Master Style
Public Company Limited

นโยบายการควบคุมความปลอดภัยทางเทคโนโลยีสารสนเทศ

บริษัท มาสเตอร์ สไตล์ จำกัด ("บริษัท")

1. <u>ความเป็นมา</u>

ในปัจจุบันมีการใช้ระบบสารสนเทศในองค์กรมากขึ้น ในขณะเดียวกันก็ทำให้มีภัยคุกคามหลากหลายประเภทตามมา ดังนั้นองค์กรที่ไม่มีการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างรัดกุมจึงมีความเสี่ยงที่จะเกิดผลกระทบจากภัยคุกคามต่าง ๆ เหล่านั้น ทำให้องค์กรจำเป็นที่จะต้องยกระดับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายขององค์กร เพื่อลดความเสี่ยงดังกล่าว โดยในปัจจุบันเป็นที่ยอมรับกันว่า "คอมพิวเตอร์" ได้กลายเป็นส่วนหนึ่งของชีวิตไปแล้ว "คอมพิวเตอร์" เข้ามามีบทบาทในงานต่าง ๆ เกือบทุกด้านในสังคมมนุษย์ การนำคอมพิวเตอร์มาใช้ในหน่วยงานนั้นจำเป็นจะต้องไปสัมพันธ์กับเจ้าหน้าที่และผู้ปฏิบัติจำนวนมาก บุคคลเหล่านี้มีแนวคิดและทัศนคติแตกต่างกันออกไป ดังนั้นเพื่อให้คนเหล่านี้ทำงานร่วมกันได้โดยไม่มีปัญหา จึงจำเป็นต้องมีระเบียบปฏิบัติที่ชัดเจน

2. <u>วัตถุประสงค์</u>

บริษัท มาสเตอร์ สไตล์ จำกัด ได้จัดให้มีเครือข่ายคอมพิวเตอร์เพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้แก่องค์กร ให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาอันอาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง อีกทั้งเพื่อให้พนักงานที่องค์กรทำสัญญาว่าจ้าง และหน่ายงานภายนอกเข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ จึงสมควรวางระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่ายขึ้นเพื่อให้พนักงานที่องค์กรทำสัญญาว่าจ้างและหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย ให้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงความปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

3. <u>ความสำคัญ</u>

พนักงานมีสิทธิ์ใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดดังกล่าวในวรรคหนึ่ง และอาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายขั้นสูงสุดแก่พนักงานที่ฝ่าฝืนทันที (อ้างอิงข้อ 31 บทลงโทษ) องค์กรต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน และปรับปรุงระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่ายเพื่อให้รองรับกับเทคโนโลยีที่ปรับเปลี่ยน ไปอย่างรวดเร็วรวมทั้งรองรับกับกฎหมาย

- นโยบายนี้จัดทำขึ้นสำหรับพนักงานหรือบุคคลทั่วไปที่จะเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ของ บริษัท มาสเตอร์ สไตล์ จำกัด (ซึ่งต่อไปจะเรียกว่า "บริษัท") รวมไปถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต โดยผ่านทางเครือข่ายของ บริษัท โดยให้ถือปฏิบัติโดยเคร่งครัด
- บริษัท สงวนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และ ดำเนินการอันสมควร หากพบว่ามีการละเมิด นโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์

4. <u>ผู้รับผิดชอบหลัก</u>

เจ้าหน้าที่ทั้งหมดขององค์กร

5. <u>คำนิยามที่เกี่ยวข้อง</u>

"องค์กร" หรือ **"บริษัท"** หมายความว่า บริษัท มาสเตอร์ สไตล์ จำกัด

"เครือข่ายระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์" หมายความว่า เครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์รวมถึงเครือข่ายสังคมออนไลน์ทุกประเภทของบริษัท มาสเตอร์ สไตล์ จำกัด

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างของบริษัท มาสเตอร์ สไตล์ จำกัด

"พนักงาน" หมายความว่า พนักงานและลูกจ้างของ บริษัท มาสเตอร์ สไตล์ จำกัด รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลงนโยบาย หรือใบสั่งซื้อ

"ผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์" หมายความว่า พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์เทคโนโลยีสารสนเทศและคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมเทคโนโลยีสารสนเทศ และคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

"ผู้บริหารองค์กร" หมายความว่า พนักงานระดับสูงของ บริษัท มาสเตอร์ สไตล์ จำกัด ที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับการดำเนินการทั้งหมดขององค์กร

"ผู้บริหารสารสนเทศ" หมายความว่า พนักงานระดับสูงของบริษัท มาสเตอร์ สไตล์ จำกัด ที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในองค์กร

"ผู้ดูแลระบบ" หมายความว่า พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ได้ เช่นบัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

"หัวหน้างานสารสนเทศ" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบพร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่ายและสารสนเทศขององค์กร และรายงานต่อผู้บริหารสารสนเทศ

"ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึก โดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย ได้แก่ ไฟล์ข้อความ ไฟล์ภาพ ไฟล์เสียง โปรแกรมคอมพิวเตอร์ เป็นต้น

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่งชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ได้แก่ คอมพิวเตอร์หรือเชื่อมต่อกันหรือไม่ก็ตาม โทรศัพท์เคลื่อนที่ อุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์ดิจิตอลต่าง ๆ เป็นต้น

"ผู้ให้บริการ" หมายความว่า ผู้ให้บริการแก่บุคคลอื่นในการเข้าถึงอุปกรณ์หรือชุดอุปกรณ์ของระบบเทคโนโลยีสารสนเทศหรือคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่งชุดคำสั่ง หรือสิ่งอื่นใด และแนวทาง

ปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ได้แก่ คอมพิวเตอร์ไม่ว่าจะเชื่อมต่อกันหรือไม่ก็ตาม โทรศัพท์เคลื่อนที่ อุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์ดิจิตอลต่าง ๆ เป็นต้น

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์นั้นรวมถึงข้อมูลทางสังคมออนไลน์ทุกประเภท ได้แก่ ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย, ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อและเครื่องที่เข้ามาใช้บริการและเครื่องที่ให้บริการและข้อมูลทางสังคมออนไลน์ทุกประเภท อาทิ เช่น ไลน์(Line) เฟสบุ๊ค (Facebook) ยูทูป (YouTube) เป็นต้น

6. หมวดทั่วไป

- ระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และ อุปกรณ์ต่อเชื่อมของ บริษัท จัดหาเพื่อให้บริการที่เกี่ยวข้องกับกิจการของ **บริษัท** เท่านั้น ไม่อนุญาตให้ใช้ในกิจการที่ไม่เกี่ยวข้องกับกิจการของ **บริษัท**
- การเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์และการต่ออินเทอร์เน็ตของ บริษัท จะต้องปฏิบัติตามขั้นตอนในการขออนุญาตเข้าใช้ โดยจะมีการลงทะเบียนการเข้าใช้งาน ตามขั้นตอนของ**บริษัท**
- ในการขออนุญาตเข้าใช้งาน ให้ผู้บังคับบัญชาโดยตรงของผู้ที่จะขอใช้บริการเป็นผู้ขอ โดยปฏิบัติตามขั้นตอนการขอเข้าใช้ระบบที่กำหนดไว้
- ผู้เข้าใช้งานจะต้องทำความเข้าใจและลงนามเพื่อยืนยัน ว่าจะปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์ และจะต้องทำความเข้าใจในส่วนเปลี่ยนแปลงแก้ไข หากมี โดยลงนามเพื่อยืนยัน
- นโยบายการใช้ระบบเครือข่ายคอมพิวเตอร์นี้ ถือเป็นส่วนหนึ่งของข้อกำหนดในการปฏิบัติงานของพนักงานทุกคน และจะถือเป็นการผิดวินัยการทำงานเช่นเดียวกันหากไม่ปฏิบัติตาม
- หากพบว่าพนักงานมีการละเมิดนโยบายการใช้งานระบบเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ จะถูกลงโทษตามกฎระเบียบของการเป็นพนักงาน รวมไปถึงอาจจะส่งตัวเพื่อดำเนินคดีตามกฎหมาย หากการละเมิดนั้นผิดต่อกฎหมายของประเทศ

7. ระเบียบปฏิบัติทั่วไป

- ให้ผู้ถือครองเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่เครื่องนั้นเกิดความเสียหาย หรือสูญหายไป
- ห้ามพนักงานใหม่ใช้งานเครื่องคอมพิวเตอร์ขององค์กรจนกว่าจะได้รับการอนุมัติให้ใช้งานโดยผ่านการลงทะเบียนก่อน
- ให้ผู้ที่เป็นเจ้าของข้อมูลที่ต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ขององค์กร จะต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น
- ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ขององค์กร จะต้องดำเนินการด้วยตนเอง โดยห้ามมิให้ผู้อื่นดำเนินการแทน
- ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ ให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
- ทำการตั้งค่าพักหน้าจอของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที ยกเว้นกรณีที่มีความที่จำเป็นต้องเปิดการใช้งานมากกว่าเวลาที่กำหนด โดยมีการขออนุมัติผ่านผู้มีอำนาจในการตัดสินใจเท่านั้น
- ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

- ระมัดระวังการใช้งาน และสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบเครือข่ายเหมือนเช่นบุคคลทั่วไปพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและระบบเครือข่ายแล้วแต่กรณี
- ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมที่นอกเหนือจากที่องค์กรได้ติดตั้งไว้ใช้งาน
- ห้ามทำการเปลี่ยนแปลง หรือแก้ไขซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องที่องค์กรจัดซื้อมา
- ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่เป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น
- ห้ามพนักงานติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย
- ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้น หรือระบบเครือข่ายขององค์กรได้
- ห้ามนำเครื่องคอมพิวเตอร์,Notebookและอุปกรณ์อิเล็คทรอนิกส์ส่วนตัวของพนักงานมาใช้กับระบบเครือข่ายขององค์กร ยกเว้น ได้ทำการขออนุญาติเป็นลายลักษณ์อักษรจากหัวหน้าสายงานและผู้บริหาร(ตำแหน่งรองประธาน เจ้าหน้าที่บริหารขึ้นไป) จึงสามารถใช้เครื่องคอมพิวเตอร์,โน๊ตบุคและอุปกรณ์อิเล็คทรอนิกส์ส่วนตัวของพนักงานได้ หลังจากได้รับการตรวจสอบเครื่องจากฝ่ายเทคโนโลยีสารสนเทศแล้ว
- กรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกสำนักงานจะต้องได้รับอนุมัติจากผู้มีอำนาจในการนำทรัพย์สินออกก่อนทุกครั้ง โดยลงชื่อเอกสารเพื่อขอยืมอุปกรณ์ IT ที่ฝ่ายบุคคล HR และขออนุมัติโดยหัวหน้าฝ่าย ยกเว้น Notebookและอุปกรณ์อิเล็คทรอนิกส์แบบพกพา ที่ได้รับมอบหมายในการทำงาน
- ให้ทำการติดตั้ง UPS สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีการใช้งานข้อมูลเป็นปริมาณมากและมีความถี่ในการใช้งานสูง
- ห้ามทำการปรับแต่งค่าระบบที่ได้รับจากการติดตั้งแต่เริ่มแรกอย่างเด็ดขาด เพราะอาจทำให้เกิดความเสียหายต่อระบบการทำงานของเครื่องคอมพิวเตอร์,Notebookและอุปกรณ์อิเล็คทรอนิกส์
- ห้ามทำการถอดหรือเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ได้รับการติดตั้งไว้ โดยไม่ได้แจ้งให้กับฝ่ายเทคโนโลยีสารสนเทศ ที่รับผิดชอบทราบล่วงหน้า
- ไม่ควรติดตั้งอุปกรณ์ต่อพ่วงใด ๆ ของคอมพิวเตอร์ด้วยตนเอง ตัวอย่างเช่น Printer หรือ อุปกรณ์ต่อพ่วงต่าง ๆ ควรแจ้งหรือติดต่อฝ่ายเทคโนโลยีสารสนเทศที่รับผิดชอบรับทราบ เพื่อที่จะได้ดำเนินการติดตั้งคอมพิวเตอร์ หรืออุปกรณ์ต่อพ่วงต่างๆ
- ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ (ห้องเครื่อง,ตู้กระจายสัญญาณ (Rack, Switch) ก่อนได้รับอนุญาต
- ผู้ใช้งานคอมพิวเตอร์ต้องรับทราบรวมถึงทำความเข้าใจและปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ณ วันที่ 23 สิงหาคม 2560 อย่างเคร่งครัด
- ให้ทำการติดตั้ง Firewall เพื่อป้องกันการบุกรุกหรือการโจรกรรมข้อมูล
- ไม่ทำการติดตั้ง Application ที่สำคัญลงบน Computer ของ Client โดยต้องทำการติดตั้งลงบน Server เท่านั้น

8. <u>ระเบียบการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อ อินเทอร์เน็ต</u>

- **บริษัท** ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบเครือข่ายคอมพิวเตอร์ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายประกอบอื่น ๆที่เกี่ยวข้อง
- **บริษัท** ไม่สนับสนุน หรือยินยอมให้พนักงานของ **บริษัท** กระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายประกอบอื่น ๆ ที่เกี่ยวข้อง
- **บริษัท** จะจัดให้มีชื่อผู้ใช้ (USER ID) และรหัสผ่าน (Password) ให้กับพนักงานที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบเครือข่ายคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตเป็นรายบุคคล และมีกฎในการใช้งานรหัสผ่านเช่น

ความยาวของตัวอักษร หรือ ระยะเวลาที่ต้องเปลี่ยนรหัสผ่าน ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม โดยกำหนดตามนโยบายที่บริษัทตั้งไว้

- รหัสผ่านของพนักงานถือเป็นทรัพย์สินของบริษัท ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และพนักงานทุกคนมีหน้าที่ในการป้องกันรหัสผ่านขององค์กรอย่างเคร่งครัด พนักงานทุกคนมีหน้าที่รับผิดชอบการกระทำต่าง ๆ ทั้งต่อระบบและข้อมูลที่เกิดขึ้นภายใต้ ชื่อผู้ใช้ (USER ID) ของตนเอง
- **บริษัท** อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน (กรณีที่เป็นการใช้งานร่วมกันในแผนก) ทั้งนี้ กรณีที่พนักงานในแผนกนั้นลาออก ต้องทำการเปลี่ยนแปลงรหัสผ่านทันที
- พนักงานอาจจะได้รับมอบหมายให้เข้าใช้ระบบงานอื่น ๆ ที่ **บริษัท** กำหนดให้ใช้ พนักงานจะต้องปฏิบัติตามกฎการใช้ระบบและเก็บรักษาชื่อและรหัสผ่านไว้ ห้ามมิให้เปิดเผยกับผู้อื่น ยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาโดยตรงเป็นลายลักษณ์อักษร
- หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่าน ให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอเลิกใช้โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน
- เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของ **บริษัท** พนักงานมีหน้าที่รักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบให้สามารถใช้งานได้ ทั้งนี้รวมไปถึงการ อัพเดท ระบบปฏิบัติการ และ โปรแกรมป้องกันไวรัส หรือชุดคำสั่งไม่พึงประสงค์
- ไม่อนุญาตให้ใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช่ของ บริษัท ในการเชื่อมต่อเข้ากับระบบเครือข่ายของ **บริษัท** ยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาโดยตรงเป็นลายลักษณ์อักษร

9. ระเบียบปฏิบัติสำหรับการใช้งานอินเทอร์เน็ต

- ห้ามทำการดาวน์โหลด หรือส่งไฟล์ประเภทสื่อลามก อนาจาร ไฟล์ที่ผิดกฎหมาย หรือสิ่งที่เป็นการละเมิดสิทธิ์ผู้อื่นโดยเด็ดขาดไม่ว่าจะเป็นการสื่อสารทางใดหรือเทคโนโลยีใดหรือระบบใดก็ตาม
- ห้ามทำการดาวน์โหลดไฟล์ที่มีขนาดใหญ่เกินกว่า 25MB โดยไม่จำเป็น
- ห้ามใช้อินเทอร์เน็ตโดยไม่เกี่ยวข้องกับงานที่รับผิดชอบ และไม่ควรใช้งานที่ไม่จำเป็นระหว่างเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น
- ห้ามเล่นเกมส์ ดูภาพยนตร์ ฟังเพลง หรือใช้สื่อสารสังคมออนไลน์ทุกประเภทที่ไม่เกี่ยวกับงานในความรับผิดชอบในการทำงานผ่านอินเทอร์เน็ต ยกเว้น ฝ่ายการตลาด ระดับผู้จัดการขึ้นไป และห้องผ่าตัด
- ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้
  - การพนัน
  - วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์
  - ลามก อนาจาร
  - อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม
- ห้ามใช้งานข้อมูลที่ได้รับ โดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ ของผู้เป็นเจ้าของข้อมูลนั้น
- ห้ามใช้อินเทอร์เน็ตเพื่อส่ง กระจาย หรือแจกจ่าย ดังต่อไปนี้
  - สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ
  - ข้อมูลที่เป็นความลับขององค์กร ไปยังบุคคลที่ไม่ได้รับอนุญาต
  - ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงขององค์กร

Master Style
Public Company Limited

10. <u>ระเบียบว่าด้วยการใช้เว็บไซต์ขององค์กรและอินเทอร์เน็ต</u>

- ห้ามพนักงานโพสต์รูปภาพ หรือข้อมูลใด ๆบนเว็บไซต์ของ บริษัท ที่
  - เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และ กฎหมายอื่นใดที่เกี่ยวข้องทั้งที่มีในปัจจุบันหรือที่จะมีในอนาคต
  - มีไวรัส หรือชุดคำสั่งไม่พึงประสงค์
  - ไม่เกี่ยวข้องกับกิจการขององค์กร
- ห้ามพนักงานดาวน์โหลดรูปภาพ หรือข้อมูลใด ๆ ที่
  - เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และ กฎหมายอื่นใดที่เกี่ยวข้องทั้งที่มีในปัจจุบันหรือที่จะมีในอนาคต
  - มีไวรัส หรือชุดคำสั่งไม่พึงประสงค์
  - ไม่เกี่ยวข้องกับกิจการขององค์กร

11. <u>ระเบียบว่าด้วยการใช้งาน Application และ โปรแกรม (HIS / Dynamics 365 Business central / Business Plus)</u>

- การเข้าใช้งาน Application (HIS / Dynamics 365 Business central / Business Plus) จะต้องได้รับอนุญาตจากเจ้าของระบบโดยให้ผู้บังคับบัญชาโดยตรงเป็นผู้ขอสิทธิในการใช้
- ให้พนักงานใช้โปรแกรมและ Application ที่ **บริษัท** กำหนดให้ใช้เท่านั้น อาทิ HIS, Dynamics 365 Business central, Business Plus, MS office เป็นต้น ยกเว้นเป็น Free License ที่ทางแผนกสารสนเทศติดตั้งให้ใช้งาน
- ห้ามพนักงานนำ โปรแกรม หรือ Application ใด ๆ มาติดตั้งบนเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่น ๆ **บริษัท** โดยไม่ได้รับความยินยอมจากฝ่ายเทคโนโลยีสารสนเทศและผู้บังคับบัญชาโดยตรง
- ห้ามพนักงานใช้โปรแกรม หรือ Application ที่ไม่ถูกต้องหรือละเมิดลิขสิทธิ์โดยเด็ดขาด
- การเข้าระบบงานต้องเข้าผ่านระบบ Windows เท่านั้น โดยทำการ Log On ด้วย User Name ที่ได้รับการอนุมัติแล้ว จากนั้นจึงทำการ Log On ขั้นที่ 2 เข้า Application ด้วย User Name (HIS / Dynamics 365 Business central / Business Plus) ที่ได้รับการอนุมัติ

12. <u>ระเบียบปฏิบัติสำหรับการใช้งาน E-mail, การสนทนาและการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่น ๆ</u>

ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ การสนทนา หรือการติดต่อสื่อสารใด ๆ ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรือจดหมายของ บริษัท ได้แก่

- ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อ **บริษัท** หรือบุคคลอื่น ๆ
- ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร
- การส่งข้อมูลใด ๆ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายอื่นใดที่เกี่ยวข้องทั้งที่มีในปัจจุบันหรือที่จะมีในอนาคต
- หากพบว่ามีการส่งข้อมูลที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือกฎหมายที่เกี่ยวข้อง หรือผิดต่อกฎระเบียบของ **บริษัท** ให้แจ้งไปที่ผู้บังคับบัญชาของผู้กระทำความผิด
- ให้ใช้ข้อความสุภาพในการส่งจดหมายอิเล็กทรอนิกส์ การสนทนา หรือการสื่อสารทาง อิเลกทรอนิกส์อื่น ๆ
- ห้ามส่งจดหมายอิเลกทรอนิกส์หรือการสื่อสารทางอิเลกทรอนิกส์ใด ๆ โดยไม่ระบุชื่อผู้ส่ง (SPAM e-mail)
- ห้ามมิให้เจ้าหน้าที่ผู้ไม่มีสิทธิเข้าถึงข้อมูล E-mail ของบุคคลอื่นใช้โดยไม่ได้รับอนุญาต
- ห้ามลงทะเบียนด้วย E-mail Address ที่องค์กรมอบให้ ไว้ตามที่อยู่เว็บไซต์ต่าง ๆ ที่ไม่เกี่ยวข้องกับงานขององค์กร
- ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
- ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
- ห้ามส่ง E-mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

- ห้ามส่ง E-mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
- ห้ามปลอมหรือปกปิดชื่อที่อยู่ E-mail ของตน เมื่อทำการส่งจดหมายไปยังผู้รับหนึ่ง
- ห้ามส่ง E-mail ที่มีลักษณะเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น
- ห้ามปลอมแปลง E-mail ของบุคคลอื่น
- ห้ามรับ หรือส่ง E-mail แทนบุคคลอื่นโดยไม่ได้รับอนุญาต
- ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-mail ของผู้รับให้ถูกต้อง
- ให้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-mail เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

13. <u>ระเบียบปฏิบัติสำหรับการป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์</u>

เจ้าหน้าที่และพนักงานจะต้องไม่ใช้ระบบเครือข่าย โดยมีวัตถุประสงค์ต่อไปนี้

- เพื่อการกระทำให้เกิดความเสียหายต่อระบบข้อมูลคอมพิวเตอร์และเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ของบริษัทโดยเด็ดขาด
- เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์ การบันเทิง หรือเพื่อประโยชน์ส่วนตน
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กร หรือบุคคลภายนอกก็ตาม
- เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่น
- เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว
- เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่องค์กร เช่น การรับ หรือส่ง ข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังเจ้าหน้าที่หรือบุคคลอื่น เป็นต้น
- เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร หรือของเจ้าหน้าที่อื่นขององค์กร หรือเพื่อให้เครือข่ายคอมพิวเตอร์ขององค์กร ไม่สามารถใช้งานได้ตามปกติ
- เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กร ไปยังที่อยู่เว็บ (website) ใด ๆ ในลักษณะที่จะก่อ หรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กรโดยฝ่ายเทคโนโลยีสารสนเทศจะทำการสุ่มตรวจเครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์แบบพกพารวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ ตามความเหมาะสม ผู้ถือครองทรัพย์สินคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ ต้องให้ความร่วมมือในการตรวจสอบอุปกรณ์ดังกล่าวทุกครั้งโดยทันที
- เพื่อจัดทำหรือเผยแพร่ชุดคำสั่งคอมพิวเตอร์ที่นำไปสู่การก่อความเสียหายต่อข้อมูล คอมพิวเตอร์หรือระบบคอมพิวเตอร์ทั้งขององค์กรและของผู้อื่น
- เพื่อปลอมแปลงข้อมูลคอมพิวเตอร์อันจะก่อให้เกิดความเสียหายต่อผู้อื่นหรือประชาชน
- เพื่อนำข้อมูลคอมพิวเตอร์ปลอมอันจะก่อให้เกิดความเสียหายต่อผู้อื่นหรือประชาชนเข้าสู่ระบบคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศ
- เพื่อเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ปลอมนั้นไปยังผู้อื่น
- เพื่อนำข้อมูลคอมพิวเตอร์เท็จอันจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนักแก่ประชาชน เข้าสู่ระบบคอมพิวเตอร์

- เพื่อสร้างข้อมูลคอมพิวเตอร์เท็จอันจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
- เพื่อเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์เท็จนั้นไปยังผู้อื่น
- เพื่อนำข้อมูลคอมพิวเตอร์ใด ๆ เข้าสู่ระบบคอมพิวเตอร์ โดยข้อมูลนั้นถือเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
- เพื่อเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ที่ถือเป็นความผิดดังกล่าวนั้นไปยังผู้อื่น
- เพื่อนำข้อมูลคอมพิวเตอร์ใด ๆ เข้าสู่ระบบคอมพิวเตอร์ ที่มีลักษณะเป็นการลามกและข้อมูลคอมพิวเตอร์นั้นพนักงานอื่นหรือประชาชนทั่วไปอาจเข้าถึงได้
- เพื่อเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ที่มีลักษณะเป็นการลามกไปยังผู้อื่น
- เพื่อสนับสนุนหรือยินยอมการนำข้อมูลคอมพิวเตอร์ใด ๆ เข้าสู่ระบบคอมพิวเตอร์โดย
  - ข้อมูลนั้นจะก่อให้เกิดความเสียหายต่อผู้อื่นหรือประชาชน
  - ข้อมูลนั้นจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศก่อให้เกิดความตื่นตระหนกแก่ประชาชน
  - ข้อมูลนั้นถือเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา หรือ ข้อมูลนั้นเป็นข้อมูลลามกซึ่งพนักงานอื่นหรือประชาชนทั่วไปอาจเข้าถึงได้
- เพื่อสร้าง ตัดต่อ เติมหรือดัดแปลงภาพด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นเกิดความเสียหายได้
- เพื่อเก็บข้อมูลคอมพิวเตอร์และเทคโนโลยีสารสนเทศที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้ผู้นั้นเกิดความเสียหายได้

14. ระเบียบการใช้งานระบบคอมพิวเตอร์

- ห้ามผู้ใช้งาน ทำการติดตั้ง ซ่อมแซม เปลี่ยนแปลงการตั้งค่า หรือดัดแปลง ชิ้นส่วนทางด้านฮาร์ดแวร์ของระบบคอมพิวเตอร์ ภายในองค์กร โดยไม่มีเจ้าหน้าที่เทคโนโลยีสารสนเทศคอยควบคุมดูแลอยู่หรือไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศก่อน โดยเด็ดขาด
- ห้ามผู้ใช้งาน ติดตั้งโปรแกรม (.exe หรือ Executable File ทุกชนิด รวมถึงโปรแกรมที่อาจมีผลเสียหายต่อระบบข้อมูลและอุปกรณ์ของบริษัท รวมทั้งโปรแกรม Screen saver และเกมทุกชนิด) ลงในระบบคอมพิวเตอร์ ขององค์กรโดยเด็ดขาด ทั้งนี้ การติดตั้งโปรแกรมทุกชนิดต้องเป็นการจัดการ หรือได้รับอนุญาตเป็นลายลักษณ์อักษร จากฝ่ายเทคโนโลยีสารสนเทศเท่านั้น
- ห้ามมิให้มีการนำซอฟต์แวร์ลิขสิทธิ์ที่เป็นขององค์กร ไปทำซ้ำ นำออก เผยแพร่ ติดตั้ง ละเมิด หรือใช้งานบนเครื่องคอมพิวเตอร์อื่นที่ไม่ใช่ขององค์กร หรือโดยไม่มีสิทธิ์ อย่างเด็ดขาด
- ห้ามใช้ระบบคอมพิวเตอร์ เพื่อวัตถุประสงค์อื่นที่นอกเหนือจากการใช้งานเพื่อปฏิบัติหน้าที่ที่ได้รับมอบหมาย ห้ามใช้งานในลักษณะที่ก่อให้เกิดปัญหา สร้างความติดขัด หรือทำให้สิ้นเปลืองพื้นที่จัดเก็บ/ทรัพยากร ของระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ขององค์กร เช่น การดาวน์โหลด/จัดเก็บข้อมูลขนาดใหญ่หรือโปรแกรมที่ไม่เกี่ยวข้องกับงาน การพิมพ์รายงานหรือรูปภาพส่วนตัว เป็นต้น
- ห้ามใช้ระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ในการพยายามเข้าถึง ไฟล์ ข้อมูล ฐานข้อมูล อีเมล์ของบุคคล สถาบัน หรือองค์กร โดยไม่มีสิทธิ์ หรือไม่ได้รับอนุญาตจากเจ้าของ
- ห้ามใช้ระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ขององค์กร เล่นเกม สังคมออนไลน์ทุกประเภทที่ไม่เกี่ยวข้องกับงานที่ดูแล ทั้งในเวลา หรือนอกเวลางานโดยเด็ดขาด
- ห้ามใช้ความรุนแรงในการใช้งานระบบคอมพิวเตอร์ เช่น ทุบ กระแทก เขย่า เป็นต้น ยกเว้นได้รับอนุญาตให้ทำการทดสอบเพื่อหาข้อบกพร่องจากทางฝ่ายเทคโนโลยีสารสนเทศ
- สำหรับจอภาพแบบ LCD ห้ามใช้นิ้ว หรือสิ่งของใด ๆ สัมผัสถูกหน้าจอเด็ดขาด เพราะอาจจะทำให้หน้าจอชำรุดและอายุใช้งานสั้นลง ยกเว้นการทำความสะอาดด้วยไม้ปัดขนไก่ หรือผ้าขนนุ่ม

- ห้ามเคลื่อนย้ายระบบเทคโนโลยีสารสนเทศและเครื่องคอมพิวเตอร์ (PC) ทั้งหมดหรือบางส่วน โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ
- ห้ามใช้งานระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ระบบอีเมล์ขององค์กร รวมทั้งสื่อบันทึกข้อมูลที่เคลื่อนย้าย เช่นแผ่นดิสก์, Removable Disk, Flash Drive โดยความประมาท เป็นเหตุให้เกิดความเสียหายจาก Virus, Spyware, Worms, Trojan หรือโปรแกรมไม่พึงประสงค์อื่น ๆ

15. ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์ Notebook หรือเครื่องคอมพิวเตอร์แบบพกพา

- กรณีที่เป็นเครื่องคอมพิวเตอร์ Notebook ที่จัดสรรไว้เป็นเครื่องกลาง ให้ทำการกรอกแบบฟอร์มขออนุญาตยืมคืนตามที่องค์กรกำหนดไว้
- ให้ผู้ใช้งานตรวจสอบว่าเครื่องคอมพิวเตอร์ Notebook ขององค์กรถูกติดตั้งโปรแกรมตามรายชื่อโปรแกรมมาตรฐานที่องค์กรกำหนดไว้หรือไม่ (โปรแกรมดังกล่าว ได้แก่ โปรแกรมไมโครซอฟต์ออฟฟิศ โปรแกรมป้องกันไวรัส หรือโปรแกรมอื่น ๆ เป็นต้น) หากพบว่ายังไม่ได้ทำการติดตั้ง ให้ทำการติดต่อเจ้าหน้าที่เทคโนโลยีสารสนเทศเพื่อขอรับการติดตั้งก่อนการใช้งาน
- เมื่อมีการนำไปใช้งานนอกสถานที่ ให้ระมัดระวัง รักษาเครื่องคอมพิวเตอร์ Notebook เพื่อป้องกันการสูญหาย (กรณีพบว่าเครื่องเสียหาย ให้ถือว่าผู้ที่ลงนามรับทรัพย์สินเป็นผู้รับผิดชอบ ตามแบบฟอร์มหนังสือรับมอบทรัพย์สิน FM-GA-005 Rev.00,13/01/63)

16. ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน

Windows (AD)

- ต้องเก็บ และ รักษารหัสผ่านที่ได้รับมอบมาจากองค์กรให้เป็นความลับ
- ต้องตั้งรหัสผ่านให้มีคุณสมบัติ ดังต่อไปนี้
  - มีความยาวไม่น้อยกว่า 8 ตัวอักษร
  - มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ, พิมพ์ใหญ่, ตัวเลขและสัญลักษณ์เข้าด้วยกัน
  - ไม่ควรตั้งรหัสผ่านจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
  - ไม่ควรกำหนดรหัสผ่านจากคำศัพท์ที่ใช้ในพจนานุกรม

HIS

- ต้องเก็บ และ รักษารหัสผ่านที่ได้รับมอบมาจากองค์กรให้เป็นความลับ
- ต้องมีรหัสผ่านเข้าระบบ โดยกำหนดรหัส Login เป็นรหัสพนักงาน และ รหัสผ่านครั้งแรก (Draft) แผนกไอทีเป็นคนตั้งให้

  และหลังจากได้รหัสผู้ใช้ต้องทำการเปลี่ยนรหัสผ่านโดยทันที

Dynamics 365 Business central

- ต้องเก็บ และ รักษารหัสผ่านที่ได้รับมอบมาจากองค์กรให้เป็นความลับ
- ต้องตั้งรหัสผ่านให้มีคุณสมบัติ ดังต่อไปนี้
  - มีความยาวไม่น้อยกว่า 8 ตัวอักษร
  - มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ, พิมพ์ใหญ่, ตัวเลขและสัญลักษณ์เข้าด้วยกัน
  - ไม่ควรกำหนดรหัสผ่านจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
  - ไม่ควรกำหนดรหัสผ่านจากคำศัพท์ที่ใช้ในพจนานุกรม

Business Plus

- ต้องเก็บ และ รักษารหัสผ่านที่ได้รับมอบมาจากองค์กรให้เป็นความลับ
- ต้องมีรหัสผ่านเข้าระบบ โดยกำหนดรหัส Login เป็นชื่อพนักงาน (ภาษาอังกฤษ) และ รหัสผ่านกำหนดโดยแผนกบุคคล
  และไม่สามารถเปลี่ยนรหัสผ่านได้
- ต้องกำหนดรหัสผ่านสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านทางระบบเครือข่าย
- ห้ามใช้โปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตนโดยอัตโนมัติ (Save Password)
- ต้องไม่จด หรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- ไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง
- กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที
- ให้กลุ่มผู้ใช้งานที่มีการใช้งานบัญชีผู้ใช้งาน และรหัสผ่านเดียวกัน จะต้องร่วมกันรับผิดชอบหากมีความเสียหาย หรือมีปัญหาเกิดขึ้นกับระบบที่เข้าถึง

17. คุณลักษณะของรหัสผ่าน

- รหัสผ่านสามารถเข้าระบบผิดได้ไม่เกิน 5 ครั้ง หากเกินระบบจะทำการล็อคต้องติดต่อให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ปลดล็อครหัสผ่าน
- หากไม่ใช้งาน Computer เกิน 5 นาทีระบบจะทำการล็อคหน้าจอ ต้องทำการ Log On เข้าระบบด้วยรหัสผ่านทุกครั้งที่มีการล็อค ยกเว้นกรณีที่มีความที่จำเป็นต้องเปิดการใช้งานมากกว่าเวลาที่กำหนด โดยมีการขออนุมัติผ่านผู้มีอำนาจในการตัดสินใจเท่านั้น
- ในการเปลี่ยนรหัสผ่านใหม่ห้ามใช้รหัสเดิมซ้ำ
- ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน หากไม่เปลี่ยนระบบจะทำการล็อค User Name อัตโนมัติ
- ต้องทำการเปลี่ยนรหัสผ่านใหม่ทันทีที่ได้รับ User Name และ Password ในการใช้งานครั้งแรก

18. ระเบียบปฏิบัติสำหรับการใช้งานห้องเครื่องแม่ข่าย

- พนักงานที่ได้รับสิทธิเข้าห้องเครื่องแม่ข่าย โดยการบันทึกลายนิ้วมือ
- ห้ามเข้าไปในบริเวณห้องเครื่องแม่ข่ายก่อนได้รับอนุญาต
- ห้ามพนักงานเข้าไปในบริเวณห้องเครื่องแม่ข่ายโดยไม่มีกิจที่เกี่ยวข้อง
- ห้ามนำอาหาร และ เครื่องดื่มเข้าไปในบริเวณห้องเครื่องแม่ข่าย
- ให้ติดบัตร Visitor ตลอดเวลาเพื่อให้สามารถสังเกตเห็นได้อย่างชัดเจน หากไม่ใช่พนักงานของบริษัท
- ให้ทำการลงบันทึกการเข้าออกห้องเครื่องแม่ข่ายโดยบุคคลภายนอก โดยระบุถึงเหตุผลการเข้าและต้องได้รับอนุมัติโดยผู้มีอำนาจ
- หากพบเห็นความผิดปกติในห้องเครื่องแม่ข่าย เช่น มีทรัพย์สินเสียหาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งเจ้าหน้าที่เทคโนโลยีสารสนเทศ
- ห้ามนำอุปกรณ์ที่สามารถบันทึกภาพได้เข้าไปภายในห้องเครื่องแม่ข่าย เช่น โทรศัพท์เคลื่อนที่, กล้องดิจิตอล กล้องวิดีโอ เป็นต้น
- ให้ปฏิบัติตามคำแนะนำของเจ้าหน้าที่ที่ดูแลห้องเครื่องแม่ข่ายอย่างเคร่งครัด

Master Style
Public Company Limited

19. <u>ระเบียบปฏิบัติสำหรับการจัดการสารสนเทศ</u>

สำหรับสารสนเทศที่อยู่ในรูปแบบเอกสารกระดาษ

- ให้ใช้เครื่องทำลายเอกสารเพื่อทำลายเอกสารที่เป็นความลับหรือเอกสารเกี่ยวกับข้อมูลลูกค้า หรือที่มีระดับความสำคัญสูง (อันได้แก่ ตัวเลขเงิน และเอกสารเกี่ยวกับข้อมูลลูกค้า ห้ามนำเอกสารนั้นมาใช้ Recycle อีกเด็ดขาด
- ให้ป้องกันเอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงที่ถูกพิมพ์ออกมาทางเครื่องพิมพ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ให้จัดหมวดหมู่เอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างพอเพียง
- ให้สำเนาเอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงได้ก็ต่อเมื่อได้รับอนุญาตจากผู้เป็นเจ้าของแล้ว
- ให้ระมัดระวังการกระจาย หรือแจกจ่ายเอกสารที่เป็นความลับขององค์กรไปยังกลุ่มผู้รับใด ๆทั้งที่มีความจำเป็นและไม่จำเป็นต้องรับรู้รับทราบในเอกสารนั้น
- ให้ทำการตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน
- ห้ามนำเอกสารเกี่ยวกับลูกค้าของบริษัททุกประเภททุกอย่างรวมถึงข้อมูลสำคัญของบริษัทอื่นใดส่งออกนอกองค์กรหรือนอกฝ่ายที่รับผิดชอบโดยเด็ดขาดไม่ว่าจะเป็นทางไปรษณีย์ทางE-mail หรือการนำออกไปโดยวิธีใด ๆ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารเท่านั้น

สำหรับสารสนเทศที่เป็นข้อมูลอิเลกทรอนิกส์ (เช่น ไฟล์อิเลกทรอนิกส์, ข้อมูลบนเว็บ, E-mail, Voice-Mail, ข้อมูลมัลติมีเดีย)

- ให้จัดหมวดหมู่ข้อมูลอิเลกทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างเพียงพอ
- ให้สำเนาข้อมูลอิเลกทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงได้ก็ต่อเมื่อได้รับอนุญาตจากผู้เป็นเจ้าของแล้ว
- ให้ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเลกทรอนิกส์ที่เป็นความลับขององค์กรไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลอิเลกทรอนิกส์นั้น
- ให้ผู้เป็นเจ้าของข้อมูลอิเลกทรอนิกส์ ทำการตรวจสอบความถูกต้องของข้อมูลอิเลกทรอนิกส์ก่อนนำไปใช้งาน
- ห้ามผู้เป็นเจ้าของข้อมูลอิเลกทรอนิกส์ที่เป็นความลับ หรือที่มีระดับความสำคัญสูง ทำการส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่องค์กรกำหนดไว้
- ให้ส่งเครื่องคอมพิวเตอร์ที่ได้จะต้องจำหน่ายออกให้กับฝ่ายเทคโนโลยีสารสนเทศเพื่อทำการฟอร์แมตข้อมูลอิเลกทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์นั้น
- ห้ามมิให้ผู้ใดทำการคัดลอกสำเนา (Copy) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ออกไปนอกบริษัทไม่ว่าจะด้วยวิธีการใดก็ตาม (เช่น การบันทึกลงในสื่อบันทึกต่าง ๆ อาทิ เช่น ฟลอปปีดิสก์, ฮาร์ดดิสก์, แผ่น CD, แผ่น DVD, Handy Drive /Flash Drive เป็นต้น) รวมถึงห้ามมิให้ส่ง Email, ถ่ายรูป, หรือนำออกโดยตรง หรือคัดลอก หรือดำเนินการโดยวิธีอื่นใดก็ตามโดยเด็ดขาด

หมายเหตุ : หากผู้ใดมีความจำเป็นต้องนำข้อมูลเหล่านั้นออกนอกบริษัท ต้องแจ้งให้ผู้บังคับบัญชาทราบและอนุญาตก่อน มิฉะนั้นจะถือว่ามีเจตนามิชอบ

Master Style
Public Company Limited

20. <u>ระเบียบปฏิบัติสำหรับการเข้าถึงระบบงาน</u>

- เมื่อพนักงานใหม่เข้ามาปฏิบัติหน้าที่ ให้ผู้บังคับบัญชาของพนักงานดังกล่าวส่งความประสงค์ขอเข้าใช้ระบบงานผ่านระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือกรอกแบบฟอร์ม เพื่อขอรหัสเข้าใช้งานระบบคอมพิวเตอร์, เครื่องพิมพ์ เพื่อนำเสนอต่อผู้บังคับบัญชาตามลำดับขั้นและแจ้งความประสงค์มายังฝ่ายเทคโนโลยีสารสนเทศ
- การแจ้งความประสงค์ขอเข้าใช้ระบบงานผ่านระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือกรอกแบบฟอร์มต้องระบุระบบงานที่ต้องการใช้ อุปกรณ์ที่ต้องการใช้ โดยต้องได้รับอนุมัติโดยหัวหน้าฝ่าย และเจ้าของระบบงานรวมทั้งฝ่ายเทคโนโลยีสารสนเทศ
- พนักงานแต่ละฝ่ายควรมีสิทธิเข้าถึงระบบงานต่างกันตามแต่ละหน้าที่ โดยต้องแยกให้ชัดเจนระหว่าง ผู้บันทึก ผู้อนุมัติ หรือ User Name ที่ใช้เพื่อการเรียกดู
- ต้องไม่เข้าถึงระบบงานอื่นที่ตนไม่ได้รับอนุมัติให้ใช้งานโดยเด็ดขาด
- ต้องไม่เข้าถึงข้อมูลคอมพิวเตอร์ที่ได้มีการป้องกันเอาไว้ และตนไม่ได้รับอนุญาตการใช้งาน
- ต้องออกจากระบบงานโดยทันทีที่ใช้งานสำเร็จ
- ต้องไม่เปิดเผยข้อมูลที่เกี่ยวข้องกับมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ขององค์กรให้แก่บุคคลภายนอก
- ต้องไม่ใช้ทรัพยากรคอมพิวเตอร์ขององค์กรเพื่อดักรับข้อมูลคอมพิวเตอร์ขององค์กรหรือของผู้อื่นที่อยู่ระหว่างการส่งและตนไม่ได้รับสิทธิการเข้าถึง

21. <u>ระเบียบปฏิบัติสำหรับการแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย</u>

- ให้เจ้าหน้าที่ทำการแจ้งไปยังฝ่ายเทคโนโลยีสารสนเทศ โดยทันที เมื่อพบเห็นเหตุการณ์ทางด้านความมั่นคงปลอดภัย ได้แก่
  - โปรแกรมไม่ประสงค์ดีหรือมีการใช้โปรแกรมโดยผู้ไม่ประสงค์ดี
  - ระบบถูกบุกรุกทางเครือข่าย
  - ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย
  - มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
  - การนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์
  - การใช้ทรัพยากรสารสนเทศผิดวัตถุประสงค์
  - การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน
  - ระบบถูกโจมตีจนไม่สามารถให้บริการได้
  - ทรัพยากรสารสนเทศถูกขโมย
  - การอนุญาตให้บุคคลภายนอกเข้าใช้ระบบงานขององค์กร
  - การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายหรือเหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัยขององค์
- ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา หรือผู้ดูระบบเครือข่ายในการตรวจสอบเหตุการณ์ทางด้านความปลอดภัยที่เกิดขึ้น และ/หรือ ระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลและระบบเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา หรือผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด
- มีการจัดทำ log การเข้า – ออก ห้อง server อย่างเหมาะสมปลอดภัย
- จัดให้มีอุปกรณ์ดับเพลิงที่ไม่ทำลายระบบคอมพิวเตอร์ในกรณีฉุกเฉิน

Master Style
Public Company Limited

22. <u>ระเบียบปฏิบัติสำหรับการใช้งานอุปกรณ์เสริม สำหรับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์อย่างปลอดภัย</u>

อุปกรณ์เสริมสำหรับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ หมายรวมถึง Notebook, กล้องถ่ายรูป, อุปกรณ์ที่เชื่อมต่อทาง USB Port, Wi-Fi, Bluetooth ที่มีหน่วยความจำในการบันทึกข้อมูล หรือถ่ายภาพได้ เป็นต้น รวมถึงอุปกรณ์อื่นใดที่จะมีในอนาคต ฝ่ายเทคโนโลยีสารสนเทศ จะดูแลอุปกรณ์เสริมต่าง ๆ ที่อยู่ในความรับผิดชอบของฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

- ไม่นำอุปกรณ์เสริมสำหรับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ และอุปกรณ์เสริมส่วนตัวอื่น ๆ มาใช้งานในระบบเครือข่ายและคอมพิวเตอร์ของบริษัท ยกเว้นในกรณีที่ได้รับอนุมัติจากผู้บังคับบัญชาแล้ว หากพบว่ามีการใช้งานโดยไม่ได้รับอนุญาตผู้ดูแลระบบสามารถระงับการเชื่อมต่อเข้าใช้งานออกจากระบบเครือข่ายได้ทันที
- การใช้งานอุปกรณ์เสริมสำหรับคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และอุปกรณ์เสริมส่วนตัวอื่น ๆ บนระบบเครือข่ายคอมพิวเตอร์ของบริษัทจะต้องแจ้งให้ผู้บังคับบัญชาทราบเพื่อให้ผู้บังคับบัญชาได้ตรวจสอบข้อมูลทุกครั้งเพื่อขึ้นทะเบียนก่อนนำมาใช้งานบนระบบเครือข่ายคอมพิวเตอร์ของบริษัท
- ไม่นำอุปกรณ์เสริมสำหรับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ รวมทั้งอุปกรณ์เสริมส่วนตัวอื่น ๆ ที่ขึ้นทะเบียนแล้ว มาใช้งานเพื่อบันทึกไฟล์ที่เป็นสื่อบันเทิงใด ๆ ที่นอกเหนือจากงานที่ได้รับมอบหมาย
- ไม่นำอุปกรณ์เสริมสำหรับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ และอุปกรณ์เสริมอื่น ๆ ของบริษัทออกไปใช้งานภายนอกบริษัท ยกเว้นในกรณีที่ได้รับอนุมัติจากผู้บังคับบัญชาแล้ว และหากเกิดการสูญหาย ผู้ครอบครองอุปกรณ์ดังกล่าวจะต้องรับผิดชอบ
- หากอุปกรณ์ที่ครอบครองเกิดการเสียหายจากการใช้งาน ผู้ถือครองจะต้องทำเรื่องขออนุมัติในการซ่อมแซม และส่งให้ฝ่ายเทคโนโลยีสารสนเทศ พิจารณาต่อไป
- ไม่ถ่ายภาพและไม่นำอุปกรณ์บันทึกภาพเข้ามาในบริเวณบริษัทและบริเวณรอบนอกบริษัท หากเป็นกล้องถ่ายภาพดิจิตอลที่ติดมากับ Notebook หรือโทรศัพท์เคลื่อนที่ ต้องงดเว้นการใช้งาน กรณีที่เป็นกล้องถ่ายภาพของโทรศัพท์เคลื่อนที่, Tablet ห้ามนำเข้ามาในบริเวณบริษัททุกกรณี เว้นแต่ได้รับอนุมัติจากผู้มีอำนาจก่อนเท่านั้น ผู้ฝ่าฝืนจะได้รับโทษตามระเบียบของบริษัทอย่างเคร่งครัด
- หากตรวจสอบพบว่าอุปกรณ์ กล้องถ่ายรูป, อุปกรณ์ที่มีความสามารถในการถ่ายภาพ, Handy Drive, โทรศัพท์เคลื่อนที่, Tablet หรือ Notebook รวมทั้งอุปกรณ์เสริมอื่น ๆ มีการบันทึกข้อมูลนอกเหนือจากงานที่ได้รับมอบหมาย ฝ่ายเทคโนโลยีสารสนเทศ มีสิทธิทำลายข้อมูลออกจากอุปกรณ์ทันที และผู้ถือครองอุปกรณ์จะได้รับโทษตามระเบียบของบริษัทโดยเคร่งครัด

23. <u>ระเบียบข้อปฏิบัติการใช้งานระบบข้อมูล</u>

- การพัฒนาระบบข้อมูลหรือการแก้ไข จะต้องมีการทดสอบร่วมกันระหว่างผู้ใช้งานและผู้ดูแลระบบข้อมูลก่อนการใช้งานจริง โดยทำการบันทึกผ่านระบบที่ฝ่ายเทคโนโลยีสารสนเทศ และอนุมัติตามขั้นตอนโดยผู้มีอำนาจอนุมัติ
- การพัฒนาหรือขอเปลี่ยนแปลงใด ๆ ต้องระบุประเภทของการเปลี่ยนแปลงในแบบฟอร์มและขออนุมัติจากเจ้าของระบบงาน
- ต้องระบุรายละเอียดการเปลี่ยนแปลงโดยละเอียด
- การเปลี่ยนแปลงต้องได้รับอนุมัติโดยฝ่ายเทคโนโลยีสารสนเทศ
- ผู้ขอต้องทดสอบระบบอีกครั้งก่อนการนำมาใช้จริงและลงลายมือชื่อทุกครั้งของการทดสอบ
- เมื่อทดสอบเรียบร้อยแล้วให้ผู้มีอำนาจอนุมัตินำมาใช้งานจริงในขั้นตอนสุดท้าย
- การใช้งานระบบข้อมูล ให้เป็นไปตามการกำหนดสิทธิที่ส่วนจัดการระบบข้อมูลได้ตกลงไว้กับผู้ใช้งาน ตามตารางกำหนดสิทธิที่จัดทำไว้
- การทดสอบระบบจะต้องทำบน Server Test เท่านั้นห้ามกระทำบน Production เพื่อป้องกันความเสียหายของข้อมูล

Master Style
Public Company Limited

24. ระเบียบปฏิบัติสำหรับการยืมคืนอุปกรณ์คอมพิวเตอร์และอุปกรณ์เสริม ประจำห้องคอมพิวเตอร์

- เจ้าหน้าที่ผู้ยืมต้องลงบันทึกการยืมในแบบฟอร์มยืมอุปกรณ์แต่ละชนิด ก่อนการใช้งานทุกครั้ง และระบุช่วงเวลาการใช้งาน รวมทั้งรายละเอียดอื่น ๆ ให้ครบถ้วนชัดเจน
- กรณีการยืมอุปกรณ์ไปใช้งาน เช่น กล้องถ่ายวีดีโอ, กล้องดิจิตอล, เครื่องอัดเสียง, ถ่านชาร์จ, ปลั๊กไฟ, ลำโพง, Notebook, Projector, Handy drive ฯลฯ ถ้าอุปกรณ์นั้นว่างอยู่ไม่มีผู้ใดใช้งานในช่วงเวลานั้น จะสามารถนำไปใช้ได้ตามเวลาที่ขอทันที แต่หากอุปกรณ์นั้นอยู่ในช่วงเวลาที่มีการจองมาก่อน จะต้องรอตามลำดับการจอง
- ก่อนรับอุปกรณ์ พนักงานต้องตรวจนับจำนวนและตรวจสอบสภาพของอุปกรณ์ให้เรียบร้อย
- เนื่องจากอุปกรณ์ส่วนใหญ่มีราคาแพง ผู้ใช้งานจึงควรใช้ด้วยความระมัดระวัง หากอุปกรณ์มีปัญหาในระหว่างการใช้งาน และมีสาเหตุมาจากความบกพร่องของผู้ยืม ผู้ยืมต้องเป็นผู้รับผิดชอบค่าซ่อมแซมในราคาที่จ่ายจริงหรือกรณีไม่สามารถซ่อมแซมได้ ผู้ยืมต้องเป็นผู้รับผิดชอบจัดหามาคืนให้ครบถ้วนตามรายการและจำนวนที่ยืม
- ห้ามยืมอุปกรณ์ต่อจากผู้ยืมท่านอื่น
- หลังจากใช้งานอุปกรณ์แล้ว ผู้ยืมต้องโหลดงานหรือ File และลบงานหรือ File ให้เรียบร้อยก่อนส่งอุปกรณ์คืน ห้ามเก็บงานหรือ File ไว้ในอุปกรณ์ซึ่ง ฝ่ายเทคโนโลยีสารสนเทศ จะไม่รับผิดชอบในกรณีที่เกิดสูญหายขึ้นและห้ามเก็บข้อมูลสำคัญ หรือข้อมูลความลับของบริษัทไว้ในอุปกรณ์ โดยเด็ดขาด
- การส่งมอบอุปกรณ์คืน ต้องให้เจ้าหน้าที่ผู้ให้ยืมตรวจสอบอุปกรณ์ว่าครบถ้วนและอยู่ในสภาพที่สามารถใช้งานได้

25. ระเบียบข้อปฏิบัติพนักงาน

- พนักงานทุกคนมีสิทธิใช้ระบบเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ และระบบข้อมูลภายใต้ข้อกำหนดของบริษัทที่กำหนดขึ้นเท่านั้น การฝ่าฝืนจนเป็นเหตุหรืออาจเป็นเหตุให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใด บริษัทจะพิจารณาดำเนินการทางวินัยและกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสม
- พนักงานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ไม่ Download/ Upload ข้อมูลหรือสิ่งอื่นใด ที่ไม่เกี่ยวข้องกับงาน หรือใช้ Website ที่ไม่เกี่ยวข้องกับงานหรือกิจการของบริษัท
- พนักงานพึงใช้ข้อความสุภาพ หรือใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น รวมทั้งปฏิบัติให้ถูกต้องตามธรรมเนียมปฏิบัติของการใช้เครือข่าย
- พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่พึงอนุญาตให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง
- เพื่อป้องกันหากมีผู้อื่นล่วงรู้และนำรหัสผ่านของพนักงานไปใช้ในทางที่ผิดและเกิดความเสียหายต่อบริษัทพนักงานจะต้องเก็บรหัสผ่านไว้เป็นความลับ และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ(Save Password) สำหรับคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่
- เพื่อความปลอดภัยในการใช้ระบบเครือข่ายคอมพิวเตอร์ กรณีพนักงานพบไวรัสคอมพิวเตอร์จะต้องแจ้งให้ผู้ดูแลระบบดำเนินการกำจัดไวรัสโดยเร็ว
- พนักงานพึงลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล
- พนักงานพึงให้ความร่วมมือและอำนวยความสะดวกแก่ ผู้ดูแลระบบ หรือ ฝ่ายเทคโนโลยีสารสนเทศ ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำที่เกี่ยวข้องกับความปลอดภัยในระบบเครือข่ายดังกล่าวของบริษัทฯ
- ห้ามพนักงานใช้ระบบเครือข่ายและคอมพิวเตอร์ เพื่อการดังต่อไปนี้
  - การกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
  - การกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
  - การค้าหรือการแสวงหาผลกำไร หรือผลประโยชน์ส่วนตัว

- การเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้บริษัท ไม่ว่าจะเป็นข้อมูลบริษัท พนักงาน หรือบุคคลภายนอกก็ตาม
- การกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของบริษัท หรือบุคคลอื่น
- การกระทำเพื่อให้ทราบข้อมูลข่าวสารบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว
- การรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัท เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือการส่งข้อมูลที่ได้รับจากบุคคล ภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังพนักงาน หรือบุคคลอื่น เป็นต้น
- การขัดขวางการใช้งานเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของบริษัท หรือพนักงาน หรือทำให้เครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ของบริษัทไม่สามารถ ใช้งานได้ตามปกติ
- แสดงความเห็นส่วนบุคคลในเรื่องที่เกี่ยวกับการดำเนินงานของบริษัทไปยังที่อยู่เว็บ (Website) ใด ๆ ในลักษณะที่ก่อให้เกิดหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง หรือ ก่อให้เกิดความเสียหายแก่บริษัทหรือบุคคลอื่น
- การอื่นใดที่อาจขัดต่อผลประโยชน์ของบริษัท หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่บริษัท

➢ ห้ามมิให้พนักงานติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์ต่อพ่วงอื่นใด นอกเหนือจากที่บริษัทได้จัดไว้ให้ กรณีมีความจำเป็นต้องติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงเพิ่มเติม ให้แจ้งผู้ดูแลระบบเป็นผู้ดำเนินการให้

➢ ห้ามมิให้พนักงานส่ง E-mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น

➢ พนักงานต้องทำการศึกษาการใช้งานระบบโปรแกรม ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวกับงานที่ตนเองรับผิดชอบให้เข้าใจก่อนดำเนินการใช้งาน เพื่อไม่ให้เกิดความเสียหายต่อระบบโปรแกรมและข้อมูลบริษัท กรณีไม่แน่ใจให้สอบถามผู้รู้ก่อนดำเนินการทุกครั้งเพื่อไม่ให้เกิดความเสียหาย

26. ระเบียบปฏิบัติสำหรับการจัดการการลาออกของพนักงาน

➢ พนักงานที่ประสงค์จะลาออก ต้องยืนหนังสือตามระเบียบข้อบังคับเกี่ยวกับการทำงานของบริษัทสำหรับผู้ที่ใช้คอมพิวเตอร์และอุปกรณ์ต่อพ่วงในการปฏิบัติงานนั้น ให้กรอกข้อมูลแจ้งการส่งคืนทรัพย์สินและอุปกรณ์ส่วนบุคคลที่ฝ่ายบุคคล

➢ พนักงานทดลองงาน ยื่นล่วงหน้าไม่น้อยกว่า 30 วัน

➢ พนักงาน ต้องยืนล่วงหน้าไม่น้อยกว่า 30 วัน

➢ พนักงานระดับผู้บริหาร ต้องยื่นล่วงหน้าไม่น้อยกว่า 30 วัน

➢ เมื่อได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคลถึงการลาออกของพนักงาน เจ้าหน้าที่เทคโนโลยีสารสนเทศ ต้องทำการตรวจสอบคอมพิวเตอร์ หรืออุปกรณ์ที่มีการใช้งานโดยพนักงานที่ลาออกนั้น ว่ายังอยู่ในสภาพที่พร้อมใช้งานอยู่หรือไม่

➢ หากอุปกรณ์เสียหาย อันเนื่องจากความประมาทหรือเสียหายโดยที่ไม่ได้เสื่อมตามอายุ การใช้งานตามปกติพนักงานต้องเป็นผู้รับผิดชอบค่าซ่อมแซม หรือในกรณีที่ไม่สามารถซ่อมแซมได้ ต้องเป็นผู้รับผิดชอบจัดหามาคืนให้ครบถ้วนตามรายการและจำนวนที่ครอบครอง แต่หากเกิดการสูญหายพนักงานต้องเป็นผู้รับผิดชอบชดใช้คืนแก่บริษัท

➢ จัดทำสิทธิของพนักงานที่โยกย้ายตำแหน่ง/ฝ่าย ตามหน้าที่ความรับผิดชอบใหม่ให้สามารถเริ่มใช้งานได้ ตามวันที่ระบุของวันที่โยกย้ายตำแหน่ง/ฝ่าย ที่ได้รับแจ้งจากฝ่าย บริหารทรัพยากรบุคคล

➢ เจ้าหน้าที่เทคโนโลยีสารสนเทศ ถอดถอนสิทธิของผู้ที่ลาออก ออกจากระบบต่าง ๆ ตามวันที่ระบุของวันที่ลาออกตามที่ได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคล โดยทำการกรอกแบบฟอร์ม คืนอุปกรณ์และ User Name ให้ผู้มีอำนาจอนุมัติ

Master Style
Public Company Limited

27. <u>ระเบียบปฏิบัติสำหรับการจัดการโยกย้ายตำแหน่ง/ฝ่ายของพนักงาน</u>

- พนักงานที่ได้รับคำสั่งโยกย้ายตำแหน่ง/ฝ่าย และมีการใช้คอมพิวเตอร์และอุปกรณ์ฟ่วงในการปฏิบัติงานนั้น ต้องยื่นเอกสารระบุรายละเอียดเกี่ยวกับการส่งคืนทรัพย์สินและอุปกรณ์ความปลอดภัยส่วนบุคคล ให้กับฝ่ายทรัพยากรบุคคล
  - พนักงานทดลองงาน ยื่นล่วงหน้าไม่น้อยกว่า 7 วัน
  - พนักงาน ต้องยื่นล่วงหน้าไม่น้อยกว่า 7 วัน
  - พนักงานระดับผู้บริหาร ต้องยื่นล่วงหน้าไม่น้อยกว่า 7 วัน
- เมื่อได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคลถึงการโยกย้ายตำแหน่ง/ฝ่ายของพนักงาน เจ้าหน้าที่เทคโนโลยีสารสนเทศจะต้องทำการตรวจสอบคอมพิวเตอร์หรืออุปกรณ์ที่มีการใช้งาน ว่ายังอยู่ในสภาพที่พร้อมใช้งานอยู่หรือไม่
- หากอุปกรณ์เสียหาย อันเนื่องจากความประมาท หรือเสียหายโดยที่ไม่ได้เสื่อมตามอายุการใช้งานตามปกติ พนักงานต้องเป็นผู้รับผิดชอบค่าซ่อมแซม หรือในกรณีที่ไม่สามารถซ่อมแซมได้ ต้องเป็นผู้รับผิดชอบจัดหามาคืนให้ครบถ้วนตามรายการและจำนวนที่ครอบครอง แต่หากเกิดการสูญหาย พนักงานต้องเป็นผู้รับผิดชอบชดใช้คืนแก่บริษัท
- จัดทำสิทธิของพนักงานที่โยกย้ายตำแหน่ง/ฝ่าย ตามหน้าที่ความรับผิดชอบใหม่ให้สามารถเริ่มใช้งานได้ ตามวันที่ระบุของวันที่โยกย้ายตำแหน่ง/ฝ่าย ที่ได้รับแจ้งจากฝ่ายทรัพยากรบุคคล
- ถอดถอนสิทธิเดิมของผู้โยกย้ายตำแหน่ง/ฝ่ายออกจากระบบต่าง ๆ เดิมทั้งหมด ตามวันที่ระบุของวันที่โยกย้ายตำแหน่ง/ฝ่าย ที่ได้รับแจ้งจากฝ่ายทรัพยากรบุคคล

28. <u>ระเบียบข้อปฏิบัติสำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์</u>

ข้อปฏิบัติของผู้ดูแลระบบเครือข่าย

- ควบคุม ดูแลบำรุงรักษาและปรับปรุงเครือข่ายเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ กรณีพบความผิดปกติเกิดขึ้นในระบบ ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจระงับการใช้เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเพื่อป้องกันความเสียหายได้
- ไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ
- จัดเก็บข้อมูลการจราจรคอมพิวเตอร์ โดยถือปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้องในปัจจุบันและที่จะมีในอนาคต
- ควบคุมดูแลระบบฮาร์ดแวร์และอุปกรณ์ที่เกี่ยวข้องรวมถึงซอฟต์แวร์และโปรแกรมต่าง ๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนของพนักงาน ให้ถูกต้องตามลิขสิทธิ์ของซอฟต์แวร์หรือโปรแกรมที่ติดตั้งอยู่
- จัดทำคู่มือการใช้งานระบบเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ เพื่อเป็นแนวทางและวิธีปฏิบัติแก่ผู้ใช้งานระบบ
- ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายตามที่ผู้บังคับบัญชามอบหมาย
- ควบคุมดูแลตรวจสอบด้านความปลอดภัยของข้อมูลและด้านอื่น ๆ ในระบบเทคโนโลยีสารสนเทศและคอมพิวเตอร์ขององค์กรอย่างดีและสม่ำเสมอ
- ตรวจสอบสถานะ Server ทุกวันว่าสภาพแวดล้อมและตัวเครื่องอยู่ในสภาพพร้อมใช้งานโดยจดบันทึกรายการตรวจสอบไว้เป็นหลักฐาน
- มีการบันทึก Security Log เพื่อตรวจสอบความปลอดภัยรวมถึงระมัดระวังผู้บุกรุกระบบคอมพิวเตอร์

Master Style
Public Company Limited

29. ข้อปฏิบัติสำหรับผู้ดูแลระบบข้อมูล

- พัฒนา ปรับปรุง และบำรุงรักษาระบบข้อมูล รวมทั้งต้องระบุข้อกำหนดความปลอดภัย
- กำหนดสิทธิการใช้งานระบบ ก่อนการใช้งาน
- ควบคุมการติดตั้งซอฟต์แวร์ต่าง ๆ ลงในระบบข้อมูลระบบเทคโนโลยีสารสนเทศและในเครื่องคอมพิวเตอร์ของพนักงานโดยไม่ให้กระทบต่อระบบหลักและไม่ก่อให้เกิดความเสียหายต่อระบบรวม
- ระงับการใช้งานระบบงานของพนักงาน เมื่อมีการตรวจสอบพบว่าใช้งานไม่ถูกต้องหรือละเมิดข้อตกลงการใช้งาน
- จัดทำคู่มือการใช้งานระบบข้อมูล เพื่อเป็นแนวทางและวิธีปฏิบัติให้แก่ผู้ใช้งานระบบ
- ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับระบบข้อมูลตามที่ผู้บังคับบัญชามอบหมาย
- ทำการสอบทานสิทธิการเข้าถึงระบบอย่างน้อยทุก 3 เดือน โดยให้เจ้าของระบบงานแต่ละระบบลงลายมือชื่อสอบทานสิทธิ์
- ทำ Backup ประจำวันทุกระบบ (Business Plus, Dynamics 365 Business central, Express) ไว้ที่ Drive กลาง พร้อมจดบันทึกลง Google Sheet
- ทำ Full Backup ลงในระบบ Cloud ทุกสิ้นเดือนหรือ Backup ทุกสิ้นเดือนพร้อมจดบันทึกลง Google Sheet

30. ระเบียบการบริหารการเปลี่ยนแปลงระบบสารสนเทศ

- การสั่งซื้ออุปกรณ์ใหม่ / ซอฟต์แวร์ใหม่ / เพิ่มประสิทธิภาพของอุปกรณ์ที่มีอยู่

  -พนักงาน / หน่วยงานที่ร้องขอ ทำการแจ้งงานผ่าน ระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือฟอร์มIT Support

  -แผนกไอทีทำการรับเรื่อง และตอบกลับ

  -แผนกไอทีทำการหาสเปคตามความต้องการของผู้ใช้และติดต่อผู้ขายเพื่อให้เสนอราคา

  -แผนกไอทีนำส่งข้อมูลให้แผนกที่ร้องขอ เพื่อยืนยันสเปค และนำส่งให้แผนกจัดซื้อ

  -ผู้ตรวจ คือ ผู้อำนวยการของแต่ละหน่วยงานที่ร้องขอ

  -ผู้อนุมัติ คือ CEO / VCEO
- การซ่อมอุปกรณ์ที่มีอยู่

  -พนักงาน / หน่วยงานที่ร้องขอ ทำการแจ้งงานผ่าน ระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือฟอร์มIT Support

  -แผนกไอทีทำการรับเรื่อง และตอบกลับ

  -แผนกไอทีทำการตรวจสอบปัญหาเบื้องต้น ดำเนินการแก้ไข / ส่งซ่อมเพื่อให้เสนอราคา

  -แผนกไอทีนำส่งข้อมูลให้แผนกที่ร้องขอ รับทราบผลการแก้ไข / มีค่าใช้จ่ายในการซ่อม

  -ผู้ตรวจ คือ ผู้อำนวยการของแต่ละหน่วยงานที่ร้องขอ

  -ผู้อนุมัติ คือ CEO / VCEO
- การปรับปรุงค่าของซอฟต์แวร์ที่มีอยู่

  -พนักงาน / หน่วยงานที่ร้องขอ ทำการแจ้งงานผ่าน ระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือฟอร์มIT Support

  -แผนกไอทีทำการรับเรื่อง และตอบกลับ

  -แผนกไอทีทำการตรวจสอบหัวข้อ หรือรายการที่ต้องการแก้ไขปรับหรุง

  -แผนกไอทีนำส่งข้อมูลให้แผนกที่ร้องขอ รับทราบผลการแก้ไข / มีค่าใช้จ่ายในการปรับปรุง

  -ผู้ตรวจ คือ ผู้อำนวยการของแต่ละหน่วยงานที่ร้องขอ

  -ผู้อนุมัติ คือ CEO / VCEO
- พนักงานใหม่ขอสิทธิใช้ระบบ

-เจ้าหน้าที่ HR ทำการแจ้งรายชื่อพนักงานใน ระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือฟอร์มIT Support (ขั้นตอนพนักงานเข้าใหม่/ลาออก (HR) โดยใส่รายละเอียด รหัสพนักงาน, ชื่อ-นามสกุล, ตำแหน่งงาน, แผนก, Email, วันเริ่มงาน, โปรแกรมที่ใช้งาน

-แผนกไอทีทำการกดรับงาน และตอบกลับงานที่เสร็จใน ระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือฟอร์มIT Support

-แผนก HR ตรวจงานและประเมิน NPS เมื่อตรวจสอบความถูกต้องแล้ว

- ถอนสิทธิ์พนักงานที่ลาออกแล้ว

-เจ้าหน้าที่ HR ทำการแจ้งรายชื่อพนักงานใน ระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือฟอร์มIT Support (ขั้นตอนพนักงานเข้าใหม่/ลาออก (HR) โดยใส่รายละเอียด รหัสพนักงาน, ชื่อ-นามสกุล, ตำแหน่งงาน, แผนก, Email, วันที่ลาออก

-แผนกไอทีทำการกดรับงาน ทำการปิดสิทธิในการเข้าแต่ละโปรแกรม และตอบกลับงานที่เสร็จใน ระบบ Online ที่ฝ่ายสารสนเทศกำหนดให้ใช้ หรือฟอร์มIT Support

-แผนก HR ตรวจงานและประเมิน NPS เมื่อตรวจสอบความถูกต้องแล้ว

31. <u>บทลงโทษ</u>

ในกรณีตรวจสอบพบการฝ่าฝืน หรือไม่ปฏิบัติตามนโยบายการควบคุมความปลอดภัยทางเทคโนโลยีสารสนเทศของบุคคล หรือกลุ่มบุคคล บริษัทจะดำเนินการตักเตือนหรือลงโทษบุคคล หรือกลุ่มบุคคลนั้น ดังนี้

- ครั้งที่ 1 ตักเตือนด้วยวาจา พร้อมออกใบเตือน
- ครั้งที่ 2 ตักเตือนเป็นหนังสือ-พักงานไม่จ่ายค่าจ้าง
- ครั้งที่ 3 ให้ออก เลิกจ้าง .

หรือหากเป็นการกระทำความผิดร้ายแรงจนเป็นเหตุให้ระบบงานของบริษัทติดขัดไม่สามารถทำงานได้ หรือเกิดความเสียหายสูญหายกับบริษัทหรือข้อมูลรั่วไหล หรือเจตนาที่ไม่บริสุทธิ์ ของพนักงานผู้นั้น บริษัทจะเลิกจ้างทันทีโดยไม่มีการเตือนและบริษัทสามารถเรียกค่าเสียหายได้

32. <u>คำจำกัดความ</u>

"กฎหมาย" หมายถึง พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 บทเฉพาะกาลอื่น ๆ ที่เกี่ยวข้องรวมถึงกฎหมายที่มีการบัญญัติในปัจจุบันหรือที่จะมีในอนาคต

Master Style
Public Company Limited

33. <u>การทบทวนนโยบาย</u>

โดยภายในระยะเวลา 2 ปี บริษัทต้องทบทวนและปรับปรุงนโยบายฉบับนี้ตามความจำเป็นและความเหมาะสม อย่างน้อย 1 ครั้ง

นโยบายการควบคุมความปลอดภัยทางเทคโนโลยีสารสนเทศฉบับนี้ อนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2565 ประกาศและให้มีผลบังคับใช้ตั้งแต่วันที่ 14 มิถุนายน 2565 เป็นต้นไป

.....

(นพ.เจษฎา โชคดำรงสุข)

ประธานกรรมการบริษัท

บริษัท มาสเตอร์ สไตล์ จำกัด (มหาชน)