นโยบายการรักษาความปลอดภัยระบบคอมพิวเตอร์และข้อมูลสารสนเทศ
บริษัท ทริพเพิล ไอ โลจิสติกส์ จำกัด (มหาชน) และบริษัทย่อย

นโยบายการรักษาความปลอดภัย

1. บริษัท จะดำเนินการทุกวิถีทาง เพื่อให้ระบบงานบริการต่างๆ ที่จำเป็นต่อการดำเนินธุรกิจอันได้แก่ ระบบข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่ายโทรศัพท์ ระบบเครือข่ายสื่อสาร หรือที่เรียกว่า ระบบเทคโนโลยีสารสนเทศ ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา ข้อมูลมีความถูกต้องเชื่อถือได้ บริษัทจึงให้ความสำคัญอย่างยิ่งในเรื่องการรักษาความปลอดภัยระบบต่างๆ ดังกล่าว
2. บริษัท มีพันธะผูกพันตามกฎหมาย และคำสัญญาต่อลูกค้า คู่ค้า ผู้ลงทุน และพนักงาน ในการปกปิดข้อมูลที่ได้ให้แก่บริษัท รวมถึงข้อมูลข่าวสารของบุคคลหรือนิติบุคคลที่ได้มาจากกระบวนการทางคอมพิวเตอร์ หรือจากการสื่อสารผ่านเครือข่ายของบริษัทไว้เป็นความลับ ดังนั้น ผู้บริหาร และพนักงานทุกระดับจะต้องปฏิบัติตามข้อกำหนดมาตรฐาน คำแนะนำ และกระบวนการการรักษาความปลอดภัยโดยเคร่งครัด เพื่อป้องกันมิให้ข้อมูล และข่าวสารที่สำคัญถูกเปิดเผย หรือมีการเข้าถึงแหล่งข้อมูลข่าวสารโดยพลการ หรือโดยมีเจตนาที่ไม่บริสุทธิ์
3. บริษัทได้จัดให้มีหน่วยงานทำหน้าที่โดยตรงในการดูแลความปลอดภัยระบบคอมพิวเตอร์และข้อมูลสารสนเทศตามระเบียบฉบับนี้ ทำการติดตามและตรวจสอบการปฏิบัติของหน่วยงานต่างๆ อย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการรักษาความปลอดภัยระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัทโดยรวมอยู่ในเกณฑ์ตามที่บริษัทกำหนด

วัตถุประสงค์

1. เพื่อสร้างความรู้ความเข้าใจ ให้พนักงานปฏิบัติตามระเบียบที่ถูกต้อง รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศ
2. เพื่อให้พนักงานและผู้ที่ต้องใช้ หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัทได้อย่างถูกต้องเหมาะสม
3. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท ถูกบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

หน้าที่ และความรับผิดชอบ

1. **หน้าที่ของผู้บังคับบัญชา**
   1.1 ชี้แจงให้พนักงานทราบถึงระเบียบ คำสั่ง และแนวปฏิบัติทั้งหลายของบริษัท ที่เกี่ยวกับการรักษาความปลอดภัยระบบคอมพิวเตอร์ และข้อมูลสารสนเทศ

1.2 ดูแล แนะนำ และตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

1.3 พิจารณาลงโทษทางวินัยแก่ผู้กระทำผิดอย่างเสมอภาค และเป็นธรรม

2. **หน้าที่ของพนักงาน**

2.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามระเบียบ คำสั่ง และแนวปฏิบัติทั้งหลายของบริษัท ที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบคอมพิวเตอร์ และข้อมูลสารสนเทศโดยเคร่งครัด

2.2 ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท

2.3 แจ้งให้บริษัททราบทันทีเมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม หรือพบเห็นการบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมที่อาจสร้างความเสียหายต่อบริษัท

3. **พนักงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์** ต้องปฏิบัติดังต่อไปนี้

3.1 ต้องออกจากระบบ (Log-out, Log-off) ทุกระบบ และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงอื่นทันทีเมื่อไม่ได้ใช้งานเป็นเวลานาน หรือหลังเลิกงาน

3.2 ต้องกำหนดรหัสผ่าน (Password) เพื่อล็อคหน้าจอ (Lock Screen) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นการชั่วคราว หรือในระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน

3.3 ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย

3.4 รหัสผ่าน (Password) และรหัสอื่นใดที่บริษัท กำหนดให้กับพนักงาน เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลของบริษัท ถือเป็นความลับส่วนตัวพนักงานจะต้องเก็บรักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้ พนักงานจะต้องเปลี่ยนรหัสผ่าน และรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนด หรือเมื่อพนักงานเห็นสมควรต้องทำการเปลี่ยนรหัสผ่านโดยตั้งรหัสผ่าน และรหัสอื่นใด ด้วยความรอบคอบ ห้ามตั้งรหัสซ้ำกับรหัสเก่า หรือตั้งรหัสที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือตั้งรหัสซ้ำกันในทุกระบบที่พนักงานมีสิทธิ์ใช้งาน

4. **พนักงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอก** จะต้องจัดให้บุคคลภายนอกนั้นปฏิบัติตามระเบียบการใช้งานระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัท

คำจำกัดความ

1. **"บริษัท"** หมายถึง บริษัท ทริพเพิล ไอ โลจิสติกส์ จำกัด และบริษัทย่อย ทุกบริษัท
2. **"พนักงาน"** หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

3. **"ระบบคอมพิวเตอร์"** หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์ การเก็บรักษาและการถ่ายโอนข้อมูลชนิดต่างๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่างๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้าของบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัท
4. **"ข้อมูลคอมพิวเตอร์"** หมายถึง สัญญาณทางไฟฟ้า แสง เสียง หรือในรูปร่างลักษณะอื่นใดที่สามารถเปลี่ยนแปลง หรือให้ความหมายที่มนุษย์สามารถเข้าใจได้ เช่น ตัวอักษร ภาพนิ่ง ภาพเคลื่อนไหว เสียง หรือสัญลักษณ์อื่นที่สามารถสื่อความหมายระหว่างบุคคลได้โดยสามารถนำมาส่งผ่านทางอุปกรณ์อิเล็กทรอนิกส์หรืออุปกรณ์คอมพิวเตอร์จากที่หนึ่งไปยังอีกที่หนึ่ง หรือสามารถเก็บรักษาไว้ในเครื่องมืออุปกรณ์ที่สามารถนำกลับมาใช้ได้ใหม่ ไม่ว่าชั่วคราว หรือถาวร
5. **"ข้อมูลสารสนเทศ"** หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่างๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใดๆ
6. **"ข้อมูลสำคัญ"** หรือ **"ข้อมูลที่เป็นความลับ"** หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัทไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่นนอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงักด้อยประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง
7. **"ระบบที่มีความสำคัญ"** หมายถึง ระบบคอมพิวเตอร์ หรือระบบสารสนเทศที่บริษัท ใช้ประโยชน์เพื่อให้บริการทางธุรกิจ ทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัท ให้เป็นปกติ หรือระบบที่ได้รับการกำหนดโดยระบบสารสนเทศของบริษัท ทั้งนี้ หากระบบที่มีความสำคัญดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก หรือด้อยประสิทธิภาพ
8. **"ผู้ดูแลระบบ"** หมายถึง พนักงานที่ได้รับมอบหมาย (หมายรวมถึง พนักงานสารสนเทศทั้งพนักงานของบริษัท ทริพเพิล ไอ โลจิสติกส์ จำกัด (มหาชน) (พนักงานภายใน) และบริษัทที่ให้บริการด้านสารสนเทศ (บุคคลภายนอก) ที่ได้รับการว่าจ้างหรือได้รับมอบหมายจากทางบริษัท ทริพเพิล ไอ โลจิสติกส์ จำกัด (มหาชน) ให้เข้ามารับผิดชอบดูแลระบบสารสนเทศของบริษัท) ให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware, Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบ

คอมพิวเตอร์ของบริษัท ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจ และมีความปลอดภัย

9. **"การรักษาความปลอดภัย"** หรือ **"ความปลอดภัย"** หมายถึง กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบ และข้อมูลสำคัญให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงานจนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย

วินัยและการลงโทษ

1. ผู้บังคับบัญชาตามสายงานจะต้องดูแลรับผิดชอบให้พนักงานปฏิบัติตามวินัย และละเว้นต่อการกระทำใดๆ อันเป็นการฝ่าฝืน หากมีการละเลยหรือฝ่าฝืน ผู้บังคับบัญชาจะต้องลงโทษผู้กระทำความผิดตามควรแก่กรณี
2. ลักษณะการกระทำ ต่อไปนี้ถือเป็นความผิดทางวินัย
   - 2.1 ทำการเปลี่ยนแปลง แก้ไขข้อมูลในการติดต่อสื่อสารของบุคคลอื่นโดยไม่ได้รับอนุญาต
   - 2.2 เปิดเผยความรู้ หรือข้อมูลข่าวสารทางธุรกิจอันเป็นเรื่องลับ หรือเรื่องปกปิดของบริษัท ให้แก่ผู้อื่นโดยไม่ได้รับอนุญาตจากบริษัท
   - 2.3 ทำการลักลอบ ปลอมแปลง รหัสผ่าน (Password) หรือรหัสอื่นใด เพื่อเข้าใช้งานหรือเข้าถึงระบบคอมพิวเตอร์โดยจงใจ เจตนาเพื่อกระทำการทุจริตต่อทรัพย์สิน เงินทองทั้งของบริษัท หรือลูกค้า หรือทำให้เสื่อมเสียชื่อเสียง
   - 2.4 ใช้รหัสผ่าน (Password) หรือรหัสอื่นใด ของบุคคลอื่นเข้าสู่ระบบคอมพิวเตอร์ของบริษัท ทำการอ่าน คัดลอกข้อมูล อนุมัติ แก้ไข เปลี่ยนแปลง ลบทิ้ง ไม่ว่าเพื่อประโยชน์ใดทั้งของส่วนตัว หรือของบุคคลอื่น
   - 2.5 ประมาท เลินเล่อ ไม่ระมัดระวังการใช้รหัสผ่าน (Password) หรือรหัสอื่นใด หรือยินยอม จงใจให้บุคคลอื่นใช้รหัสผ่าน หรือ รหัสอื่นใด และสิทธิ์ในการใช้งานระบบคอมพิวเตอร์ของตนเอง
   - 2.6 จงใจ เจตนา ลักลอบ หรือนำข้อมูลของบริษัท ไปเปิดเผย จำหน่าย จ่ายแจก แก่บุคคลอื่น เพื่อประโยชน์ส่วนตน หรือบุคคลอื่นโดยไม่ได้รับอนุญาต หรือทำให้บริษัท ได้รับความเสียหาย
   - 2.7 ประมาท เลินเล่อ ไม่ระมัดระวังจนเป็นเหตุให้บุคคลอื่นสามารถลักลอบ หรือนำข้อมูลของบริษัทไปเปิดเผย จำหน่าย จ่ายแจก
   - 2.8 พยายามเข้าถึงข้อมูลคอมพิวเตอร์ ข้อมูลสารสนเทศ ข้อมูลสำคัญ ข้อมูลที่เป็นความลับ ระบบที่มีความสำคัญโดยที่ไม่มีสิทธิ์ หรือไม่ได้รับอนุญาตให้ใช้งาน
   - 2.9 จงใจ หรือเจตนาก่อกวน แทรกแซง หรือทำลายข้อมูลสารสนเทศ ระบบคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อสร้างความเสียหายต่อบริษัท

2.10 ทำการลักลอบ เฝ้าดู ดักฟัง ค้นหาเส้นทาง หรือถอดรหัสข้อมูลสารสนเทศ เพื่อให้ได้มาซึ่งข้อมูลหรือความลับ ของบุคคลอื่น หรือของบริษัท โดยจงใจก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อบริษัท

2.11 ทำการติดตั้ง มีไว้ในการครอบครอง หรือใช้งาน Software ประเภท Hacking Tools หรือ Software อื่นใดที่เกี่ยวข้องกับการตรวจสอบ และรักษาความปลอดภัยของระบบคอมพิวเตอร์และข้อมูลสารสนเทศ ยกเว้นบุคคล หรือหน่วยงานที่ทำหน้าที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์และข้อมูลสารสนเทศโดยเฉพาะ หรือได้รับอนุมัติจากหน่วยงานที่ทำหน้าที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ และข้อมูลสารสนเทศโดยเฉพาะ หรือระบบสารสนเทศของบริษัทเท่านั้น

2.12 ทำการเชื่อมต่อคอมพิวเตอร์ที่มิใช่ทรัพย์สินของบริษัท เข้ากับระบบคอมพิวเตอร์ หรือเครือข่ายของบริษัท ไม่ว่าจะเป็นการเชื่อมต่อจากภายในหรือภายนอกบริษัท โดยมิได้รับอนุญาตจากหน่วยงานที่รับผิดชอบ

2.13 ทำการกำหนด และติดตั้ง หรือเปลี่ยนแปลง IP Address หรือ MAC Address ด้วยตนเอง โดยไม่ได้รับอนุญาตจากหน่วยงานที่รับผิดชอบ

2.14 ทำการแก้ไข ดัดแปลง ถอด ติดตั้งเพิ่มเติม หรือเคลื่อนย้ายชิ้นส่วนองค์ประกอบระบบคอมพิวเตอร์โดยพลการหรือนำชิ้นส่วนอุปกรณ์คอมพิวเตอร์อื่นใดที่ไม่ใช่ทรัพย์สินของบริษัท อันอาจก่อให้เกิดความเสียหายแก่บริษัท มาต่อหรือติดตั้งเพิ่มเติมกับทรัพย์สินของบริษัท โดยไม่ได้รับอนุญาต

2.15 ทำการดึงข้อมูล ส่ง เข้าไปดู หรือมีไว้ครอบครองในสิ่งที่ไม่สมควร หรือเป็นการผิดกฎหมาย เช่น ข้อความ สื่อลามกอนาจาร ฯลฯ หรือสิ่งอื่นใดอันเป็นการดูหมิ่น บ่อนทำลายสถาบันชาติ ศาสนา และพระมหากษัตริย์ หรือที่เป็นการปลุกระดมให้เกิดความแตกแยกในหมู่ประชาชน หรือพนักงาน หรือสร้างความเสียหายแก่บริษัท

2.16 ทำการส่งข้อความ หรือข้อมูลที่ไม่เหมาะสมโดยใช้ระบบ Email หรือใช้เครื่องมือสื่อสารของบริษัท เช่น หมิ่นประมาท คุกคาม ขู่กรรโชก กล่าวร้ายป้ายสี หยาบคาย หรือส่งจดหมายลูกโซ่ เป็นต้น

2.17 ใช้งานระบบ Internet หรือระบบ Intranet หรือ Email ในเรื่องที่ไม่เกี่ยวข้องกับธุรกิจของบริษัท

2.18 ใช้เครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ อันเป็นทรัพย์สินของบริษัท เพื่อความบันเทิงหรือประโยชน์ส่วนตัว

2.19 ใช้ Software ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย หรือที่บริษัทไม่ได้อนุญาตให้ใช้ หรือที่อาจก่อให้เกิดความเสียหายต่อบริษัท

2.20 ให้ความช่วยเหลือหรือร่วมมือกับบุคคลภายนอก เพื่อให้เข้าถึงระบบคอมพิวเตอร์ หรือระบบข้อมูลสารสนเทศของบริษัท กระทำการคัดลอกหรือทำลายข้อมูลสารสนเทศหรือระบบคอมพิวเตอร์ของบริษัท

2.21 จงใจ หรือประมาทเลินเล่อ หรือสนับสนุนการกระทำความผิดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายอื่นใดที่เกี่ยวข้อง

3. บริษัท สงวนสิทธิ์ที่จะตรวจสอบการใช้งานระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของพนักงาน ทุกคน เพื่อให้มั่นใจว่า การรักษาความปลอดภัยของข้อมูลสารสนเทศ และระบบคอมพิวเตอร์เป็นไปอย่างเหมาะสมโดยบริษัท สามารถตรวจสอบข้อมูลที่ผ่านระบบคอมพิวเตอร์ของบริษัท ได้ตลอดเวลา

4. การลงโทษ

4.1 ตักเตือนด้วยวาจา

4.2 ตักเตือนเป็นลายลักษณ์อักษร

4.3 พักงาน

4.4 เลิกจ้าง

การลงโทษพนักงาน บริษัท ไม่จำเป็นต้องปฏิบัติตามลำดับดังกล่าวข้างต้น บริษัท อาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

5. นโยบายการรักษาความปลอดภัยระบบคอมพิวเตอร์ และข้อมูลสารสนเทศ ให้ถือเป็นส่วนหนึ่งของระเบียบข้อบังคับเกี่ยวกับการทำงาน

นโยบายฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ 16 ธันวาคม 2568 โดยการอนุมัติของคณะกรรมการบริษัทในการประชุมครั้งที่ 8/2568

.....

(นายเกริกไกร จีระแพทย์)

ประธานคณะกรรมการบริษัท