บริษัท ฟู้ดโมเม้นท์ จำกัด (มหาชน)

นโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ได้รับการอนุมัติโดยที่ประชุมคณะกรรมการบริษัท
ครั้งที่ 3/2566 เมื่อวันที่ 30 มีนาคม 2566
และมีผลบังคับใช้ตั้งแต่วันที่ 30 มีนาคม 2566 เป็นต้นไป

นโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ บริษัท ฟู้ดโมเม้นท์ จำกัด (มหาชน)

ปัจจุบันระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจและเข้ามาช่วยอำนวยความสะดวกในการดำเนินงานของบริษัท ฟู้ดโมเม้นท์ จำกัด (มหาชน) ("**บริษัท**") และบริษัทย่อย ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานผ่านการเชื่อมต่อข้อมูลผ่านระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์เป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่างๆ เป็นต้น แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูงและอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติงานได้เช่นกัน เพราะมีการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อและเชื่อมโยงข้อมูลระหว่างหน่วยงานต่างๆ ภายในบริษัท จึงทำให้ข้อมูลสารสนเทศของบริษัทมีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย (Malware) หรือการบุกรุกโจมตีทางไซเบอร์ (Cyber Threats) ผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับของบริษัท ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้บริษัทอาจสูญเสียชื่อเสียงหรือภาพพจน์ อีกทั้ง หากระบบเทคโนโลยีสารสนเทศมีเหตุขัดข้องหรือสถานการณ์ฉุกเฉินเกิดขึ้นก็จะส่งผลกระทบต่อการดำเนินงานของบริษัทอีกด้วย ดังนั้น ผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศของบริษัทจึงมีความจำเป็นต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

1. หลักการและเหตุผล

บริษัทมีความมุ่งมั่นที่จะทำให้ระบบเทคโนโลยีสารสนเทศของบริษัทนั้นมีความมั่นคงปลอดภัย คงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ และให้ระบบเทคโนโลยีสารสนเทศนั้นดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและป้องกันการถูกคุกคามจากภัยต่างๆ เช่น การโจมตีการทำลายระบบสารสนเทศ และการจารกรรมข้อมูลทางไซเบอร์ บริษัทจึงได้จัดทำนโยบายฉบับนี้ เพื่อให้บริษัทมีกรอบการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศระดับบริษัทที่ดี โดยกำหนดมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ และเพื่อให้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศสากล รวมถึงกฎหมาย และข้อกำหนดอื่นๆ ที่เกี่ยวข้อง

2. วัตถุประสงค์และขอบเขตการบังคับใช้

2.1 การจัดทำนโยบายนี้เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท ทำให้การดำเนินงานของบริษัทเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล บรรลุวัตถุประสงค์และเป้าหมายหลักของกิจการ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสมสอดคล้องกับหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance)

2.2 นโยบายฉบับนี้มีผลบังคับใช้กับบริษัทและบริษัทย่อย รวมถึงกรรมการ ผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงข้อมูลสารสนเทศของบริษัทในแต่ละระดับชั้นความลับ

2.3 นโยบายฉบับนี้มีไว้เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้กรรมการ ผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของบริษัทในการดำเนินงาน ยึดถือ และปฏิบัติตามอย่างเคร่งครัด

2.4 บริษัทควรจัดให้มีการดำเนินการตรวจสอบและประเมินผลสัมฤทธิ์ของการใช้นโยบายฉบับนี้ตามระยะเวลาอย่างน้อย 1 ครั้งต่อปี

3. คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

คำศัพท์		คำนิยาม
บริษัท	หมายถึง	บริษัท ฟู้ดโมเม้นท์ จำกัด (มหาชน)
ผู้บังคับบัญชา	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัท
ผู้บริหารเทคโนโลยีสารสนเทศ	หมายถึง	ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของบริษัท ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ
ศูนย์สารสนเทศ	หมายถึง	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในของบริษัท
การรักษาความมั่นคงปลอดภัย	หมายถึง	การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของบริษัท
มาตรฐาน (Standard)	หมายถึง	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
ขั้นตอนการปฏิบัติ (Procedure)	หมายถึง	รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
แนวทางปฏิบัติ (Guideline)	หมายถึง	แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
ผู้ใช้งาน	หมายถึง	บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัท โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งบริษัทได้กำหนดไว้

คำศัพท์		คำนิยาม
กรรมการ	หมายถึง	ผู้ที่ได้รับการแต่งตั้งให้ทำหน้าที่กำหนดทิศทาง กลยุทธ์ และการดำเนินงานของบริษัท
ผู้บริหาร	หมายถึง	ผู้มีอำนาจบริหารในระดับสูงของบริษัทที่ได้รับการแต่งตั้งให้ทำงานในตำแหน่งที่มีหน้าที่ในการสั่งการ มอบหมายงาน กำกับ หรือควบคุมการปฏิบัติงานของพนักงานอื่น
ผู้ดูแลระบบ (System Administrator)	หมายถึง	พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีจดหมายอิเล็กทรอนิกส์ (Email Account) เป็นต้น
พนักงาน	หมายถึง	บุคคลที่ตกลงทำงานให้แก่บริษัท เพื่อรับค่าตอบแทนภายหลัง ซึ่งในที่นี้ หมายความรวมถึง พนักงานที่ได้ผ่านพ้นกำหนดระยะทดลองงาน พนักงานทดลองงาน ลูกจ้างชั่วคราว พนักงานที่มีสัญญาจ้างพิเศษ พนักงานรายเดือน และพนักงานรายวันของบริษัท
บุคคลภายนอก	หมายถึง	องค์กรหรือหน่วยงานภายนอกที่บริษัทอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินสารสนเทศต่างๆ ของบริษัท โดยผู้ใช้งานจะได้รับสิทธิในการเข้าใช้งานระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
ข้อมูลคอมพิวเตอร์	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
สารสนเทศ (Information)	หมายถึง	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ
ระบบคอมพิวเตอร์	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ระบบเครือข่าย (Network System)	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัทได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet) เป็นต้น

คำศัพท์		คำนิยาม
ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet)	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ของหน่วยงานภายในบริษัทเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
ระบบอินเทอร์เน็ต (Internet)	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
ระบบเทคโนโลยีสารสนเทศ (Information Technology System)	หมายถึง	ระบบงานของบริษัทที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่บริษัทสามารถนำมาใช้ประโยชน์ในการวางแผนการบริหาร การสนับสนุนการบริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)	หมายถึง	พื้นที่ที่บริษัทอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็นพื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)
เจ้าของข้อมูล	หมายถึง	ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
สิทธิของผู้ใช้งาน	หมายถึง	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	หมายถึง	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก
ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง	การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

คำศัพท์		คำนิยาม
เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)	หมายถึง	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการ หรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายการรักษาความมั่นคงปลอดภัยฉบับนี้ หรือมาตรการป้องกันนั้นล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัยเกิดขึ้น
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)	หมายถึง	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
จดหมายอิเล็กทรอนิกส์ (Email)	หมายถึง	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
รหัสผ่าน (Password)	หมายถึง	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
ชุดคำสั่งไม่พึงประสงค์	หมายถึง	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
ข้อมูลจราจรทางคอมพิวเตอร์	หมายถึง	ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ได้แก่ ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อและเครื่องที่เข้ามาใช้บริการและเครื่องที่ให้บริการ เป็นต้น

4. นโยบายการกำกับดูแล การบริหารจัดการ และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัทกำหนดนโยบายการกำกับดูแล การบริหารจัดการ และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ดังนี้

4.1 คณะกรรมการบริษัทมีหน้าที่กำหนดนโยบายการกำกับดูแล การบริหารจัดการ และรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และกำกับดูแลให้กรรมการและผู้บริหารปฏิบัติตามนโยบายให้สอดคล้องกับความต้องการของบริษัท รวมทั้ง สนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความเสี่ยง เพื่อให้สามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัท

4.2 ผู้บริหารมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศ ส่งเสริม และสนับสนุนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้ตอบสนองต่อพันธกิจและนโยบายของบริษัท

4.3 ผู้บริหารมีหน้าที่พัฒนาและรักษากรอบการดำเนินงานหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทให้สอดคล้องกับมาตรฐานสากล กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

4.4 ผู้บริหารมีหน้าที่กำหนดให้มีการจัดระดับความสำคัญของข้อมูลและทรัพย์สินสารสนเทศ เพื่อทำให้แน่ใจว่าข้อมูลและทรัพย์สินสารสนเทศดังกล่าวได้รับการปกป้องจากภัยคุกคามต่างๆ ตามระดับความสำคัญ และดำเนินการจัดเก็บข้อมูลและทรัพย์สินสารสนเทศของบริษัทให้ปลอดภัย

4.5 ผู้บริหารมีหน้าที่กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ จัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งในระดับองค์กร และระดับปฏิบัติการ และกำหนดมาตรการในการจัดการความเสี่ยงประเภทต่างๆ

4.6 ผู้บริหารมีหน้าที่กำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนนโยบายฉบับนี้ ซึ่งอาจรวมถึงการดำเนินการทางวินัย การเลิกจ้าง หรือยกเลิกสัญญา (แล้วแต่กรณี)

4.7 ผู้บริหารมีหน้าที่กำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความปลอดภัย ถูกต้อง สมบูรณ์ และพร้อมใช้งานอยู่เสมอ

4.8 บริษัทจะเผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้กรรมการ ผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทและผู้ที่เกี่ยวข้อง ตลอดจนส่งเสริมให้บุคคลดังกล่าวมีการศึกษาอย่างต่อเนื่อง เพื่อให้ตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดการดำเนินงานและเพื่อให้มีการปฏิบัติตามอย่างเคร่งครัด

4.9 กรรมการและผู้บริหารมีหน้าที่ติดตาม ตรวจสอบการดำเนินงานตามนโยบายฉบับนี้อย่างสม่ำเสมอและปรับปรุงนโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

5. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงและครอบคลุมในเรื่องดังต่อไปนี้

5.1 การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5.2 ผู้บริหารเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

5.3 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)

5.4 ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ควรมีการควบคุมการเข้า-ออกและการใช้งาน

5.5 ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัท เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีโปรแกรมประสงค์ร้าย (Malware) การคุกคามทางไซเบอร์ (Cyber Threats) หรือไวรัสคอมพิวเตอร์ หรือมีช่องโหว่เชื่อมต่อเครือข่ายภายนอก เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น

5.6 ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัท ควรมีการตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ใช้งาน เช่น ระบบป้องกันการเข้าออกในการใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่งจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นต้น

5.7 ความเสี่ยงด้านบุคคล ควรมีการกำหนดสิทธิ์การใช้งานเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ และข้อมูล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูล

5.8 การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

5.8.1 ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี

5.8.2 ความเสี่ยงจากผู้ปฏิบัติงาน ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลเกินกว่าหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้

5.8.3 ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น

5.8.4 ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่ทำการใช้งานอยู่อาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

ทั้งนี้ เพื่อให้การประเมินความเสี่ยงสอดคล้องกับสภาวการณ์ของบริษัท บริษัทอาจดำเนินการด้วยวิธีการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ (Penetration Test) ร่วมด้วยก็ได้

5.9 การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้

5.10 จัดทำตารางลักษณะรายละเอียดความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

5.11 กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

6. องค์ประกอบของนโยบาย

6.1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
6.2 การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
6.3 การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
6.4 การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
6.5 การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์
6.6 การรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์
6.7 การรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต
6.8 ความมั่นคงปลอดภัยของการสำรองข้อมูล
6.9 นโยบายการควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศ
6.10 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
6.11 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
6.12 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อที่จะทำให้บริษัทมีมาตรการในการรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และพนักงานของบริษัท ทำให้บริษัทสามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฉบับนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท ซึ่งกรรมการ ผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้บริษัทจะต้องปฏิบัติตามอย่างเคร่งครัด

6.1 นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ และข้อมูลสารสนเทศ ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและบุคคลภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

2. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

2.1 ให้ศูนย์สารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้งาน พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

2.2 ให้ศูนย์สารสนเทศเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.3 ให้ศูนย์สารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.4 บุคคลภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในบริษัทจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีพนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนามอนุญาตเป็นคราวๆ ไป

2.5 ให้ผู้ใช้งานที่ถือครองเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่เครื่องนั้นเกิดความเสียหายหรือสูญหาย

2.6 ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของบริษัทจะต้องดำเนินการด้วยตนเอง โดยห้ามมิให้ผู้อื่นดำเนินการแทน

2.7 ให้ผู้ที่เป็นเจ้าของข้อมูลที่ต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของบริษัท จะต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น

2.8 ให้ผู้ใช้งานปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง และในกรณีที่ผู้ใช้งานไม่ได้อยู่ที่หน้าจอคอมพิวเตอร์ หรือไม่ได้ใช้งานนานกว่า 10 นาทีให้ทำการตั้งค่าการล็อคหน้าจอด้วย

2.9 ให้ผู้ใช้งานลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตน เพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

2.10 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมที่นอกเหนือจากที่บริษัทได้ติดตั้งไว้ให้ใช้งาน

2.11 ห้ามทำการเปลี่ยนแปลง หรือแก้ไขซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องที่บริษัทจัดซื้อมา

2.12 ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

2.13 ให้ทำการติดตั้งเครื่องสำรองไฟสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีการใช้งานข้อมูลเป็นปริมาณมากและมีความถี่ในการใช้งานสูง

2.14 ห้ามทำการปรับแต่งค่าระบบที่ได้รับจากการติดตั้งแต่เริ่มแรกอย่างเด็ดขาด เพราะอาจทำให้เกิดความเสียหายต่อระบบการทำงานของเครื่องคอมพิวเตอร์

2.15 ห้ามทำการถอดเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงที่ได้รับการติดตั้งไว้ โดยไม่ได้แจ้งให้กับผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศทราบล่วงหน้า

2.16 ผู้ใช้งานคอมพิวเตอร์ต้องรับทราบรวมถึงทำความเข้าใจและปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

6.2 นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก การคุกคามทางไซเบอร์ (Cyber Threats) หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศและระบบเครือข่ายของบริษัทให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของบริษัทได้อย่างถูกต้อง

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทมีดังนี้

2.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.1.1 บริษัทกำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารเทคโนโลยีสารสนเทศ

2.1.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของพนักงานในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

2.1.3 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

2.1.4 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

2.2 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.2.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนพนักงานใหม่ของบริษัท และกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งกำหนดขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก การเปลี่ยนตำแหน่งงานภายในบริษัท เป็นต้น

2.2.2 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

2.2.3 ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของพนักงานดังต่อไปนี้

1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
2) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย และควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน
3) กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อเข้าใช้งานในครั้งแรก
4) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
5) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
6) ให้ผู้ใช้งานตั้งรหัสผ่านมีความยาวไม่น้อยกว่า 8 ตัวอักษร มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
7) ในกรณีมีความจำเป็น ต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานคนดังกล่าวต่างจากรหัสผู้ใช้งานตามปกติ

2.2.4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ เพื่อควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ และกำหนดวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
2) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ยืนยันตัวตนของผู้ใช้ข้อมูล ก่อนการเข้าถึงข้อมูลในแต่ละชั้นความลับ
3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

5) ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ทั้งนี้ บริษัทไม่สนับสนุนให้ใช้รหัสผ่านเดิมซ้ำกับรหัสผ่านครั้งล่าสุด เพื่อป้องกันการคาดเดาเกี่ยวกับรหัสผ่านของบุคคลที่ไม่มีสิทธิในการเข้าถึงข้อมูล

6) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น หากส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2.3 การควบคุมการเข้าถึงระบบปฏิบัติการ

2.3.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของบริษัท

2.3.2 ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของบริษัทร่วมกัน

2.3.3 ผู้ใช้งานตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นให้ผู้ใช้งานต้องใส่รหัสผ่านอีกครั้งเพื่อเข้าใช้งานเมื่อต้องการใช้งาน

2.3.4 ผู้ใช้งานออกจากระบบ (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

2.3.5 ต้องไม่จด หรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

2.3.6 กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

2.3.7 ให้กลุ่มผู้ใช้งานที่มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านเดียวกัน จะต้องร่วมกันรับผิดชอบหากมีความเสียหายหรือมีปัญหาเกิดขึ้นกับระบบที่เข้าถึง

2.3.8 ห้ามกำหนดรหัสลับในส่วนของเครื่องคอมพิวเตอร์ทั้งในระดับไบออส และระดับแบบปฏิบัติการด้วยตนเอง นอกเหนือจากผู้บังคับบัญชาของฝ่ายเทคโนโลยีสารสนเทศและผู้ที่ได้รับมอบหมาย

2.3.9 เมื่อผู้ใช้งานทำการใส่รหัสผ่านเพื่อเข้าถึงระบบงานใดๆ ผิดพลาดเกินที่กำหนดในบัญชีผู้ใช้งานของระบบปฏิบัติการนั้นๆ จะถูกล็อคและไม่สามารถเข้าถึงระบบงานได้จนกว่าผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศจะทำการปลดล็อคให้ ทั้งนี้ เนื่องจากบริษัทมีการใช้งานระบบที่หลากหลาย ดังนั้น จำนวนครั้งในการใส่รหัสผ่านผิดพลาดจนเกิดการล็อคบัญชีและการไม่สามารถใช้งานระบบนั้นๆ ได้ จะถูกตั้งค่าตามหลักปฏิบัติทั่วไปของแต่ละระบบปฏิบัติการแต่ละระบบ

2.4 การควบคุมการเข้าถึงสำหรับการลาออกของพนักงาน

2.4.1 พนักงานที่ประสงค์จะลาออก ต้องยื่นหนังสือตามระเบียบข้อบังคับเกี่ยวกับการทำงานของบริษัท (ถ้ามี) สำหรับผู้ที่ใช้คอมพิวเตอร์และอุปกรณ์ต่อพ่วงในการปฏิบัติงานนั้น ให้กรอกข้อมูลในแบบฟอร์มตรวจสอบการส่งคืนทรัพย์สินและอุปกรณ์ความปลอดภัยส่วนบุคคล

2.4.2 พนักงานหรือพนักงานทดลองงานต้องยื่นหนังสือลาออกล่วงหน้าไม่น้อยกว่าหนึ่งรอบการจ่ายค่าจ้าง

2.4.3 ฝ่ายบริหารทรัพยากรบุคคลทำการแจ้งมายังฝ่ายสารสนเทศ โดยมีรายละเอียดดังนี้

1) เมื่อได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคลถึงการลาออกของพนักงาน เจ้าหน้าที่ฝ่ายสารสนเทศต้องทำการตรวจสอบคอมพิวเตอร์ หรืออุปกรณ์ที่มีการใช้งานโดยพนักงานที่ลาออกนั้น ว่ายังอยู่ในสภาพที่พร้อมใช้งานอยู่หรือไม่

2) หากอุปกรณ์เสียหาย สูญหาย พนักงานต้องเป็นผู้รับผิดชอบค่าซ่อมแซม หรือในกรณีที่ไม่สามารถซ่อมแซมได้ ต้องเป็นผู้รับผิดชอบจัดหามาคืนให้ครบถ้วนตามรายการและจำนวนที่ครอบครอง

3) เจ้าหน้าที่ฝ่ายสารสนเทศจะถอดถอนสิทธิของผู้ที่ลาออกออกจากระบบต่างๆ ตามวันที่ระบุของวันที่ลาออกหรือมีผลเป็นการลาออกตามที่ได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคล

2.5 การควบคุมการเข้าถึงสำหรับการโยกย้ายตำแหน่งของพนักงาน

2.5.1 เมื่อมีพนักงานโยกย้ายตำแหน่ง/ฝ่าย และมีการใช้คอมพิวเตอร์และอุปกรณ์ต่อพ่วงในการปฏิบัติงานนั้น ให้ฝ่ายบริหารทรัพยากรบุคคลแจ้งเจ้าหน้าที่ฝ่ายสารสนเทศทราบรวมถึงรายละเอียดเกี่ยวกับวันที่โยกย้ายตำแหน่ง/ฝ่ายด้วย

2.5.2 เมื่อได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคลถึงการโยกย้ายตำแหน่ง/ฝ่ายของพนักงาน เจ้าหน้าที่ฝ่ายสารสนเทศต้องจัดทำสิทธิของพนักงานที่โยกย้ายตำแหน่ง/ฝ่ายตามหน้าที่ความรับผิดชอบใหม่ให้สามารถเริ่มใช้งานได้ ตามวันที่ระบุของวันที่โยกย้ายตำแหน่ง/ฝ่ายที่ได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคล และถอดถอนสิทธิเดิมของผู้โยกย้ายตำแหน่ง/ฝ่ายออกจากระบบต่างๆ เดิมทั้งหมด ตามวันที่ระบุของวันที่โยกย้ายตำแหน่ง/ฝ่าย ตามที่ได้รับแจ้งจากฝ่ายบริหารทรัพยากรบุคคล

6.3 นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

1. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย ทำความเข้าใจ ตลอดจนปฏิบัติตามเพื่อเป็นการรักษาทรัพยากรและข้อมูลของบริษัทให้เป็นความลับ มีความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

2. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

บริษัทกำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

2.1 ผู้ดูแลระบบต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศและตามกลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2 หากผู้ใช้งานจะนำเครื่องคอมพิวเตอร์และอุปกรณ์ส่วนตัวมาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของบริษัท ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

2.3 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่บริษัท จะต้องขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศและจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่นๆ

2.4 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้ง เพิ่มเติม หรือกระทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

2.5 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

2.5.1 ต้องกำหนดวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น และต้องกำหนดวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

2.5.2 ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

2.5.3 ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกบริษัท ควรให้มีการเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือคุกคาม รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) หรือการคุกคามทางไซเบอร์ (Cyber Treats) ด้วย

2.5.4 การเข้าสู่ระบบเครือข่ายภายในบริษัท โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

2.5.5 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของบริษัท จำเป็นต้องมีการป้องกันมิให้บุคคลภายนอกที่เชื่อมต่อระบบสามารถมองเห็นได้

2.5.6 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.5.7 การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.5.8 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

2.6 บริษัทกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังต่อไปนี้

2.6.1 ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล ทั้งนี้ ผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของบริษัท (IT Auditor) หรือบุคคลที่บริษัทมอบหมาย

2.6.2 ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

2.6.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

2.6.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

2.7 บริษัทกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

2.7.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของบริษัทจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศ

2.7.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

2.7.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศ

2.7.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับบริษัทอย่างเพียงพอ

2.7.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของบริษัท

6.4 นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของบริษัทมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

2.1 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

2.2 ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในบริษัท ไม่ว่าจะเป็น Access Point, Wireless Router, Wireless USB client หรือ Wireless card

2.3 ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

2.4 กรณีที่ผู้บังคับบัญชาอนุญาตให้มีการติดตั้ง Wireless ให้ผู้ดูแลระบบดำเนินการ ดังนี้

2.4.1 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจะต้องวางในระบบเครือข่ายภายในที่เป็น Internal Network และต้องเพิ่มการรับรองและการเข้ารหัส (Authentication, Encryption) ด้วย

2.4.2 ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้ให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

2.4.3 ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

2.4.4 ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

2.4.5 ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

2.4.6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคลากรหรือบุคคลภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของบริษัท

2.4.7 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือนให้ผู้บริหารเทคโนโลยีสารสนเทศ และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการศูนย์สารสนเทศทราบทันที

6.5 นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

1. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายฉบับนี้เท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในบริษัท

2. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยของไฟร์วอลล์ของบริษัทมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

2.1 ศูนย์สารสนเทศมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของบริษัท

2.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

2.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

2.4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ในครั้งแรกของการใช้งานด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User password) ที่ได้รับจากศูนย์สารสนเทศ

2.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

2.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

2.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

2.8 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมของบริษัทอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศก่อน

2.9 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารเทคโนโลยีสารสนเทศ โดยต้องระบุข้อมูลดังนี้

2.9.1 หมายเลข Port ที่ต้องการขอให้เปิด

2.9.2 หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

2.9.3 วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

2.9.4 วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

2.10 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

2.11 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

2.12 บริษัทมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบายฉบับนี้ ประกาศ กฎระเบียบของบริษัท หรือกฎหมายอื่นใดของหน่วยงานที่เกี่ยวข้อง หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

2.13 ภายหลังการอนุญาตให้ใช้งาน หากพบว่ามีการใช้งานที่ขัดต่อนโยบายฉบับนี้ ประกาศ กฎระเบียบของบริษัท หรือกฎหมายอื่นใดของหน่วยงานที่เกี่ยวข้อง หรืออาจจะทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของบริษัท ทางศูนย์สารสนเทศจะยกเลิกการให้บริการทันที

2.14 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศก่อน

6.6 นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัท ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด เพื่อทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของบริษัทมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท โดยยื่นคำขอกับพนักงานที่ศูนย์สารสนเทศ

2.2 เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่านโดยทันที

2.3 ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

2.4 สนับสนุนให้ผู้ใช้งานทุกคนเปลี่ยนรหัสผ่านเป็นประจำ เช่น ทุก 3-6 เดือน

2.5 ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ต้องร่วมรับผิดชอบต่อการอนุญาตให้ผู้อื่นใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

2.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการหรือตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

2.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

2.8 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของบริษัทหรือก่อให้เกิดความเสียหายต่อบริษัท

2.9 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเพื่อเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือสิ่งอื่นใดซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของบริษัท ทั้งนี้ การส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.10 การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน 25 เมกะไบท์

2.11 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Logout) ทุกครั้ง

6.7 นโยบายการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของบริษัทซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด เพื่อทำให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

ผู้ใช้งานเครือข่ายอินเทอร์เน็ตของบริษัทมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตเป็นครั้งแรกต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของบริษัท โดยยื่นคำขอกับพนักงานที่ศูนย์สารสนเทศ โดยผู้ใช้งานต้องเป็นพนักงานของบริษัท สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศหรือผู้ที่ได้รับมอบหมายเป็นคราวๆ ไป

2.2 ไม่ใช้ระบบอินเทอร์เน็ตของบริษัทเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับบริษัท

2.3 ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

2.4 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

2.5 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

2.6 ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

2.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของบริษัท ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัท การทำลายความสัมพันธ์กับพนักงานของหน่วยงานอื่นๆ ภายในบริษัท

2.8 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจากเครือข่ายอินเทอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

6.8 นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ เพื่อให้สามารถกู้ข้อมูลสารสนเทศกลับคืนได้ภายในระยะเวลาที่เหมาะสม

2. แนวทางปฏิบัติในการสำรองข้อมูล

2.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศของบริษัทจากจำเป็นมากไปหาน้อย

2.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

2.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

2.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

2.5 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลหรือฐานข้อมูลองค์กรทุกวัน ให้สามารถย้อนหลังการสำรองข้อมูลได้ ทั้งนี้ ระยะเวลาการจัดเก็บขึ้นอยู่กับประเภทและชนิดของระบบนั้นๆ ว่ามีเพียงใด โดยบริษัทจะเลือกใช้กรอบระยะเวลามาตรฐานที่ระบบดังกล่าวกำหนด

2.6 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศต้องทำสำเนาฐานข้อมูลไว้ทุกๆ 1 เดือน

2.7 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศควรทำการทดสอบกู้ข้อมูลอย่างน้อยปีละ 1 ครั้ง ในการทดสอบต้องบันทึกเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของหรือผู้ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบ

6.9 นโยบายการควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศ (Data Accessibility Policy)

1. วัตถุประสงค์

เพื่อให้สามารถจัดการและกำหนดสิทธิของผู้ใช้งานในการเข้าถึงข้อมูลนั้นๆ ได้อย่างเหมาะสมตามความจำเป็นที่ต้องใช้งานเท่านั้น

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศ

2.1 การควบคุมการเข้าถึงข้อมูลและใช้งานระบบสารสนเทศ

2.1.1 จำแนกกลุ่มของข้อมูลในระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

2.1.2 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้สารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

1) กำหนดสิทธิของผู้ใช้งานในการเข้าถึงข้อมูล
   - อ่านอย่างเดียว
   - สร้างข้อมูล
   - แก้ไขข้อมูล
   - อนุมัติ
   - ไม่มีสิทธิ

2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

2.1.3 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

1) จัดแบ่งประเภทข้อมูลออกเป็นข้อมูลสารสนเทศในแผนกต่างๆ เช่น ข้อมูลแผนกเทคโนโลยีสารสนเทศ ข้อมูลแผนกบัญชี ข้อมูลแผนกทรัพยากรบุคคล เป็นต้น

2) จัดแบ่งระดับชั้นความลับของข้อมูลออกเป็น 3 ระดับคือ
   - ลับมาก (Confidential)
   - สามารถใช้งานได้ภายในบริษัท (Internal Use Only)
   - ทั่วไปเปิดเผยได้ (Public)

2.2 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

2.2.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

2.2.2 เจ้าของข้อมูลควรทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

2.2.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลแต่ละชั้นความลับข้อมูล

6.10 นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับพนักงานและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

2. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.1 จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

2.2 จัดสัมมนาเพื่อเผยแพร่แนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับพนักงาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

2.3 ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

2.4 ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

6.11 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

1. วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

2. แนวทางปฏิบัติในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

1.1 ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท

1.2 ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน

1.3 หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ

1.4 กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

1.5 ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน

1.6 ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

6.12 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

1. วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของบริษัท อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัท

2. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

2.1 ส่วนเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนรองรับเหตุการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Information Technology Crisis Management Plan) ของบริษัท

2.2 ควรดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นอย่างน้อยปีละ 1 ครั้ง

2.3 ควรทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

2.4 ควรมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง และซักซ้อมบุคลากรภายในบริษัทเพื่อให้เกิดความเข้าใจที่ถูกต้องอย่างน้อยปีละ 1 ครั้ง

7. บทลงโทษ

ผู้ใช้งานคนใดที่ฝ่าฝืนนโยบายฉบับนี้ บริษัทจะพิจารณาลงโทษทางวินัยตามระเบียบบริหารงานบุคคล รวมทั้งอาจมีความรับผิดทั้งทางอาญาและทางแพ่ง

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากฝ่ายจัดการและหน่วยงานที่กำกับดูแลด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้พนักงานรับทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

ทั้งนี้ เพื่อให้นโยบายฉบับนี้มีความเป็นปัจจุบันและเหมาะสมกับระเบียบ ข้อบังคับ และสถานการณ์ต่างๆ ที่เปลี่ยนแปลงไป คณะกรรมการบริษัทอาจพิจารณาทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง หรือตามที่คณะกรรมการบริษัทเห็นสมควร และหากคณะกรรมการบริษัทมีมติให้ปรับปรุงนโยบายฉบับนี้ ให้จัดทำตารางสรุปรายละเอียดการทบทวนไว้ท้ายนโยบายฉบับนี้ด้วย

นโยบายการกำกับดูแล การบริหารจัดการ และรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ ได้รับการอนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 3/2566 เมื่อวันที่ 30 มีนาคม 2566 และมีผลบังคับใช้ตั้งแต่วันที่ 30 มีนาคม 2566 เป็นต้นไป

ประกาศ ณ วันที่ 30 มีนาคม 2566

(นายเจษฎาวัฒน์ เพรียบจริยวัฒน์)
ประธานกรรมการบริษัท