้าถึง และใช้งานข้อมูลอย่างปลอดภัย แบ่งออกเป็น 5 ระดับ ดังนี้

- สาธารณะ (Public)
  - ข้อมูลที่สามารถเผยแพร่สู่ภายนอกได้โดยไม่มีผลกระทบต่อองค์กร
  - **ตัวอย่าง :** เว็บไซต์บริษัท ข้อมูลประชาสัมพันธ์ รายงานประจำปีที่เผยแพร่สู่สาธารณะ ประกาศรับสมัครงาน ข้อมูลเกี่ยวกับสวัสดิการพนักงานที่เผยแพร่สู่สาธารณะ ข่าวประชาสัมพันธ์เกี่ยวกับผลิตภัณฑ์ และบริการของบริษัท เอกสารที่ใช้ในการนำเสนอแก่ลูกค้า หรือผู้สนใจ
- ใช้ภายในทั่วไป (Restricted / Internal Use)
  - ข้อมูลที่ใช้ได้ภายในบริษัทฯ อาจส่งต่อระหว่างสายงานได้ แต่ยังคงต้องมีข้อจำกัด
  - **ตัวอย่าง :** แผนงานกิจกรรมของบริษัท เช่น กำหนดการสัมมนาภายใน เป็นต้น รายงานผลการดำเนินงานที่ใช้ในการประชุมภายใน คู่มือการใช้งานระบบเทคโนโลยีสารสนเทศภายในองค์กร ประกาศภายในเกี่ยวกับสวัสดิการ สิทธิพนักงาน และรายละเอียดเกี่ยวกับนโยบายการเบิกค่าใช้จ่าย
- ภายในองค์กร (Restricted / Internal Use Only)
  - ข้อมูลที่ใช้ภายในบริษัทฯ เฉพาะสายงานเท่านั้น และไม่ควรเปิดเผยสู่บุคคลภายนอก
  - **ตัวอย่าง :** นโยบาย และคู่มือปฏิบัติงานของแต่ละสายงาน รายงานการประชุมของแต่ละสายงานที่ยังไม่เผยแพร่สู่ภายนอก รายชื่อพนักงาน ข้อมูลติดต่อภายใน ข้อมูลการฝึกอบรม แผนพัฒนาบุคลากร และระบบการขออนุมัติเอกสารภายในบริษัทฯ
- ความลับมาก (Highly Confidential)
  - ข้อมูลที่อาจส่งผลกระทบต่อบริษัทฯ หากรั่วไหล แต่ไม่รุนแรงเท่าระดับ "ความลับจำกัดเฉพาะ"
  - **ตัวอย่าง :** แผนกลยุทธ์ทางธุรกิจที่ยังไม่เปิดเผยสู่สาธารณะ รายงานผลประกอบการรายไตรมาสก่อนเผยแพร่ ข้อมูลเกี่ยวกับลูกค้ารายสำคัญ เช่น ข้อตกลงสัญญาทางธุรกิจ เป็นต้น รายละเอียดเกี่ยวกับโครงสร้างเงินเดือนของพนักงาน รายชื่อซัพพลายเออร์พร้อมข้อตกลงด้านราคา และเงื่อนไขพิเศษ
- ความลับเฉพาะ (Restricted)
  - ข้อมูลที่หากรั่วไหลจะส่งผลกระทบร้ายแรงต่อบริษัทฯ เช่น ความเสียหายทางการเงิน การละเมิดกฎหมาย หรือความเสี่ยงด้านความปลอดภัยสูง
  - **ตัวอย่าง :** แผนควบรวมกิจการหรือแผนซื้อขายหุ้นที่ยังไม่เปิดเผย รหัสผ่านระดับสูงของเซิร์ฟเวอร์ และฐานข้อมูลหลักของบริษัทฯ ข้อมูลเชิงลึกด้านยุทธศาสตร์ หรือเทคโนโลยีที่ยังไม่เปิดเผย ข้อมูลส่วนตัวของผู้บริหารระดับสูง เช่น สำเนาบัตรประชาชน รายได้ ทรัพย์สิน เป็นต้น และข้อมูลทางกฎหมายที่อยู่ระหว่างกระบวนการพิจารณาของศาล

4.2 การบริหารจัดการสื่อบันทึกข้อมูล

บริษัทฯ กำหนดให้มีการบริหารจัดการสื่อบันทึกข้อมูลอย่างเป็นระบบ โดยครอบคลุมถึงอุปกรณ์จัดเก็บข้อมูล เอกสารสำคัญ และเอกสารการปฏิบัติงานภายในบริษัทฯ เช่น นโยบาย แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ขั้นตอนปฏิบัติงาน คู่มือการตั้งค่าระบบ และบันทึกต่าง ๆ

4.3 กระบวนการบริหารจัดการเอกสาร และข้อมูล:

- ขึ้นทะเบียนเอกสารใหม่ พร้อมอนุมัติจากผู้บริหารระดับสูงหรือบุคคลที่เกี่ยวข้องก่อนนำไปใช้งาน
- กำหนดแนวทางการเผยแพร่ การทบทวน และการแก้ไขเอกสารให้เป็นไปตามมาตรฐานความปลอดภัย
- มีมาตรการยกเลิก และทำลายเอกสารที่หมดอายุ หรือเลิกใช้งาน
- แบ่งระดับการรักษาความมั่นคงปลอดภัยของเอกสารตามชั้นความลับของข้อมูล
- ใช้มาตรการป้องกัน เช่น การกำหนดรหัสผ่าน และสิทธิ์การเข้าถึงระบบสารสนเทศ

มาตรการเหล่านี้มีเป้าหมายเพื่อให้มั่นใจว่าข้อมูลของบริษัทฯ ได้รับการปกป้อง และสนับสนุนการดำเนินธุรกิจได้อย่างยั่งยืน

5. การสำรองข้อมูล และการกู้คืนระบบ

บริษัทฯ มีนโยบายในการสำรองข้อมูล และการกู้คืนระบบเพื่อให้มั่นใจว่าข้อมูลสำคัญ รวมถึงระบบสามารถฟื้นฟูได้ในกรณีที่เกิดเหตุการณ์ไม่คาดคิดหรือภัยพิบัติ โดยกำหนดแนวทางการดำเนินงาน ดังนี้

5.1 การสำรองข้อมูล

- กำหนดให้มีการสำรองข้อมูลอย่างสม่ำเสมอโดยใช้เทคโนโลยีที่มีความปลอดภัย และเชื่อถือได้
- ใช้การสำรองข้อมูลในรูปแบบ ออฟไลน์ (Offline Backup) และ ออนไลน์ (Online Backup) เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้อย่างรวดเร็ว และครบถ้วน
- จัดทำแนวทาง และมาตรฐานในการสำรองข้อมูลให้เหมาะสมกับความสำคัญของข้อมูล
- ควบคุมการเข้าถึงข้อมูลสำรอง เพื่อป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต

5.2 การกู้คืนระบบ

- กำหนดแผนการกู้คืนระบบที่ชัดเจน โดยคำนึงถึงผู้ปฏิบัติงานที่เกี่ยวข้อง หน้าที่ความรับผิดชอบ กระบวนการ ข้อปฏิบัติ และมาตรการต่าง ๆ
- แผนการกู้คืนต้องครอบคลุมทั้ง การกู้คืนข้อมูล และการกู้คืนระบบสารสนเทศ ให้สามารถกลับมาดำเนินการได้ตามปกติ
- ทดสอบแผนกู้คืนระบบอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าการกู้คืนสามารถดำเนินการได้อย่างมีประสิทธิภาพ
- ปรับปรุง พัฒนาแนวทางการกู้คืนให้สอดคล้องกับเทคโนโลยี และสถานการณ์ที่เปลี่ยนแปลง

มาตรการเหล่านี้มีเป้าหมายเพื่อให้การดำเนินงานของบริษัทฯ ไม่หยุดชะงัก และสามารถรับมือกับสถานการณ์ที่เกิดขึ้นได้ อย่างมีประสิทธิภาพ

6. การบริหารจัดการสินทรัพย์ทางเทคโนโลยีสารสนเทศ และขีดความสามารถสารสนเทศ

6.1 การบริหารจัดการสินทรัพย์ทางเทคโนโลยีสารสนเทศ

บริษัทฯ กำหนดให้มีแนวทางในการบริหารจัดการสินทรัพย์ทางเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ และปลอดภัย โดยครอบคลุมสินทรัพย์ประเภทต่าง ๆ ดังต่อไปนี้

- **ประเภทสินทรัพย์ที่อยู่ภายใต้การบริหารจัดการ**
  - ข้อมูล
  - อุปกรณ์ฮาร์ดแวร์
  - ซอฟต์แวร์
  - อุปกรณ์ส่วนบุคคล (Bring Your Own Device : BYOD) ที่นำมาใช้ในงาน
  - บุคลากร
  - การบริการ
  - โดเมน
  - คลาวด์ และสื่อสังคมออนไลน์
- **มาตรการบริหารจัดการสินทรัพย์**
  - กำหนดมาตรการควบคุมการใช้งานสินทรัพย์ให้เหมาะสมตลอดวงจรชีวิตของสินทรัพย์
  - วงจรชีวิตของสินทรัพย์ประกอบด้วย:
    - การจัดหา
    - การลงทะเบียน
    - การบำรุงรักษา
    - การจำหน่าย
    - การทำลายสินทรัพย์
  - การบริหารจัดการต้องเป็นไปตามลำดับชั้นความลับของข้อมูลที่อยู่ในสินทรัพย์นั้น ๆ
  - มีการตรวจสอบและทบทวนสินทรัพย์อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าทะเบียนสินทรัพย์เป็นปัจจุบัน
  - ป้องกันความเสี่ยงจากการใช้เทคโนโลยีที่ล้าสมัย ที่อาจส่งผลกระทบต่อความเสียหายของฮาร์ดแวร์และซอฟต์แวร์
  - กำหนดหน้าที่และความรับผิดชอบต่อสินทรัพย์ของผู้ใช้งาน
  - รองรับการพัฒนาอย่างยั่งยืนในอนาคต

6.2 การบริหารจัดการขีดความสามารถสารสนเทศ

บริษัทฯ กำหนดแนวทางในการบริหารจัดการขีดความสามารถสารสนเทศเพื่อให้มั่นใจว่าทรัพยากรด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพ และเพียงพอ โดยครอบคลุมแนวทางดังต่อไปนี้

- **ทรัพยากรสารสนเทศที่อยู่ภายใต้การบริหารจัดการ**
  - ข้อมูลสารสนเทศ
  - บุคลากร
  - อุปกรณ์
  - เทคโนโลยี
  - เครือข่ายผู้ให้บริการสารสนเทศ
- **มาตรการบริหารจัดการขีดความสามารถสารสนเทศ**
  - ควบคุมการใช้งานทรัพยากรสารสนเทศให้เกิดประสิทธิภาพสูงสุด
  - ตอบสนองต่อความต้องการของบริษัทฯ และตรงตามความต้องการของผู้ใช้งาน
  - สนับสนุนการดำเนินงานของบริษัทฯ ให้มีความต่อเนื่อง มั่นคง และเพียงพอ
  - กำหนดมาตรการจัดหาทรัพยากรสารสนเทศที่มีคุณภาพ และเพียงพอต่อการให้บริการ
  - ควบคุมให้สอดคล้องกับงบประมาณที่กำหนด
  - บำรุงรักษา อัปเกรดทรัพยากรสารสนเทศอย่างสม่ำเสมอ เพื่อรักษาความเสถียร และความปลอดภัยของระบบทั้งหมด

7. การจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ

7.1 การจัดหาและพัฒนาระบบสารสนเทศ

บริษัทฯ มุ่งมั่นในการจัดหา พัฒนาระบบสารสนเทศเพื่อให้ตอบสนองต่อความต้องการทางธุรกิจอย่างมีประสิทธิภาพและปลอดภัย โดยกำหนดนโยบายให้มีการควบคุมกระบวนการติดตั้งซอฟต์แวร์ที่ได้รับอนุญาต และมีมาตรฐานความปลอดภัยสูง

7.2 การอัปเดท และบำรุงรักษาระบบสารสนเทศ

บริษัทฯ มีการตรวจสอบ อัปเดตซอฟต์แวร์อย่างสม่ำเสมอเพื่อป้องกันช่องโหว่ทางเทคนิคที่อาจเกิดขึ้น ทั้งนี้จะมีการจัดการ รวมถึงบำรุงรักษาระบบสารสนเทศให้สามารถทำงานได้อย่างต่อเนื่อง และปลอดภัย

7.3 การทดสอบระบบสารสนเทศก่อนใช้งานจริง

บริษัทฯ ให้ความสำคัญกับการทดสอบระบบก่อนการใช้งานจริง ดำเนินการแก้ไขช่องโหว่ที่พบเพื่อไม่ให้เกิดความเสี่ยงต่อข้อมูล และระบบของบริษัทฯ โดยการปฏิบัติตามนโยบายนี้ช่วยให้ระบบสารสนเทศของบริษัทฯ มีความมั่นคงพร้อมรองรับการเปลี่ยนแปลง และการเติบโตของธุรกิจอย่างยั่งยืน

8. การบริหารจัดการระบบเครือข่าย และการสื่อสาร

8.1 มาตรการรักษาความปลอดภัยของเครือข่าย

บริษัทฯ มีนโยบายในการบริหารจัดการระบบเครือข่าย และการสื่อสารอย่างเคร่งครัด เพื่อให้เครือข่ายมีประสิทธิภาพสูงสุด และปลอดภัยจากภัยคุกคามต่าง ๆ โดยกำหนดแนวทางการใช้งานที่เหมาะสม พร้อมกับการติดตั้งระบบรักษาความปลอดภัย เช่น ไฟร์วอลล์ (Firewall) โปรแกรมแอนตี้ไวรัส (Anti-Virus) และระบบป้องกันการบุกรุก (Intrusion Prevention System) เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

8.2 การควบคุมการเข้าถึงระบบเครือข่าย และการสื่อสารข้อมูล

บริษัทฯ กำหนดให้มีการควบคุมการเข้าถึงระบบเครือข่ายผ่านโครงข่ายแบบมีสาย ไร้สาย รวมถึงการปฏิบัติงานภายนอกบริษัทฯ ในการรับส่งข้อมูล โดยคำนึงถึงระดับความสำคัญของข้อมูล ครอบคลุมหน่วยงานภายใน และภายนอก เพื่อป้องกันการเข้าถึงระบบสารสนเทศของบริษัทฯ จากผู้ที่ไม่ได้รับอนุญาต รวมถึงลดความเสี่ยงจากภัยคุกคามที่อาจส่งผลกระทบต่อการดำเนินงานของบริษัทฯ

8.3 การสื่อสาร และการทบทวนมาตรการ

บริษัทฯ ให้ความสำคัญกับการสื่อสารมาตรการด้านความปลอดภัยเครือข่ายไปยังผู้ที่เกี่ยวข้อง เพื่อให้เกิดความเข้าใจ และปฏิบัติตามอย่างถูกต้อง พร้อมทั้งดำเนินการทบทวนมาตรการดังกล่าวเป็นระยะ เพื่อให้มั่นใจว่ายังคงมีประสิทธิภาพ สอดคล้องกับสถานการณ์ปัจจุบัน

9. การบริหารจัดการการให้บริการจากหน่วยงานภายนอก

9.1 การควบคุมคุณภาพ และความปลอดภัยของบริการภายนอก

บริษัทฯ กำหนดนโยบายเพื่อให้มั่นใจว่าบริการที่ได้รับจากหน่วยงานภายนอกมีคุณภาพ สอดคล้องกับมาตรฐานความปลอดภัย และเป็นไปตามข้อกำหนดของบริษัทฯ โดยมีการควบคุมและตรวจสอบข้อตกลงการให้บริการ (Service Level Agreement : SLA) อย่างเคร่งครัด เพื่อกำหนดระดับการบริการ การตอบสนองในกรณีฉุกเฉิน และการปฏิบัติตามกฎระเบียบที่เกี่ยวข้อง

9.2 การประเมิน และติดตามผลการให้บริการ

บริษัทฯ ดำเนินการประเมินประสิทธิภาพของบริการจากหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ให้บริการมีการปรับปรุง สามารถตอบสนองต่อการให้บริการตามความต้องการของบริษัทฯ ได้อย่างมีประสิทธิภาพและปลอดภัย ทั้งนี้ เพื่อรักษามาตรฐานการบริการ ความมั่นคงของข้อมูล และระบบที่เกี่ยวข้องกับการให้บริการจากหน่วยงานภายนอก

9.3 การกำกับดูแล และการจัดการการเปลี่ยนแปลง

บริษัทฯ กำหนดระเบียบ ข้อบังคับ หลักเกณฑ์ และแนวปฏิบัติในการดำเนินงาน เพื่อใช้ในการติดตาม ทบทวน และบริหารจัดการการเปลี่ยนแปลงการให้บริการ รวมถึงการตรวจประเมินการส่งมอบบริการของหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อควบคุมการเข้าถึงหรือใช้งานข้อมูลและระบบสารสนเทศของบริษัทฯ ให้เป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

10. การบริหารจัดการการเปลี่ยนแปลง

10.1 กระบวนการบริหารจัดการการเปลี่ยนแปลงในระบบสารสนเทศ และกระบวนการทางธุรกิจ

บริษัทฯ มุ่งมั่นในการบริหารจัดการการเปลี่ยนแปลงในระบบสารสนเทศ กระบวนการทางธุรกิจ อย่างเป็นระเบียบและควบคุม เพื่อให้มั่นใจว่าการเปลี่ยนแปลงทุกครั้งจะไม่ส่งผลกระทบต่อความเสถียรและความปลอดภัยของระบบ โดยกำหนดกระบวนการที่ชัดเจน ตั้งแต่การวางแผน การทดสอบ ไปจนถึงการติดตามผลหลังจากดำเนินการเปลี่ยนแปลงเสร็จสิ้น

10.2 การควบคุม ตรวจสอบ และปรับปรุงกระบวนการเปลี่ยนแปลง

บริษัทฯ ควบคุม ตรวจสอบการเปลี่ยนแปลงระบบสารสนเทศ รวมถึงกระบวนการทางธุรกิจทุกขั้นตอนให้เป็นไปตามมาตรฐาน และข้อกำหนดของบริษัทฯ โดยมีการประเมินผล ปรับปรุงกระบวนการอย่างต่อเนื่อง เพื่อเพิ่มประสิทธิภาพและลดความเสี่ยงจากการเปลี่ยนแปลงในอนาคต

11. การบริหารความต่อเนื่องในการดำเนินงาน และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

11.1 การวางแผนและป้องกันความเสี่ยงในการดำเนินงาน

บริษัทฯ มีนโยบายในการบริหารความต่อเนื่องในการดำเนินงาน โดยมุ่งเน้นการป้องกันและฟื้นฟูการดำเนินงานในกรณีฉุกเฉิน เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างไม่หยุดชะงักแม้ในสถานการณ์ที่ไม่คาดคิด โดยกำหนดแผนและแนวทางในการรับมือกับเหตุการณ์ฉุกเฉินที่อาจส่งผลกระทบต่อการดำเนินงาน เช่น ภัยธรรมชาติ การขัดข้องของระบบ หรือเหตุการณ์ทางเทคนิคที่สำคัญ

11.2 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

บริษัทฯ กำหนดให้มีแนวทางการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ครอบคลุมการตอบสนองต่อเหตุการณ์ด้านความปลอดภัย รวมถึงการป้องกันการบุกรุกและเหตุการณ์ละเมิดความปลอดภัยของระบบ โดยมีการกำหนดหน้าที่ของผู้ที่เกี่ยวข้อง ขั้นตอนปฏิบัติในการเฝ้าระวัง การรายงานเหตุการณ์ การวิเคราะห์ การเก็บรวบรวมหลักฐาน การแก้ปัญหา การบันทึกเหตุการณ์ที่เกิดขึ้น เพื่อให้การตอบสนองเป็นไปอย่างรวดเร็ว มีประสิทธิภาพ และมีแบบแผน

11.3 การติดตาม ทบทวน และปรับปรุงกระบวนการ

บริษัทฯ มีการติดตาม ทบทวน ปรับปรุง จัดเตรียมทรัพยากรที่จำเป็น และทำการฝึกซ้อมแผนกู้คืน แผนความต่อเนื่องในการดำเนินงาน และแนวทางการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ โดยนำความรู้ที่ได้รับจากการวิเคราะห์เหตุการณ์ที่เกิดขึ้นไปใช้ในการพัฒนาแนวทางป้องกัน เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง ลดโอกาสและผลกระทบของเหตุการณ์ที่อาจเกิดขึ้นซ้ำในอนาคต

12. การประเมินผล รายงาน และการปฏิบัติตามข้อกำหนด

12.1 การประเมินผล และรายงาน

บริษัทฯ มุ่งมั่นตรวจสอบ ประเมินผล มีการรายงานต่อคณะกรรมการบริหารความเสี่ยงบริษัทฯ และดำเนินงานตามนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยจะมีการทบทวน ปรับปรุงนโยบาย แนวปฏิบัติ มาตรฐาน กระบวนการทำงาน เอกสาร ข้อกำหนด กฎหมาย และข้อบังคับของบริษัทฯ ที่เกี่ยวข้องให้สอดคล้องกับกลยุทธ์ อย่างสม่ำเสมอ หรือมีการเปลี่ยนแปลงที่สำคัญ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศ และสภาพแวดล้อมที่เกิดขึ้น อย่างมีประสิทธิภาพ ได้ประสิทธิผล

12.2 การปฏิบัติตามข้อกำหนด

บริษัทฯ มีการติดตามและตรวจสอบการปฏิบัติตามข้อกฎหมาย ระเบียบข้อบังคับ ข้อผูกพันตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ มาตรฐาน และข้อกำหนดด้านความมั่นคงปลอดภัยของบริษัทฯ อย่างต่อเนื่อง โดยมีการสื่อสารกับผู้ที่เกี่ยวข้องทั้งภายใน ภายนอก ผู้มีส่วนได้เสีย คู่ค้า ลูกค้า ผู้ปฏิบัติงานให้รับทราบ รวมทั้งมีการทบทวนและตรวจสอบการปฏิบัติตามนโยบายของบริษัทฯ

13. ช่องทางเผยแพร่นโยบาย และแนวปฏิบัติ

เผยแพร่นโยบาย แนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้พนักงานบริษัทฯ ผู้มีส่วนได้เสีย ลูกค้า คู่ค้า และผู้ที่เกี่ยวข้องรับทราบ ผ่านช่องทางต่าง ๆ ดังนี้

- เว็บไซต์ เช่น intranet.icc.co.th www.icc.co.th investor.icc.co.th และอื่น ๆ
- แอปพลิเคชันต่าง ๆ เช่น ICCHR App
- เอกสาร และสัญญาต่างๆ ที่เกี่ยวข้อง

ประกาศฉบับนี้ให้มีผลใช้บังคับตั้งแต่ วันจันทร์ ที่ 3 มีนาคม 2568 เป็นต้นไป

.....

(นายธรรมรัตน์ โชควัฒนา)

ประธานกรรมการบริหาร

บันทึกเสนอที่ประชุมคณะกรรมการบริษัท ครั้งที่ .....ในวันที่ 21 เดือนกุมภาพันธ์ พ.ศ. 2568

เรียน คณะกรรมการบริษัท

เรื่อง ประกาศนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ปี พ.ศ. 2568

☑ เพื่อพิจารณา
☐ เพื่อทราบ
☐ เพื่อให้สัตยาบัน

ข้อมูลเดิม

บริษัท ไอ.ซี.ซี. อินเตอร์เนชั่นแนล จำกัด (มหาชน) ได้ประกาศใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตั้งแต่วันที่ 16 มกราคม พ.ศ. 2560 ซึ่งมีผลบังคับใช้มาเป็นเวลา 8 ปี ทั้งนี้ บริษัทฯ ได้กำหนดให้มีการจัดทำ เพื่อความเหมาะสม มีประสิทธิภาพ และมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี และดิจิทัล ตลอดจนป้องกันปัญหาที่อาจเกิดจากการใช้งานที่ไม่ถูกต้อง หรือภัยคุกคามทางไซเบอร์ต่าง ๆ ที่อาจส่งผลกระทบต่อบริษัทฯ

คำเสนอ

นโยบายต้องมีการทบทวนอย่างน้อยปีละหนึ่งครั้ง เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว ส่งผลให้ภัยคุกคามทางไซเบอร์ซับซ้อนยิ่งขึ้น บริษัทฯ จึงเห็นสมควรปรับปรุงแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (เดิม) ให้สอดคล้องกับโครงสร้าง และการดำเนินธุรกิจที่เปลี่ยนแปลง เสริมสร้างระบบเทคโนโลยีสารสนเทศให้ทันสมัย ลดความเสี่ยง ผลกระทบจากภัยคุกคามทางไซเบอร์ ตลอดจนสนับสนุนธุรกิจ และดิจิทัล

ข้อสรุป

นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ปี พ.ศ. 2568 (ใหม่) ถูกประกาศใช้ทดแทนแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (เดิม) โดยมุ่งเน้นให้ระบบสารสนเทศมีการอำนวยความสะดวก เพิ่มประสิทธิภาพ ประสิทธิผล ความมั่นคงปลอดภัย เพื่อความยั่งยืน และความต่อเนื่องทางธุรกิจ

ข้อคิดเห็นของผู้เสนอ

ดังนั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ มีเสถียรภาพ มั่นคง และปลอดภัย ข้อมูลสารสนเทศครบถ้วน พร้อมใช้งาน จึงขอพิจารณา ประกาศใช้นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ปี พ.ศ. 2568 ที่ปรับปรุงใหม่ ในวันจันทร์ที่ 3 มีนาคม ปี พ.ศ. 2568

ผู้เสนอ .....

(ดร. สุรัตน์ วงศ์รัตนภัสสร)
ประธานเจ้าหน้าที่บริหาร
สายงานเทคโนโลยีสารสนเทศ

บันทึกเสนอที่ประชุมคณะกรรมการบริษัท ครั้งที่ .....ในวันที่ 21 เดือนกุมภาพันธ์ พ.ศ. 2568

เรียน คณะกรรมการบริษัท

เรื่อง ประกาศนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ปี พ.ศ. 2568

☑ เพื่อพิจารณา
☐ เพื่อทราบ
☐ เพื่อให้สัตยาบัน

1. ได้รับอนุมัติจากมติที่ประชุมคณะกรรมการบริหารความเสี่ยง
วันที่ 5 ก.พ. 68

.....
(นายณัฐพร จาตุศรีพิทักษ์)
ประธานคณะกรรมการบริหารความเสี่ยง

2. ได้รับอนุมัติจากมติที่ประชุมคณะกรรมการบริษัท
วันที่ 21 ก.พ. 68

.....
(นายบุญเกียรติ โชควัฒนา)
ประธานกรรมการบริษัท
ประธานที่ประชุมคณะกรรมการบริษัท