นโยบายด้านความปลอดภัยเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของบริษัท ชิน สตีล (ประเทศไทย) จัดกัด ที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ เพื่อเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท บริษัทฯ จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนสารสนเทศ ดังนี้

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานในนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

- "บริษัท" หมายความว่า บริษัท ชิน สตีล (ประเทศไทย) จำกัด
- "ผู้ปฏิบัติงาน" หมายความว่า ผู้ปฏิบัติงาน ลูกจ้างทดลองงาน พนักงานประจำ และลูกจ้างชั่วคราวของบริษัท
- "ผู้ใช้งานที่เกี่ยวข้อง" หมายความว่า บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของบริษัท ที่เข้ามาดำเนินกิจกรรมภายในบริษัท
- "ผู้ดูแลระบบ" หมายความว่า ผู้จัดการส่วนเทคโนโลยีสารสนเทศ หรือผู้ปฏิบัติงานอื่น ที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป
- "ระบบเครือข่าย" หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet และระบบการสื่อสารอื่นๆ
- "สินทรัพย์" หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับบริษัท ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัท

สารบัญ

1.ปฏิบัติเกี่ยวกับนโยบายด้านความปลอดภัยเทคโนโลยีสารสนเทศ IT

(Information Security Policy)

วัตุประสงค์

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อปฏิบัติ

- ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น
- ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
- ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก
- ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นจ้าของข้อมูลนั้นๆ
- ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์
- ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง
- ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน
- ห้ามใช้ทรัพยากรอินเทอร์เน็ตขององค์กรในกิจกรรมส่วนตัวที่ไม่เกี่ยวข้องกับงาน เช่น การเล่นเกมออนไลน์หรือการท่องเว็บไซต์ส่วนตัว
- หากต้องการใช้อินเทอร์เน็ตสำหรับกิจกรรมส่วนตัว พนักงานต้องทำในเวลาที่ไม่กระทบกับการทำงานและไม่ใช้ทรัพยากรขององค์กร เช่น เครือข่ายหรืออุปกรณ์ขององค์กร
- พนักงานสามารถเข้าถึงเว็บไซต์ที่เกี่ยวข้องกับงานได้ เช่น เว็บไซต์สำหรับค้นหาข้อมูลทางธุรกิจ เว็บไซต์ของคู่ค้า ลูกค้า หรือหน่วยงานราชการ

2.การบริหารจัดการสินทรัพย์สารสนเทศ

1. **การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์** (Computer and Peripheral Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

ข้อปฏิบัติ

- ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
- ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
- ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
- ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
- ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

3. การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจการใช้โปรแกรมที่ถูกต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

ข้อปฏิบัติ

- ต้องใช้โปรแกรมคอมพิวเตอร์ โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท
- โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน
- ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาตโดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย
- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

4.การควบคุมและการเข้าใช้งานระบบคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้การใช้งานระบบคอมพิวเตอร์ขององค์กรเป็นไปอย่างมีประสิทธิภาพและปลอดภัย นโยบายนี้จึงถูกจัดทำขึ้นเพื่อกำหนดแนวทางปฏิบัติในการควบคุมและเข้าใช้งานระบบ

ข้อปฏิบัติ

- ออกจากระบบสารสนเทศ (Log out) โดยทันทีเมื่อเสร็จสิ้นงาน
- ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
- การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 5 นาที
- ให้มีการขออนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายขึ้นไป ในกรณีที่ต้องการนำทรัพย์สินด้านสารสนเทศต่างๆ เช่น เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกบริษัททุกครั้ง โดยปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- ระมัดระวังและดูแลทรัพย์สินของบริษัท ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

5.การใช้อินเทอร์เน็ต

วัตถุประสงค์

จัดทำขึ้นเพื่อกำหนดแนวทางการใช้อินเทอร์เน็ตขององค์กรอย่างมีประสิทธิภาพ ปลอดภัย และเป็นไปตามกฎหมาย เพื่อป้องกันการใช้ทรัพยากรอินเทอร์เน็ตขององค์กรในทางที่ไม่เหมาะสม และลดความเสี่ยงที่อาจเกิดขึ้นจากการเข้าถึงเว็บไซต์หรือเนื้อหาที่ไม่ปลอดภัย

ข้อปฏิบัติ

- ห้ามใช้ทรัพยากรอินเทอร์เน็ตขององค์กรในกิจกรรมส่วนตัวที่ไม่เกี่ยวข้องกับงาน เช่น การเล่นเกมออนไลน์หรือการท่องเว็บไซต์ส่วนตัว
- หากต้องการใช้อินเทอร์เน็ตสำหรับกิจกรรมส่วนตัว พนักงานต้องทำในเวลาที่ไม่กระทบกับการทำงาน และไม่ใช้ทรัพยากรขององค์กร เช่น เครือข่ายหรืออุปกรณ์ขององค์กร
- พนักงานสามารถเข้าถึงเว็บไซต์ที่เกี่ยวข้องกับงานได้ เช่น เว็บไซต์สำหรับค้นหาข้อมูลทางธุรกิจ เว็บไซต์ของคู่ค้า ลูกค้า หรือหน่วยงานราชการ
- ห้ามเข้าถึงเว็บไซต์ที่มีเนื้อหาผิดกฎหมาย หรือที่อาจเสี่ยงต่อความปลอดภัย เช่น เว็บไซต์ที่เกี่ยวข้องกับการพนัน, การละเมิดลิขสิทธิ์, หรือเว็บไซต์ที่มีมัลแวร์
- ใช้อินเทอร์เน็ตขององค์กรเพื่อวัตถุประสงค์ทางธุรกิจเป็นหลัก
- ห้ามแชร์ข้อมูลส่วนตัวหรือข้อมูลสำคัญขององค์กรผ่านอินเทอร์เน็ตโดยไม่ผ่านช่องทางที่มีความปลอดภัย เช่น อีเมลที่มีการเข้ารหัส
- หากพบการใช้อินเทอร์เน็ตที่ละเมิดนโยบาย เช่น การเข้าถึงเว็บไซต์ที่ไม่เหมาะสม จะมีการเตือนหรือดำเนินการตามขั้นตอนที่องค์กรกำหนด

6. การใช้จดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

จัดทำขึ้นเพื่อควบคุมการใช้งานอีเมลภายในองค์กรอย่างมีประสิทธิภาพและปลอดภัย โดยกำหนดแนวทางการใช้งานที่ชัดเจน เพื่อป้องกันการละเมิดข้อมูล การส่งข้อมูลผิดพลาด หรือการใช้งานในทางที่ไม่เหมาะสม

ข้อปฏิบัติ

- ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้องและนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด
- หน่วยงานหรือผู้ปฏิบัติงานผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัท
- ผู้ปฏิบัติงานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล
- การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
- การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
- การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท
- ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัท
- หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง
- กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิกหรือระงับการบริการชั่วคราวแก่ผู้ปฏิบัติงานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ

- ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น
- หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด เกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท

7. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

วัตถุประสงค์

จัดทำขึ้นเพื่อกำหนดมาตรการและแนวทางในการคุ้มครองข้อมูลขององค์กรจากภัยคุกคามที่อาจเกิดขึ้น รวมทั้งการรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล เพื่อให้การทำงานขององค์กรดำเนินไปได้อย่างราบรื่นและปลอดภัย

ข้อปฏิบัติ

- ข้อมูลสำคัญต้องจัดเก็บในพื้นที่ที่มีการเข้ารหัสหรือระบบป้องกันการเข้าถึง
- พนักงานต้องจัดเก็บข้อมูลในระบบที่กำหนดเท่านั้น
- จำกัดการเข้าถึงข้อมูลตามระดับความจำเป็นของพนักงาน
- การแบ่งปันข้อมูลต้องได้รับการอนุมัติจากผู้มีอำนาจ
- พนักงานต้องรายงานทันทีหากพบข้อมูลที่มีการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- ห้ามใช้สื่อสาธารณะในการส่งข้อมูล เช่น โซเชียลมีเดีย
- ข้อมูลสำคัญต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ โดยใช้วิธีการที่ปลอดภัยและสามารถกู้คืนข้อมูลได้เมื่อเกิดปัญหา
- มีการตรวจสอบและทดสอบกระบวนการสำรองข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้ในกรณีฉุกเฉิน

8. ความปลอดภัยเครือข่าย (Network Security)

วัตถุประสงค์

จัดทำขึ้นเพื่อให้การใช้งานเครือข่ายภายในองค์กรมีความปลอดภัยจากภัยคุกคามทั้งภายนอกและภายใน ซึ่งจะช่วยปกป้องข้อมูลขององค์กรจากการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีจากแฮกเกอร์ หรือการรั่วไหลของข้อมูลผ่านเครือข่าย รวมถึงการรักษาความพร้อมใช้งานของระบบเครือข่ายที่รองรับการดำเนินธุรกิจ

ข้อปฏิบัติ

- พนักงานทุกคนต้องใช้งานเครือข่ายองค์กรผ่านการอนุมัติและตามสิทธิ์ที่ได้รับจากฝ่าย IT
- ห้ามเชื่อมต่ออุปกรณ์ส่วนตัวกับเครือข่ายองค์กรโดยไม่ได้รับอนุญาตจากฝ่าย IT
- การเข้าถึงเครือข่ายจากภายนอก (เช่น ผ่าน VPN) จะต้องได้รับการอนุมัติ
- ระบบเครือข่ายต้องติดตั้งและใช้งาน Firewall ที่ได้รับการตั้งค่าตามมาตรฐานความปลอดภัย เพื่อป้องกันการเข้าถึงจากแหล่งที่ไม่พึงประสงค์
- Firewall ต้องได้รับการปรับปรุงและตรวจสอบเป็นประจำ เพื่อให้สามารถป้องกันภัยคุกคามใหม่ๆ ได้
- ทุกอุปกรณ์ที่เชื่อมต่อกับเครือข่ายต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่ได้รับการอนุมัติจากฝ่าย IT
- การเข้าถึงระบบหรือทรัพยากรในเครือข่ายจะต้องจำกัดตามหน้าที่การงาน และจำเป็นต้องได้รับการอนุมัติจากฝ่าย IT
- พนักงานจะได้รับสิทธิ์การเข้าถึงที่สอดคล้องกับหน้าที่ที่ได้รับมอบหมายเท่านั้น
- ทุกกิจกรรมที่เกิดขึ้นในเครือข่าย เช่น การเข้าถึงระบบ การถ่ายโอนข้อมูล หรือการเชื่อมต่อจะต้องมีการบันทึกข้อมูล (Log) เพื่อให้สามารถตรวจสอบย้อนกลับได้

9. ความปลอดภัยเซิร์ฟเวอร์ (Server Security)

วัตถุประสงค์

จัดทำขึ้นเพื่อให้การใช้งานและการบริหารจัดการเซิร์ฟเวอร์ภายในองค์กรมีความปลอดภัยจากภัยคุกคามทั้งภายในและภายนอก และเพื่อรักษาความสมบูรณ์ของข้อมูลในเซิร์ฟเวอร์ รวมถึงป้องกันการรั่วไหลของข้อมูลหรือการเข้าถึงที่ไม่ได้รับอนุญาต

ข้อปฏิบัติ

- เซิร์ฟเวอร์ทุกเครื่องต้องติดตั้งระบบปฏิบัติการที่ได้รับการตรวจสอบจากฝ่าย IT
- การกำหนดค่าเซิร์ฟเวอร์ต้องทำตามมาตรฐานความปลอดภัยที่กำหนด โดยเฉพาะการกำหนดสิทธิ์การเข้าถึงและการตั้งค่าการรักษาความปลอดภัย
- ทุกเซิร์ฟเวอร์ต้องมีการใช้ระบบการยืนยันตัวตนที่เข้มงวด เช่น รหัสผ่านที่มีความปลอดภัย
- ต้องตรวจสอบการตั้งค่ารหัสผ่านให้มีความซับซ้อน และเปลี่ยนรหัสผ่านเป็นประจำ
- ห้ามใช้งานเซิร์ฟเวอร์ในการเก็บข้อมูลหรือโปรแกรมที่ไม่เกี่ยวข้องกับงานขององค์กร
- ทุกการใช้งานเซิร์ฟเวอร์จะต้องได้รับการอนุมัติจากฝ่าย IT และต้องมีการบันทึกข้อมูลการใช้งานทุกครั้ง
- ข้อมูลในเซิร์ฟเวอร์ต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ
- ข้อมูลสำรองต้องถูกจัดเก็บในสถานที่ที่ปลอดภัยและเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตจากฝ่าย IT
- ต้องมีการทดสอบการกู้คืนข้อมูลจากการสำรองอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าสามารถกู้คืนข้อมูลได้ในกรณีที่เกิดเหตุการณ์ไม่คาดคิด
- ทุกเซิร์ฟเวอร์ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส, มัลแวร์, และเครื่องมือป้องกันภัยคุกคามอื่นๆ
- ระบบเซิร์ฟเวอร์ต้องมีการอัปเดตซอฟต์แวร์เป็นประจำ เพื่อป้องกันช่องโหว่และภัยคุกคามใหม่ๆ
- เซิร์ฟเวอร์ทุกเครื่องต้องได้รับการอัปเดตแพตช์ความปลอดภัยทันทีที่มีการปล่อยแพตช์ใหม่จากผู้ผลิต
- การอัปเดตจะต้องดำเนินการตามมาตรการที่กำหนด และต้องตรวจสอบให้แน่ใจว่าไม่มีผลกระทบต่อระบบที่ใช้งาน

- เซิร์ฟเวอร์ต้องปิดการใช้งานบริการหรือฟีเจอร์ที่ไม่จำเป็น เพื่อป้องกันการเปิดช่องทางให้กับภัยคุกคามที่อาจเกิดขึ้นจากบริการเหล่านั้น
- ทุกเซิร์ฟเวอร์ต้องเปิดใช้งานการบันทึกเหตุการณ์ (Log) เพื่อบันทึกการใช้งานและการกระทำที่สำคัญ เช่น การเข้าสู่ระบบ, การแก้ไขข้อมูล, หรือการติดตั้งซอฟต์แวร์
- ฝ่าย IT ต้องมีการติดตามและวิเคราะห์ข้อมูล Log เพื่อระบุปัญหาหรือการโจมตีที่อาจเกิดขึ้น

10. การจัดการอุปกรณ์และซอฟต์แวร์ (Device and Software Management)

วัตถุประสงค์

จัดทำขึ้นเพื่อให้การใช้งานอุปกรณ์และซอฟต์แวร์ในองค์กรมีความปลอดภัยและมีประสิทธิภาพสูงสุด การจัดการอุปกรณ์และซอฟต์แวร์ต้องเป็นไปตามมาตรฐานความปลอดภัยที่กำหนดไว้ และต้องป้องกันการใช้ซอฟต์แวร์หรืออุปกรณ์ที่ไม่เหมาะสมหรือเสี่ยงต่อความปลอดภัยของข้อมูลและระบบในองค์กร

ข้อปฏิบัติ

- อุปกรณ์ทุกชิ้นที่ใช้ในองค์กรต้องได้รับการอนุมัติจากฝ่าย IT ก่อนใช้งาน
- ห้ามใช้หรือเชื่อมต่ออุปกรณ์ส่วนบุคคล (เช่น แล็ปท็อป, โทรศัพท์มือถือ, แฟลชไดรฟ์) กับระบบหรือเครือข่ายขององค์กรโดยไม่ได้รับอนุญาตจากฝ่าย IT
- ทุกอุปกรณ์ที่ใช้ในองค์กรจะต้องได้รับการตรวจสอบอย่างสม่ำเสมอเพื่อให้มั่นใจว่าอุปกรณ์ทำงานได้ตามมาตรฐานและไม่ก่อให้เกิดความเสี่ยงด้านความปลอดภัย
- ฝ่าย IT ต้องมีการบำรุงรักษาและจัดการอุปกรณ์ที่มีการใช้งานอย่างสม่ำเสมอ เช่น การอัปเดตซอฟต์แวร์หรือการเปลี่ยนอะไหล่เมื่อจำเป็น
- ห้ามปล่อยให้อุปกรณ์ที่เกี่ยวข้องกับข้อมูลสำคัญหรือข้อมูลส่วนตัวอยู่ในที่ที่ไม่ปลอดภัย
- การติดตั้งซอฟต์แวร์ในอุปกรณ์ขององค์กรต้องได้รับการอนุมัติจากฝ่าย IT
- ห้ามติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตหรือซอฟต์แวร์ที่อาจก่อให้เกิดความเสี่ยงด้านความปลอดภัย เช่น ซอฟต์แวร์เถื่อน หรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเป็นประจำ
- ซอฟต์แวร์ทุกตัวต้องติดตั้งการอัปเดตอัตโนมัติหากเป็นไปได้ และฝ่าย IT จะต้องตรวจสอบการอัปเดตและดำเนินการติดตั้งแพตช์ที่จำเป็น
- ทุกซอฟต์แวร์ที่ใช้ในองค์กรต้องมีการจัดการลิขสิทธิ์ที่ถูกต้องและเป็นไปตามกฎหมาย
- ฝ่าย IT จะต้องตรวจสอบให้มั่นใจว่าซอฟต์แวร์ทั้งหมดที่ติดตั้งในองค์กรมีลิขสิทธิ์ที่ถูกต้อง และไม่มีการใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์

12. การจัดการรหัสผ่าน (Password Policy)

วัตถุประสงค์

จัดทำขึ้นเพื่อกำหนดมาตรฐานการใช้งานและการจัดการรหัสผ่าน (Password) ในองค์กร โดยมีเป้าหมายเพื่อรักษาความปลอดภัยของข้อมูล ระบบ และทรัพยากรต่างๆ ขององค์กร รวมถึงลดความเสี่ยงจากการโจมตีที่เกี่ยวข้องกับการใช้รหัสผ่าน

ข้อปฏิบัติ

- รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8–12 ตัวอักษร
- ต้องประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่ (A-Z), ตัวพิมพ์เล็ก (a-z), ตัวเลข (0-9) และสัญลักษณ์พิเศษ (@, #, $, ฯลฯ)
- ห้ามใช้คำที่เกี่ยวข้องกับชื่อผู้ใช้งาน, ชื่อองค์กร, หรือคำที่คาดเดาได้ง่าย
- ไม่อนุญาตให้ใช้รหัสผ่านที่เคยใช้ในระบบเดียวกันซ้ำเกินกว่า 5 ครั้งล่าสุด
- เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เช่น ทุก 90 วัน
- ระบบต้องปฏิเสธการตั้งรหัสผ่านที่คาดเดาได้ง่าย เช่น "password123," "12345678," หรือ "qwerty"
- ห้ามแชร์รหัสผ่านกับผู้อื่น รวมถึงเพื่อนร่วมงาน
- หากสงสัยว่ารหัสผ่านถูกเปิดเผยหรือใช้งานโดยไม่ได้รับอนุญาต ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที
- หากมีความพยายามเข้าสู่ระบบผิดเกิน 5 ครั้ง ระบบต้องล็อกบัญชีชั่วคราวเป็นระยะเวลา 15 นาที
- ห้ามใช้รหัสผ่านเดียวกันในหลายระบบ โดยเฉพาะระบบที่มีความสำคัญและระบบภายนอก
- ผู้ใช้งานจะต้องใช้รหัสผ่านเดิมอย่างน้อย 1 วัน ก่อนที่จะสามารถเปลี่ยนรหัสผ่านใหม่ได้อีกครั้ง เพื่อป้องกันการเปลี่ยนรหัสผ่านหลายครั้ง
- รหัสผ่านผู้ใช้งานที่ถูกล็อค จะได้รับการปลดล็อคหรือรีเซตรหัสผ่านใหม่จาก ผู้ดูแลระบบเท่านั้น

13. การใช้ Thumb drive (USB Flash Drive) ในองค์กร

วัตถุประสงค์

เพื่อควบคุมและกำกับดูแลการใช้ Thumb drive ภายในองค์กร ลดความเสี่ยงจากไวรัส มัลแวร์ และการรั่วไหลของข้อมูล

ข้อปฏิบัติ

- พนักงานสามารถใช้ Thumb drive ที่ได้รับอนุมัติจากองค์กรเท่านั้น
- ห้ามใช้ Thumb drive ส่วนตัวกับคอมพิวเตอร์ขององค์กรโดยไม่ได้รับอนุญาต
- Thumb drive ต้องได้รับการสแกนไวรัสก่อนใช้งานทุกครั้ง
- ควรเข้ารหัส (Encryption) ข้อมูลที่จัดเก็บใน Thumb drive หากมีข้อมูลสำคัญ
- ห้ามคัดลอกหรือถ่ายโอนข้อมูลที่เป็นความลับขององค์กรลงใน Thumb drive โดยไม่ได้รับอนุมัติ
- ตั้งค่าคอมพิวเตอร์ให้จำกัดการใช้งาน Thumb drive เฉพาะที่ได้รับอนุญาต
- Thumb drive มีไวรัสหรือมัลแวร์ ต้องแจ้งฝ่าย IT ทันที

14. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของบริษัท อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัท

ข้อปฏิบัติ

- ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้น อย่างน้อย ปีละ 1 ครั้ง
- ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
- ข้อมูลสำคัญต้องมีการสำรอง (Backup) อย่างสม่ำเสมอ และจัดเก็บในสถานที่ที่ปลอดภัย เช่น ศูนย์ข้อมูลสำรอง (Offsite Data Center)
- จัดทำ แผนความต่อเนื่องทางธุรกิจ (BCP) และ แผนกู้คืนระบบ (Disaster Recovery Plan - DRP) สำหรับระบบสารสนเทศและข้อมูลสำคัญ
- กำหนดบทบาทและความรับผิดชอบของบุคลากรในกรณีฉุกเฉิน เช่น ผู้ประสานงาน ผู้ดูแลระบบ และผู้จัดการความต่อเนื่อง
- ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อยปีละ 1 ครั้ง

ผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดที่บริษัทกำหนดไว้ ทั้งนี้ผู้บริหารระดับสูงสุดของหน่วยงาน (กรรมการผู้จัดการ)เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

นโยบายความปลอดภัยด้านเทคโนโลด้านสารสนเทศนี้ให้ใช้บังคับกับ พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของบริษัทฯ รวมถึงบุคคลภายนอก และหน่วยงานภายนอกที่ให้บริการแก่บริษัทฯ

นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัทฯ ครั้งที่ 1/2568 เมื่อวันที่ 25 กุมภาพันธ์ 2568 ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 26 กุมภาพันธ์ 2568 เป็นต้นไป

ประกาศใช้ ณ วันที่ 26 กุมภาพันธ์

.....

(ศ.ดร. อาษา ประทีปเสน)

ประธานกรรมการ