P P PRIME

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ

ประกาศ บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ

ว่าด้วยนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ ได้ทำการกำหนดนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร ให้สอดคล้องกับกฎหมายที่เกี่ยวข้อง เพื่อประสิทธิภาพและเป็นไปตามนโยบายการบริหารจัดการองค์กรในลักษณะแบบรวมศูนย์เพื่อเกิดความเป็นเอกภาพ จึงวางระเบียบการใช้ระบบเทคโนโลยีสารสนเทศและเครือข่ายองค์กร ไว้ดังนี้

วัตถุประสงค์

เพื่อสนับสนุนการดำเนินธุรกิจและการปฏิบัติงานของบุคลากรให้เกิดประสิทธิภาพสูงสุด บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ จัดทำนโยบายความปลอดภัยการใช้งานเทคโนโลยีสารสนเทศไว้เป็นลายลักษณ์อักษร โดยได้กำหนดแนวทางการดำเนินงานขององค์กรและบุคลากร เพื่อเป็นการสนับสนุนให้การดำเนินงานและการบริหารจัดการขององค์กร มีมาตรฐาน ซึ่งจะเป็นส่วนที่จะช่วยผลักดันและส่งเสริมให้พนักงานใช้ทรัพยากรและระบบเครือข่ายขององค์กรได้ตามวัตถุประสงค์และเป้าหมายเพื่อให้มั่นใจว่าได้ว่าบริษัทมีการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และ/หรือข้อกำหนดของหน่วยงานที่กำกับดูแล รวมถึงได้มีการปฏิบัติตามมาตรฐานการบริหารจัดการความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ขอบเขต

ขอบเขตของนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร ครอบคลุมถึงทรัพย์สินหรือทรัพยากรของบริษัททุกประเภท ไม่ว่าทรัพย์สินนั้นจะอยู่ในบริษัทฯ หรือไม่ก็ตาม ซึ่งรวมถึง

ข้อมูล (ฐานข้อมูล เอกสาร ฯลฯ)

ซอฟท์แวร์ (โปรแกรม ฯลฯ)

ทรัพย์สินทางกายภาพ (สถานที่ อุปกรณ์ ฯลฯ)

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์ (ภาคผนวก)

ข้อปฏิบัติผู้ดูแลระบบคอมพิวเตอร์ (ภาคผนวก)

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กรเป็นสิ่งที่บุคลากรทุกคน ทุกระดับ รวมถึงที่ปรึกษาลูกจ้างรายวัน หรือบุคคลใดซึ่งกระทำการเพื่อและ/หรือในนามของบริษัทซึ่งมีหน้าที่เกี่ยวข้องกับการดำเนินการของบริษัทจะต้องรับทราบและถือปฏิบัติอย่างเคร่งครัด

ข้อ 1 ระเบียบนี้เรียกว่า **"ระเบียบ บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ ว่าด้วยนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร พ.ศ. 2561**

ข้อ 2. นิยาม หรือคำจำกัดความ

"บริษัท หรือ กลุ่มบริษัท หรือ องค์กร" หมายถึง บริษัท พีพี ไพร์ม จำกัด (มหาชน)และ/หรือบริษัทที่จัดตั้งขึ้นใหม่ในภายหน้า และบริษัทในเครือ

"พนักงาน หรือ บุคลากร" หมายถึง พนักงานของบริษัท พีพี ไพร์ม จำกัด (มหาชน)และ/หรือบริษัทที่จัดตั้งขึ้นใหม่ในภายหน้า และบริษัทในเครือ

"สารสนเทศองค์กร" หมายถึง ซอฟท์แวร์ ฮาร์ดแวร์ ระบบเครือข่ายคอมพิวเตอร์ และข้อมูลองค์กร

"ผู้บังคับบัญชา" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการจัดการองค์กร

"บัญชีผู้ใช้" หมายถึง พนักงานที่ได้รับอนุญาตให้ใช้งานในระบบสารสนเทศองค์กร

"ข้อมูล" หมายถึง ข้อเท็จจริง หรือสิ่งที่สื่อความหมายในเรื่องนั้น หรือสิ่งใด ๆ ไม่ว่าจะจัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาดภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏและตรวจสอบได้

"ข้อมูลสำคัญ" หรือ "ข้อมูลที่เป็นความลับ (Sensitive Information)" หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือบริษัท มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจหรือสัญญา ซึ่งบริษัท ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่นนอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง

"ทรัพย์สิน หรือทรัพยากร" หมายถึง ทรัพย์สิน หรือทรัพยากรของบริษัทซึ่งรวมถึงสิ่งที่มีตัวตน เช่น อาคาร สถานที่ อุปกรณ์ทางเทคโนโลยีสารสนเทศ เช่น ลิขสิทธิ์ หรือสิทธิบัตร เป็นต้น

"ผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ" หมายถึง พนักงานและ/หรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ดูแลหรือรับผิดชอบในการรักษาระบบเครือข่ายสารสนเทศและสามารถเข้าถึงโปรแกรมหรืออุปกรณ์เครือข่ายเทคโนโลยีสารสนเทศเพื่อการจัดการให้เกิดความปลอดภัยต่อผู้ใช้งานในเครือข่ายสารสนเทศ

ข้อ 3. ระเบียบนี้ให้มีผลบังคับใช้กับพนักงานทุกคนในบริษัทฯ ซึ่งบรรจุเข้าเป็นพนักงานประจำ ตามระเบียบ บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ ว่าด้วยการบรรจุพนักงาน โดยให้ รวมถึงที่ปรึกษา

ลูกจ้างรายวัน หรือบุคคลใดซึ่งกระทำการเพื่อหรือในนามของบริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ ได้กำหนดนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร เพื่อใช้เป็นกรอบหรือแนวทางในการบริหารจัดการ เพื่อให้มั่นใจได้ว่าระบบสารสนเทศขององค์กรมีความพร้อมและสามารถนำข้อมูลในระบบมาใช้งานได้ทันทีเมื่อต้องการ (Availability) และข้อมูลมีความถูกต้องน่าเชื่อถือ(Integrity) โดยสามารถเข้าถึงข้อมูลได้เฉพาะผู้ที่มีสิทธิหรือผู้ที่ได้รับอนุญาตเท่านั้น (Confidentiality) ซึ่งนโยบายดังกล่าวประกอบด้วย

1 ความรับผิดชอบด้านความปลอดภัย (Security Responsibilities)

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ กำหนดให้มีการแบ่งหน้าที่และความรับผิดชอบของบุคลากรอย่างชัดเจนในการพัฒนา การนำไปใช้ รวมทั้งการติดตามผู้เกี่ยวข้องในการดำเนินการที่เกี่ยวกับความปลอดภัยการใช้งานสารสนเทศ ตลอดจนการพัฒนาและการปรับปรุงระบบความปลอดภัยอย่างต่อเนื่อง

2 การแบ่งประเภทของทรัพย์สินและการควบคุม (Asset Classification and Control)

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ กำหนดให้มีการทำทะเบียนทรัพย์สินของบริษัทในทุกประเภททั้งทรัพย์สินที่มีตัวตน และทรัพย์สินที่ไม่มีตัวตน พร้อมทั้งจัดสรรและมอบหมายความเป็นเจ้าของในทรัพย์สินดังกล่าวให้กับหน่วยงานหรือผู้ที่ถือครองทรัพย์สินดังกล่าว โดยเจ้าของทรัพย์สินจะต้องดูแลรับผิดชอบ และปฏิบัติตามนโยบายความปลอดภัยการใช้งานสารสนเทศอย่างเคร่งครัด รวมถึงจัดทำแนวปฏิบัติและการควบคุมอย่างเหมาะสมสำหรับการนำทรัพย์สินไปใช้งาน

3 ความปลอดภัยด้านบุคลากร (Personal Security)

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ มีมาตรการในการควบคุมการใช้งานระบบเครือข่าย เพื่อให้มั่นใจได้ว่าพนักงานที่ปฏิบัติงานจะมีความตระหนักและให้ความสำคัญกับความปลอดภัยสารสนเทศ

4 การจัดการระบบสื่อสารและการดำเนินการ (Communication and Operation Management)

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ กำหนดให้มีการนำเทคโนโลยีสารสนเทศและระบบเครือข่ายมาใช้งานในองค์กร เพื่อเพิ่มประสิทธิภาพในการดำเนินงานและมั่นใจว่าระบบดังกล่าวจะสามารถ

ใช้งานได้ตามหลักการข้างต้น โดยมุ่งหวังว่าจะเป็นมาตรฐานสำหรับการปฏิบัติงาน และการใช้งานเป็นไปตามข้อกำหนดอย่างถูกต้องและเกิดประสิทธิภาพอย่างสูงสุด

5. การควบคุมการเข้าถึงข้อมูล (Access Controls)

กำหนดให้มีการควบคุมการเข้าถึงข้อมูลในทุกระบบงานและระบบเครือข่ายของบริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ อย่างปลอดภัยโดยกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งานในระบบและกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศเท่านั้น

6 การปฏิบัติ (Compliance)

บริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ กำหนดให้ผู้ใช้งานระบบคอมพิวเตอร์และเครือข่ายจะต้องปฏิบัติตามนโยบายอย่างเคร่งครัด เพื่อให้การดำเนินงานเป็นไปตามกฎหมายและหรือข้อบังคับเกี่ยวกับความปลอดภัยสารสนเทศของแต่ละประเทศที่บริษัทเข้าไปทำธุรกรรม ตลอดจนให้มีการปฏิบัติตามนโยบายภายในเรื่องความเสี่ยงขององค์กร รวมถึงข้อกำหนดทางด้านความมั่นคงปลอดภัยและจรรยาบรรณบริษัท พีพี ไพร์ม จำกัด (มหาชน)

ความรับผิดชอบ การใช้งานและการลงโทษ

เพื่อเป็นกรอบและแนวทางในการปฏิบัติเกี่ยวกับการใช้งานระบบสารสนเทศและเครือข่ายองค์กร อันก่อให้เกิดประสิทธิภาพโดยรวม และ/หรือไม่ก่อให้เกิดความเสียหาย หรือผลกระทบแก่องค์กร บริษัท พีพี ไพร์ม จำกัด (มหาชน) จึงกำหนดข้อปฏิบัติในการใช้งานระบบเครือข่าย ดังนี้

หน้าที่และความรับผิดชอบ

พนักงาน ทุกคน ทุกระดับและทุกหน่วยงาน ตลอดรวมถึงที่ปรึกษา ลูกจ้างรายวัน หรือบุคคลใดซึ่งกระทำการเพื่อหรือในนามของบริษัท พีพี ไพร์ม จำกัด (มหาชน)ต้องดำเนินงานภายใต้นโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร หน่วยงานเทคโนโลยีสารสนเทศหรือผู้รับผิดชอบจะต้องจัดให้มีการปฐมนิเทศน์พนักงานใหม่ รวมถึงการอบรมหรือให้ความรู้เกี่ยวกับความปลอดภัยให้กับพนักงานซึ่งปฏิบัติงานอยู่แล้วให้มีความรู้ความเข้าใจและสามารถใช้งานระบบได้ทำให้เกิดความตระหนักและเล็งเห็นถึงผลกระทบหากไม่ปฏิบัติตามนโยบายดังกล่าว

หน่วยงานด้านเทคโนโลยีสารสนเทศ

เป็นหน่วยงานกลางเกี่ยวกับการใช้คอมพิวเตอร์และเครือข่ายขององค์กรเป็นศูนย์ปฏิบัติการเกี่ยวกับกิจกรรมด้านความปลอดภัยของระบบสารสนเทศขององค์กร โดยมีหน้าที่ในการกำกับดูแล รับผิดชอบในการ

รักษาความปลอดภัยสารสนเทศทั้งในระดับกลยุทธ์และระดับปฏิบัติการ รวมถึงการดำเนินการเพื่อดำรงไว้ซึ่งสถานะของบริษัทในการเป็นผู้นำด้านการให้บริการที่มีความปลอดภัยในระบบสารสนเทศและเครือข่าย โดยเป็นผู้ประสานการดำเนินงานระหว่างหน่วยงานและกลุ่มงาน เพื่อให้มั่นใจว่าได้มีการปฏิบัติตามมาตรฐานความปลอดภัยสารสนเทศ

การลงโทษ

เพื่อให้พนักงาน และ/หรือผู้เกี่ยวข้องซึ่งจะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร และ/หรือกฎหมายที่เกี่ยวข้องปฏิบัติหรือดำเนินการตามนโยบายที่กำหนด บริษัทฯ จึงกำหนดมาตรการลงโทษไว้ดังนี้

1.กรณีที่ตรวจสอบและพบว่าพนักงาน และ/หรือผู้เกี่ยวข้องไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศและเครือข่ายองค์กร พนักงาน และ/หรือผู้เกี่ยวข้องนั้น จะต้องถูกลงโทษตามระเบียบบริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ ว่าด้วยการปฏิบัติงาน

2. บริษัทฯ สงวนสิทธิ์ในการตรวจสอบการใช้งานในระบบสารสนเทศของพนักงาน ทั้งการสื่อสารทางอีเมลและการใช้งานบนเครือข่ายอินเตอร์เน็ต เพื่อให้แน่ใจว่าการใช้งานในระบบดังกล่าวเป็นไปตามนโยบายมาตรฐานและกฎหมายที่เกี่ยวข้อง

ฝ่ายบริหารจึงเห็นควรประกาศแจ้งมาเพื่อให้พนักงานใน บริษัท พีพี ไพร์ม จำกัด (มหาชน และบริษัทในเครือ รับทราบเพื่อนำไปใช้ปฏิบัติให้เป็นแนวทางเดียวกันทั่วทั้งองค์กร

ประกาศ ณ วันที่ 01 มีนาคม 2566 เป็นต้นไป

ลงนาม .....

(คุณสุพัตรา นาคมณฑนาคุ้ม)

ประธานเจ้าหน้าที่บริหาร

หมวดที่ 1 ว่าด้วย ระเบียบปฏิบัติทั่วไป

ภาคผนวก

แนวปฏิบัติประกอบระเบียบบริษัท พีพี ไพร์ม จำกัด (มหาชน) และบริษัทในเครือ ว่าด้วยการใช้ระบบสารสนเทศและเครือข่ายองค์กร

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์การป้องกันไวรัสคอมพิวเตอร์ในระบบเครือข่าย

ข้อปฏิบัติเกี่ยวกับการป้องกันไวรัสคอมพิวเตอร์ในระบบเครือข่าย

1. ผู้ใช้งานต้องไม่ปิดการใช้งานโปรแกรม Anti-Virus หรือเปลี่ยนการตั้งค่าการใช้งานที่หน่วยงานสารสนเทศกำหนด หรือตั้งค่าไว้
2. ผู้ใช้งานไม่ควรยุติการสแกนไวรัสอัตโนมัติที่หน่วยงานสารสนเทศกำหนด หรือตั้งค่าไว้ในเครื่อง ซึ่งการสแกนดังกล่าวอาจมีผลกระทบต่อประสิทธิภาพการทำงานบ้าง
3. กรณีเกิดปัญหาการทำงานของระบบเครือข่าย ผู้ใช้งานต้องติดต่อแผนกเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเพื่อตรวจสอบ หรือแก้ไขเท่านั้น
4. ไฟล์ทั้งหมดที่ได้รับจากแหล่งภายนอก ผู้ใช้งานระบบเครือข่ายจะต้องสแกนหาไวรัสและทำลายก่อนที่จะเปิดใช้งาน ซึ่งรวมถึงไฟล์ที่อยู่ใน Removable Media เช่น แผ่น CD / อุปกรณ์ USB / Flash Drive ไฟล์ข้อมูลดาวน์โหลดจากอินเทอร์เน็ต ไฟล์แนบของอีเมล์หรือไฟล์ที่ใช้ร่วมกันผ่านทางเครือข่าย
5. เมื่อมีการตรวจพบไวรัสในระบบ และโปรแกรม Anti-Virus ที่ติดตั้งอยู่ในเครื่อง ไม่สามารถทำลายไวรัสที่ตรวจพบได้ ผู้ใช้งานจะต้องแจ้งไปยังหน่วยงานสารสนเทศ เพื่อดำเนินการตรวจสอบและแก้ไขในทันที

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์การใช้รหัสผ่านและการรักษาความปลอดภัย

การรักษาความปลอดภัยรหัสผ่าน

ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทั้งหมดที่เกิดขึ้นจากบัญชีผู้ใช้งานส่วนตัว โดยต้องเก็บรักษารหัสผ่านไว้เป็นความลับ และไม่ควรให้บุคคลอื่นนำบัญชีผู้ใช้งานของตนไปใช้งาน โดยกำหนดใช้รหัสผ่านที่ง่ายต่อการจำแต่ยากต่อการเดาของบุคคลอื่น โดยการสร้างรหัสผ่านดังนี้

1. ไม่ใช้ชื่อตน ชื่อย่อ คำนำหน้าชื่อของตัวเอง ชื่อครอบครัว ชื่อเพื่อนร่วมงาน คำฮิตที่นิยมในขณะนั้น ชื่อระบบงาน หรือ ชื่อของบริษัทเพียงอย่างเดียว
2. ไม่ใช้ข้อมูลส่วนตัวบุคคล เช่น วันเกิด, ที่อยู่, หมายเลขโทรศัพท์
3. ไม่ใช้คำที่พบบ่อยในพจนานุกรมภาษาอังกฤษ
3. ไม่ใช่คำที่มีรูปแบบซ้ำหรือเรียงอย่างมีรูปแบบ
4. รหัสผ่านที่แข็งแกร่งนั้นควรประกอบด้วยอักขระ 8 ตัวขึ้นไป ประกอบด้วยการผสมผสานของตัวเลข (1, 2, 3), ตัวอักษรพิเศษ (! @, #, $) ตัวพิมพ์ใหญ่ (A, B, C,) และตัวพิมพ์เล็ก (a, b, c,)

5. ถ้าผู้ใช้งาน ใส่ Password ผิดติดต่อกันเกิน 3 ครั้ง ระบบจะทำการล็อคบัญชีชื่อผู้ใช้งานนั้นทันที การปลดล็อค ให้ติดต่อผู้ดูแลระบบเครือข่ายสารสนเทศ (IT) เพื่อทำการปลดล็อค

<u>การป้องกันรหัสผ่าน</u>

1. ผู้ใช้งานไม่ควรเปิดเผยรหัสผ่านของตนแก่ผู้ใด รวมทั้งเพื่อร่วมงาน หรือพนักงานของหน่วยงานเทคโนโลยีสารสนเทศ
2. ผู้ใช้งานจะต้องไม่ร้องขอให้ผู้อื่น รวมถึงเพื่อนร่วมงานให้รหัสผ่านแก่ตนเอง
3. รหัสผ่านทั้งหมดจะได้รับการปฏิบัติในฐานะที่เป็นข้อมูลลับ และไม่พึงเปิดเผยต่อผู้อื่น
4. กรณีที่รหัสผ่านจำเป็นต้องถูกใช้ร่วมกันภายใต้สถานการณ์ที่หลีกเลี่ยงไม่ได้ ควรเปลี่ยนรหัสผ่านใหม่โดยเจ้าของรหัสผ่านทุกครั้ง สำหรับในการเข้าสู่ระบบในครั้งต่อไป
5. ผู้ใช้งานควรจะตรวจสอบให้แน่ใจว่าไม่มีใครมองดูอยู่ในขณะที่กำลังใส่รหัสผ่านเพื่อเข้าสู่ระบบ ในทางกลับกันผู้ใช้งานก็ไม่ควรมองดูหรือพยามจดจำคนอื่นใส่รหัสผ่านด้วยเช่นกัน
6. ผู้ใช้งานไม่ควรเก็บสำเนารหัสผ่าน โดยการเขียนใส่กระดาษ หรือเก็บไว้ในรูปแบบอิเล็กทรอนิกส์ไว้ในสถานที่เข้าถึงได้ง่าย และหากจำเป็นต้องทำสำเนารหัสผ่านไว้ควรตรวจสอบให้แน่ใจก่อนว่าสถานที่ที่จัดเก็บเป็นที่ที่ปลอดภัยและมิดชิดเพียงพอ
7. ผู้ใช้งานควรเปลี่ยนรหัสผ่านของตนอย่างสม่ำเสมอ โดยบางระบบงานสามารถกำหนดให้มีการเปลี่ยนแปลงรหัสผ่านทุก 90 วัน

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์การใช้งานอินเทอร์เน็ตบนระบบเครือข่าย

<u>การใช้งานอินเทอร์เน็ต</u>

1. อินเทอร์เน็ตมีไว้เพื่อการเพิ่มประสิทธิภาพในการปฏิบัติงาน และอยู่ในความรับผิดชอบผู้ใช้งานจึงควรเข้าถึงอินเทอร์เน็ตเพื่อใช้เป็นแหล่งข้อมูลประกอบการทำงานเท่านั้น โดยจะต้องคำนึงถึงผลกระทบต่อประสิทธิภาพของงานในความรับผิดชอบต่อส่วนรวมด้วย
2. พนักงานต้องเข้าถึงอินเทอร์เน็ตผ่านช่องทางการเชื่อมต่อที่บริษัทจัดไว้ให้เท่านั้น ไม่ควรตั้งค่าการใช้งานการเข้าถึงอินเทอร์เน็ตเอง โดยที่ไม่ได้รับอนุญาต การเชื่อมต่ออินเทอร์เน็ตเป็นการเปิดช่องให้ผู้ใช้งานที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลบริษัทฯ จึงต้องมีการควบคุมและติดตามตรวจสอบการใช้งานอย่างใกล้ชิด
3. การใช้งานอินเทอร์เน็ตทั้งหมดจะต้องมีการตรวจสอบสิทธิ์ *<u>บริษัทสงวนสิทธิ์ที่จะทำการกลั่นกรองและห้ามเข้าถึงบางเว็บไซต์ที่ไม่เหมาะสม</u>*
4. ผู้ใช้งานไม่ควรใช้บริการอินเทอร์เน็ตเพื่อดาวน์โหลดซอฟท์แวร์ใด ๆ จากภายนอก หรือจากเครื่องมืออื่นใดซึ่งอาจเป็นช่องทางในการเผยแพร่ไวรัสได้

   4.1 ห้ามดาวน์โหลด หรือแจกจ่ายซอฟท์แวร์ที่เป็นการละเมิดลิขสิทธิ์

   4.2 ห้ามเปิดเผยข้อมูลลับของบริษัทไปยังเว็บไซต์อินเทอร์เน็ตใด ๆ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา และ/หรือเจ้าของข้อมูลก่อน

   4.3 ห้ามใช้ระบบเครือข่ายในการกล่าวหาว่าร้าย หรือหมิ่นประมาทบนระบบเครือข่าย ซึ่งอาจส่งผลกระทบหรือความเสียหายกับบริษัทได้

   4.4 ห้ามกระทำสิ่งที่ผิดกฎหมาย หรือผิดจรรยาบรรณในเว็บไซต์อินเทอร์เน็ตใด ๆ รวมถึงการพนัน การเข้าถึงข้อมูล ลามก อนาจาร หรือการให้ร้ายต่อบริษัท หรือบุคคลภายนอก

   4.5 กรณีที่มีการกระทำความผิดจากการเข้าถึงอินเทอร์เน็ตดังกล่าว และมีการตรวจพบ บริษัทสามารถยุติบัญชีของผู้ใช้งานอินเทอร์เน็ตของผู้นั้นได้ทันที และจะดำเนินมาตรการทางวินัยตามระเบียบบริษัทอย่างเคร่งครัด
5. ผู้ใช้งานจะต้องรับผิดชอบต่อการใช้งานใด ๆ ซึ่งผิดวัตถุประสงค์ของการเข้าถึงอินเทอร์เน็ตที่มาจากบัญชีของตน

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์การใช้งานจดหมายอิเล็กทรอนิกส์ หรืออีเมลบนระบบเครือข่าย

<u>การใช้งานจดหมายอิเล็กทรอนิกส์ หรืออีเมลบนระบบเครือข่าย</u>

1. บริษัทให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อประกอบการปฏิบัติงาน ผู้ใช้งานจึงไม่ควรใช้อีเมลเพื่อวัตถุประสงค์ส่วนตัว
2. ผู้ใช้งานที่เป็นเจ้าของบัญชีอีเมลจะต้องรับผิดชอบต่อข้อมูล หรือเนื้อหาของอีเมลจากการตอบ หรือส่งต่อจากบัญชีของตนไปให้ผู้อื่น
3. ผู้ใช้งานไม่ได้รับอนุญาตในการส่งประเภทของอีเมลต่อไปนี้
    - อีเมลที่มีข้อความหมิ่นประมาท ทำให้เสียชื่อเสียง เป็นที่น่ารังเกียจ หรือลามก อนาจาร
    - อีเมลที่มี Virus หรือ Worm
    - อีเมลห่วงโซ่ ลวง ระดมแคมเปญสนับสนุนทางการเมือง
    - อีเมลที่ไม่พึงประสงค์ไปยังผู้ใช้งานจำนวนมาก ซึ่งถือได้ว่าเป็นสแปมอีเมล
    - อีเมลที่มีเอกสารใด ๆ ซอฟท์แวร์หรือข้อมูลที่ได้รับการคุ้มครองตามกฎหมายลิขสิทธิ์ หรือการคุ้มครองความเป็นส่วนตัว
    - ส่งอีเมลที่ไม่พึงประสงค์รวมทั้งการส่ง "อีเมลขยะ" หรือโฆษณาอื่น ๆ ให้กับผู้อื่นโดยที่เขาไม่ได้เจาะจงขอมา (อีเมลขยะ)

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์ การป้องกันบัญชีผู้ใช้งานบนระบบเครือข่าย

<u>การป้องกันบัญชีผู้ใช้งานบนระบบเครือข่าย</u>

1. ผู้ใช้งานจะต้องปกป้องบัญชีอีเมลของตนด้วยการใส่รหัสผ่านที่ยากแก่การเข้าถึงของผู้อื่นและไม่ควรให้ผู้อื่นร่วมใช้รหัสผ่าน หรือบัญชีอีเมลของตน
2. ผู้ใช้งานจะต้องใช้ความระมัดระวังในการให้ชื่อบัญชีอีเมล หรือข้อมูลอื่นใดกับบุคคลในเว็บบอร์ด Internet ต่าง ๆ เช่น รายการกระดานสนทนา หรือรายนามผู้ใช้งาน e-mail โดยต้องปฏิบัติตามแนวทางดังนี้
    - 2.1 ไม่สมัครเป็นสมาชิกเพื่อรับจดหมายโดยใช้ชื่อบัญชีอีเมลบริษัท *<u>(ที่ไม่เกี่ยวข้องกับงาน)</u>* เนื่องจากปริมาณของอีเมลดังกล่าว อาจจะใช้พื้นที่มากจนทำให้กล่องจดหมายเต็มได้
    - 2.2 ไม่ใช้บัญชีอีเมลบริษัท สำหรับโพสต์ข้อความใด ๆ ไปยังกลุ่มอินเทอร์เน็ต ข่าวสารหรือกระดานสนทนา เพราะอาจเป็นเป้าหมายของผู้ส่งอีเมลขยะ
    - 2.3 ไม่เปิดเผยรายชื่อบัญชีอีเมลของผู้ใช้งานอื่น ๆ ของบริษัท ซึ่งเป็นข้อมูลลับหรือข้อมูลลับเฉพาะไปยังเว็บไซต์ กลุ่มข่าวสารหรือกระดานสนาทนาใด ๆ โดยที่ไม่ได้รับการอนุญาตจากบริษัทก่อน

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์ข้อปฏิบัติในการใช้งานระบบคอมพิวเตอร์และเครือข่าย

ข้อปฏิบัติในการใช้งานระบบคอมพิวเตอร์และเครือข่าย

1. ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิ์ในทรัพย์สินทางปัญญา ของบุคคลอื่น หรือติดตั้งโปรแกรมคอมพิวเตอร์อื่นใดโดยมิได้รับความเห็นชอบจากผู้ดูแลระบบคอมพิวเตอร์
2. ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาต หรือความเห็นชอบจากบริษัทก่อน
3. ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองใช้งาน หรือรับผิดชอบอยู่เมื่อเสร็จสิ้นงานประจำวัน เว้นแต่เครื่องนั้นต้องใช้งานตลอด 24 ชั่วโมง
4. ระมัดระวังการใช้งานอินเตอร์เน็ต โดยไม่หลงเชื่อโฆษณา หรือเนื้อหาในเว็บไซต์ที่ไม่เหมาะสม และทำการศึกษาเนื้อหาเงื่อนไขให้ละเอียดก่อนทำการ Download ข้อมูลเสมอ
5. ลบข้อมูลที่ไม่จำเป็นออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเองเพื่อเป็นการประหยัดหน่วยความจำสื่อบันทึกข้อมูล
6. ให้ความร่วมมือกับผู้บังคับบัญชา และผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของตน รวมทั้งปฏิบัติตามคำแนะนำอย่างเคร่งครัด
7. ผู้ใช้งานคอมพิวเตอร์ (Computer PC และ Notebook) มีหน้าที่ และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ด้วยความระมัดระวังในการใช้งาน และสงวนรักษาเหมือนเช่นวิญญูชนทั่วไปจะพึงกระทำต่อเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบคอมพิวเตอร์ โดยมีข้อปฏิบัติ ดังนี้
    a. ไม่ควรนำอาหาร หรือเครื่องดื่ม อยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
    b. ไม่ควรวางสื่อแม่เหล็ก เช่น ลำโพง ไว้ใกล้เครื่องคอมพิวเตอร์ , External Hard Disk
    c. ปิดเครื่อง (Shutdown) ทุกครั้งหลักจากเสร็จสิ้นการใช้งาน
8. ไม่เข้าไปในที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาต
9. คืนทรัพย์สินที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์ซึ่งเป็นของบริษัท เมื่อพ้นสภาพการเป็นพนักงาน

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์ข้อห้ามในการใช้งานคอมพิวเตอร์และระบบเครือข่าย

ข้อห้ามในการใช้งานคอมพิวเตอร์และระบบเครือข่าย

1. ห้ามพนักงานใช้คอมพิวเตอร์และระบบอินเตอร์เน็ตของบริษัทเพื่อกระทำการใด ๆ ที่เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และ/หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด
2. ห้ามพนักงานเข้าถึงระบบคอมพิวเตอร์ที่มีระบบป้องกันการเข้าถึง หมายถึงระบบที่มีการติดตั้ง Password โดยมิได้รับอนุญาต
3. ห้ามพนักงานเปิดเผยมาตรการป้องการเข้าถึงระบบคอมพิวเตอร์อันจะให้เกิดความเสียหายต่อข้อมูลหรือระบบคอมพิวเตอร์ของบริษัทให้บุคคลอื่นทราบ
4. ห้ามพนักงานกระทำการใด ๆ โดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับ หรือรับข้อมูลคอมพิวเตอร์ของบุคคลอื่นในการส่งของมูลในระบบ โดยข้อมูลนั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลอื่นทั่วไปใช้ประโยชน์
5. ห้ามพนักงานใช้ระบบคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้
   - 5.1 เพื่อการกระทำความผิดตามกฎหมาย หรือก่อให้เกิดความเสียหายแก่บุคคลอื่น
   - 5.2 เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือ ศีลธรรมอันดีงาม
   - 5.3 เพื่อเปิดเผย รหัสผ่านส่วนบุคคล หรือระบบความมั่งคงของบุคคลอื่น
   - 5.4 เพื่อดัดแปลง แก้ไข ทำลาย ข้อมูลบุคคลอื่น โดยไม่ได้รับ ความยินยอม
   - 5.5 เพื่อเผยแพร่โปรแกรมที่ใช้กระทำความผิด
   - 5.6 เพื่อเปิดเผยข้อมูลที่เป็นความลับที่ได้มาจากการปฏิบัติงานให้แก่บริษัท ไม่ว่าจะเป็นข้อมูลบริษัทหรือของบุคคลภายนอกก็ตาม
   - 5.7 เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของบริษัท หรือของบุคคลอื่น
   - 5.8 เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่น โดยมิได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้มีสิทธิในข้อมูลนั้น
   - 5.9 เพื่อการรับหรือส่งข้อมูลซึ่งอาจก่อให้เกิดความเสียหายให้แก่บริษัท เช่น การรับส่งข้อมูลที่มีลักษณะจดหมายลูกโซ่ หรือการรับส่งข้อมูลจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิบุคคลอื่นไปยังพนักงานหรือบุคคล อื่น ๆ เป็นต้น
   - 5.10 เพื่อการดักจับอีเมล ส่วนตัวของบุคคลอื่นขณะทำการส่ง และไม่กระทำการสร้างตัดต่อ

ดัดแปลงข้อมูล ส่งต่อภาพลามก เนื้อหาที่ทำลายความมั่งคงของประเทศ หรือก่อความเสียหาย ชื่อเสียงต่อบุคคลอื่น

5.11 เพื่อขัดขวางการใช้งานระบบคอมพิวเตอร์ของบริษัท หรือบุคคลอื่นในบริษัท หรือเพื่อให้ระบบคอมพิวเตอร์ของบริษัท ไม่สามารถทำงานได้ตามปกติ

5.12 เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวของกับการดำเนินงานของบริษัท ไปยังเว็บไซต์ใด ๆ ในลักษณะที่อาจก่อความเข้าใจคลาดเคลื่อนไปจากความจริง

5.13 เพื่อการ Download เพลง ภาพยนต์ เกมส์ หรือ เล่นเกมส์ออนไลน์ ผ่านทางระบบคอมพิวเตอร์

5.14 เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของบริษัท หรือก่อให้เกิดความขัดแย้ง หรือความเสียหายแก่บริษัท

ข้อปฏิบัติผู้ใช้งานระบบคอมพิวเตอร์ ข้อปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและเครือข่าย

<u>ข้อปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและเครือข่าย</u>

1. ผู้ดูแลระบบฯ จะต้องดูแลรักษาระบบเครือข่ายให้สามารถใช้งานได้ดีตลอดเวลา หากพบว่าผู้ใช้งานผู้รายใดมีปฏิบัติที่ส่อไปในทางที่จะมีการละเมิดแนวทางปฏิบัติที่เกี่ยวกับความปลอดภัยกับการใช้งานของระบบเครือข่าย ผู้ดูแลระบบเครือข่ายจะต้องรายงานให้ผู้บังคับบัญชาของผู้ใช้งานนั้นให้ทราบโดยเร็วที่สุด และกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่บริษัท ผู้ดูแลระบบมีอำนาจที่จะระงับการใช้งานระบบคอมพิวเตอร์ของพนักงานดังกล่าวได้ทันที
2. ผู้ดูแลระบบฯ มีหน้าที่เสนอความคิดเห็น และข้อสังเกตต่อผู้บังคับ และ/หรือคณะกรรมการกำกับดูแลเทคโนโลยีสารสนเทศเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพการบริหารระบบเทคโนโลยีสารสนเทศ
3. ผู้ดูแลระบบฯ มีหน้าที่ในการเชื่อมต่ออุปกรณ์ ซอฟต์แวร์ ระบบอื่น ๆ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ตลอดจนบำรุงรักษาให้ระบมีความพร้อมในการใช้งานอยู่เสมอ
4. ผู้ดูแลระบบฯ จะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านระบบเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และต้องไม่เปิดเผยข้อมูลที่ตนได้รับหรือจากการดูแลระบบจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้ผู้ใดทราบ
5. ผู้ดูแลระบบฯ จะต้องคืนทรัพย์สินบริษัทที่ใช้ในการปฏิบัติหน้าที่ของตนให้แก่บริษัททันทีที่พ้นหน้าที่หรือพ้นสภาพการเป็นพนักงาน และให้ผู้บังคับบัญชาทำตรวจสอบรายการทรัพย์สินของผู้ดูแลระบบที่พ้นหน้าที่ดังกล่าวโดยละเอียด