ประกาศ
ที่ ISS 03/2563
เรื่อง นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ
(Information Technology Security Policy)

ด้วยบริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย ("บริษัท") ได้จัดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงานทั้งระบบ ทั้งนี้เพื่อให้การใช้บริการ และการให้บริการสามารถดำเนินการใช้งานร่วมกันได้อย่างเหมาะสม สอดคล้องกับนโยบายทางธุรกิจ และป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องทั้งจากผู้ใช้งาน และภัยคุกคามต่าง ๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของบริษัทให้ได้รับความเสียหายได้ ดังนั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ จึงเห็นสมควรกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อให้ถือเป็นแนวทางในการปฏิบัติเดียวกันดังต่อไปนี้

1. วัตถุประสงค์

1.1. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

1.2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม

1.3. เพื่อให้พนักงาน และผู้ที่ต้องใช้ หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม

1.4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลายแทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

2. ขอบเขตของประกาศ

นโยบายฉบับนี้ใช้กับบริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย (ยกเว้นบริษัท สยามแม็คโคร จำกัด (มหาชน) และบริษัทในกลุ่มฯ) ทั้งนี้ให้ครอบคลุมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคม เพื่อเข้าถึงสารสนเทศของ

บริษัท โดยให้ยกเลิกประกาศ ที่ สรบ.035/2551 เรื่องนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Technology Security Policy)

3. **หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)**

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้
- ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ
- การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต
- การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

การรักษาความมั่นคงปลอดภัยอย่างได้ผล จำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย

- การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของพนักงานและบุคคลภายนอกทุกคน
- การบริหาร และการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา
- การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบาย

ให้พนักงานและบุคคลภายนอกทราบอย่างชัดเจน เพื่อให้มีความเข้าใจในหน้าที่ และความรับผิดชอบในการรักษาความปลอดภัย ที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

4. คำจำกัดความ

4.1. "บริษัท (Company)" หมายถึง บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย

4.2. "หน่วยงานเทคโนโลยีสารสนเทศ" หมายถึง หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศของบริษัท ได้แก่ บริษัท โกซอฟท์ (ประเทศไทย) จำกัด และสำนัก Information System & Service (ISS)

4.3. "พนักงาน (Employee)" หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

4.4. "ผู้ใช้งาน (User)" หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท

4.5. "ผู้บังคับบัญชา" หมายถึง พนักงานซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท

4.6. "ระบบคอมพิวเตอร์ (Computer System)" หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่างๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่างๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัท

4.7. "ข้อมูลสารสนเทศ (Information Technology)" หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมายและสัญลักษณ์ต่างๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใดๆ

4.8. "ข้อมูลสำคัญ" หรือ "ข้อมูลที่เป็นความลับ (Sensitive Information)" หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจ

เป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง

4.9. "ระบบที่มีความสำคัญ (Important System)" หมายถึง ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์ เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัทให้เป็นปกติ และระบบที่ได้รับการกำหนดโดยหน่วยงานด้านความปลอดภัยข้อมูลและระบบสารสนเทศของบริษัท ทั้งนี้หากระบบที่มีความสำคัญดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงักหรือด้อยประสิทธิภาพ

4.10. "Remote Access" หมายถึง การเข้าสู่ระบบสารสนเทศของบริษัทจากระยะไกล

4.11. "เจ้าของระบบ (System Owner)" หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้นๆ

4.12. "ผู้ดูแลข้อมูล (Custodian)" หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศในการสนับสนุนงานการดูแล จัดการ และควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศกำหนด

4.13. "ผู้ดูแลระบบ (Administrator)" หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของบริษัท ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย

4.14. "การรักษาความมั่นคงปลอดภัย" หรือ "ความมั่นคงปลอดภัย (Security)" หมายถึง กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย

4.15. "บุคคลภายนอก (External Party)" หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น

- บริษัทคู่ค้า (Business Partner)
- ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
- ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier)

- ผู้ให้บริการต่างๆ (Service Provider)
- ที่ปรึกษา (Consultant)

5. หน้าที่ความรับผิดชอบ

5.1. หน้าที่ของกรรมการผู้จัดการและประธานเจ้าหน้าที่บริหาร (MD&CEO)

5.1.1. กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

5.2. หน้าที่ของ Chief Information Officer (CIO)

5.2.1. ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท

5.2.2. ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

5.3. หน้าที่ของ Cyber Security Officer (CSO)

5.3.1. กำหนดเป้าหมาย นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทโดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท

5.3.2. จัดการพัฒนานโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ Policy, Standard, Procedure และ Guideline เพื่อให้บริษัทได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)

5.3.3. จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน

5.3.4. มีการบริหารความเสี่ยงและการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจของบริษัท

5.3.5. นำเสนอผู้บริหารระดับสูง เช่น กรรมการผู้จัดการและประธานเจ้าหน้าที่บริหาร (MD&CEO) Chief Information Officer (CIO) เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง

5.3.6. เตรียมพร้อมรับสถานการณ์ และเรียนรู้เทคนิคใหม่ ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ

5.4. หน้าที่ของผู้บังคับบัญชา

5.4.1. ชี้แจง และส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

5.5. หน้าที่ของผู้ใช้งาน

5.5.1. ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทโดยเคร่งครัด

5.5.2. ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทให้มีความปลอดภัย

5.5.3. รายงานต่อบริษัททันที เมื่อพบว่าอุปกรณ์ หรือข้อมูลสารสนเทศสำคัญสูญหาย หรือพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อบริษัท

5.6. หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

5.6.1. จัดให้มีการจัดทำเอกสาร มาตรการ และขั้นตอนควบคุมการเข้าถึงข้อมูล ให้เป็นไปตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

5.6.2. ดูแลให้พนักงานปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

5.6.3. ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ

5.6.4. รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ

5.6.5. แจ้งหน่วยงานเทคโนโลยีสารสนเทศที่รับผิดชอบด้านการบริหารบัญชีผู้ใช้งานและสิทธิ์ในการใช้ระบบสารสนเทศเพื่อลบ/เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงาน / อำนาจหน้าที่ / โอนย้าย

5.7. หน้าที่ของหน่วยงานตรวจสอบภายใน (Internal Audit)

5.7.1. ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศตามความจำเป็น

6. บริษัทกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศในประเด็นสำคัญ ประกอบด้วย

6.1. ความปลอดภัยเกี่ยวกับทรัพย์สินสารสนเทศ

6.1.1. ทรัพย์สินด้านสารสนเทศ ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด ต้องมีการจัดทำบัญชีทรัพย์สินโดยผู้เป็นเจ้าของข้อมูล และผู้เกี่ยวข้องหน่วยงานสารสนเทศต้องร่วมจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศ รวมถึงต้องจัดทำและจัดการป้ายชื่อ สำหรับปิดฉลากเอกสารข้อมูลของอุปกรณ์ทรัพย์สินด้านสารสนเทศ

6.1.2. บริษัทต้องกำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม เอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลนั้น

6.1.3. การใช้งานทรัพย์สินที่เหมาะสม ต้องมีการจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรเพื่อป้องกันความเสียหายต่อทรัพย์สินด้านสารสนเทศ

6.2. ความปลอดภัยเกี่ยวกับบุคลากร

6.2.1. ต้องมีการกำหนดหน้าที่ และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร สำหรับผู้ใช้งาน หรือที่ว่าจ้างหน่วยงานภายนอกมาปฏิบัติงาน รวมทั้งกำหนดมาตรการป้องกันและดูแลรักษาความปลอดภัยสำหรับสารสนเทศของบริษัท

6.2.2. ต้องมีการตรวจสอบคุณสมบัติของผู้สมัครเข้าทำงานทุกกรณีโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และต้องสร้างความตระหนักเรื่องความมั่นคงปลอดภัยเบื้องต้นให้พนักงานเข้าใหม่พร้อมทั้งจัดให้พนักงานมีการลงนามหนังสือยินยอมการใช้ระบบเทคโนโลยีสารสนเทศของบริษัทอย่างมั่นคงปลอดภัย (เอกสารแนบท้าย)

6.2.3. จัดอบรมให้ความรู้แก่ผู้ใช้งานทุกคนเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากร ถ้ามีการเปลี่ยนแปลงทางด้านความมั่นคงปลอดภัยต้องแจ้งให้พนักงานทราบ

6.2.4. ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎและแนวปฏิบัติของบริษัท หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำ และเป็นไปตามระเบียบบริษัท

6.2.5. หากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตำแหน่งใดๆ สายงานทรัพยากรบุคคล ต้องแจ้งให้ผู้รับการว่าจ้างทราบ และผู้รับการว่าจ้างต้องปฏิบัติตามเงื่อนไขในสัญญาจ้างจนกว่าจะสิ้นสุดการว่าจ้าง และพนักงานซึ่งพ้นตำแหน่งจากการจ้างงานไม่ว่ากรณีใด ต้องคืนทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ เช่น กุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออกศูนย์คอมพิวเตอร์ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน ซึ่งหน่วยงานเทคโนโลยีสารสนเทศต้องถอดถอนสิทธิการเข้าใช้งานดังกล่าวด้วย

6.3. ความปลอดภัยเกี่ยวกับพื้นที่จัดเก็บข้อมูลและปฏิบัติงาน

6.3.1. ต้องมีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ และต้องจัดให้มีการป้องกันภัยคุกคามต่างๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อความไม่สงบ เป็นต้น รวมถึงการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัยต้องมีการจัดการป้องกันที่เพียงพอ

6.3.2. การส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก ต้องมีบริเวณเฉพาะที่จัดไว้ต่างหากเพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศของบริษัทโดยไม่ได้รับอนุญาต

6.3.3. พนักงานต้องป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

6.3.4. ทรัพย์สินด้านสารสนเทศจะต้องอยู่ในพื้นที่ที่เหมาะสมมีความปลอดภัย มีการจำแนกพื้นที่ในการใช้งานระบบสารสนเทศอย่างเหมาะสม มีการแยกศูนย์คอมพิวเตอร์ออกจากสถานที่ทำงานทั่วไป และกั้นเป็นห้องต่างหาก มีการควบคุมการเข้า-ออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยให้เข้า-ออกได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบและผู้ที่ได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร โดยแสดงบัตรประชาชน หรือบัตรที่ราชการออกให้

6.3.5. มีระบบไฟฟ้าสำรองเพื่อให้สามารถทำงานได้ตลอดเวลา และต้องมีการตรวจสอบระบบไฟฟ้าสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อเป็นการลดความเสียหายที่อาจจะเกิดขึ้น

6.3.6. การเดินสายเคเบิลต่าง ๆ ต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการเดินสายนั้นต้องติดป้ายกำกับให้รู้ต้นทางปลายทางของสาย

6.3.7. ต้องบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอหรือตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

6.3.8. ต้องมีมาตรการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น

6.3.9. พนักงานต้องมีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะนำอุปกรณ์ดังกล่าวทิ้งไป โดยต้องเป็นไปตามที่หน่วยงานเทคโนโลยีสารสนเทศกำหนด

6.3.10. ต้องมีขั้นตอนปฏิบัติสำหรับการจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

6.3.11. ต้องมีการกำหนดมาตรการการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

6.3.12. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการ และจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6.3.13. ต้องมีมาตรการการกำจัดสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร เช่น การเผา ตัด หั่น หรือทำลายสื่อบันทึกข้อมูลที่มีข้อมูลสำคัญในนั้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้มีบุคลากรผู้ทำหน้าที่ในการสอดส่องและดูแลการกำจัดหรือการทำลายสื่อบันทึกข้อมูล (ทั้งทำลายเองหรือจ้างบริษัทรับทำลายเป็นผู้ทำลายสื่อบันทึกข้อมูลเหล่านั้น) การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

6.4. ความปลอดภัยเกี่ยวกับการดูแลระบบสารสนเทศ

6.4.1. ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน เช่น ขั้นตอนการกู้คืนระบบ ขั้นตอนการบำรุงรักษาและดูแลระบบเป็นต้น และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานเมื่อมีการเปลี่ยนแปลงขั้นตอนหรือผู้รับผิดชอบ และต้องทบทวนอย่างน้อยปีละ 1 ครั้ง และต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบคอมพิวเตอร์ ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ฮาร์ดแวร์และซอฟต์แวร์

6.4.2. ต้องมีการแบ่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต

6.4.3. ต้องมีการแยกระบบสำหรับการพัฒนา และทดสอบแยกออกจากระบบงานจริงเพื่อป้องกันการเข้าถึงข้อมูล หรือเปลี่ยนแปลงต่อระบบงานที่ให้บริการจริงจากผู้ที่ไม่ได้รับอนุญาต และต้องติดตามสภาพการใช้งาน การวิเคราะห์ขีดความสามารถของทรัพยากรสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

6.4.4. การยอมรับระบบใหม่ต้องจัดให้มีเกณฑ์ในการยอมรับ และจัดให้มีการทดสอบระบบใหม่ก่อนที่จะตรวจรับระบบนั้นอย่างเป็นลายลักษณ์อักษร

6.5. ความปลอดภัยเกี่ยวกับการบริการของหน่วยงานภายนอก

6.5.1. ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการโดยหน่วยงานภายนอก เช่น มีการยอมรับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท และขอบเขต รายละเอียด ระดับการให้บริการ ต้องได้รับการตรวจสอบจากฝ่ายกฎหมายซีพี ออลล์ รวมถึงสัญญาในการไม่เปิดเผยข้อมูลของบริษัท เป็นต้น

6.5.2. หน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ที่ได้รับอนุญาตในการเข้าถึงระบบสารสนเทศของบริษัทต้องยอมรับและปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

6.5.3. บริษัทจะประเมินความเสี่ยงในการเข้าถึงระบบสารสนเทศ หรือที่มีผลกระทบต่อบริษัท ของหน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ถ้าจำเป็นต้องมีการเปิดเผยข้อมูลนั้นออกไป หน่วยงานภายนอกหรือบุคคลภายนอกนั้นต้องเซ็นสัญญาว่าจะไม่เปิดเผยความลับของบริษัท

6.5.4. ต้องตรวจสอบการให้บริการหรือสัญญาที่ทำกับหน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาให้บริการกับบริษัท โดยมีการทบทวนอย่างสม่ำเสมอตามความจำเป็น รวมถึงต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เช่น เมื่อมีการปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การเปลี่ยนเทคโนโลยีใหม่ เป็นต้น

6.6. ความปลอดภัยเกี่ยวกับเครือข่ายคอมพิวเตอร์

6.6.1. ต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และกำหนดสิทธิ์ผู้ที่ใช้งานผ่านเครือข่ายโดยอนุญาตเฉพาะผู้ที่มีสิทธิ์เท่านั้น

6.6.2. ต้องจำกัดการเชื่อมต่อจากภายนอกเข้าสู่ระบบเครือข่ายภายใน เช่นการเข้าถึงเครือข่ายจากระยะไกลผ่านทางอินเตอร์เน็ต รวมถึงไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย โดยไม่ได้รับอนุญาต

6.7. ความปลอดภัยเกี่ยวกับการแลกเปลี่ยนข้อมูลและสารสนเทศ

6.7.1. ต้องกำหนดนโยบาย แนวปฏิบัติ และมาตรการเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศภายในบริษัท ภายในกลุ่มบริษัท และหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิดอย่างเป็นลายลักษณ์อักษร เช่น การส่งข้อความทางอิเล็กทรอนิกส์ เป็นต้น

6.7.2. ต้องมีมาตรการตรวจทานก่อนส่งข้อมูลสารสนเทศออกสู่สาธารณะ โดยมีการประเมินความเสี่ยงและกำหนดมาตรการลดความเสี่ยงก่อนนำข้อมูลไปเผยแพร่

6.8. ความปลอดภัยเกี่ยวกับธุรกรรมออนไลน์

6.8.1. ต้องกำหนดมาตรการป้องกันสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ รวมถึงการป้องกันสารสนเทศที่รับ – ส่ง ที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ – ส่ง หรือสารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย

6.8.2. สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะต้องได้รับการป้องกันให้มีความถูกต้อง และความสมบูรณ์ก่อนที่จะนำไปเผยแพร่

6.9. ความปลอดภัยเกี่ยวกับการตรวจสอบการเข้าใช้งานระบบสารสนเทศ

6.9.1. ต้องกำหนดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศและกิจกรรมการใช้งานของผู้ใช้งานอย่างสม่ำเสมอ และต้องมีมาตรการป้องกันข้อมูลที่บันทึกที่เกี่ยวข้องกับการใช้งานสารสนเทศ ไม่ให้มีการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต รวมถึงต้องบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบนั้นๆ ด้วย

6.9.2. ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดที่เกี่ยวข้องวิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร และต้องตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องของบริษัทถูกบุกรุก

6.9.3. การเข้าถึงและการใช้งานระบบสารสนเทศของพนักงานจะต้องถูกสอบทานและทบทวนตามรอบระยะเวลาที่กำหนดไว้จากส่วนงานตรวจสอบภายใน โดยส่วนงานตรวจสอบภายในมีสิทธิ์ที่จะสอดส่องดูแลการกระทำใดๆ ที่ผู้ตรวจสอบสงสัยว่ามีการฝ่าฝืนนโยบายดังกล่าว

6.10. ความปลอดภัยเกี่ยวกับการควบคุมการเข้าถึงระบบสารสนเทศ

6.10.1. ต้องกำหนดให้มีขั้นตอนสำหรับการลงทะเบียนต่างๆ เพื่อให้มีสิทธิ์และควบคุมสิทธิ์ในการเข้าถึงสารสนเทศและระบบสารสนเทศของบริษัทตามความจำเป็น รวมถึงขั้นตอนการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น รวมถึงต้องมีกระบวนการจัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานตามความเหมาะสมหรือที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย

6.10.2. ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษาบัญชีผู้ใช้งาน และรหัสผ่านของตนให้มีความมั่นคงปลอดภัยเพียงพอ

6.10.3. พนักงานต้องมีวิธีป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล เช่น แจ้งหัวหน้าหน่วยงาน หรือเจ้าหน้าที่รักษาความปลอดภัยทุกครั้งที่พบเห็น รวมถึงมีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัยหรือพบเห็นได้ง่าย

6.10.4. ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมว่าบริการใดอนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้

6.10.5. การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทจะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงานและหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศสามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องถูกจำกัดการเข้าถึง ให้เฉพาะผู้ที่ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น และต้องได้รับความยินยอมจากเจ้าของข้อมูล

6.10.6. การเข้าถึงระบบสารสนเทศทุกระบบต้องได้รับการพิสูจน์ และยืนยันตัวตนทุกครั้งอย่างน้อยด้วย UserID และ Password ที่ได้รับจากผู้ดูแลระบบ ก่อนที่จะเข้าใช้งานได้ตามสิทธิที่ได้รับ และหากเป็นระบบสำคัญ หรือเป็นการใช้งานจากระยะไกล (Remote Access) จะต้องกำหนดให้มีการยืนยันตัวตนแบบ 2 ขั้นตอน (Two -Factor Authentication) ทั้งนี้ สิทธิ์ในการใช้งานต้องถูกทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง

6.10.7. การเปลี่ยนแปลงระบบสารสนเทศ /ระบบเน็ตเวิร์ค หรือแอพพลิเคชั่นใดๆ จะต้องได้รับการตรวจสอบและอนุญาตจากเจ้าของข้อมูล รวมถึงได้รับอนุมัติจากหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศ

6.10.8. ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

6.10.9. ต้องจัดให้มีระบบ หรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

6.10.10. ต้องจำกัดและควบคุมการใช้โปรแกรมยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น จำกัดการใช้งานโปรแกรมดังกล่าวให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เป็นต้น และต้องกำหนดวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ เพื่อเครื่องคอมพิวเตอร์นั้นไม่ได้ใช้งานเป็น

ระยะเวลาหนึ่ง รวมถึงต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูงด้วย

6.10.11. ต้องมีการแยกระบบที่มีความสำคัญสูงไว้ในบริเวณแยกต่างหากสำหรับระบบงานนี้โดยเฉพาะ และต้องมีการกำหนดนโยบาย และขั้นตอนปฏิบัติสำหรับผู้ใช้งานที่จำเป็นต้องปฏิบัติงานของบริษัทจากภายนอกสำนักงาน

6.10.12. การเข้าถึงแอพพลิเคชั่นใดๆ ต้องถูกควบคุมและจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตหรือได้รับมอบหมายให้มีสิทธิ์ เช่น ผู้ดูแลระบบ เป็นต้น รวมถึงการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ ต้องอนุญาตเฉพาะผู้ที่มีสิทธิ์ตามจำนวนที่ซื้อเท่านั้น

6.10.13. การควบคุมการเข้าถึงเครือข่าย ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งานต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเตอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยของบริษัทจัดสรรไว้ และออกแบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

6.10.14. การควบคุมการเข้าถึงระบบปฏิบัติการ หรือการดำเนินการในด้านผู้ดูแลระบบหรือการแก้ไขปัญหาบนระบบที่สำคัญ จะต้องดำเนินการผ่านขั้นตอนที่กำหนดเพื่อเข้าถึงระบบดังกล่าว เช่น การขออนุมัติจากหัวหน้า และแสดงตนต่อผู้ดูแลศูนย์คอมพิวเตอร์ หรือกรณีเข้าถึงผ่านจากเครื่องส่วนกลางที่มีการควบคุม เช่นจาก Terminal Service หรือที่เรียกว่า Jump Server เพื่อเชื่อมต่อไปยังเครื่องปลายทางที่ได้รับมอบหมายในการเข้าถึงนั้นและให้มีการเก็บหลักฐานการปฏิบัติงานด้วย

6.10.15. ต้องมีการแบ่งแยกระบบเครือข่ายตามกลุ่มที่ให้บริการ เช่น โซนภายในบริษัท โซนระบบสำคัญ โซนภายนอกบริษัท เป็นต้น เพื่อให้สามารถป้องกันการบุกรุกได้อย่างเป็นระบบ

6.11. ความปลอดภัยเกี่ยวกับคอมพิวเตอร์แบบพกพา

6.11.1. บริษัทมีนโยบายให้ผู้ใช้งานใช้อุปกรณ์พกพาเฉพาะที่เป็นของบริษัท ในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทเท่านั้น หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทต้องได้รับการอนุมัติจากหัวหน้าหน่วยงาน หรือเลขานุการบริษัทกรณีเป็นกรรมการ

6.11.2. อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทจะต้องเป็นอุปกรณ์พกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย เช่น "Jail breaking" หรือ "Rooting" ไม่ติดตั้ง Software ที่ละเมิดลิขสิทธิ์ รวมทั้งต้องกำหนดค่ารหัสผ่าน และเข้ารหัสข้อมูลหรืออุปกรณ์พกพาตามนโยบายที่

หน่วยงานเทคโนโลยีสารสนเทศกำหนด ทั้งนี้ผู้ใช้งานต้องได้รับการอนุมัติการใช้งานจากผู้บังคับบัญชาหรือเลขานุการบริษัทกรณีผู้ใช้งานเป็นกรรมการและหน่วยงานเทคโนโลยีสารสนเทศก่อนการใช้งาน

6.11.3. บริษัทขอสงวนสิทธิ์ในการตรวจสอบ ระงับ เพิกถอนการใช้งาน และลบข้อมูลทั้งหมด (Wipe) บนอุปกรณ์พกพาทั้งที่เป็นของบริษัท และของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐาน หรือข้อมูลและสารสนเทศของบริษัท

6.12. ความปลอดภัยเกี่ยวกับการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ

6.12.1. ผู้พัฒนาและผู้เป็นเจ้าของระบบต้องกำหนดความต้องการด้านความมั่นคงปลอดภัย สำหรับระบบที่จัดหา หรือพัฒนาขึ้นมาใช้งาน โดยการประเมินความเสี่ยง และระบุข้อกำหนดด้านความมั่นคงปลอดภัยเพื่อลดความเสี่ยงนั้น โดยอย่างน้อยต้องสอดคล้องกับแนวทางการพัฒนาโปรแกรมประยุกต์บนเว็บที่มั่นคงปลอดภัยจาก Open Web Application Security Project (OWASP)

6.12.2. เพื่อป้องกันความผิดพลาดของสารสนเทศ การสูญหายของสารสนเทศหรือการใช้งานสารสนเทศผิดวัตถุประสงค์ ต้องมีการตรวจสอบข้อมูลนำเข้า ซึ่งผู้พัฒนาระบบต้องกำหนดกลไกว่าข้อมูลนำเข้านั้นมีความถูกต้อง และเหมาะสมก่อน ที่จะนำไปประมวลผลต่อไป ทั้งระหว่างประมวลผล และการตรวจสอบข้อมูลนำออก ซึ่งผู้พัฒนาระบบและเจ้าของระบบต้องกำหนดกลไกเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

6.12.3. ก่อนนำโปรแกรมหรือระบบงานขึ้นให้บริการ (Production) จะต้องทำการทดสอบโปรแกรมด้านความปลอดภัย และให้มั่นใจว่าจะต้องไม่มีช่องโหว่ในระดับของโปรแกรมตามที่กำหนดในช่องโหว่ความเสี่ยงประจำปี 10 อันดับของแนวทางการพัฒนาโปรแกรมประยุกต์บนเว็บที่มั่นคงปลอดภัยจาก Open Web Application Security Project (OWASP)

6.12.4. อุปกรณ์เครือข่าย (Network) เครื่องให้บริการ (Server) และระบบงาน (Application) จะต้องมีการดูแล ปรับปรุง และบำรุงรักษาอย่างต่อเนื่อง เพื่อคงความพร้อมต่อการให้บริการได้อย่างมีประสิทธิภาพ

6.13. ความปลอดภัยเกี่ยวกับการเข้ารหัสข้อมูล

6.13.1. ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้ในบริษัท และต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า

หรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้ จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานของบริษัท

6.14. ความปลอดภัยเกี่ยวกับไฟล์ของระบบสารสนเทศ

6.14.1. ต้องกำหนดมาตรการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์ปิดช่องโหว่ลงในเครื่องที่ใช้งาน โดยก่อนติดตั้งต้องผ่านการตรวจสอบว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

6.14.2. ผู้พัฒนาระบบต้องหลีกเลี่ยงการใช้ข้อมูลจริงในการทดสอบระบบ หากจำเป็นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน และผู้พัฒนาระบบต้องควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง และควรเก็บ Source Code ไว้ในที่ ๆ ปลอดภัย

6.14.3. ต้องกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง และต้องตรวจสอบเมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง เพื่อให้มั่นใจว่าแอปพลิเคชั่นที่ทำงานอยู่นั้น ทำงานผิดปกติหรือเกิดปัญหาขึ้นหรือไม่ รวมทั้งไม่แก้ไขเปลี่ยนแปลงต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นให้แก้ไขตามความจำเป็นเท่านั้น

6.14.4. ต้องป้องกันการรั่วไหลของสารสนเทศ หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไปและต้องกำหนดมาตรการควบคุม และตรวจสอบการว่าจ้างให้พัฒนาระบบต้องมีความชัดเจน รวมถึงการรับรองคุณภาพของระบบ และกำหนดขอบเขตในการว่าจ้างด้วย

6.14.5. เพื่อลดความเสี่ยงจากการโจมตี โดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่ต้องมีการติดตามข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ อย่างสม่ำเสมอ และให้ดำเนินการปิดช่องโหว่ที่สำคัญทันที ทั้งนี้ให้มีแนวปฏิบัติการทำงานที่เหมาะสมทั้งด้านเครื่องผู้ใช้งาน และเครื่องให้บริการที่มีความสำคัญที่แตกต่างกัน

6.14.6. เครื่องให้บริการ และระบบงาน ทั้งหมดจะต้องผ่านการค้นหาช่องโหว่ (vulnerability assessment) อย่างต่อเนื่อง และดำเนินการปิดช่องโหว่ตามขั้นตอนที่กำหนด พร้อมทั้งมีการทดสอบเจาะระบบ (penetration testing) โดยเฉพาะระบบที่สำคัญ และระบบที่ให้บริการผ่านเครือข่ายภายนอกจะต้องดำเนินการก่อนเปิดให้บริการ และดำเนินการอย่างต่อเนื่องโดยอย่างน้อยต้องดำเนินการปีละ 1 ครั้ง

6.15. ความปลอดภัยเกี่ยวกับการบริหารเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศ

6.15.1. ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท เช่น จุดอ่อนใดๆ ให้แก่ผู้บังคับบัญชา หรือหน่วยงานเทคโนโลยีสารสนเทศทันทีที่พบหรือสงสัยว่ามีสิ่งผิดปกติเกิดขึ้น และต้องกำหนดหน้าที่และความรับผิดชอบเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน โดยต้องมีการบันทึกเหตุการณ์ พิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดขึ้นจากความเสียหาย

6.15.2. ต้องเก็บรวบรวมหลักฐานตามกฎ หรือหลักเกณฑ์ เพื่อใช้สำหรับอ้างอิงในกระบวนการศาลหรือที่เกี่ยวข้อง

6.16. ความปลอดภัยเกี่ยวกับความต่อเนื่องในการดำเนินงาน

6.16.1. ต้องจัดลำดับความสำคัญของกระบวนการสร้างความต่อเนื่องทางธุรกิจ ระบุเหตุการณ์ที่ทำให้กระบวนการทางธุรกิจหยุดชะงัก ความเป็นไปได้ และผลกระทบที่จะเกิดขึ้น และแผนบริหารความต่อเนื่องทางธุรกิจจะจัดทำขึ้นสำหรับระบบงานที่มีความสำคัญ

6.16.2. แผนบริหารความต่อเนื่องทางธุรกิจทั้งหมดจะได้รับการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดเหตุฉุกเฉินสามารถนำแผนมาใช้งานได้จริง

6.16.3. ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจเพื่อให้แผนทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

6.16.4. จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทสามารถให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉิน หรือในกรณีที่ไม่สามารถดำเนินการได้อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง และแผนบริหารความต่อเนื่องทางธุรกิจดังกล่าวต้องถูกทบทวนและปรับปรุงหากมีความจำเป็น

6.17. ความปลอดภัยเกี่ยวกับโปรแกรมอันตรายมัลแวร์

6.17.1. บริษัท และหน่วยงานเทคโนโลยีสารสนเทศจะต้องใช้ซอฟต์แวร์ที่มีกระบวนการในการจัดการและป้องกันโปรแกรมไม่ประสงค์ดี หรือเรียกว่ามัลแวร์ที่เหมาะสม

กับสภาพแวดล้อมปัจจุบัน และพนักงานทุกคนต้องให้ความร่วมมือปฏิบัติตามนโยบายดังกล่าวรวมทั้งไม่ติดตั้งซอฟต์แวร์เอง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ทำงานแทน

6.18. ความปลอดภัยเกี่ยวกับการปฏิบัติตามข้อกำหนด

6.18.1. ผู้ใช้งานทุกคนมีหน้าที่ต้องทำความเข้าใจ และปฏิบัติตามนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ทั้งนี้รวมถึงแต่ไม่จำกัดเฉพาะ

- นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ
- พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ 2550
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ 2544
- พ.ร.บ. ลิขสิทธิ์ พ.ศ 2537
- พ.ร.บ. เครื่องหมายการค้า พ.ศ 2534
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562

6.18.2. ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก ซอฟต์แวร์หรือวัสดุอื่นๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตรหรือลิขสิทธิ์ของบุคคลภายนอก

6.18.3. ต้องกำหนดให้มีการป้องกันข้อมูล ที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและแนวปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติและสัญญาที่เกี่ยวข้อง

6.18.4. ต้องกำหนดให้มีการป้องกัน สารสนเทศ ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิ์ และต้องกำหนดให้ใช้มาตรการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย

6.18.5. การทบทวน ตรวจสอบการใช้งานระบบทุกระบบเป็นสิทธิ์ที่บริษัทสามารถกระทำได้ หากบริษัทเห็นว่าจำเป็น โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

6.18.6. ต้องมีการตรวจสอบระบบว่ามีความมั่นคงปลอดภัยเพียงพอหรือไม่โดยใช้ซอฟต์แวร์ค้นหาช่องโหว่ และทดสอบการโจมตีระบบเพื่อตรวจข้อบกพร่องของระบบด้วย

6.18.7. ต้องระบุข้อกำหนด และกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ และต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ ไม่ให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด โดยกำหนดให้มีการแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบระบบสารสนเทศ

6.19. พนักงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติดังต่อไปนี้

6.19.1. ต้องออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน

6.19.2. ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน

6.19.3. ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้งโดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย

6.19.4. ต้องระมัดระวังการโพสต์ข้อความ หรือการแสดงความคิดเห็นต่าง ๆ ผ่านสื่อโซเชียลมีเดีย (Social Media) ต่าง ๆ ที่อาจเข้าข่ายละเมิดบุคคลอื่นๆ หรืออันทำให้เกิดความเข้าใจผิดต่อบริษัทได้

6.19.5. ต้องระมัดระวังการได้รับข้อมูลปลอมต่างๆ หรือที่เรียกว่าการหลอกลวง "ฟิชชิ่ง" ซึ่งเป็นการหลอกให้ผู้ใช้งานคลิก หรือกรอกข้อมูล ต่างๆ ทั้งจากอีเมล เว็บ ไลน์ หรืออื่น ๆ อันมีเจตนาที่จะได้ข้อมูลสำคัญจากผู้ใช้งาน

6.19.6. ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับเฉพาะตนเองเท่านั้น ห้ามมิให้ผู้อื่นล่วงรู้ และใช้งานร่วมกัน

6.19.7. พนักงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอกจะต้องสื่อสารและดำเนินการให้บุคคลภายนอกนั้นปฏิบัติตามนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทด้วย

6.20. ลักษณะการกระทำที่ถือเป็นความผิดทางวินัย

6.20.1. ทำการเปลี่ยนแปลงแก้ไขข้อมูลในการติดต่อสื่อสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

6.20.2. เปิดเผยความรู้หรือข้อมูลข่าวสารทางธุรกิจอันเป็นเรื่องลับหรือเรื่องปกปิดของบริษัทให้แก่ผู้อื่นโดยไม่ได้รับอนุญาตจากบริษัท

6.20.3. ทำการลักลอบปลอมแปลงรหัสผ่าน (Password) หรือรหัสประจำตัวผู้ใช้อื่นเพื่อเข้าระบบงานระบบคอมพิวเตอร์โดยจงใจเจตนา เพื่อกระทำการทุจริตต่อทรัพย์สินเงินทองทั้งของบริษัท หรือลูกค้า หรือทำให้เสื่อมเสียชื่อเสียง

6.20.4. ใช้รหัสผ่าน (Password) หรือรหัสประจำตัวผู้ใช้อื่น หรือรหัสผ่านแบบครั้งเดียว (OTP: One Time Password) ของบุคคลอื่นเข้าสู่ระบบคอมพิวเตอร์ของบริษัท ทำการอ่าน คัดลอกข้อมูล อนุมัติ แก้ไข เปลี่ยนแปลง ลบทิ้งไม่ว่าเพื่อประโยชน์ใดทั้งของส่วนตัวหรือของบุคคลอื่น

6.20.5. ประมาท เลินเล่อ ไม่ระมัดระวังการใช้รหัสผ่าน (Password) หรือรหัสประจำตัวผู้ใช้อื่น หรือ รหัสผ่านแบบครั้งเดียว (OTP: One Time Password) หรือยินยอมจงใจให้บุคคลอื่นใช้รหัสผ่าน หรือรหัสประจำตัวผู้ใช้ และสิทธิในการใช้งานระบบคอมพิวเตอร์ของตนเอง

6.20.6. จงใจ เจตนา ลักลอบ หรือนำข้อมูลของบริษัทไปเปิดเผย จำหน่าย จ่ายแจก แก่บุคคลอื่นเพื่อประโยชน์ส่วนตน หรือบุคคลอื่นโดยไม่ได้รับอนุญาตหรือทำให้บริษัทได้รับความเสียหาย

6.20.7. ประมาท เลินเล่อ ไม่ระมัดระวัง จนเป็นเหตุให้บุคคลอื่นสามารถลักลอบหรือนำข้อมูลของบริษัทไปเปิดเผย จำหน่าย จ่ายแจก

6.20.8. พยายามเข้าถึงระบบที่ไม่มีสิทธิ์ หรือไม่ได้รับอนุญาตให้ใช้งาน

6.20.9. จงใจ หรือเจตนาก่อกวน หรือทำลายข้อมูลสารสนเทศ ระบบคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อสร้างความเสียหายต่อบริษัท

6.20.10. ทำการลักลอบ เฝ้าดู ดักฟัง ค้นหาเส้นทางหรือถอดรหัสข้อมูลอิเล็กทรอนิกส์ โดยใช้เครื่องมือหรือเทคโนโลยีอื่นใดเพื่อให้ได้มาซึ่งข้อมูล หรือความลับของบุคคลอื่นหรือของบริษัท โดยจงใจก่อให้เกิดความเสียหายต่อบุคคลอื่นหรือต่อบริษัท

6.20.11. ทำการติดตั้ง หรือใช้งาน Software ประเภท Hacking Tools หรือ Software อื่นใดที่เกี่ยวข้องกับการตรวจสอบและเข้าถึงข้อมูลสำคัญของบริษัท ยกเว้นบุคคลหรือหน่วยงานที่ทำหน้าที่เกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยเฉพาะ

6.20.12. ทำการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่นใดเข้ากับระบบคอมพิวเตอร์หรือเครือข่ายของบริษัทโดยไม่ได้รับอนุญาตจากหน่วยงานที่รับผิดชอบ

6.20.13. ทำการกำหนดและติดตั้ง หรือเปลี่ยนแปลง IP Address ด้วยตนเองโดยไม่ได้รับอนุญาตจากหน่วยงานที่รับผิดชอบ

6.20.14. ทำการแก้ไข ดัดแปลง หรือเคลื่อนย้ายชิ้นส่วนองค์ประกอบระบบคอมพิวเตอร์ โดยพลการหรือนำชิ้นส่วนอุปกรณ์คอมพิวเตอร์อื่นใดไม่ใช่ทรัพย์สินของบริษัท มาต่อหรือติดตั้งเพิ่มเติมกับทรัพย์สินของบริษัทโดยไม่ได้รับอนุญาต

6.20.15. ทำการดึงข้อมูล หรือมีไว้ครอบครองในสิ่งที่ไม่สมควรหรือเป็นการผิดกฎหมาย เช่น ข้อความ ภาพลามกอนาจาร ฯลฯ หรือสิ่งอื่นใดอันเป็นการดูหมิ่น บ่อนทำลาย สถาบันชาติ ศาสนา และพระมหากษัตริย์ หรือที่เป็นการปลุกระดมให้เกิดความแตกแยกในหมู่ประชาชนหรือ พนักงาน หรือสร้างความเสียหายแก่บริษัท

6.20.16. ทำการส่งข้อความหรือข้อมูลที่ไม่เหมาะสมโดยใช้ระบบ E-mail หรือใช้เครื่องมือสื่อสารของบริษัท เช่น หมิ่นประมาท คุกคาม ขู่กรรโชก กล่าวร้ายป้ายสีหยาบคาย หรือส่งจดหมายลูกโซ่ เป็นต้น

6.20.17. ใช้งานระบบ Internet หรือระบบ Intranet หรือ E-mail ในเรื่องที่ไม่เกี่ยวข้องกับธุรกิจของบริษัท ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ อันเป็นทรัพย์สินของบริษัทเพื่อความบันเทิง หรือประโยชน์ส่วนตัว

6.20.18. ใช้ Software ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายหรือที่บริษัท ไม่ได้อนุญาตให้ใช้ หรือที่อาจก่อให้เกิดความเสียหายต่อบริษัท

6.20.19. ให้ความช่วยเหลือ หรือร่วมมือกับบุคคลภายนอกเพื่อให้เข้าถึงระบบคอมพิวเตอร์ หรือระบบข้อมูลสารสนเทศของบริษัท กระทำการคัดลอก หรือทำลายข้อมูลสารสนเทศหรือระบบคอมพิวเตอร์ของบริษัท

7. การแจกจ่ายเอกสารนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

7.1. แผนการเผยแพร่นโยบาย

7.1.1. เอกสารนโยบายฉบับนี้จะจัดทำให้ผู้ใช้งานทุกคนได้อ่าน ทำความเข้าใจ และประกาศบนเว็บไซต์ของบริษัท

7.2. แผนการฝึกอบรม

7.2.1. วิเคราะห์ว่าพนักงานส่วนไหนได้รับผลกระทบจากนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

7.2.2. พนักงานที่ได้รับผลกระทบดังกล่าวต้องได้รับการฝึกอบรมเรื่องนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

7.2.3. ทำแผนการฝึกอบรมเรื่องนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศตามความจำเป็น

8. วิธีการปฏิบัติให้เป็นไปตามนโยบาย

หน่วยงานเทคโนโลยีสารสนเทศ ได้จัดทำนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศโดยอ้างอิงมาตรฐาน ISO/IEC 27001:2013 Information Security Management Systems เพื่อให้เกิดความมั่นคงปลอดภัยแก่สารสนเทศ

9. การลงโทษทางวินัย

9.1. ตักเตือนด้วยวาจา

9.2. ตักเตือนเป็นลายลักษณ์อักษร

9.3. พักงานชั่วคราวโดยไม่ได้รับค่าจ้าง

9.4. ปลดออก

9.5. ไล่ออก

9.6. การดำเนินทางกฎหมายอาญาหรือแพ่ง

กรณีการลงโทษพนักงาน บริษัทไม่จำเป็นต้องปฏิบัติตามลำดับดังกล่าวข้างต้น บริษัทอาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

10. การทบทวนนโยบาย

ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำอย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้ประธานกรรมการบริหารอนุมัติหากมีการเปลี่ยนแปลง

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 1 ตุลาคม พ.ศ. 2563

ประกาศ ณ วันที่ 30 กันยายน พ.ศ. 2563

(นายก่อศักดิ์ ไชยรัศมีศักดิ์)

ประธานกรรมการบริหาร

(เอกสารแนบท้าย)

หนังสือยินยอม
การใช้ระบบเทคโนโลยีสารสนเทศ บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย
(Acceptable Use Policy Agreement)

วันที่ _____เดือน_____พ.ศ._____

ข้าพเจ้า นาย / นาง / นางสาว _____

รหัสพนักงาน_____ ตำแหน่ง _____

แผนก_____ฝ่าย / ด้าน / ส่วนงาน_____

สำนัก/หน่วยงาน_____บริษัท_____

ได้รับทราบ และยินดีปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย ทุกประการ

อนึ่ง ข้าพเจ้าตระหนักดีว่าการใช้ระบบเทคโนโลยีสารสนเทศนี้ หากข้าพเจ้ากระทำการอย่างใดอย่างหนึ่งที่เป็นการละเมิด หรือฝ่าฝืน นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ บริษัท ซีพี ออลล์ จำกัด (มหาชน) และบริษัทย่อย ย่อมได้รับโทษทางวินัยตามสมควรแก่กรณี

จึงได้ลงลายมือชื่อสำคัญไว้ ดังนี้

นาย / นาง / นางสาว _____

(_____)

_____/_____/_____