นโยบายและแนวทางในการควบคุมการปฏิบัติงาน
และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1) เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่อง
2) เพื่อบริหารความเสี่ยง และกำหนดแนวทางป้องกันปัญหาที่เกิดขึ้นจากการใช้งานอุปกรณ์เครื่องมือเทคโนโลยีสารสนเทศอย่างไม่ถูกต้อง และป้องกันภัยคุกคามต่าง ๆ
3) เพื่อให้สอดคล้องกับหลักการกำกับดูแลกิจการที่ดี และข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง คู่มือจรรยาบรรณทางธุรกิจและนโยบายระบบบริหารจัดการแบบบูรณาการของบริษัทฯ

บริษัทฯ มีทรัพย์สินสารสนเทศเพื่อสนับสนุนประสิทธิภาพการดำเนินงานให้สามารถตอบสนองเป้าหมายทางธุรกิจ ดังนั้นจึงถือว่าทรัพย์สินสารสนเทศเป็นทรัพย์สินที่สำคัญ ผู้ปฏิบัติงานจะต้องใช้และดูแลรักษาให้อยู่ในสภาพที่พร้อมใช้งานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา

ด้วยเหตุนี้ บริษัทฯ จึงได้ประกาศนโยบายเพื่อกำหนดให้มีมาตรฐาน แนวปฏิบัติ และขั้นตอนการปฏิบัติงาน ให้ครอบคลุมการบริหารจัดการทรัพย์สินสารสนเทศ และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการใช้งานที่เหมาะสมตามคู่มือจรรยาบรรณทางธุรกิจและสอดคล้องกับนโยบายระบบบริหารจัดการแบบบูรณาการของบริษัทฯ

เมื่อประกาศนโยบายฉบับนี้มีผลบังคับใช้ โดยความเห็นชอบของคณะกรรมการ และผู้บริหารแล้ว คณะกรรมการ และผู้บริหารต้องให้การสนับสนุนนโยบาย งบประมาณ ทรัพยากรและอื่น ๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศมีการพัฒนาและปรับปรุงอย่างต่อเนื่อง ต้องจัดให้มีการเผยแพร่นโยบายให้กับเจ้าหน้าที่ ผู้ให้บริการภายนอก และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติ ต้องดำเนินการทบทวน และตรวจสอบนโยบายอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญซึ่งมีผลต่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัทฯ

ข้อกำหนด พรบ. กฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ รวมทั้งกฎระเบียบและนโยบายของบริษัทฯ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น หากผู้ใช้งานกระทำผิดตามข้อกำหนด พรบ. กฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

กรณีที่ผู้ใช้งานหรือผู้ให้บริการภายนอกละเมิด หรือกระทำความผิด บริษัทฯ ขอสงวนสิทธิ์ดำเนินการตามขั้นตอนในแนวทางเดียวกันกับคู่มือจรรยาบรรณทางธุรกิจ ตามความเหมาะสม

ความหมายและคำจำกัดความ

องค์กร / บริษัทฯ	หมายความว่า	บริษัท ไทยฟิล์มอินดัสตรี่ จำกัด (มหาชน)
ความเสี่ยง	หมายความว่า	โอกาสที่ทรัพย์สินสารสนเทศจะถูกละเมิดการรักษาความปลอดภัย และ/หรือ ก่อให้เกิดความเสียหายด้านข้อมูล ด้านทรัพย์สิน รวมถึงความน่าเชื่อถือขององค์กร
ทรัพย์สินสารสนเทศ	หมายความว่า	
ก) ทรัพย์สินสารสนเทศประเภทระบบ	ได้แก่	ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
ข) ทรัพย์สินสารสนเทศประเภทอุปกรณ์	ได้แก่	ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่น ๆ
ค) ทรัพย์สินสารสนเทศประเภทข้อมูล	ได้แก่	ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
ระบบเครือข่ายคอมพิวเตอร์	หมายความว่า	ระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ
ระบบงานคอมพิวเตอร์	หมายความว่า	การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงาน เพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบจัดเก็บเอกสาร ระบบบัญชี
ระบบสารสนเทศ	หมายความว่า	ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร
เครื่องคอมพิวเตอร์แม่ข่าย	หมายความว่า	เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน หรือจัดเก็บข้อมูล หรือโปรแกรมสำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่น ๆ หรือใช้ในการควบคุมการทำงานของระบบเครือข่าย
เครื่องคอมพิวเตอร์	หมายความว่า	อุปกรณ์ที่ใช้ในการบันทึกและประมวลผลข้อมูล เช่น คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal computer) และคอมพิวเตอร์แบบพกพา (Notebook Computer)
อุปกรณ์คอมพิวเตอร์	หมายความว่า	อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์
การใช้งานอุปกรณ์เคลื่อนที่	หมายความว่า	การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (Mobile Device) เพื่อเข้าถึงระบบสารสนเทศที่มีความสำคัญโดยผ่านการเชื่อมต่อกับระบบเครือข่ายภายในองค์กร
เหตุการณ์ผิดปกติ (Incident)	หมายความว่า	เหตุการณ์ใด ๆ ที่มีผลกระทบต่อการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ระบบป้องกันการบุกรุก (Firewall)	หมายความว่า	ระบบรักษาความปลอดภัยที่ประกอบด้วย อุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้หรือเข้าถึงระบบ และจำกัดการใช้งานของผู้ใช้งานภายในให้เป็นไปตามนโยบายที่บริษัทฯ กำหนด

ผู้ปฏิบัติงาน / ผู้ใช้งาน / User	หมายความว่า	ผู้บริหาร พนักงาน ลูกจ้างทดลองงาน และลูกจ้างชั่วคราว
ผู้ให้บริการ / หน่วยงานภายนอก	หมายความว่า	องค์กรซึ่งบริษัทฯ อนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูลหรือใช้งานทรัพย์สินสารสนเทศของบริษัทฯ โดยจะได้รับสิทธิตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของบริษัทฯ โดยไม่ได้รับอนุญาต
ผู้ดูแลระบบ	หมายความว่า	เจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ หรือพนักงานอื่นที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับผู้จัดการฝ่ายขึ้นไป ให้มีหน้าที่รับผิดชอบในการดูแลรักษาคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ และ/หรือได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไขและดูแลระบบข้อมูลและโปรแกรมต่าง ๆ ที่ใช้งานอยู่ในบริษัทฯ หรือหน่วยงานที่มีหน้าที่และรับผิดชอบในการดูแลคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์หรือระบบข้อมูลโดยตรง ตลอดจนสามารถระงับการใช้งานระบบงานของผู้ใช้งาน เมื่อมีการตรวจสอบพบว่าใช้งานไม่ถูกต้องหรือละเมิดข้อตกลงการใช้งาน

หมวดที่ 1
การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศสำหรับองค์กร

1.1 บริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ โดยสร้างความร่วมมือจากทุกฝ่าย ให้มีความรู้ความเข้าใจในทรัพย์สินสารสนเทศ เพื่อทำให้ประสิทธิภาพของการดำเนินงานภายใต้ทรัพย์สินสารสนเทศมีค่าสูงสุด

1.2 จัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจ และการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้ตามที่กำหนดไว้ เช่น

1.2.1 ฝ่ายบริหาร มีการวางแผน หรือมีนโยบายในการจัดสรรบุคคลากร

1.2.2 ฝ่ายบุคคล

1.2.2.1 ประกาศ และรับพนักงานตามนโยบาย

1.2.2.2 แจ้งผู้ดูแลระบบ เพื่อจัดเตรียมทรัพย์สินสารสนเทศให้เหมาะสมและเพียงพอตามนโยบาย

1.2.3 ผู้ดูแลระบบ

1.2.3.1 จัดสรร โอนย้าย หรือจัดซื้อทรัพย์สินสารสนเทศตามตำแหน่งความรับผิดชอบ

1.2.3.2 ทำทะเบียนควบคุมทรัพย์สินสารสนเทศ และจัดทำสำเนาเอกสารที่เกี่ยวข้องแยกเก็บเพื่อสะดวกต่อการตรวจสอบ เช่น ใบกำกับภาษี สำหรับเครื่องคอมพิวเตอร์ อุปกรณ์ ลิขสิทธิ์ (License) กรณีที่เป็นการโอนย้ายจากสำนักงานใหญ่ไปยังสาขาต้องทำการสำเนาเอกสารดังกล่าวแยกเก็บด้วย

1.2.4 ฝ่ายจัดซื้อ จัดซื้อทรัพย์สินสารสนเทศ (กรณีไม่มีทรัพย์สินสารสนเทศสำรอง)

1.2.5 ฝ่ายบัญชี/การเงิน ทำการขึ้นทะเบียนทรัพย์สินสารสนเทศ

1.2.6 อื่น ๆ

หมวดที่ 2
การกำหนดนโยบาย มาตรการ โครงสร้างการบริหารจัดการ
เพื่อรักษาความมั่งคงปลอดภัยของระบบสารสนเทศ
การบริหารจัดการทรัพย์สินสารสนเทศ และการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

2.1 การจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.1.1 การติดตั้งระบบป้องกันการบุกรุก (Firewall)

2.1.2 การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ มัลแวร์ รวมถึงการปรับปรุง Security Patch อยู่เสมอ

2.1.3 การกำหนดสิทธิ์การเข้าถึง หรือการเข้าใช้ข้อมูลสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของแต่ละผู้ใช้ หรือแต่ละกลุ่มของผู้ใช้งาน

2.1.4 การกำหนดสิทธิ์การใช้อุปกรณ์ต่อพ่วงผ่าน USB Port กรณีที่ต้องการใช้ ต้องทำเอกสารขออนุมัติผ่านหัวหน้างาน ผู้มีอำนาจ หรือผู้บริหาร พร้อมส่งเอกสารมายังผู้ดูแลระบบเพื่อดำเนินการ

2.1.5 การกำหนดสิทธิ์การใช้งานสื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (อาทิ Thumb–Drive, CD, DVD) ที่มีข้อมูลลับของบริษัทฯ บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง กรณีที่เป็นอุปกรณ์ส่วนตัวต้องมีการขึ้นทะเบียน รวมถึงต้องทำเอกสารขออนุมัติผ่านหัวหน้างาน ผู้มีอำนาจ หรือผู้บริหาร พร้อมส่งเอกสารมายังผู้ดูแลระบบเพื่อดำเนินการก่อนการใช้งานเสมอ

2.1.6 ข้อมูลที่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ดูแลระบบต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาเกิดขึ้น

2.1.7 การสำรองข้อมูลควรจัดเก็บอย่างน้อย 2 สถานที่ เช่น สำนักงานใหญ่ และสาขา เป็นต้น

2.1.8 ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ของบริษัทฯ อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์คอมพิวเตอร์ของบริษัทฯ ที่ได้รับมอบหมาย

2.1.9 เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งหมดของบริษัทฯ ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้ง ควร Log Off คอมพิวเตอร์ทุกครั้งเมื่อไม่ได้ใช้งาน

2.1.10 ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัทฯ ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมาต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัทฯ

2.1.11 ผู้ใช้งานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ไม่ Download/ Upload ข้อมูลหรือสิ่งอื่นใดที่ไม่เกี่ยวข้องกับงาน กรณีที่เข้าใช้งานอินเทอร์เน็ตห้ามมิให้ผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่ไม่มีความเกี่ยวข้องกับงาน เนื่องจากอาจมีโปรแกรมในการโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน หรือใช้ Website ที่ไม่เกี่ยวข้องกับงานหรือกิจการของบริษัทฯ การใช้งานต้องไม่เป็นสาเหตุให้บริษัทฯ และบุคคลอื่นเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำผิดกฎหมาย หรือ พรบ. คอมพิวเตอร์ ทั้งนี้บริษัทฯ สงวนสิทธิ์ในการตรวจสอบ และบันทึกประวัติการใช้คอมพิวเตอร์ของผู้ใช้งานเพื่อตรวจสอบการเข้าใช้งานในลักษณะที่ไม่เหมาะสม

2.1.12 จัดอบรมให้ความรู้แก่ผู้ใช้งาน เกี่ยวกับความความสำคัญ แนวปฏิบัติ ขั้นตอนการปฏิบัติงาน และความเสี่ยงเพื่อป้องกัน และสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับกฎหมาย ข้อกำหนด นโยบาย และการเปลี่ยนแปลงที่เกี่ยวข้องด้านทรัพย์สินสารสนเทศของบริษัทฯ ด้วย

2.1.13 ทำการปรับปรุงเอกสารทะเบียนควบคุมทรัพย์สินสารสนเทศ อย่างสม่ำเสมอ

2.1.14 ทบทวน และปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง ควรปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

2.2 การใช้งานอีเมล์ (E-mail)

2.2.1 บัญชีอีเมล์ต้องได้รับการปกป้องด้วยรหัสผ่าน

2.2.2 บัญชีอีเมล์ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์หรือระบบเครือข่ายของบริษัทฯ ถือเป็นสินทรัพย์ของบริษัทฯ

2.2.3 พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมล์ ได้ตามปกติอีกต่อไป หากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้ ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่บริษัทฯ กำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ ตามที่กฎหมายกำหนดไว้เท่านั้น

2.2.4 ห้ามใช้บัญชีอีเมล์ของบริษัทฯ เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย พรบ. ข้อกำหนด หรือนโยบายต่าง ๆ ที่บริษัทฯ ได้ประกาศไว้

2.2.5 ซอฟต์แวร์สำหรับใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน ชื่อบริษัท และเบอร์โทรศัพท์ติดต่ออีเมล์บริษัทฯ ทุกฉบับต้องมีข้อความแสดงเจตจำนง/ ข้อยกเว้นความรับผิดชอบของบริษัทฯ แนบท้าย กรณีที่เป็นอีเมล์ติดต่อลูกค้าให้กำกับข้อมูลการชำระเงิน เช่น เลขบัญชี ชื่อบัญชี ประเภทบัญชีสำหรับรับชำระเงิน ว่าไม่มีการเปลี่ยนแปลงใด ๆ เพื่อป้องกันการปลอมแปลงโจรกรรมข้อมูล การหลอกลวงทางอินเทอร์เน็ต (Phishing Mail) เพื่อให้ได้ข้อมูล หรือหลอกลวงให้ลูกค้าชำระเงินด้วยช่องทางอื่น

2.2.6 ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าอีเมล์ที่ส่งออกนั้นกระทำในนามตัวแทนของบริษัทฯ ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหาหรือรูปภาพที่ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศหรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนา รวมถึงอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบัน พระมหากษัตริย์โดยเด็ดขาด หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัทฯ

2.2.7 ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)

2.2.8 เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์มีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

2.3 การรักษาความปลอดภัยทางกายภาพ

2.3.1 ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย

2.3.2 อนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ดูแลระบบ ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือ ไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ หรือแนบเอกสาร Plant Visit Gate Pass โดยผู้ดูแลระบบจะต้องจดบันทึกบุคคลการขอเข้า-ออก หรือเก็บเอกสาร Plant Visit Gate Pass เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่อนุญาตให้

เข้าพื้นที่) และต้องมีการบันทึก ข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Server Room/Data Center) ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี (หรือตามความเหมาะสม)

2.3.3 ไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server Room/Data Center) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ / ไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล / ไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ / ไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

2.4 การใช้งานระบบเครือข่ายจากเครื่องคอมพิวเตอร์ที่ไม่ใช่ทรัพย์สินสารสนเทศของบริษัทฯ จะต้องได้รับอนุญาตจากผู้ดูแลระบบก่อน และหากพบว่ามีการใช้งานโดยไม่ได้รับอนุญาต ผู้ดูแลระบบสามารถตัดการใช้งานออกจากระบบเครือข่ายได้ทันที กรณีที่ผู้ใช้งานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนทรัพย์สินสารสนเทศของบริษัทฯ ผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

2.5 ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอกโดยต้องประกอบไปด้วยรายละเอียดดังนี้

2.5.1 การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

2.5.2 ขอบเขต รายละเอียด และระดับการให้บริการ (Service Level Agreement)

2.5.3 เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้านกายภาพและด้าน Logical

2.5.4 ข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก

2.5.5 สัญญาในการไม่เปิดเผยข้อมูลของบริษัทฯ

2.5.6 การยืมหรือการร้องขอใช้อุปกรณ์ของบริษัทฯ รวมถึงการต่อพ่วงอุปกรณ์ภายนอกอื่น ๆ

2.5.7 ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

2.5.8 ให้ผู้ดูแลระบบทบทวนและตรวจสอบบริการจาก ผู้ให้บริการฯ ภายนอกตามข้อตกลงที่กำหนด

2.5.9 ให้ผู้ดูแลระบบเป็นผู้รับผิดชอบในการบริหารจัดการการเปลี่ยนแปลงในการให้บริการฯ จากผู้ให้บริการภายนอก รวมถึงการประเมินผู้บริการ เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ทั้ง 3 ด้านคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

หมวดที่ 3
การรักษาความมั่งคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ และการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

3.1 มาตรการการรักษาความปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

3.1.1 หน่วยงานเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

3.1.2 หน่วยงานเทคโนโลยีสารสนเทศต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

3.1.3 ระบบเครือข่ายทั้งหมดของบริษัทฯ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Package Filtering เช่น การใช้ Firewall หรือ อุปกรณ์อื่น ๆ ที่ต้องมีความสามารถในการตรวจจับไวรัส ผู้ให้บริการภายนอกต้องมีระบบการกรองข้อมูลเว็บไซต์ที่ไม่ได้รับอนุญาตตามพรบ. คอมพิวเตอร์ กรณีที่ผู้ใช้งานต้องการเข้าถึงเว็บไซต์ที่ไม่ได้รับอนุญาตหากมีความจำเป็นต้องใช้งาน ต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

3.1.4 บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุม ข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทฯ

3.1.5 ห้ามผู้ใช้งานติดตั้งโมเด็มหรืออุปกรณ์อื่น ๆ หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย เช่น Router, Switch, Hub และ Wireless Access Point เข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัทฯ โดยไม่ได้รับอนุญาตจากหน่วยงานเทคโนโลยีสารสนเทศ

3.1.6 ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทฯ โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขอ อนุมัติอย่างเหมาะสมก่อนทุกครั้ง

3.1.7 ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัทฯ ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัทฯ โดยเด็ดขาด

3.1.8 จัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยถือปฏิบัติตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

3.1.9 ควบคุม ดูแลบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ กรณีพบความผิดปรกติเกิดขึ้นในระบบ ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจระงับการใช้เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเพื่อป้องกันความเสียหายได้

3.2 มาตรการการรักษาความปลอดภัยด้านการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

3.2.1 หน่วยงานเทคโนโลยีสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน อาทิ เขียน อ่าน ลบ ได้ กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

3.2.2 มีการกำหนดระยะเวลาในการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและอย่างเหมาะสมกับการทำงานเท่านั้น

3.2.3 บุคคลภายนอกต้องปฏิบัติตามนโยบายของบริษัทฯ อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ

3.2.4 สิทธิ์การเข้าถึงไฟล์ข้อมูลสารสนเทศต้องได้รับการควบคุม และได้รับการพิจารณาอนุมัติเท่าที่จำเป็นเท่านั้น เพื่อให้ไฟล์ข้อมูลสารสนเทศได้รับการรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ รวมทั้งเป็นการแบ่งแยกสิทธิ์และหน้าที่ของผู้ใช้งาน

3.2.5 ควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงในระบบข้อมูลหรือในเครื่องคอมพิวเตอร์ของพนักงานโดยไม่ให้กระทบต่อระบบหลักหรือก่อให้เกิดความเสียหายต่อระบบรวม

3.3 มีการตรวจสอบระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ อย่างน้อยปีละ 1 ครั้งดังนี้

3.3.1 วางแผนการตรวจสอบระบบฯ ให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

3.3.2 กำหนดขอบเขตในการตรวจสอบระบบฯ ทางเทคนิคให้ครอบคลุมถึงจุดเสี่ยงที่สำคัญ โดยการตรวจสอบดังกล่าวต้องไม่กระทบต่อการปฏิบัติงาน

3.3.3 ตรวจสอบระบบฯ นอกเวลาทำงาน ในกรณีที่การตรวจสอบนั้นอาจส่งผลกระทบต่อความพร้อมในการใช้งานระบบดังกล่าว

3.3.4 ทบทวน และปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง รวมถึงปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

หมวดที่ 4
หลักเกณฑ์อื่น ๆ

4.1 พนักงาน / ผู้ใช้งาน

4.1.1 ปฏิบัติตามคู่มือพนักงาน คู่มือจรรยาบรรณทางธุรกิจอย่างเคร่งครัด

4.1.2 พนักงานทุกคนมีสิทธิใช้ทรัพย์สินสารสนเทศภายใต้ข้อกำหนดดังกล่าว การฝ่าฝืนจนเป็นเหตุหรืออาจเป็นเหตุให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใด บริษัทฯ จะพิจารณาดำเนินการทางวินัยและกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสม

4.1.3 พนักงานพึงใช้ข้อความสุภาพ หรือใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น รวมทั้งปฏิบัติให้ถูกต้องตามธรรมเนียมปฏิบัติของการใช้เครือข่าย

4.1.4 พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่พึงอนุญาตให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

4.1.5 เพื่อป้องกันหากมีผู้อื่นล่วงรู้และนำรหัสผ่านของพนักงานไปใช้ในทางที่ผิดและเกิดความเสียหายต่อบริษัทฯ พนักงานจะต้องเก็บรหัสผ่านไว้เป็นความลับ และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่

4.1.6 เพื่อความปลอดภัยในการใช้ระบบเครือข่ายคอมพิวเตอร์ กรณีพนักงานพบไวรัสคอมพิวเตอร์จะต้องแจ้งให้ผู้ดูแลระบบดำเนินการกำจัดไวรัสโดยเร็ว

4.1.7 พนักงานพึงลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

4.1.8 พนักงานพึงให้ความร่วมมือและอำนวยความสะดวกแก่ ผู้ดูแลระบบในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำที่เกี่ยวข้องกับความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ

อนุมัติโดยคณะกรรมการบริษัท
การประชุมคณะกรรมการบริษัท ครั้งที่ 3/2560
วันที่ 10 สิงหาคม 2560

(คุณอำนาจ กิตติกรัยฤทธิ์)
กรรมการผู้จัดการ
ประกาศ ณ วันที่ 10 สิงหาคม 2560