



นโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน)

ในปัจจุบันมีการใช้ระบบเทคโนโลยีสารสนเทศในองค์กรมากขึ้น ขณะเดียวกัน ทำให้มีภัยคุกคามหลากหลายประเภท ตามมาดั่งนั้นองค์กร ที่ไม่เตรียมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างรัดกุม จึงมีความเสี่ยงที่จะเกิดผลกระทบจากภัยคุกคามต่างๆ เหล่านั้น ทำให้องค์กรจำเป็นต้องยกระดับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และ เครือข่ายขององค์กร เพื่อลดความเสี่ยงดังกล่าว โดยในปัจจุบันเป็นที่ยอมรับกันว่า “คอมพิวเตอร์” ได้ เข้ามามีบทบาทในการทำงานต่างๆเกือบทุกด้าน การนำคอมพิวเตอร์มาใช้ในหน่วยงานนั้น จำเป็นจะต้องไปสัมพันธ์กับเจ้าหน้าที่ และ ผู้ปฏิบัติจำนวนมาก ซึ่งบุคคลเหล่านี้มีแนวคิด และ ทักษะแตกต่างกันออกไป ดังนั้นเพื่อให้คนเหล่านี้สามารถทำงานร่วมกันได้ โดยไม่มีปัญหา จึงจำเป็นต้องมีการกำหนดระเบียบปฏิบัติที่ชัดเจน

วัตถุประสงค์

บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน) ได้จัดให้มีเครือข่ายคอมพิวเตอร์เพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงาน ให้แก่ องค์กร การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสม และ มีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหา อันอาจจะ เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์อย่างไม่ถูกต้องเหมาะสม อีกทั้งเพื่อให้พนักงานที่องค์กรทำสัญญาว่าจ้าง และ หน่วยงานภายนอกเข้าใจถึงบทบาท และ หน้าที่ความรับผิดชอบของตน เพื่อลดความเสี่ยงอันเกิดจากการขโมย การ سوء โกง การ นำข้อมูลอันเป็นความลับ ไปใช้อย่างผิดวิธี และ การใช้อุปกรณ์ผิดวัตถุประสงค์ องค์กรจึงกำหนดวางระเบียบปฏิบัติสำหรับการ ใช้งานคอมพิวเตอร์และระบบเครือข่ายขึ้น เพื่อให้พนักงานที่องค์กรทำสัญญาว่าจ้าง และ หน่วยงานภายนอกได้ ตระหนักถึง ภัย คุกคาม ปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย และ หน้าที่ความรับผิดชอบ ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทาง กฎหมาย ให้เรียนรู้ และ ทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงความปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิด จากความผิดพลาดในการปฏิบัติหน้าที่

ความสำคัญ

พนักงานมีสิทธิ์ใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดนโยบายการใช้งาน ระบบเทคโนโลยีสารสนเทศนี้ หรือกระทำการใดๆอันก่อ หรือ อาจทำให้เกิดความเสียหายแก่องค์กร หรือ บุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาคำเนิการทางวินัย และ ทางกฎหมายขั้นสูงสุดแก่พนักงานที่ฝ่าฝืนทันที ดังนั้นองค์กรจึงกำหนด ลงมือ ปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน และ ปรับปรุงระเบียบปฏิบัติ สำหรับการใช้งานคอมพิวเตอร์ และ ระบบเครือข่ายเพื่อให้ รองรับกับเทคโนโลยีสารสนเทศที่ปรับเปลี่ยนไปอย่างรวดเร็ว รวมทั้งรองรับกับกฎหมาย โดยผู้รับผิดชอบหลัก พนักงาน ทั้หมดขององค์กร ตามคำนิยามที่เกี่ยวข้อง

“องค์กร”	: บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน)
“เครือข่ายคอมพิวเตอร์”	: เครือข่ายคอมพิวเตอร์ของ บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน)
“ผู้บังคับบัญชา”	: ผู้มีอำนาจสั่งการตามโครงสร้างของ บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน)
“พนักงาน”	: พนักงาน และ ลูกจ้างของ บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน) รวมถึงบุคคลอื่นที่องค์กรมอบหมาย ให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือ ใบสั่งซื้อ หรือผู้ที่องค์กรสามารถให้เข้าถึงเครือข่าย คอมพิวเตอร์ขององค์กรได้
“ผู้ดูแลเครือข่ายคอมพิวเตอร์”	: พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึง โปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
“ผู้บริหารองค์กร”	: พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และ มีอำนาจตัดสินใจเกี่ยวกับการดำเนินงานทั้งหมดขององค์กร ที่มีหน้าที่บริหารจัดการ และ มีอำนาจตัดสินใจ
“ผู้บริหารสารสนเทศ”	: พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารเกี่ยวกับระบบเทคโนโลยีสารสนเทศภายในองค์กร
“ผู้ดูแลระบบ”	: พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และ สามารถเข้าถึงโปรแกรมคอมพิวเตอร์ หรือ ข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีอีเมลอิเล็กทรอนิกส์ (Email Account) เป็นต้น
“หัวหน้างานสารสนเทศ”	: พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบ พร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่าย และสารสนเทศขององค์กร รวมทั้งรายงานต่อผู้บริหารสารสนเทศ
“หน่วยงานภายนอก”	: องค์กรอื่น ๆ หรือ คู่ค้าที่เกี่ยวข้องกับบริษัท เช่น บริษัทขายฮาร์ดแวร์ หรือ ซอฟต์แวร์ บริษัท ให้คำปรึกษาเกี่ยวกับระบบเทคโนโลยีสารสนเทศ เป็นต้น
“ข้อมูล”	: สิ่งสื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้น จะทำได้โดยสภาพของสิ่งนั้นเอง หรือ โดยผ่านวิธีการใดๆ และ ไม่ว่าจะได้จัดทำไว้ใน รูปแบบของ

เอกสาร แฟ้มรายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่ายฟิล์ม การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือ วิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ได้แก่ ไฟล์ข้อความ ไฟล์ภาพ ไฟล์เสียง โปรแกรม คอมพิวเตอร์ เป็นต้น

“ระบบคอมพิวเตอร์” : หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือ สิ่งอื่นใด และ แนวทางปฏิบัติงานให้อุปกรณ์หรือชุด อุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ได้แก่ คอมพิวเตอร์หรือเชื่อมต่อกัน หรือ ไม่ก็ตาม โทรศัพท์เคลื่อนที่ เป็นต้น

“ผู้ให้บริการ” : ผู้ให้บริการแก่บุคคลอื่นในการเข้าถึงอุปกรณ์ หรือ ชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด ชุดคำสั่ง หรือ สิ่งอื่นใด และ แนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ได้แก่ คอมพิวเตอร์ (ไม่ว่าจะเชื่อมต่อกันหรือไม่ก็ตาม) โทรศัพท์เคลื่อนที่ เป็นต้น

“ข้อมูลจราจรทางคอมพิวเตอร์” : ข้อมูลเกี่ยวกับการติดต่อสื่อสาร การติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรือ อื่น ๆ ที่เกี่ยวข้อง กับการติดต่อสื่อสารของระบบคอมพิวเตอร์ฯ ได้แก่ ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการ เข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย, ข้อมูลเกี่ยวกับวัน และ เวลา ที่มีการติดต่อสื่อสาร และ เครื่องที่เข้ามาใช้บริการ และ เครื่องที่ให้บริการ เป็น ต้น

หมวดที่ 1 : ว่าด้วยระเบียบปฏิบัติทั่วไป

ผู้ถือครองเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่เครื่องนั้นเกิดความเสียหายต่อตัวเครื่อง หรือ ระบบปฏิบัติการจากการใช้งานผิดวิธี หรือสูญหายไป

- ห้ามพนักงานใหม่ใช้งานเครื่องคอมพิวเตอร์ขององค์กรจนกว่าจะได้รับการอนุมัติให้ใช้งานผ่านการลงทะเบียนก่อน
- ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติ และ มีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการ ตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติให้รีบแจ้งเจ้าหน้าที่เทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยทันที (ทางฝ่ายเทคโนโลยีสารสนเทศเปิดอบรมหลักสูตรวิธีการตรวจสอบโปรแกรม Anti-Virus)
- ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
- ทำการตั้งค่า Screen Server ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการ “การ Lock หน้าจอ” หลังจากที่ไม่ได้ใช้งานเกินกว่า 10 นาที
- ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำ บนสื่อบันทึกข้อมูล
- ระมัดระวังการใช้งาน และ สงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบเครือข่ายเหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งาน เครื่องคอมพิวเตอร์ส่วนบุคคลและระบบเครือข่าย แล้วแต่กรณี
- ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมที่นอกเหนือจากที่องค์กรได้ติดตั้งไว้ให้ใช้งาน
- ห้ามทำ การเปลี่ยนแปลง หรือแก้ไขซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องที่องค์กรจัดซื้อ
- ห้ามนำอุปกรณ์เครื่องคอมพิวเตอร์ส่วนบุคคลมาใช้ในองค์กร เว้นแต่จะได้รับการอนุมัติ และ มีการขึ้นทะเบียนเท่านั้น ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่น สามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้น หรือระบบเครือข่ายขององค์กรได้
- ห้ามนำ เครื่องคอมพิวเตอร์ส่วนตัวของพนักงานมาใช้กับระบบเครือข่ายขององค์กร เว้นแต่จะได้รับการอนุมัติ และ มีการขึ้นทะเบียน จากฝ่ายเทคโนโลยี สารสนเทศ
- กรณีที่ต้องการนำ อุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกสำนักงานจะต้องได้รับอนุมัติจากผู้มีอำนาจในการนำทรัพย์สินออกก่อนทุกครั้ง
- ทำการติดตั้ง UPS สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีการใช้งานข้อมูลเป็นปริมาณมากและมีความถี่ในการใช้งานสูงห้ามทำการปรับแต่งค่าระบบที่ได้รับจากการติดตั้งแต่เริ่มแรกอย่างเด็ดขาด เพราะอาจทำให้เกิดความเสียหายต่อระบบการทำงานของเครื่องคอมพิวเตอร์

- ห้ามทำ การถอดหรือเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ได้รับการติดตั้งไว้ โดยไม่ได้แจ้งให้กับฝ่ายเทคโนโลยีสารสนเทศที่รับผิดชอบทราบล่วงหน้า
- ห้ามติดตั้งเพิ่มเติมอุปกรณ์ต่อพ่วงใด ๆ ของคอมพิวเตอร์ เช่น หูฟัง, ไมโครโฟน, Printer โดยพลการ ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศที่รับผิดชอบเพื่อดำเนินการติดตั้งให้
- ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ (Server room) ก่อนได้รับอนุญาต ผู้ใช้งานคอมพิวเตอร์ต้องรับทราบรวมถึงทำความเข้าใจและปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ณ วันที่ 23 มกราคม 2560 อย่างเคร่งครัด

หมวดที่ 2: ระเบียบปฏิบัติสำหรับการใช้งานอินเทอร์เน็ต

- ห้ามทำ การดาวน์โหลด หรือส่งไฟล์ประเภทสื่อลามก อนาจาร
- ห้ามทำ การดาวน์โหลดไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น
- ห้ามใช้อินเทอร์เน็ตโดยไม่เกี่ยวข้องกับงานที่รับผิดชอบ และไม่ควรงานที่ไม่จำเป็นระหว่างเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น
- ห้ามเล่นเกมส์ ดูภาพยนตร์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ต
- ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้
 - การพนัน
 - การประมุข
 - วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา และ พระมหากษัตริย์ลามก อนาจาร ผิด พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มาตรา 14
 - อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม
- ห้ามใช้โปรแกรมสนทนาในห้องสนทนา เช่น สังคมออนไลน์ (Facebook/Instagram/ We chat/Line/Skype/Twitter ฯลฯ) และ ยกเว้นส่วนงานที่ได้รับอนุญาตให้ใช้งานเท่านั้น
- ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น ห้ามใช้อินเทอร์เน็ตเพื่อส่งกระจาย หรือแจกจ่าย ดังต่อไปนี้
 - สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ
 - ข้อมูลที่เป็นความลับขององค์กรไปยังบุคคลที่ไม่ได้รับอนุญาต
 - ข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต
- ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์ และ ชื่อ ชื่อเสียงขององค์กร

๒

หมวดที่ 3 : ระเบียบปฏิบัติสำหรับการใช้งาน E-mail

- ห้ามมิให้พนักงานหรือผู้ไม่มีสิทธิเข้าถึงข้อมูล E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต
- ห้ามลงทะเบียนด้วย E-mail Address ที่องค์กรมอบให้ ตามที่อยู่เว็บไซต์ต่าง 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 เมื่อทำการส่ง E-Mail ไปยังผู้อื่น
- ห้ามส่ง E-mail ที่มีลักษณะเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น
- ห้ามปลอมแปลง E-mail ของบุคคลอื่น
- ห้ามรับ หรือส่ง E-mail แทนบุคคลอื่นโดยไม่ได้รับอนุญาต
- ใช้คำที่ไม่สุภาพในการส่ง E-mail
- ห้ามส่ง E-mail ที่มีขนาดไฟล์ใหญ่เกินกว่า 10 เมกะไบต์ หรือตามที่องค์กรระบุไว้
- ห้ามส่ง E-mail ที่เป็นความลับขององค์กร เว้นเสียแต่จะใช้วิธีการเข้ารหัสข้อมูล E-mail ที่องค์กรกำหนดไว้
- ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-mail ของผู้รับให้ถูกต้อง
- ให้ระบุชื่อของผู้ส่งใน E-mail ทุกฉบับที่ส่งไป
- ให้ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-mail เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

หมวดที่ 4 : ระเบียบปฏิบัติสำหรับการป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

พนักงานจะต้องไม่ใช้ระบบเครือข่าย โดยมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือ ศีลธรรมอันดีของประชาชน หรือการเมือง
- เพื่อการพาณิชย์ การบันเทิง หรือ เพื่อประโยชน์ส่วนตัว

24

- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กร ไม่ว่าจะป็นข้อมูลขององค์กร หรือ บุคคลภายนอกก็ตาม
- เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือ ของบุคคลอื่น เพื่อให้ทราบข้อมูล ข่าวสารของบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ หรือ ผู้ที่มีสิทธิในข้อมูลดังกล่าว เพื่อแสดงความคิดเห็น ส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กร ไปยังที่อยู่เว็บ (website) ใด ๆ ใน ลักษณะที่จะก่อ หรืออาจ ก่อให้เกิดความเข้าใจที่คลาดเคลื่อน ไปจากความเป็นจริง
- เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรือ อาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร
- ฝ่ายเทคโนโลยีสารสนเทศจะทำการคุ้มครองเครื่องคอมพิวเตอร์ หรือ เครื่องคอมพิวเตอร์แบบพกพา รวมทั้งอุปกรณ์ต่อ พ่วงต่างๆ ตามความเหมาะสม ผู้ถือครองทรัพย์สินคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ ต้องให้ความร่วมมือในการ ตรวจสอบอุปกรณ์ดังกล่าว
- เพื่อปลอมแปลงข้อมูลคอมพิวเตอร์อันจะก่อให้เกิดความเสียหายต่อผู้อื่นหรือประชาชน
- เพื่อเผยแพร่ หรือ ส่งต่อข้อมูลคอมพิวเตอร์ปลอมนั้น ไปยังผู้อื่น
- เพื่อนำข้อมูลคอมพิวเตอร์ที่จันจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน เข้าสู่ระบบคอมพิวเตอร์
- เพื่อเผยแพร่ หรือ ส่งต่อข้อมูลคอมพิวเตอร์ที่จันนั้น ไปยังผู้อื่น
- เพื่อนำข้อมูลคอมพิวเตอร์ใด ๆ เข้าสู่ระบบคอมพิวเตอร์ โดยข้อมูลนั้นถือเป็นการผิดเกี่ยวกับความมั่นคงแห่ง ราชอาณาจักร หรือ ความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
- เพื่อนำข้อมูลคอมพิวเตอร์ใด ๆ เข้าสู่ระบบคอมพิวเตอร์ ที่มีลักษณะเป็นการลามก อนาจาร และ ข้อมูลคอมพิวเตอร์นั้น พนังงานอื่นหรือประชาชนทั่วไปอาจเข้าถึงได้
- เพื่อเผยแพร่ หรือ ส่งต่อข้อมูลคอมพิวเตอร์ที่มีลักษณะเป็นการลามก อนาจาร ไปยังผู้อื่น
- เพื่อสร้างข้อมูลคอมพิวเตอร์ ดัดต่อ ต่อเติม หรือ ดัดแปลงภาพ ด้วยวิธีการทางอิเล็กทรอนิกส์ หรือ วิธีการอื่นใดที่จะ ทำให้ผู้อื่นเกิดความเสียหายได้
- เพื่อเก็บข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และ ภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ดัดต่อ ต่อเติม หรือ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้อันนั้นเกิดความเสียหายได้

หมวดที่ 5: ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน

- ต้องจัดเก็บ และ รักษารหัสผ่านที่ได้รับมอบมาจากองค์กรให้เป็นความลับ
- ต้องตั้งรหัสผ่านให้มีคุณสมบัติดังต่อไปนี้

- มีความยาวไม่น้อยกว่า 8 ตัวอักษร
 - มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ, ตัวพิมพ์ใหญ่, ตัวเลขและสัญลักษณ์เข้าด้วยกัน
 - ไม่กำหนดรหัสผ่านจาก ชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์
คน
 - ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ใช้ในพจนานุกรม
- การตั้งชื่อผู้ใช้งานนั้น ต้องกำหนดการตั้งชื่อ ไม่ซ้ำกัน (Unique User ID)
 - ต้องกำหนดรหัสผ่านสำหรับการใช้เพิ่มข้อมูลร่วมกับบุคคลอื่นผ่านทางระบบเครือข่าย ห้ามใช้โปรแกรมคอมพิวเตอร์
เพื่อช่วยในการจำรหัสผ่านของตนโดยอัตโนมัติ (Save Password)
 - ต้องไม่จด หรือ บันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
 - ไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้งานของตนเอง
 - กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้ว ต้องทำการเปลี่ยนรหัสผ่าน
โดยทันที
 - ให้กลุ่มผู้ใช้งานที่มีการใช้งานบัญชีผู้ใช้งาน และ รหัสผ่านเดียวกัน จะต้องร่วมกันรับผิดชอบหากมีความเสียหาย หรือ
มีปัญหาเกิดขึ้นกับระบบที่เข้าถึง
 - ห้ามกำหนดรหัสลับ (Set Password) ส่วนของเครื่องคอมพิวเตอร์ (Hardware) ทั้งในระดับ BIOS และ ระดับแบบ
ปฏิบัติการ (Operating System) ด้วยตนเอง นอกเหนือจากผู้บังคับบัญชาของส่วนเทคโนโลยีสารสนเทศ และ ผู้ที่
ได้รับมอบหมาย
 - รหัสผ่านของพนักงานถือเป็นทรัพย์สินของ บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน) ไม่อนุญาตให้มีการแจ้งรหัสผ่าน
ที่เป็นข้อมูล ส่วนตัวให้กับบุคคลอื่น และ พนักงานทุกคนมีหน้าที่ในการป้องกันรหัสผ่านของบริษัท โลหะกิจ เม็ท
ทอล จำกัด (มหาชน) อย่างเคร่งครัด
 - หากจะต้องการยกเลิกชื่อ ผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ต้องแจ้งกับผู้บังคับบัญชาโดยตรงเพื่อ ทำ
เรื่องขอยกเลิกใช้งาน และ ต้องกระทำทันทีที่จะเลิกใช้งาน โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศที่ได้รับการ มอบหมาย
ต้องทำการยกเลิกผู้ใช้งาน และ รหัสผ่านทันทีที่ได้รับการแจ้งยกเลิก
 - หากชื่อผู้ใช้งาน และ รหัสผ่านของพนักงานท่านใด ตรวจสอบมีการกระทำความผิดตาม พ.ร.บ.คอมพิวเตอร์ที่
ก่อให้เกิดความเสียหายแก่ บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน) ผู้ที่รับผิดชอบชื่อผู้ใช้งาน และ รหัสผ่านต้อง
ยอมรับความผิดแต่ เพียงผู้เดียว

หมวดที่ 6 : การเข้าถึงและการใช้งาน เครื่องแม่ข่าย (Server)

- ห้ามเข้าไปในบริเวณห้องเครื่องแม่ข่าย (Server) ก่อนได้รับอนุญาต
- ห้ามพนักงานเข้าไปในบริเวณห้องเครื่องแม่ข่าย (Server) โดยไม่มีกิจที่เกี่ยวข้อง ห้ามนำ อาหาร และ เครื่องดื่มเข้าไปในบริเวณห้องเครื่องแม่ข่าย (Server)
- บุคคลภายนอกที่เข้ามาติดต่อให้ติดบัตร Visitor ตลอดเวลาเพื่อให้สามารถสังเกตเห็นได้อย่างชัดเจน หากไม่ใช่พนักงานของบริษัท ให้ทำการลงบันทึกการเข้าออกห้องเครื่องแม่ข่าย (Server) โดยบุคคลภายนอกในสมุดบันทึกการเข้า - ออกห้องเครื่องแม่ข่าย (Server) ทุกครั้ง
- หากพบเห็นความผิดปกติในห้องเครื่องแม่ข่าย (Server) เช่น มีทรัพย์สินหาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทันที
- ห้ามนำอุปกรณ์ที่สามารถบันทึกภาพได้เข้าไปภายในห้องเครื่องแม่ข่าย (Server) เช่น โทรศัพท์เคลื่อนที่, กล้องดิจิทัล, กล้องวิดีโอ
- ให้ปฏิบัติตามคำแนะนำของพนักงานที่ดูแลห้องเครื่องแม่ข่าย (Server Room) อย่างเคร่งครัด

หมวดที่ 7 : ระเบียบปฏิบัติสำหรับการจัดการสารสนเทศ สำหรับสารสนเทศที่อยู่ในรูปแบบเอกสารกระดาษ

- ให้ใช้เครื่องทำลายเอกสารเพื่อทำลายเอกสารที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูง
- ให้ป้องกันเอกสารที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูงที่ถูกพิมพ์ออกมาทางเครื่องพิมพ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ให้จัดหมวดหมู่เอกสารที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูงไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างพอเพียง
- ให้สำเนาเอกสารที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูงได้ก็ต่อเมื่อได้รับอนุญาตจากผู้เป็นเจ้าของแล้ว ให้ระมัดระวังการกระจาย หรือ แจกจ่ายเอกสารที่เป็นความลับขององค์กร ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้รับทราบในเอกสารนั้น
- ให้ทำการตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน
- ให้ผู้เป็นเจ้าของเอกสารกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างพอเพียงสำหรับเอกสารที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูงที่จะถูกส่งไปทางไปรษณีย์

หมวดที่ 8 : สารสนเทศที่เป็นข้อมูลอิเล็กทรอนิกส์

- ให้จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูงไว้ต่างหาก และ ต้องป้องกันให้ความปลอดภัยอย่างพอเพียง
- ให้สำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูงได้ก็ต่อเมื่อได้รับอนุญาตจากผู้เป็นเจ้าของให้ระดับการกระจาย หรือ แจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับขององค์กรไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลอิเล็กทรอนิกส์นั้น
- ให้ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ ทำการตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน ห้ามผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือ ที่มีระดับความสำคัญสูง ทำการส่งข้อมูลดังกล่าวไปทางไปรษณีย์ เว้นเสียแต่จะใช้วิธีการเข้ารหัสข้อมูลที่ต้องกรณกำหนดไว้
- ให้ส่งเครื่องคอมพิวเตอร์ที่จะจำหน่ายออกให้กับฝ่ายเทคโนโลยีสารสนเทศเพื่อการทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์นั้น
- ห้ามมิให้ผู้ใดทำการคัดลอกสำเนา (Copy) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ออกไปนอกบริษัทไม่ว่าจะด้วยวิธีการใดก็ตาม (เช่น การ บันทึกลงในสื่อบันทึกต่างๆ อาทิ เช่น, ฮาร์ดดิสก์, แผ่น CD, แผ่นDVD, Handy Drive / Flash Drive เป็นต้น) ซึ่งการกระทำดังกล่าวผิด พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

มาตรา 18

หมายเหตุ : หากผู้ใดมีความจำเป็นต้องนำข้อมูลเหล่านั้นออกนอกบริษัท ต้องแจ้งให้ผู้บังคับบัญชาทราบ และ อนุญาตก่อน มิฉะนั้นจะถือว่ามีเจตนามิชอบ

หมวดที่ 9 : ระเบียบปฏิบัติสำหรับการเข้าถึงระบบงาน

เมื่อพนักงานใหม่เข้ามาปฏิบัติหน้าที่ ให้ผู้บังคับบัญชาของพนักงานดังกล่าวส่งความประสงค์ขอเข้าใช้ระบบงานของ “บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน)” ในแบบฟอร์มขอสิทธิเข้าใช้ระบบงาน แจ้งขอรหัสเข้าใช้งานระบบงาน ของ”บริษัท โลหะกิจ เม็ททอล จำกัด (มหาชน)” เพื่อนำเสนอต่อผู้บังคับบัญชาตามลำดับ และ แจ้งความประสงค์มายังส่วนเทคโนโลยีสารสนเทศ

- ต้องไม่เข้าถึงระบบงานอื่นที่ตนไม่ได้รับอนุมัติให้ใช้งาน (การอนุมัติให้ใช้งานในระบบงาน จะต้องกระทำโดยผ่าน “แบบฟอร์มขอสิทธิเข้าใช้ระบบงาน” ของบริษัทเท่านั้น)
- ต้องไม่เข้าถึงข้อมูลคอมพิวเตอร์ที่ได้มีการป้องกันเอาไว้ และ ไม่ได้รับอนุญาตการเข้าใช้งาน
- ต้องออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ
- ต้องไม่เปิดเผยข้อมูลที่เกี่ยวข้องกับมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ขององค์กรให้แก่บุคคลภายนอก

- ต้องไม่ใช้ทรัพยากรคอมพิวเตอร์ขององค์กร เพื่อดักจับข้อมูลคอมพิวเตอร์ขององค์กร หรือ ของผู้อื่น ที่อยู่ระหว่างการส่งข้อมูล หรือ ไม่ได้รับสิทธิการเข้าถึงระบบงาน

หมวดที่ 10 ระเบียบปฏิบัติสำหรับการแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย

ให้เจ้าหน้าที่ทำการแจ้งไปยังฝ่ายเทคโนโลยีสารสนเทศ โดยทันทีเมื่อพบเห็นเหตุการณ์ทางด้านความมั่นคงปลอดภัยได้แก่

- โปรแกรมไม่ประสงค์ดี
- ระบบถูกบุกรุกทางเครือข่าย
- ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือ สูญหาย
- มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- การนำ ข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์
- การใช้ทรัพยากรเทคโนโลยีสารสนเทศผิดวัตถุประสงค์ การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือ ฮาร์ดแวร์ที่ใช้งาน
- ระบบถูกโจมตีจนไม่สามารถให้บริการได้
- ทรัพยากรเทคโนโลยีสารสนเทศถูกขโมย
- การอนุญาตให้บุคคลภายนอกเข้าใช้ระบบงานขององค์กร
- การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูล หรือ ดักดูข้อมูลในเครือข่าย หรือ เหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัยขององค์กร ให้ความร่วมมือ และ อำนาจความสะดวกแก่ผู้บังคับบัญชา หรือ ผู้ดูแลระบบเครือข่ายในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น และ/หรือ ระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล และ ระบบเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา หรือ ผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด

หมวดที่ 11 ระเบียบปฏิบัติสำหรับการสำรองข้อมูล

- มีการสำรองข้อมูลที่สำคัญเก็บไว้
- มีการจัดทำสำรองข้อมูล และจัดเก็บไว้อย่างถูกต้องเหมาะสม
- ต้องมีแผนความพร้อมกรณีฉุกเฉินให้สามารถกู้ระบบกลับมาได้ในเวลาที่เหมาะสม

หมวดที่ 12 : บทลงโทษ

- ในกรณีที่พนักงานมีการฝ่าฝืนนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศฉบับนี้ จนเป็นเหตุให้องค์กรได้รับความเสียหาย หรือ อาจจะพิสูจน์ได้ว่า จะได้รับความเสียหายตามความเห็นของผู้บริหารองค์กร พนักงานที่กระทำความผิดดังกล่าวรับทราบ และยินยอมให้องค์กรสามารถทำการ ให้อภัยแก่พนักงานได้ตามความเหมาะสมของเหตุการณ์ที่เกิดขึ้น ไม่ว่าจะเป็นการว่ากล่าวตักเตือน ออกหนังสือแจ้ง คำตักเตือน หรือ ให้อภัยจากการเป็นพนักงานได้ตามกฎระเบียบข้อบังคับขององค์กร
- ในกรณีที่เกิดความเสียหายอย่างร้ายแรง โดยการกระทำที่จงใจ หรือประมาทเลินเล่ออย่างร้ายแรงจนเป็นเหตุให้องค์กรได้รับความเสียหาย พนักงานที่กระทำความผิดดังกล่าวรับทราบ และ ยินยอมให้องค์กรสามารถกระทำการตามข้อข้างต้นได้ รวมถึงยินยอมที่จะชดเชยความเสียหายที่เกิดขึ้นตามจริงให้แก่องค์กร ในการกระทำผิดดังกล่าว ทั้งนี้ให้มีผลตั้งแต่วันที่ประกาศใช้ เป็นต้นไป

จึงประกาศมาเพื่อทราบ และถือปฏิบัติโดยทั่วกัน



(นายประธาน อัครพงศ์พิศักดิ์)

ประธานเจ้าหน้าที่บริหาร