Plan B Media Public Company Limited
1700, Plan B Tower, New Petchburi Road, Makkasan, Ratchathewi, Bangkok 10400
Tel.+662 530 8053-6 | Fax.+662 530 8057 | E-mail : info@planbmedia.co.th | Tax ID. 0107556000507
www.planbmedia.co.th

นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์

บริษัท แพลน บี มีเดีย จำกัด (มหาชน) รวมถึงบริษัทย่อย บริษัทร่วม และบริษัทที่บริษัทมีอำนาจควบคุม (ต่อไปนี้เรียกว่า "**บริษัท**") ให้ความสำคัญต่อการพัฒนาเทคโนโลยีดิจิทัลและการใช้ข้อมูลในการดำเนินธุรกิจของบริษัท ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของข้อมูล รวมถึงการป้องกันภัยคุกคามทางไซเบอร์ นโยบายนี้จัดทำขึ้นเพื่อสร้างแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลและไซเบอร์ของบริษัท

ขอบเขตนโยบาย

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์ของบริษัท ทั้งที่อยู่ภายในหรือภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคลาวด์ที่บริษัทจัดหา ซึ่งครอบคลุมถึง

1) พนักงานและหน่วยงานทั้งหมดของบริษัท
2) บุคคลภายนอกบริษัทที่ได้รับสิทธิเข้าถึงสินทรัพย์ที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท

การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขององค์กรที่ดี (Governance of Enterprise IT)

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายเพื่อทำให้แน่ใจว่าบริษัทสามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ การบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากร และข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายขององค์กรและบริการความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่าเทคโนโลยีนั้นบริษัทนำมาใช้งานสามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในการดำเนินธุรกิจและสร้างศักยภาพในการแข่งขัน รวมทั้งเพิ่มมูลค่าให้กับบริษัทในระยะยาว

แนวปฏิบัติ

1. การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

- **การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)**
  - จัดให้มีมาตรการต่าง ๆ เพื่อให้มั่นใจว่าการรักษาความปลอดภัยของข้อมูลมีความเพียงพอและเหมาะสมสอดคล้องกับการดำเนินธุรกิจและระดับความสำคัญของข้อมูล รวมถึงปัจจัยภายในและภายนอกที่ส่งผลกระทบต่อความปลอดภัยของข้อมูลของบริษัท ให้ความสำคัญกับการรักษาความลับ ความพร้อมใช้งาน ความครบถ้วนและถูกต้องของข้อมูล เพื่อให้เป็นไปตามกฎหมาย กฎเกณฑ์ และข้อบังคับของบุคคลภายนอกที่เกี่ยวข้อง
  - กรรมการ ผู้บริหาร และพนักงานทุกคนจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์ของบริษัทอย่างเคร่งครัด โดยไม่ละเมิดความเป็นส่วนตัวของผู้อื่น ไม่ใช้ข้อมูลที่เป็นความลับที่ไม่ได้รับอนุญาต รวมถึงการเข้าถึงข้อมูลและไฟล์ของผู้ใช้งานรายอื่นโดยไม่ได้รับอนุญาต ตามกฎและข้อบังคับของบริษัทเกี่ยวกับการใช้อุปกรณ์ และ/หรือเครื่องมือในระบบคอมพิวเตอร์
  - บริษัทกำหนดบทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการดำเนินงานระบบสารสนเทศและการรักษาความปลอดภัยของข้อมูลไว้อย่างชัดเจน พร้อมจัดลำดับขั้นตอนการดำเนินการให้เหมาะสมกับลักษณะของงาน รวมถึงการกำหนดสิทธิ์ในการเข้าถึงข้อมูลที่มีความสำคัญ โดยอุปกรณ์และสถานที่ที่ใช้จัดเก็บข้อมูลสำคัญจะต้องได้รับการควบคุมทั้งในด้านกายภาพและระบบสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- เจ้าของข้อมูลมีหน้าที่ในการทบทวนความเหมาะสมของสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสิทธิ์ที่ได้รับการกำหนดยังคงมีความเหมาะสมกับบทบาทหน้าที่ในปัจจุบัน
- ผู้ดูแลระบบมีหน้าที่ควบคุมการเข้าถึงข้อมูลในแต่ละระดับชั้นความลับ ทั้งในกรณีการเข้าถึงข้อมูลโดยตรงและผ่านระบบสารสนเทศ โดยต้องจัดทำรายชื่อบัญชีผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบและยืนยันตัวตนของผู้ใช้งานสำหรับการเข้าถึงข้อมูลแต่ละระดับ
- กำหนดนโยบายรหัสผ่านให้สอดคล้องกับการดำเนินธุรกิจและสถานการณ์ปัจจุบัน ตลอดจนสื่อสารให้พนักงานทุกคนทราบว่าจะต้องเก็บรหัสผ่านและรหัสอื่นใดที่บริษัทกำหนดไว้เพื่อเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลบริษัทหรือข้อมูลส่วนบุคคลอย่างเป็นความลับ รหัสผ่านจะต้องถูกเก็บไว้โดยไม่ให้ผู้อื่นทราบและห้ามแบ่งปันกับบุคคลอื่น ต้องปฏิบัติตามนโยบายรหัสผ่านอย่างเคร่งครัด
- การใช้อุปกรณ์ส่วนบุคคลเชื่อมต่อระบบข้อมูลของบริษัทจะต้องเป็นไปตามกฎและข้อบังคับที่กำหนดโดยผู้รับผิดชอบระบบข้อมูล
- ในระหว่างการจ้างงาน พนักงานจะต้องไม่กระทำการใด ๆ และ/หรือ ละเว้นการกระทำใด ๆ ที่ก่อให้เกิดความเสียหายแก่บริษัท อันเป็นผลจากข้อมูลอันเป็นเท็จ และ/หรือ รายงาน หรือบันทึก หรือการสื่อสาร ไม่ว่าจะด้วยวิธีใดก็ตาม หากมีการจงใจละเมิดนโยบายหรือมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลที่ก่อให้เกิดความเสียหายต่อบริษัท ผู้ที่ฝ่าฝืนจะถูกลงโทษตามกฎและข้อบังคับของบริษัท รวมทั้งจะถูกดำเนินคดีตามกฎหมาย หากการกระทำนั้นเป็นการละเมิดกฎหมาย
- ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น
- การเข้าถึงระบบสารสนเทศของบริษัทจากภายนอก ต้องเชื่อมต่อผ่านระบบ VPN (Virtual Private Network) ที่บริษัทกำหนดเท่านั้น เพื่อให้แน่ใจว่ามีการเข้ารหัสข้อมูลที่ส่งผ่านเครือข่ายสาธารณะ ทั้งนี้ การใช้ VPN จะต้องผ่านการพิสูจน์ตัวตน และมีการบันทึกการใช้งาน (Log) เพื่อใช้ในการตรวจสอบย้อนหลัง

- **การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)**
  - กำหนดบทบาท ความรับผิดชอบ และหน้าที่ในการดำเนินการให้เหมาะสมกับการดำเนินงานเกี่ยวกับระบบสารสนเทศและความปลอดภัยของข้อมูล รวมถึงการตั้งค่าการอนุญาตและการควบคุมการเข้าถึงข้อมูลสำคัญ นอกจากนี้อุปกรณ์หรือพื้นที่ที่ใช้ในการจัดเก็บข้อมูลสำคัญ ควรได้รับการควบคุมอย่างเหมาะสมผ่านระบบจัดเก็บข้อมูลทางกายภาพและสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต
  - พนักงานต้องใช้ทรัพย์สินของบริษัทอย่างระมัดระวังและรับผิดชอบ อุปกรณ์ที่ได้รับจากบริษัทควรอยู่ในสภาพดีอย่างสม่ำเสมอ โดยสามารถติดต่อแผนกซ่อมแซมเมื่อเกิดความเสียหาย ทรัพย์สินของบริษัทจะต้องไม่สูญหายหรือถูกทำลาย แม้อุปกรณ์นั้นจะไม่ได้เป็นความรับผิดชอบของพนักงานโดยตรง ห้ามนำทรัพย์สินใด ๆ ไปใช้เพื่อวัตถุประสงค์อื่น เว้นแต่เพื่อผลประโยชน์ของบริษัท อุปกรณ์ใด ๆ ที่มีข้อมูลสำคัญหรือสามารถเข้าถึงระบบข้อมูลของบริษัทได้ จะต้องป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตนำไปใช้ เช่น การตั้งรหัสผ่านหรือโปรแกรมรักษาหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน หากอุปกรณ์สูญหายหรือถูกขโมย ให้แจ้งฝ่ายระบบสารสนเทศเพื่อการจัดการโดยเร็วที่สุด เพื่อความปลอดภัยของข้อมูล
  - มีการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการจัดเก็บไว้ที่ส่วนกลาง เพื่อรักษาให้อุปกรณ์อยู่ในสภาพดีและพร้อมใช้งานอย่างต่อเนื่อง

- บริษัทต้องจัดให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท

2. การจัดการข้อมูลสารสนเทศและการรักษาความลับ

- **การจำแนกประเภทของข้อมูลสารสนเทศ (Information Classification)**

บริษัทมีการแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับขององค์กร ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยมีการกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

1) มีการจัดแบ่งประเภทของข้อมูล แบ่งออกเป็น 2 ประเภท
   - ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี
   - ข้อมูลสารสนเทศด้านการใช้งานของแต่ละหน่วยงาน เป็นข้อมูลที่เกี่ยวข้องกับการใช้งานของแต่ละหน่วยงานตามฟังก์ชันของการทำงานของหน่วยงานนั้น ๆ
2) การจัดแบ่งระดับความสำคัญของข้อมูล แบ่งออกเป็น 3 ระดับ
   - ข้อมูลที่มีระดับความสำคัญมากที่สุด
   - ข้อมูลที่มีระดับความสำคัญปานกลาง
   - ข้อมูลที่มีระดับความสำคัญน้อย
3) การจัดแบ่งลำดับชั้นของข้อมูล แบ่งออกเป็น 4 ระดับ
   - ข้อมูลลับที่สุด (Top Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
   - ข้อมูลลับมาก (Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
   - ข้อมูลลับ หรือ ใช้ภายใน (Internal Use) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
   - ข้อมูลทั่วไป หรือ สาธารณะ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้
4) การจัดแบ่งลำดับชั้นการเข้าถึง แบ่งออกเป็น 3 ระดับ
   - ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่ที่มีและลำดับชั้นในบัญชีรายชื่อในหน่วยงานนั้น
   - ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป
   - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับอนุญาตตามกฎหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิที่ได้รับในขอบเขตมาตามอำนาจหน้าที่

- **การสำรองข้อมูล (Backup)**
   - ข้อมูลที่มีความสำคัญต้องได้รับการจัดเก็บอย่างปลอดภัย พร้อมทั้งมีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และขั้นตอนการตอบสนองต่อเหตุการณ์ฉุกเฉิน (Incident Response Plan) โดยแผนการกู้คืนข้อมูลจากเหตุการณ์เสียหายจะต้องได้รับการทดสอบอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถนำไปใช้งานได้จริงในสถานการณ์ฉุกเฉิน

- ผู้ดูแลระบบ หรือบุคลากรที่ได้รับมอบหมาย มีหน้าที่ดำเนินการสำรองข้อมูลและทดสอบความสมบูรณ์ของข้อมูลที่สำรองไว้ตามรอบระยะเวลาที่กำหนด และให้เป็นไปตามนโยบายการสำรองและกู้คืนข้อมูลของบริษัท
- ในกรณีที่เกิดปัญหาซึ่งส่งผลให้ไม่สามารถดำเนินการสำรองข้อมูลได้อย่างสมบูรณ์ ให้ดำเนินการวิเคราะห์สาเหตุแก้ไขปัญหา และจัดทำรายงานสรุปผล พร้อมนำเสนอผู้จัดการฝ่ายเทคโนโลยีสารสนเทศเพื่อพิจารณาและดำเนินการในขั้นตอนถัดไป

- **การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)**

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และป้องกันข้อมูลที่เป็นข้อมูลที่มีขั้นความลับ การปลอมแปลงหรือความถูกต้องของข้อมูลสารสนเทศ ไม่ให้มีการรั่วไหลออกไปสู่บุคคลภายนอกที่ไม่เกี่ยวข้องหรือไม่มีสิทธิในการเข้าถึงข้อมูล บริษัทจึงได้มีการจัดทำมาตรการการควบคุมการเข้ารหัสข้อมูล รายละเอียดดังนี้

การบริหารจัดการข้อมูล

- บริษัทกำหนดบทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการดำเนินงานระบบสารสนเทศและการรักษาความปลอดภัยของข้อมูลไว้อย่างชัดเจน พร้อมจัดลำดับขั้นตอนการดำเนินการให้เหมาะสมกับลักษณะของงาน รวมถึงการกำหนดสิทธิ์ในการเข้าถึงข้อมูลที่มีความสำคัญ โดยอุปกรณ์และสถานที่ที่ใช้จัดเก็บข้อมูลสำคัญจะต้องได้รับการควบคุมทั้งในด้านกายภาพและระบบสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- บริษัทกำหนดนโยบายรหัสผ่านให้สอดคล้องกับการดำเนินธุรกิจและสถานการณ์ปัจจุบัน ตลอดจนสื่อสารให้พนักงานทุกคนทราบว่าจะต้องเก็บรหัสผ่านและรหัสอื่นใดที่บริษัทกำหนดไว้เพื่อเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลบริษัท หรือข้อมูลส่วนบุคคลอย่างเป็นความลับ รหัสผ่านจะต้องถูกเก็บไว้โดยไม่ให้ผู้อื่นทราบและห้ามแบ่งปันกับบุคลอื่น ต้องปฏิบัติตามนโยบายรหัสผ่านอย่างเคร่งครัด
- ในกรณีที่มีการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ บริษัทจะใช้เทคโนโลยีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้งานระบบรักษาความปลอดภัยแบบชั้นข้อมูล หรือ SSL (Secure Socket Layer) และการเชื่อมต่อเครือข่ายผ่าน VPN (Virtual Private Network) เป็นต้น
- บริษัทมีการกำหนดมาตรการด้านความปลอดภัยในกรณีที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการทำงานออกนอกพื้นที่ของบริษัท เช่น ในกรณีที่ต้องส่งซ่อมหรือให้ผู้ให้บริการเข้าดำเนินการ ณ สถานที่ติดตั้ง อุปกรณ์จะต้องผ่านกระบวนการลบหรือปกปิดข้อมูลภายในก่อนทุกครั้ง เพื่อป้องกันความเสี่ยงจากการรั่วไหลของข้อมูล

การควบคุมในการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

- บริษัทดำเนินการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ที่ใช้ในการประมวลผลข้อมูล โดยคำนึงถึงลักษณะการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ มีการกำหนดแนวทางและหลักเกณฑ์ในการให้สิทธิ์การเข้าถึงอย่างเหมาะสม เพื่อให้พนักงานในแต่ละระดับมีความเข้าใจและปฏิบัติตามอย่างเคร่งครัด พร้อมทั้งตระหนักถึงความสำคัญในการรักษาความปลอดภัยของระบบ เช่น การติดตั้งโปรแกรมในระบบสามารถดำเนินการได้โดยผู้บริหารที่ได้รับมอบหมายให้มีสิทธิระดับผู้ดูแลระบบเท่านั้น หรือการเข้าห้องควบคุมแม่ข่ายข้อมูล (Server) ต้องมีการบันทึกประวัติการเข้าออกและจำกัดสิทธิ์เฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น
- การกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิ์ในการใช้โปรแกรมภายในองค์กร (Application System) สิทธิ์ในการเข้าถึงอินเทอร์เน็ต สิทธิ์การใช้พื้นที่จัดเก็บข้อมูลร่วม เป็นต้น จะต้องให้เฉพาะเท่าที่จำเป็นต่อการปฏิบัติงาน เช่น พนักงานสามารถเข้าถึงไฟล์ที่เป็นของแผนกตนเองได้ ส่วนข้อมูลของแผนกอื่นจะเข้าถึงได้เฉพาะในส่วนที่กำหนดไว้ให้ใช้ร่วมกันเท่านั้น ทั้งนี้ ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษรและมีการทบทวนสิทธิ์การใช้งานเป็นระยะอย่างสม่ำเสมอ

- ในกรณีที่มีความจำเป็นต้องให้สิทธิ์แก่บุคคลอื่น เพื่อใช้งานระบบสารสนเทศหรือเครือข่ายของบริษัทในลักษณะเร่งด่วนหรือชั่วคราว จะต้องมีขั้นตอนและแนวปฏิบัติที่ชัดเจน โดยต้องได้รับการอนุมัติจากผู้มีอำนาจ พร้อมทั้งมีการบันทึกเหตุผลและระยะเวลาที่ได้รับสิทธิ์อย่างชัดเจน และต้องดำเนินการระงับสิทธิ์ดังกล่าวทันทีเมื่อสิ้นสุดระยะเวลาที่กำหนด

การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- บริษัทมีมาตรการปกป้องข้อมูลรหัสผ่านของผู้ใช้งาน โดยใช้ระบบเข้ารหัสไฟล์ที่จัดเก็บรหัสผ่าน เพื่อป้องกันไม่ให้ผู้อื่นสามารถเข้าถึงหรือแก้ไขข้อมูลได้ เช่น การเข้ารหัสรหัสผ่านก่อนจัดเก็บลงในฐานข้อมูลของระบบ
- มีการตรวจสอบรายชื่อบัญชีผู้ใช้งานในระบบที่มีความสำคัญอย่างสม่ำเสมอ โดยเฉพาะบัญชีที่ไม่มีสิทธิ์ใช้งานแล้ว เช่น บัญชีของพนักงานที่ลาออก หรือบัญชีที่ระบบสร้างขึ้นโดยอัตโนมัติ โดยบริษัทจะดำเนินการระงับสิทธิ์ทันทีเมื่อพบความไม่เหมาะสม เช่น ปิดการใช้งาน ลบบัญชี หรือเปลี่ยนรหัสผ่านใหม่
- ระบบมีการยืนยันตัวตนและตรวจสอบสิทธิ์ของผู้ใช้งานก่อนเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด เช่น การใช้ระบบยืนยันตัวตนสองขั้นตอน รวมถึงการกำหนดให้ผู้ใช้งานแต่ละรายมีบัญชีส่วนตัวเฉพาะราย เพื่อความปลอดภัยในการเข้าถึงระบบ นอกจากนี้ ยังมีมีการกำหนดแนวทางการตั้งรหัสผ่านที่ปลอดภัยและยากต่อการคาดเดา พร้อมควบคุมการใช้งานรหัสผ่านอย่างรัดกุม ดังนี้
    1) รหัสผ่านต้องมีความยาวไม่น้อยกว่า 9 ตัวอักษร และควรประกอบด้วยทั้งตัวอักษรและตัวเลข
    2) ต้องมีอักขระพิเศษ เช่น : ; < > $ @ # เป็นต้น
    3) ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน
    4) ไม่สามารถใช้รหัสผ่านเดิมซ้ำกับรหัสผ่านที่เคยใช้ใน 4 ครั้งล่าสุด
    5) หากมีการใส่รหัสผ่านผิดเกิน 5 ครั้ง ระบบจะระงับการเข้าถึงเพื่อป้องกันความเสี่ยง
    6) ผู้ใช้งานที่ได้รับรหัสผ่านเริ่มต้น หรือได้รับรหัสผ่านใหม่ จะต้องเปลี่ยนรหัสผ่านทันทีที่เข้าสู่ระบบครั้งแรก

- **การป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personally Identifiable Information)**
    - จัดให้มีการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์ตลอดจนการสื่อสารที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ความปลอดภัยของข้อมูล และภัยคุกคามทางไซเบอร์ให้กับพนักงานทุกคนอย่างสม่ำเสมอ
    - กรรมการ ผู้บริหาร และพนักงานทุกคนจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลและไซเบอร์ของบริษัทอย่างเคร่งครัด โดยไม่ละเมิดความเป็นส่วนตัวของผู้อื่น ไม่ใช้ข้อมูลที่เป็นความลับที่ไม่ได้รับอนุญาต รวมถึงการเข้าถึงข้อมูลและไฟล์ของผู้ใช้งานรายอื่นโดยไม่ได้รับอนุญาต ตามกฎและข้อบังคับของบริษัทเกี่ยวกับการใช้อุปกรณ์ และ/หรือเครื่องมือในระบบคอมพิวเตอร์
    - กำหนดนโยบายรหัสผ่านให้สอดคล้องกับการดำเนินธุรกิจและสถานการณ์ปัจจุบัน ตลอดจนสื่อสารให้พนักงานทุกคนทราบว่าจะต้องเก็บรหัสผ่านและรหัสอื่นใดที่บริษัทกำหนดไว้เพื่อเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลบริษัทหรือข้อมูลส่วนบุคคลอย่างเป็นความลับ รหัสผ่านจะต้องถูกเก็บไว้โดยไม่ให้ผู้อื่นทราบและห้ามแบ่งปันกับบุคคลอื่น ต้องปฏิบัติตามนโยบายรหัสผ่านอย่างเคร่งครัด
    - พนักงานต้องใช้ทรัพย์สินของบริษัทอย่างระมัดระวังและรับผิดชอบ อุปกรณ์ที่ได้รับจากบริษัทควรอยู่ในสภาพดีอย่างสม่ำเสมอ โดยสามารถติดต่อแผนกซ่อมแซมเมื่อเกิดความเสียหาย ทรัพย์สินของบริษัทจะต้องไม่สูญหายหรือ

ถูกทำลาย แม้อุปกรณ์นั้นจะไม่ได้เป็นความรับผิดชอบของพนักงานโดยตรง ห้ามนำทรัพย์สินใด ๆ ไปใช้เพื่อวัตถุประสงค์อื่น เว้นแต่เพื่อผลประโยชน์ของบริษัท อุปกรณ์ใด ๆ ที่มีข้อมูลสำคัญหรือสามารถเข้าถึงระบบข้อมูลของบริษัทได้ จะต้องป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตนำไปใช้ เช่น การตั้งรหัสผ่านหรือโปรแกรมรักษาหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน หากอุปกรณ์สูญหายหรือถูกขโมย ให้แจ้งฝ่ายระบบสารสนเทศเพื่อการจัดการโดยเร็วที่สุด เพื่อความปลอดภัยของข้อมูล

- พนักงานต้องรับทราบและปฏิบัติตามแนวปฏิบัติในการใช้คอมพิวเตอร์และระบบเครือข่ายอย่างเหมาะสม รวมถึงขั้นตอนการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันมิให้ข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ตั้งใจ บริษัทส่งเสริมให้การรักษาความปลอดภัยของข้อมูลเป็นส่วนหนึ่งของการประเมินประสิทธิภาพการทำงานของพนักงานเพื่อการพัฒนาทรัพยากรบุคคลอย่างเหมาะสม
- ในระหว่างการจ้างงาน กรรมการ ผู้บริหาร และพนักงานทุกคน ต้องตระหนักถึงข้อมูลของบริษัทที่เรียกว่า "**ความลับทางการค้า**" ซึ่งหมายถึง ข้อมูลการค้าที่ยังไม่รู้จักกันโดยทั่วไปหรือยังเข้าถึงไม่ได้ในหมู่บุคคล ซึ่งโดยปกติแล้วบุคคลที่เข้าได้จะต้องเกี่ยวข้องกับข้อมูลดังกล่าว ข้อมูลที่เป็นประโยชน์ทางการค้าเนื่องจากเป็นความลับ และเป็นข้อมูลที่ผู้ควบคุมความลับทางการค้าใช้มาตรการที่เหมาะสมในการรักษาความลับ เพื่อให้ข้อมูลดังกล่าวสามารถระบุไว้ในสัญญาหรือข้อตกลงอื่นใดของบริษัท ตามที่ระบุไว้ในพระราชบัญญัติความลับทางการค้า พ.ศ. 2545 กรรมการ ผู้บริหาร และพนักงานทุกคน ตกลงที่จะรักษาความลับทางการค้าของบริษัทที่ได้ทราบหรือได้รับเพราะการทำงานในบริษัท และจะไม่ส่งต่อหรือคัดลอกไปยังบุคคลอื่นโดยไม่ได้รับอนุญาต รวมถึงการเปิดเผยและ/หรือ กระทำหรือไม่กระทำใด ๆ ที่ทำให้เสียหายต่อชื่อเสียงหรือธุรกิจของบริษัท
- รักษาความลับของลูกค้า คู่ค้าทางธุรกิจ หรือบุคคลที่เกี่ยวข้องอื่นของบริษัท
- ไม่เปิดเผยความลับ เอกสาร หรือความลับทางการค้าใด ๆ เป็นเวลา 1 ปี หลังจากพ้นจากตำแหน่งหน้าที่

3. การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

- **การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (Communications Security)**
  - ห้ามใช้ทรัพย์สินหรือใช้งานอินเทอร์เน็ตของบริษัท เพื่อวัตถุประสงค์ทางการค้าหรือเพื่อผลประโยชน์ส่วนตัว ยกเว้นเพื่อประโยชน์โดยตรงของบริษัท รวมทั้งหลีกเลี่ยงการใช้เว็บไซต์หรือจดหมายอิเล็กทรอนิกส์ที่เสี่ยงต่อการถูกคุกคามทางไซเบอร์ รวมไปถึงการใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ในการกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขายหรือเผยแพร่สิ่งที่ผิดกฎหมายหรือขัดต่อศีลธรรมอันดี เป็นต้น
  - ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่นเพื่อแก้ไข ลบเพิ่มเติม หรือคัดลอก
  - ห้ามติดตั้งซอฟต์แวร์หรือทำการบันทึกข้อมูลใด ๆ ลงในอุปกรณ์ และ/หรือเครื่องมือในระบบคอมพิวเตอร์ของบริษัทโดยไม่ได้รับอนุญาต
  - ห้ามนำซอฟต์แวร์ของบริษัทไปให้กับบุคคลอื่น ซึ่งรวมถึงซัพพลายเออร์ ผู้รับเหมา ลูกค้าของบริษัท และเพื่อวัตถุประสงค์ส่วนตัว นอกจากนี้การใช้งานอินเทอร์เน็ตหรือเชื่อมต่ออินเทอร์เน็ตโดยพนักงานเพื่อการโอนข้อมูล การเผยแพร่สื่อลามก การส่งและรับข้อมูลทางอีเมล (e-mail) ที่ฝ่าฝืนกฎหมายหรือละเมิดกฎหมายลิขสิทธิ์ โดยมีเจตนาหรือวัตถุประสงค์ที่ฝ่าฝืนนโยบายหรือข้อบังคับเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท หรือพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือกฎหมายอื่นที่เกี่ยวข้อง

- ห้ามละเมิดลิขสิทธิ์ของบริษัท และ/หรือ บริษัทอื่น ๆ ที่อนุญาตให้บริษัทใช้ซอฟต์แวร์คอมพิวเตอร์ โดยไม่คำนึงถึงสัญญา และ/หรือวิธีการใด ๆ ไม่ว่าจะมีการกระทำซ้ำ หรือแก้ไข หรือเผยแพร่สู่สาธารณะ หรือให้เช่า หรือคัดลอก ไม่ว่าจะเพื่อผลกำไรหรือไม่ก็ตาม
- มาตรการรักษาความปลอดภัยเครือข่ายที่เพียงพอและเหมาะสม ติดตั้งโปรแกรมเพื่อป้องกันการคุกคามจากภายนอกที่เป็นอันตรายต่อเซิร์ฟเวอร์หลักและเซิร์ฟเวอร์ลูกค้า และโปรแกรมควรได้รับการอัปเดตในเวลาที่เหมาะสม
- มีมาตรการรักษาความปลอดภัยเครือข่ายที่เพียงพอและเหมาะสม ติดตั้งโปรแกรมเพื่อป้องกันการคุกคามจากภายนอกที่เป็นอันตรายต่อเซิร์ฟเวอร์หลักและเซิร์ฟเวอร์ลูกค้า และโปรแกรมควรได้รับการอัปเดตในเวลาที่เหมาะสม
- มีการกำหนดควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย และต้องจัดบางเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้งานภายนอกที่ติดต่อกับบริษัท

- **การควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer)**
  - ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
  - ต้องมีการลงนามในสัญญาระหว่างบริษัทและหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA)
  - ห้ามนำซอฟต์แวร์ของบริษัทไปให้กับบุคคลอื่น ซึ่งรวมถึงซัพพลายเออร์ ผู้รับเหมา ลูกค้าของบริษัท และเพื่อวัตถุประสงค์ส่วนตัว นอกจากนี้ การใช้งานอินเทอร์เน็ตหรือเชื่อมต่ออินเทอร์เน็ตโดยพนักงานเพื่อการโอนข้อมูล การเผยแพร่สื่อลามก การส่งและรับข้อมูลทางอีเมล (e-mail) ที่ฝ่าฝืนกฎหมายหรือละเมิดกฎหมายลิขสิทธิ์ โดยมีเจตนาหรือวัตถุประสงค์ที่ฝ่าฝืนนโยบายหรือข้อบังคับเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัท หรือพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือกฎหมายอื่นที่เกี่ยวข้อง
  - การส่ง การใช้ การประมวลผล การจัดเก็บ การทำลายข้อมูล และอุปกรณ์ที่มีข้อมูลสำคัญต้องมีกระบวนการที่เหมาะสมเพื่อให้มั่นใจว่ามีการรักษาความปลอดภัยของข้อมูลเพียงพอ เพื่อป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตหรือเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
  - มีการจัดเก็บระบบสารสนเทศที่สำคัญ (Log) และกำหนดระยะเวลาการเก็บรักษาที่เหมาะสม จะถูกนำมาใช้ในการตรวจสอบและติดตามประวัติการใช้งานที่สอดคล้องตามกฎหมาย ระเบียบ และกฎระเบียบของหน่วยงานภายนอกที่เกี่ยวข้อง
  - มีกระบวนการป้องกันการหยุดชะงักของระบบสารสนเทศและการถูกโจมตีทางไซเบอร์อย่างทันท่วงที รวมถึงการพิจารณาดำเนินการเพื่อป้องกันการเกิดซ้ำของสถานการณ์ และรายงานไปยังคณะกรรมการบริหาร
  - มีการตอบสนองในกรณีเร่งด่วนที่ชัดเจน ซึ่งพนักงานและผู้มีส่วนได้เสียในองค์กรสามารถร้องเรียนหรือรายงานสิ่งที่น่าสงสัยเกี่ยวกับความปลอดภัยของข้อมูลและภัยคุกคามทางไซเบอร์ เพื่อให้บริษัทมีการปรับปรุงและมีการสื่อสารเพื่อจัดการกับปัญหา พนักงานทุกคนมีหน้าที่รายงานข้อมูลทันทีเมื่อมีเหตุการณ์ที่น่าสงสัยที่อาจนำไปสู่การละเมิดนโยบายหรือมาตรการ การโจรกรรมข้อมูล การแทรกแซง การบุกรุก หรือการทำลายระบบข้อมูลที่ส่งผลกระทบต่อความปลอดภัยของข้อมูลหรือทำให้เกิดความเสียหายต่อบริษัท

4. **การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)**
   - การพัฒนาระบบสารสนเทศต้องมีกระบวนการที่ถูกต้องและเชื่อถือได้ ครอบคลุมถึงกระบวนการออกแบบ พัฒนา ทดสอบ และการนำมาใช้งาน มีระบบที่แยกอย่างชัดเจนระหว่างระบบที่ใช้ในการพัฒนาและระบบที่ใช้งานจริง รวมถึงให้ความสำคัญกับการออกแบบระบบที่มีความปลอดภัยเพียงพอและมีการตรวจสอบความปลอดภัยก่อนใช้งานจริง
   - การแก้ไขระบบข้อมูลหรืออุปกรณ์ใด ๆ ที่เกี่ยวข้อง จะต้องมีขั้นตอนและกระบวนการที่เหมาะสม มีการประเมินผลกระทบและมีการสื่อสารกับผู้ที่เกี่ยวข้อง รวมถึงการทดสอบที่เพียงพอและอัปเดตเอกสารที่เกี่ยวข้องเป็นปัจจุบัน