นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
บริษัท สกาย ไอซีที จำกัด (มหาชน) และ บริษัทในเครือ

หลักการและเหตุผล

ในปัจจุบันระบบสารสนเทศเป็นระบบหนึ่งที่มีส่วนช่วยให้บริษัทสามารถดำเนินการเกี่ยวกับธุรกิจได้อย่างสะดวก ช่วยให้เวลาในการส่งข้อมูลหรือไฟล์ต่าง ๆ สามารถทำได้ง่ายด้วยการส่งผ่านระบบ E-Mail หรือการใช้ สื่อบันทึกข้อมูลต่าง ๆ แต่การใช้งานสื่อเหล่านี้ก็เป็นการใช้งานทั่ว ๆ ไปโดยไม่ผ่านกระบวนการในการป้องกันถึงการส่งข้อมูลออกไปแล้วนั้น ข้อมูลที่ส่งไปจะไม่รั่วไหลออกไปยังกลุ่มของผู้ไม่พึงประสงค์เพื่อการนำข้อมูลออกไปขายให้กับบริษัทที่เป็นคู่แข่งอาจจะนำข้อมูลเหล่านี้ไปใช้งานหรือนำไปขายก่อนที่เราจะทำการเปิดตัวในข้อมูลเหล่านั้น หรือการที่ระบบเครือข่ายภายในของบริษัทถูกผู้ไม่ประสงค์ดีใช้กระบวนการของการโจมตีด้วย Social Engineering ที่เป็นลักษณะ การส่ง Phishing Mail ไปหาพนักงานในบริษัท และพนักงานคนนั้นไม่ทราบว่าเป็นการโจมตีด้วย Phishing Mail จึงทำให้ผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบของบริษัทโดยไม่ได้รับอนุญาต หลังจากนั้นจะทำการปิดระบบโดยคำสั่งของผู้ดูแลระบบ (Ransomware) เมื่อปิดระบบได้แล้วจะเข้าสู่กระบวนการเรียกค่าไถ่ระบบจากบริษัทและจะทำการปลดล็อก ซึ่งการเรียกค่าไถ่ในแต่ละครั้งบางที่อาจจะเสียค่าไถ่เป็นมูลค่าที่มหาศาลจนถึงขั้นต้องปิดตัวลง เป็นต้น และนี้คือเหตุผลที่ในปัจจุบันการรักษาความมั่นคงปลอดภัยสารสนเทศจึงมีความจำเป็นอย่างมากสำหรับ หน่วยงานราชการ องค์กรเอกชน รัฐวิสาหกิจ ธนาคารต่าง ๆ .ในการสร้างกระบวนการในการรักษาความมั่นคงปลอดภัยสารสนเทศสามารถทำได้หลากหลายรูปแบบไม่ว่าจะเป็น การสร้างความตระหนักถึงความมันคงปลอดภัยสารสนเทศ กำหนดกระบวนการในปฏิบัติงานให้เป็นไปตามกระบวนการที่ถูกต้องและเหมาะสม รวมถึงการประเมินผลการปฏิบัติงาน

สกาย ไอซีที จำกัด (มหาชน) และ บริษัทในเครือ **(“บริษัท”)** เป็นบริษัทที่ให้ความสำคัญกับการสร้าง การพัฒนาในด้านของการนำเทคโนโลยีสารสนเทศและไซเบอร์มาประยุกต์ให้ใช้ได้ในวิธีชีวิตประจำวัน เพิ่มประสิทธิผลและประสิทธิภาพของสินค้าบริการ รวมถึงการปรับปรุงระบบงานภายใน ตั้งแต่โครงสร้างพื้นฐานการสื่อสารทั้งภายในและภายนอก การเก็บและการรวบรวมข้อมูลตลอดสายโซ่ธุรกิจเพื่อเพิ่มคุณภาพการให้บริการทั้งก่อนและหลังการขาย การซ่อมบำรุง เป็นต้น ในเบื้องต้นทางบริษัทได้ดำเนินแนวทางในการสร้างความมั่นคงปลอดภัยสารสนเทศให้กับระบบเครือข่ายด้วยการสร้างระบบการเข้าใช้งานและการยืนยันตัวตนของพนักงานจะมีการสร้าง Account ในการเข้าใช้งานเพื่อการเข้าถึงระบบและส่วนบริการของบริษัทกำหนดสิทธิ์ในการเข้าถึงตามแต่ระดับที่ได้รับอนุญาตในการเข้าถึง และความจำเป็น ทางบริษัทได้มีการกำหนดนโยบายในด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Policy) เพื่อให้ผู้บริหาร พนักงาน ลูกจ้างร่วมไปถึงพนักงานฝึกงาน และคู่ค้าธุรกิจได้มีความตระหนักถึงการใช้งานเทคโนโลยีสารสนเทศและไซเบอร์ให้เกิดความมั่นคงปลอดภัย เพื่อเป็นแนวทางในการใช้งานข้อมูล การเข้าถึง และการบำรุงรักษาระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างเหมาะสมสอดคล้องกับกฎหมายตลอดจนข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง รวมทั้งได้มีการนำมาตรฐานด้านการให้บริการเทคโนโลยีสารสนเทศอย่างมีคุณภาพ มาใช้เป็นกรอบในการดำเนินการในส่วนของการบริหารงานด้านเทคโนโลยีสารสนเทศและไซเบอร์

วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทได้ถูกใช้งานโดยผู้ใช้งาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัยและอีกทั้งยังสามารถดำเนินงานในการใช้งานระบบได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยในหลากหลายรูปแบบที่มีผลต่อการดำเนินการทางธุรกิจอีกทั้งยังช่วยลดความเสี่ยงที่มีแนวโน้มว่าจะเกิดขึ้น โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.๑. การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ของบริษัท ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลที่ดีที่สุด

๑.๒. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐานสากลและมีการปรับปรุงอย่างต่อเนื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อีกทั้งยังนำกรอบการประเมินความเสี่ยงของส่วนงานมาใช้ในการจัดการกับการทำงานด้านเทคโนโลยีสารสนเทศด้วยกรอบของ Information Security คือ ความลับ Confidentiality (C) ความถูกต้อง Integrity (I) ความพร้อมใช้ Availability (A)

๑.๓. นโยบายนี้จะต้องทำการเผยแพร่ให้กับพนักงานทุกระดับได้รับทราบ และพนักงานทุกคนจะต้องยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร พนักงาน ผู้ดูแลระบบ (System Administrators) และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

๑.๖. นโยบายฉบับนี้ดำเนินการภายใต้กรอบกระบวนการคุ้มครองข้อมูลส่วนบุคคลประกาศใช้เมื่อวันที่ ๑ มิถุนายน ปีพุทธศักราช ๒๕๖๕

นโยบาย

๑. เพื่อป้องกันภัยคุกคามและความเสี่ยงต่าง ๆ ที่มีผลต่อธุรกิจของบริษัท ซึ่งอาจจะเกิดขึ้นโดยตั้งใจหรือไม่ตั้งใจ ทั้งจากภายในและภายนอกบริษัท คณะกรรมการและผู้บริหารของ บริษัท จึงเล็งเห็นความสำคัญนี้พร้อมอนุมัติให้มีการกำหนดและดำเนินการใช้นโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลฉบับนี้ โดยเป็นไปตามกฎเกณฑ์ ข้อบังคับที่มีการประกาศใช้ในประเทศไทย

๒. นโยบายฉบับนี้ครอบคลุมในเรื่องดังต่อไปนี้

๒.๑ ข้อมูลของบริษัทจะต้องได้รับการปกป้องกันจากผู้ที่**ไม่มีสิทธิ์ในการเข้าถึงข้อมูล**[๑] นั้น ๆ ข้อมูลจำเป็นต้องถือเป็นความลับของบริษัท นอกจากนี้ข้อมูลยังต้องถูกเก็บรักษาให้ครบถ้วนสมบูรณ์ ไม่มีการเปลี่ยนแปลงจากเดิมโดยไม่ได้รับอนุญาตหรือจากบุคคลที่ไม่มีสิทธิ์ในการแก้ไขเปลี่ยนแปลงข้อมูลนั้น ๆ และที่สำคัญข้อมูลนั้นจำเป็นต้อง**สามารถนำมาใช้งานได้**เมื่อจำเป็นต้องนำมาใช้ในการทำงาน

๒.๒ **หน้าที่ความรับผิดชอบ** ของข้อมูลนั้นจำเป็นต้องมีผู้ดูแลและรับผิดชอบอย่างชัดเจน

๒.๓ **การควบคุมการเข้าถึง** ข้อมูลนั้นจำเป็นต้องมีผู้ดูแลและรับผิดชอบอย่างชัดเจน

๒.๔ จำเป็นต้องมีการวางแผนสำรองเพื่อการดำเนินธุรกิจอย่างต่อเนื่อง และต้องมีการปรับปรุงดูแลแผนนั้นให้ทันต่อเหตุการณ์เสมอ พร้อมทั้งต้องมีการทดสอบแผน[๒] ภายใต้แผนฉุกเฉินของฝ่ายเทคโนโลยีสารสนเทศ

๒.๕ **การอบรมเกี่ยวกับความปลอดภัยของข้อมูล** สำหรับพนักงานทุกคนในบริษัท

๒.๖ **การพบเจอเหตุการณ์จริงหรือข้อสงสัยเกี่ยวกับช่องโหว่ของความปลอดภัยของข้อมูล** จำเป็นต้องรายงานเหตุการณ์ให้กับหน่วยงานที่ปฏิบัติหน้าที่ในการเฝ้าระวังรักษาความมั่นคงปลอดภัยสารสนเทศและข้อมูล เพื่อทำการตรวจสอบอย่างละเอียด

๓. เอกสารการปฏิบัติงานและมาตรฐานต่าง ๆ ในบริษัท ควรจะสอดคล้องกับนโยบายฉบับนี้ รวมไปถึงการตรวจจับและควบคุมไวรัสคอมพิวเตอร์ รหัสผ่าน และแผนสำรองในการดำเนินธุรกิจ

๔. ข้อมูลและระบบต่าง ๆ ต้องสามารถใช้ได้และตอบสนองความต้องการทางธุรกิจได้ทุกเมื่อ

๕. หน่วยงานที่ปฏิบัติหน้าที่ในการเฝ้าระวังรักษาความมั่นคงปลอดภัยสารสนเทศและข้อมูลมีหน้าที่ในการรับผิดชอบส่วนการปรับปรุงดูแลนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลฉบับนี้รวมไปถึงมาตรฐาน ขั้นตอนการปฏิบัติเพื่อให้เป็นไปตามนโยบาย และต้องสนับสนุน พร้อมให้ความช่วยเหลือกับหน่วยงานอื่นที่ทำการพัฒนางานที่เกี่ยวข้องกับความปลอดภัยของข้อมูล

๖. ระดับผู้จัดการทุกคนมีหน้าที่รับผิดชอบโดยตรงในการปฏิบัติใช้นโยบายและควบคุมพนักงานที่อยู่ใต้บังคับบัญชาให้ปฏิบัติตามนโยบายอย่างถูกต้อง

๗. พนักงานทุกคนต้องยึดถือและปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศและข้อมูลอย่างเคร่งครัด

๘. บริษัทมีการควบคุมการเข้าออกภายในบริษัทด้วยระบบตรวจสอบใบหน้า, ลายนิ้วมือ หรือ คีย์การ์ด โดยพนักงานจะสามารถเข้าพื้นที่ต่าง ๆ ตามสิทธิ์ของตนเองที่สามารถเข้าพื้นที่นั้น ๆ ได้ด้วยใบหน้า, ลายนิ้วมือ หรือ คีย์การ์ดของตนเองตามเวลาที่บริษัทกำหนดตามสิทธิ์เท่านั้น

๙. บริษัทมีการใช้งานระบบคอมพิวเตอร์ การเชื่อมต่ออินเทอร์เน็ต และการจัดเก็บข้อมูลการใช้งานเครือข่ายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑๐. บริษัทมีบริการติดต่อสื่อสารเพื่ออำนวยความสะดวกในการทำงานของบริษัท โดยพนักงานสามารถใช้โทรศัพท์ โทรสาร อินเทอร์เน็ต ระบบเครือข่ายไร้สายและอีเมล โดยบริษัทจะสามารถจัดเก็บข้อมูลและตรวจสอบใช้งานระบบดังกล่าวได้และพนักงานจะต้องรับผิดชอบข้อมูลที่เกิดบัญชีผู้ใช้งานของตนจากการใช้งานระบบดังกล่าว

๑๑. บริษัทจะกำหนดสิทธิ์ตามที่ได้รับหรือระดับตามบัญชีผู้ใช้งานของพนักงาน และรหัสผ่านสำหรับการใช้งานระบบภายในบริษัทเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบ โดยพนักงานจะต้องจัดเก็บบัญชีผู้ใช้งานของตนไว้เป็นความลับและจะต้องเปลี่ยนแปลงรหัสผ่านของบัญชีตามช่วงเวลาที่กำหนดให้เพื่อความปลอดภัยของการเข้าถึงระบบสารสนเทศ

๑๒. บริษัทไม่สนับสนุนการกระทำที่ผิดกฎหมายดังนั้นบริษัทจะติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้องบนเครื่องคอมพิวเตอร์ของบริษัท และรณรงค์ให้พนักงานติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้องบนเครื่องคอมพิวเตอร์พกพาของตนเองด้วย

๑๓. เครื่องคอมพิวเตอร์ที่จะใช้งานต้องมีโปรแกรมป้องกันไวรัสที่ฝ่ายเทคโนโลยีสารสนเทศให้การรับรอง

๑๔. พนักงานที่ต้องการใช้งานระบบจากภายนอกบริษัทจะต้องทำการเชื่อมต่อผ่านระบบเครือข่ายเสมือนเพื่อใช้งานระบบด้วยบัญชีผู้ใช้งานของตนเอง

๑๕. การใช้งานเครื่องแม่ข่ายของแอพพลิเคชัน และฐานข้อมูลของระบบ ควรประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อการบรรลุวัตถุประสงค์ของการประมวลผลเท่านั้น

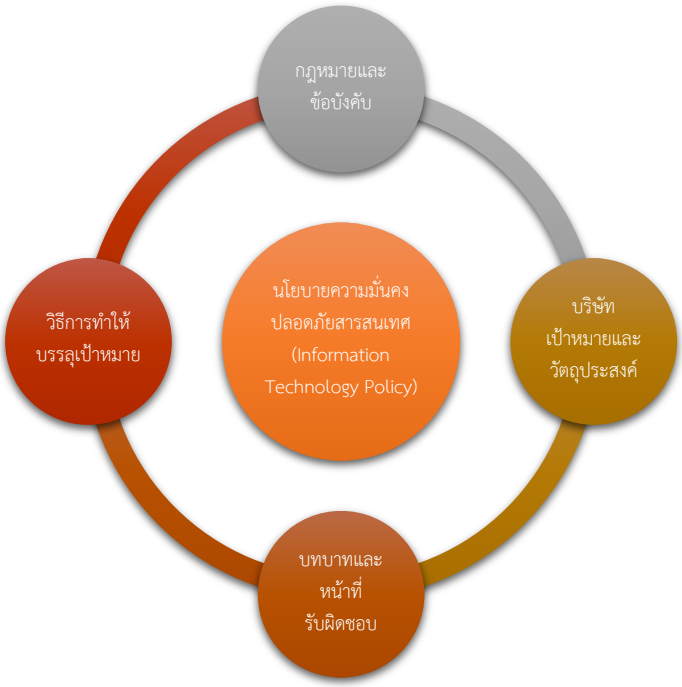
[๑] ข้อมูลมีอยู่ในหลากหลายรูปแบบ ซึ่งรวมถึงข้อมูลที่ถูกเก็บอยู่ในคอมพิวเตอร์ ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย ข้อมูลที่ทำการพิมพ์ออกมาหรือเขียนลงกระดาษ ข้อมูลที่ใช้ส่งผ่านแฟกซ์ หรือเก็บอยู่ในแผ่นดิสก์หรือเทป แม้กระทั่งข้อมูลที่เป็นการคุยระหว่างโทรศัพท์

[๒] แผนนี้จะทำให้พนักงานสามารถเข้าถึงข้อมูลและระบบที่จำเป็นต้องใช้ในการทำงานได้

สารบัญ

ส่วนประกอบของความปลอดภัยข้อมูลสารสนเทศ ๖
ขอบเขต ๗
บทบาทและหน้าที่รับผิดชอบ ๘
คำนิยาม ๑๐
๑. นโยบายความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY POLICY) ๑๔
๒. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (ORGANIZATION OF INFORMATION SECURITY) ๑๕
๓. การควบคุม ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (HUMAN RESOURCE SECURITY) ๑๘
๔. การควบคุม การบริหารจัดการทรัพย์สิน (ASSET MANAGEMENT) ๒๑
๕. การควบคุม การเข้าถึง (ASSET CONTROL) ๒๘
๖. การควบคุม การเข้ารหัสข้อมูล (CRYPTOGRAPHY) ๓๓
๗. การควบคุม ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (PHYSICAL AND ENVIRONMENTAL SECURITY) ๓๔
๘. การควบคุม ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (OPERATION SECURITY) ๓๙
๙. การควบคุม ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (COMMUNICATIONS SECURITY) ๔๔
๑๐. การควบคุม การจัดหา การพัฒนา และการบำรุงรักษาระบบ
(SYSTEM ACQUISITION,DEVELOPMENT AND MAINTENANCE) ๔๖
๑๑. การควบคุม ความสัมพันธ์กับผู้ให้บริการภายนอก (SUPPLIER RELATIONSHIPS) ๔๙
๑๒. การควบคุม การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
(INFORMATION SECURITY INCIEDNT MANAGEMENT) ๕๒
๑๓. การควบคุม ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการความต่อเนื่องทางธุรกิจ
(INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT) ๕๗
๑๔. การควบคุม ความสอดคล้อง (COMPLIANCE) ๕๙
๑๕. การควบคุม การใช้อุปกรณ์ส่วนตัวในการทำงาน ๖๒
คู่มือปฏิบัติสำหรับพนักงานและผู้ใช้งาน ๖๔
กลุ่มพนักงานส่วนงานบริหารและพัฒนาทรัพยากรบุคคล (PD) ๗๑
กลุ่มพนักงานว่าจ้างชั่วคราว หรือพนักงานว่าจากภายนอก ๗๑
กลุ่มพนักงานส่วนงานฝ่ายเทคโนโลยีสารสนเทศ (IT) ๗๓
แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ๗๕
ซอฟต์แวร์อันตราย ๗๙
ความปลอดภัยของระบบเครือข่าย ๗๙
แผนการดำเนินงานทางธุรกิจให้ต่อเนื่อง (BCP) ๘๑
ข้อปฏิบัติและข้อบังคับตามกฎหมาย ๘๒
ระเบียบและบทลงโทษ ๘๓
บทสรุป ๘๔

ส่วนประกอบของความปลอดภัยข้อมูลสารสนเทศ



ส่วนประกอบของความปลอดภัยข้อมูลสารสนเทศ

แผนผังด้านบนกล่าวถึงนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลสารสนเทศนั้นเป็นเอกสารที่มีเนื้อหาอ้างถึงเป้าหมาย วัตถุประสงค์และคุณค่าของบริษัท ซึ่งมีผลต่อภาพลักษณ์ของบริษัทเป็นหลัก ดังนั้นการนำวิธีการต่าง ๆ มาประยุกต์ใช้เพื่อให้สอดคล้องกับนโยบายและทิศทางของธุรกิจจึงเป็นเรื่องที่จำเป็นต้องมีการปฏิบัติใช้จริง นอกจากนี้กฎเกณฑ์ข้อบังคับทางกฎหมายมีส่วนสำคัญในการร่างนโยบายความมั่นคงปลอดภัยสารสนเทศและข้อมูลฉบับนี้เช่น กฎหมายในเรื่องการป้องกันข้อมูล และเอกสารทางอิเล็กทรอนิกส์ที่มีผลบังคับใช้แล้วเป็นต้น และสุดท้ายการกำหนดบทบาทหน้าที่ความรับผิดชอบของพนักงานในแต่ละส่วนงานที่เกี่ยวข้องก็เป็นองค์ประกอบที่สำคัญในการที่จะทำให้พนักงานสามารถทำงานได้ตรงตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

โครงสร้างการจัดการเรื่องความปลอดภัยข้อมูล

นโยบายและระเบียบขั้นตอนทั้งหมดถูกจัดเก็บในรูปแบบเอกสารที่ได้รับการอนุมัติและยอมรับจากทางผู้บริหารอีกทั้งพนักงานของ บริษัท ได้รับทราบถึงการมีนโยบาย ในแง่มุมมองของนโยบายฯ นั้นมีความสำคัญกับทุกฝ่ายและทุกฝ่ายทั้งบริษัท ดังนั้นข้อมูลของบริษัทที่มีให้กับพนักงานและข้อมูลที่อยู่ภายใต้ความรับผิดชอบและการกระทำของพนักงาน รักษาข้อมูล หรือระบบที่ใช้ในการประมวลผลข้อมูล หรือแม้แต่วิธีที่ใช้โอนถ่ายข้อมูล ก็จะต้องมีการตรวจสอบ

ขอบเขต

พนักงานบริษัท

ความปลอดภัยข้อมูลเป็นเรื่องของการให้ความร่วมมือและทำงานร่วมกัน ซึ่งพนักงานในบริษัทเองต้องเห็นถึงความสำคัญให้ความร่วมมือและสนับสนุนในการทำงานที่เกี่ยวกับระบบข้อมูลต่าง ๆ ดังนั้นพนักงานแต่ละคนนั้นต้องยึดถึงและปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลบริษัทและมีความเข้าใจใส่ใจกับเอกสารที่เกี่ยวข้องและได้ประกาศให้รับทราบ พนักงานบริษัทที่ไม่ใส่ใจหรือไม่ปฏิบัติตามนโยบายฉบับนี้ จะถือว่าพนักงานละเลยและจะได้รับโทษตามระเบียบของบริษัทที่ได้กำหนดไว้

ระบบ

นโยบายฯ ฉบับนี้บังคับใช้กับคอมพิวเตอร์ระบบเครือข่าย แอปพลิเคชันทุกระบบ และระบบปฏิบัติการทั้งหมดที่เป็นของบริษัท และดำเนินการโดยบริษัท และรวมไปถึงข้อมูลที่เก็บหรืออยู่ในระบบคอมพิวเตอร์และระบบเครือข่ายและทรัพยากรข้อมูลทุกชนิดที่อยู่ภายในบริษัทด้วย นโยบายฯฉบันนี้ครอบคลุมถึงข้อมูลประเภทต่าง ๆ ดังนี้

๑. ข้อมูลที่ถูกเก็บไว้ในฐานข้อมูล (Database) และ เซิร์ฟเวอร์ (Servers)

๒. ข้อมูลที่อยู่หรือเก็บไว้ในคอมพิวเตอร์และอุปกรณ์อื่น ๆ รวมถึงข้อมูลที่ส่งผ่านระบบเครือข่าย ไม่ว่าจะเป็นภายในบริษัทหรือภายนอกบริษัท และข้อมูลที่ส่งจากภายในบริษัทไปยังเครือข่ายสาธารณะ

๓. ข้อมูลที่ถูกพิมพ์หรือเขียนด้วยลายมือ และเอกสารต่าง ๆ

๔. ข้อมูลที่ส่งผ่านอีเมลหรือจดหมายอิเล็กทรอนิกส์ หรือวิธีการสื่อสารที่นอกเหนือจากนี้

๔. ข้อมูลที่เก็บอยู่ในสื่อที่สามารถเคลื่อนย้ายได้ เช่น ฮาร์ดดิสก์ (Hard disk), แผ่นดิสก์เก็ต (floppy disk), แผ่นซีดีรอม (CD-ROMs), เทป และสื่อเก็บข้อมูลอื่น ๆ ที่คล้ายคลึงกัน รวมถึงสื่อที่มีการเก็บข้อมูลถาวรด้วย

๖. ข้อมูลที่ถูกนำเสนอบนสไลด์ ข้อมูลฉายผ่านทางโปรเจกเตอร์ ข้อมูลที่มีการเขียนบนกระดานบอร์ด ข้อมูลที่มองเห็นได้ด้วยตาและข้อมูลได้ยินจากสื่อ

๗. ข้อมูลที่ถูกเก็บในลักษณะของไฟล์ (file) ซึ่งมีนามสกุลไฟล์ต่าง ๆ กันเช่น .doc, .docx, .xls, .xlsx, .ppt, .jpg และอื่น ๆ เป็นต้น

๘. ข้อมูลที่ใช้พูดสื่อสารกันทางโทรศัพท์หรือในขณะมีการประชุม

๙. ข้อมูลการบันทึกการใช้งานระบบ (Log) ที่ทำการบันทึกไว้

บทบาทและหน้าที่รับผิดชอบ

หน้าที่ความรับผิดชอบ

หน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และ การประมวลผลข้อมูลส่วนบุคคลควรได้รับการสร้างความตระหนัก เพื่อให้ทราบถึงข้อกำหนดและภาระผูกพันในการคุ้มครองข้อมูลส่วนบุคคล

๑. หน้าที่รับผิดชอบที่แยกจากกัน

บริษัท นั้นต้องมีการกำหนดในเรื่องหน้าที่ความรับผิดชอบที่แตกต่างกันอย่างชัดเจน โดยเฉพาะในระบบโปรดักชัน (Production Environment) หรือระบบที่ใช้งานจริงนั้น นักพัฒนาโปรแกรม (Developer) ต้องมีหน้าที่และความรับผิดชอบที่แยกจากเจ้าหน้าที่ดูแลระบบ (System Administrator)

๒. การจัดทำลักษณะงาน

ผู้บริหารต้องจัดทำมาตรการ ขั้นตอนต่าง ๆ ในการทำงานทั้งแบบป้องกันและตรวจจับเกี่ยวกับการตรวจสอบความปลอดภัย และปรับปรุงปฏิบัติอย่างต่อเนื่อง เพื่อให้ข้อมูลของบริษัท ไม่อยู่ในความเสี่ยงขั้นร้ายแรงที่เกี่ยวกับการแก้ไขข้อมูลที่ไม่ได้รับอนุญาตหรือไม่มีสิทธิ์ในการแก้ไข และทำให้ไม่สามารถตรวจจับได้ ซึ่งขั้นตอนการทำงานเหล่านี้จำเป็นต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรและจัดทำเป็นเอกสารอย่างชัดเจน

๓. จัดเตรียมพนักงานสำรอง

ในระบบการทำงานจริงจำเป็นต้องมีพนักงานที่สามารถทำงานแทนพนักงานที่ทำหน้าที่รับผิดชอบหลักได้ ในกรณีที่พนักงานมีที่รับผิดชอบหลักไม่สามารถปฏิบัติงานได้

๔. กำหนดความรับผิดชอบ

เจ้าของข้อมูลมีหน้าที่ดูแลและควบคุมข้อมูล รวมทั้งกำหนดการเข้าถึงข้อมูลที่ตนมีหน้าที่รับผิดชอบด้วยผู้บังคับบัญชาของเจ้าของข้อมูลหรือหัวหน้าฝ่ายของเจ้าของข้อมูล มีหน้าที่รับผิดชอบแทนเจ้าของข้อมูลในนั้นกรณีที่เจ้าของข้อมูลไม่สามารถปฏิบัติงานได้

ฝ่าย/หน่วยงานในการกำกับดูแลจัดการเรื่องความปลอดภัยข้อมูล

๑. หน่วยงานจัดการความปลอดภัยข้อมูลมีหน้าที่ จัดทำ สนับสนุน ดำเนินการ และพัฒนาปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูล มาตรฐาน และให้คำแนะนำขั้นตอนการทำงานต่าง ๆ ที่เกี่ยวกับความปลอดภัยข้อมูลบริษัท

๒. หน่วยงานนี้จะมีการปฏิบัติงานเกี่ยวกับการประเมินความเสี่ยงของระบบข้อมูลภายในบริษัทและการจัดการความเสี่ยงที่เกิดขึ้น เตรียมแผนปฏิบัติงานเกี่ยวกับระบบความปลอดภัยข้อมูล ประเมินผลิตภัณฑ์ที่ใช้ในงานความปลอดภัยข้อมูล และปฏิบัติตามแผนการที่กำหนดไว้เพื่อให้แน่ใจว่าบริษัทมีระบบความปลอดภัยข้อมูลเพียงพอ

๓. ฝ่ายงานตรวจสอบภายในต้องประสานงานกับหน่วยงานจัดการเรื่องความปลอดภัยข้อมูล เพื่อให้แน่ใจว่านโยบายต่าง ๆ ที่กำหนดขึ้นนั้นสอดคล้องกับข้อบังคับและกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศ และสามารถปฏิบัติได้อย่างถูกต้อง

๔. การปฏิบัติตามระเบียบข้อบังคับที่มีผลต่อข้อกฎหมายที่เกี่ยวกับความปลอดภัยข้อมูลนั้น เป็นหน้าที่ความรับผิดชอบของผู้จัดการของแต่ละหน่วยงานที่ต้องให้ความร่วมมือกับทางฝ่ายบุคคลของบริษัท

๕. ติดตาม แก้ไข ปรับปรุงขั้นตอน วิธีการปฏิบัติในงานซึ่งเกี่ยวข้องกับความปลอดภัยข้อมูล เพื่อให้มีผลบรรลุตามวัตถุประสงค์และเป็นไปตามนโยบาย

๖. รายงานความคืบหน้าของการทำงาน ช่องโหว่ที่ตรวจพบผลของนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลและข้อมูลอื่น ๆ ที่เกี่ยวข้องกับหน่วยงานตรงต่อคณะกรรมการตรวจสอบ (Audit Committee) และ/หรือประธานกรรมการบริษัท

หน้าที่รับผิดชอบของพนักงาน

พนักงานต้องคุ้นเคยและเข้าใจในนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลของบริษัท นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับบุคลากร รวมถึงข้อบังคับ ระเบียบมาตรฐานต่าง ๆ ที่มีผลต่อกฎหมาย ซึ่งพนักงานต้องทำความเข้าใจเป็นอย่างดีและปฏิบัติตามให้ครบถ้วน

หน้าที่ของเจ้าของข้อมูล

๑. เจ้าของข้อมูลโดยทั่วไปแล้วจะอยู่ในระดับผู้บริหาร ผู้จัดการของ บริษัท หรือสามารถมอบหมายหน้าที่นี้ให้กับผู้อื่นที่มีความรับผิดชอบโดยตรงได้ซึ่งมีหน้าที่ดูแล ครอบครอง พัฒนาแอปพลิเคชันที่ใช้งานได้จริงนั้น ๆ (ระบบที่ใช้สนับสนุนในการตัดสินใจ) เพื่อไว้ใช้ในการสนับสนุนและช่วยเหลือในการตัดสินใจต่าง ๆ และการทำงานภายในบริษัท

๒. ในส่วนแอปพลิเคชันที่ใช้งานจริงนั้นจำเป็นต้องมีการแต่งตั้งผู้เป็นเจ้าของแอปพลิเคชัน

๓. เจ้าของข้อมูลมีหน้าที่กำหนดประเภทของข้อมูล ซึ่งสามารถจัดประเภทตามระดับความสำคัญของข้อมูลลักษณะของข้อมูลว่ามีความเป็นความลับมากน้อยแค่ไหน และมีการกำหนดว่าข้อมูลควรถูกเก็บเพื่อใช้งานได้นานเท่าไรตามแต่ละประเภทของข้อมูล กระบวนการจัดประเภทของข้อมูลนี้รวมไปถึงการกำหนดระดับการเข้าถึงของผู้ใช้งานข้อมูลด้วย

๔. เจ้าของข้อมูลต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ประกาศใช้อย่างเคร่งครัดและเพื่อเป็นการรักษาสิทธิ์ในยโยบายการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของผู้ดูแลข้อมูล

๑. ผู้ดูแลข้อมูลหมายถึงพนักงานที่อยู่ในส่วนงานความปลอดภัยข้อมูลของบริษัท หรือผู้ที่ถูกมอบหมายให้ทำงานในส่วนการดูแลข้อมูล

๒. พนักงานในฝ่ายฝ่ายบริการการจัดการทรัพยากรบุคคลจะมีหน้าที่ในการขอและจัดเก็บและมอบหมายให้ส่วนงานที่เกี่ยวข้องเป็นผู้ดำเนินการตามกิจกรรมที่เกิดขึ้นโดยต้องมีการรับรองการใช้งานข้อมูลจากเจ้าของข้อมูล (Consent)

๓. พนักงานในฝ่ายเทคโนโลยีสารสนเทศ (ฝ่าย IT), ผู้ดูแลระบบ และพนักงานผู้ที่มีหน้าที่รับผิดชอบหรือทำงาน

๔. ระบบที่มีข้อมูลที่ใช้ในการทำงานของบริษัท ต้องมีผู้ดูแลอย่างเป็นทางการอย่างน้อยหนึ่งคน ผู้ดูแลมีหน้าที่รับผิดชอบในการเก็บรักษาข้อมูล ดูแลและควบคุมในเรื่องการเข้าถึงระบบ เพื่อป้องกันผู้ที่ไม่มีสิทธิ์ในการเข้าถึง เข้าถึงข้อมูลสำคัญ และต้องมีการสำรองข้อมูลเป็นประจำ (เพื่อป้องกันปัญหาเรื่องข้อมูลหาย)

คำนิยาม

- **บริษัท** หมายถึง บริษัท สกาย ไอซีที จำกัด (มหาชน)
- **พนักงาน**, **คนทำงาน**, และ **ผู้ใช้งาน** หมายถึง พนักงานที่ถูกว่าจ้างทุกประเภท เพื่อทำงานให้กับ บริษัท สกาย ไอซีที จำกัด เช่น พนักงานประจำ, พนักงานว่าจ้างตามสัญญา, พนักงานว่าจ้างชั่วคราว, และ พนักงานว่าจ้างเป็นช่วงเวลา รวมถึงผู้บริหารในระดับต่าง ๆ ของ บริษัท สกาย ไอซีที จำกัด (มหาชน) ที่อยู่ภายใต้การว่าจ้างของบริษัท
- **ระบบ** หรือ **ระบบคอมพิวเตอร์** หมายถึง เครื่องมือทุกชนิด, เซิร์ฟเวอร์ทุกประเภท และอุปกรณ์คอมพิวเตอร์ ทั้งในแบบมีสายและไร้สาย ทุกอย่างที่อยู่ในอุปกรณ์และสื่อบันทึกต่าง ๆ เพื่อใช้สำหรับส่งข้อมูลผ่านทางอินเทอร์เน็ต (ออกภายนอกบริษัท) เอ็กซ์ทราเน็ต (ภายในเครือข่ายที่เชื่อถือได้ที่ต่อกับบริษัท) และอินทราเน็ต (ภายในบริษัท) รวมถึงอุปกรณ์อิเล็กทรอนิกส์ทุกอย่างและอุปกรณ์โทรคมนาคมที่ใช้งานคล้ายคลึง กับคอมพิวเตอร์ ทั้งนี้ยังรวมไปถึงสิ่งของต่าง ๆ ที่เป็นทรัพย์สินของ บริษัทและกลุ่มบริษัทในเครือสกาย ไอซีที และที่เป็นของผู้ร่วมทำงานหรือหุ้นส่วน และที่เป็นของผู้ขายที่มีการซื้อ ติดตั้ง และตั้งอยู่ในพื้นที่ของ บริษัท สกาย ไอซีที จำกัด (มหาชน) ไม่ว่าสิ่งของหรืออุปกรณ์เหล่านั้นจะอยู่ในสภาวะแบบใด
- **ข้อมูล** หรือ **ข้อมูลคอมพิวเตอร์** หมายถึง สัญญาณอิเล็กทรอนิกส์ ไฟฟ้า เสียง หรือรูปแบบอื่น ๆ ทุกชนิดที่สามารถถูกเปลี่ยนหรือแปลงให้มีความหมายเพื่อให้มนุษย์เข้าใจได้ เช่น ตัวอักษร รูปภาพนิ่งภาพเคลื่อนไหว เสียง หรือรูปแบบอื่น ๆ ที่สามารถใช้เพื่อการสื่อสารระหว่างคนด้วยกันได้โดยใช้อุปกรณ์อิเล็กทรอนิกส์ หรืออุปกรณ์คอมพิวเตอร์ในการส่งสารจากอีกที่หนึ่งไปยังอีกที่หนึ่ง หรือเก็บบันทึกไว้ในเครื่องมืออื่น ๆ และสามารถนำไปใช้ใหม่ ชั่วคราวหรือตลอดไปได้
- **การเข้าถึง** การเข้าสถานที่ การใช้งานทางอิเล็กทรอนิกส์หรือกายภาพ รวมถึงการรับรู้ซึ่งข้อมูล
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** การตรวจสอบ การอนุมัติและการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง
- **การควบคุมการเข้าถึง** การอนุญาต การกำหนดสิทธิการเปลี่ยนแปลง การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง
- **การจัดการทรัพยากรระบบ (Capacity Management)** การบริหารจัดการทรัพยากรและการกำหนดค่าขีดความสามารถของเจ้าหน้าที่แผนการดำเนินงาน และอื่น ๆ
- **การบริหารจัดการเปลี่ยนแปลง (Change Management)** กระบวนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศหรือระบบงาน ซึ่ง การเปลี่ยนแปลงดังกล่าวจะมีผลกระทบต่อฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ ระบบ (System Software) ซอฟต์แวร์ประยุกต์ (Application Software) และระบบเครือข่าย (Network System) เป็นต้น
- **การประเมินความเสี่ยง** กระบวนการทั้งหมดในการวิเคราะห์และประเมินความเสี่ยง
- **กลุ่มข้อมูลใช้ภายใน (Internal Use)** ข้อมูลข่าวสารที่ใช้เฉพาะภายในบริษัทเท่านั้น สามารถเผยแพร่ภายในบริษัทได้แต่ห้ามเผยแพร่แก่บุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหารระดับผู้จัดการฝ่ายส่วนเจ้าของข้อมูลขึ้นไปและต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง
- **กลุ่มข้อมูลลับ (Confidential)** ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของรัฐซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้จัดการฝ่ายเจ้าของข้อมูลขึ้นไปโดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอานาจที่กฎหมายให้การรับรอง

- กลุ่มข้อมูลลับมาก (Secret) ข้อมูลข่าวสารซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยระดับผู้จัดการฝ่ายที่เป็นเจ้าของข้อมูลขึ้นไป โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

- กลุ่มข้อมูลลับที่สุด (Top Secret) ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ อย่างร้ายแรงที่สุดซึ่งผู้ที่สามารถเข้าถึงได้ต้องเป็นบุคคลที่มีสิทธิเท่านั้นและห้ามเผยแพร่ต่อบุคคลภายนอก เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

- กลุ่มข้อมูลสาธารณะ (Public) ข้อมูลข่าวสารที่เปิดเผยสามารถเผยแพร่แก่สาธารณะได้

- ข้อมูล (Data) สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของซีดี (CD) ดีวีดี (DVD) Hard Disk Thumb drive เอกสาร แฟ้มรายงาน หนังสือ แผนที่ แผนผัง ภาพวาด ภาพถ่าย การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

- ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

- ความต่อเนื่องในการดำเนินงานของบริษัท (Business Continuity Management: BCM) แนวทางในการบริหารจัดการธุรกิจได้อย่างต่อเนื่อง เมื่อบริษัทอยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของบริษัท ที่สำคัญได้รับการวางแผนความต่อเนื่องในการดำเนินงานของบริษัท (Business Continuity Plan หรือ BCP) และแผนสำรองฉุกเฉิน (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม

- เจ้าของข้อมูล (Information Owner) ผู้ซึ่งรับผิดชอบข้อมูลของบริษัทซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

- เจ้าของระบบงาน (System Owner) ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในบริษัท

- นิสิตและนักศึกษาฝึกงาน นิสิตและนักศึกษาที่บริษัทอนุญาตให้เข้ามาทดลองปฏิบัติงานโดยมีช่วงระยะเวลาที่กำหนดไว้

- โปรแกรมประยุกต์ หรือ แอปพลิเคชัน (Application) โปรแกรมประเภทหนึ่งที่ถูกสร้างขึ้นสำหรับใช้งานเฉพาะทาง

- พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspaces) พื้นที่ที่บริษัทอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น

- พื้นที่มั่นคงปลอดภัย (Secure Area) คือ พื้นที่ที่มีการควบคุมการเข้าถึง และมีระบบการป้องกันจากภัยคุกคามต่าง ๆ
- พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator / Operator Area) คือ พื้นที่สำหรับพนักงานดูแลระบบใช้ในการปฏิบัติงานในการดูแลระบบสารสนเทศของบริษัท
- ห้องปฏิบัติงานทั่วไป (Working Area) ห้องประชุม เช่น พื้นที่ปฏิบัติงานทั่วไปของพนักงานของบริษัท
- พื้นที่ทั่วไป (General Area) คือ พื้นที่สำหรับใช้รับรองบุคคลที่มาติดต่อบริษัท

- ระบบเครือข่าย (Network System) ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือส่งข้อมูลระหว่าง ระบบคอมพิวเตอร์ได้แก่ ระบบ LAN (Local Area Network) ระบบ WLAN (Wireless LAN) ระบบ Intranet และระบบ เป็นต้น

- ระบบเครือข่ายไร้สาย (Wireless LAN: WLAN) ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ รวมถึง การติดต่อสื่อสารระหว่างช่องทางการสื่อสารแทน

- ระบบสารสนเทศ (Information System) ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนามาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และ เทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น

- ระบบ Intranet เป็นระบบเครือข่ายที่สามารถเข้าถึงได้โดยผู้ใช้งานภายในบริษัทเท่านั้น โดยมีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัท

- ระบบ Internet ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ของบริษัทเข้ากับระบบคอมพิวเตอร์ทั่วโลก

- ระบบ LAN ระบบเครือข่ายแบบเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันในระยะจำกัด เช่น ในอาคารเดียวกัน หรือบริเวณเดียวกันที่สามารถลากสายถึงกันได้โดยตรง

- สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) สถานการณ์ซึ่งมีแนวโน้มทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

- สารสนเทศ (Information) ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผนการตัดสินใจ และอื่น ๆ

- สิทธิของผู้ใช้งาน สิทธิและหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัท มีดังนี้

- สิทธิใช้งานทั่วไป หมายถึง คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการผู้จัดการฝ่าย พนักงาน ลูกจ้าง บุคคลที่ใช้งานระบบสารสนเทศพื้นฐานของบริษัท ผู้ใช้งานต้องขออนุญาตจากผู้จัดการฝ่ายส่วนขึ้นไป โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่บริษัทกำหนด
- สิทธิพิเศษ หมายถึง สิทธิที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว

- สื่อสังคมออนไลน์ (Social Media) สังคมออนไลน์ที่ผู้ใช้อินเทอร์เน็ตสามารถแลกเปลี่ยนประสบการณ์ซึ่งกันและกัน โดยใช้สื่อต่าง ๆ เป็นตัวแทนในการสนทนา โดยได้มีการจัดแบ่งประเภทของ Social Media ออกเป็นหลายประเภท ได้แก่

- ประเภทสื่อสิ่งพิมพ์ (Publish) เช่น Wikipedia, WordPress, Blog gang, Blogger, OKnation ฯลฯ
- ประเภทสื่อสนทนาและส่งข้อความ (Discuss/SMS/Instant Messaging) เช่น G-chat, Line, Skype, Facebook Messenger ฯลฯ
- ประเภทเครือข่ายสังคมออนไลน์ (Social Network) เช่น Facebook, LinkedIn, Instagram, Twitter ฯลฯ
- ประเภทบริการวิดีโอออนไลน์ (Online Video) เช่น YouTube, Flickr, Slide Share, MSN, Yahoo ฯลฯ
- ประเภทบริการฝากรูปภาพ (Photo Sharing) เช่น Flickr, Photobucket ฯลฯ

- หน่วยงานภายนอก/ ผู้ให้บริการภายนอก/ บุคคลภายนอก ผู้ให้บริการภายนอก (Third Party) หรือบุคคลภายนอก ที่ใช้งานระบบสารสนเทศของบริษัท ได้เป็นครั้งคราวหรือตามสัญญา

- เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event) กรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

- อุปกรณ์เคลื่อนที่ (Mobile Device) อุปกรณ์ประมวลผลแบบพกพา ที่มีขนาดเล็กสามารถใช้เพียงมือเดียวในการใช้งานส่วนของการรับข้อมูลเป็นแบบสัมผัส โดยไม่ต้องใช้ Keyboard และสามารถเชื่อมต่อเครือข่ายแบบไร้สาย เครือข่ายโทรศัพท์ได้ เช่น Smartphone, Tablet เป็นต้น

- อุปกรณ์ประมวลผล (Computing Device) อุปกรณ์ที่มีหน่วยประมวลผล หน่วยความจำ ส่วนบันทึกข้อมูล ส่วนการเชื่อมต่อเครือข่าย ส่วนรับข้อมูล และส่วนแสดงผล ได้แก่

- คอมพิวเตอร์แบบตั้งโต๊ะ เช่น Desktop Computer เป็นต้น
- คอมพิวเตอร์แบบพกพา เช่น Notebook, Netbook เป็นต้น

๑. นโยบายความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY POLICY)

วัตถุประสงค์

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) และแนวปฏิบัติที่เกี่ยวข้องฉบับนี้ถูกจัดทำขึ้น เพื่อกำหนดทิศทาง หลักการและกรอบของข้อกำหนดในการป้องกันทรัพย์สินที่เกี่ยวข้องกับสารสนเทศให้ปลอดภัยจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลและระบบงานสารสนเทศ เพื่อผลักดันให้มีการควบคุมภายในด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง (Risk Based Approach) ที่สอดคล้องกับมาตรฐานสากล และเพื่อสนับสนุนให้ผู้ใช้งานตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศรวมถึงความสำคัญในการบริหารจัดการความเสี่ยงด้านสารสนเทศ

ผู้ปฏิบัติ

ผู้บริหาร ผู้อำนวยการ ผู้จัดการ ผู้จัดการฝ่าย พนักงาน ลูกจ้าง ผู้ใช้งานอื่น ตลอดจนหน่วยงาน/บุคคลภายนอก (External Party) ซึ่งเกี่ยวข้องกับการใช้ข้อมูลหรือสินทรัพย์สารสนเทศของบริษัทตามสิทธิและหน้าที่ความรับผิดชอบ

นโยบาย

๑.๑ ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

๑.๑.๑ นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for Information Security) จัดทำนโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรเพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ โดยนโยบายความมั่นคงปลอดภัยสารสนเทศ ดังกล่าวจะต้องได้รับการอนุมัติจากผู้บริหารของบริษัทและจัดให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศให้กับ พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบเป็นลายลักษณ์อักษรเพื่อลงนามรับทราบ

๑.๑.๒ การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the Policies for Information Security) นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลากำหนดไว้ (อย่างน้อย ๑ ครั้งต่อปี) และกรณีที่มีการเปลี่ยนแปลงที่มีนัยสำคัญให้ดำเนินการปรับปรุงนโยบายภายใน ๖ เดือน

๑.๑.๓ เพื่อให้มั่นใจว่าพนักงานในบริษัทฯ รับทราบเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการทำงาน

๒. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (ORGANIZATION OF INFORMATION SECURITY)

วัตถุประสงค์

เพื่อให้บริษัทมีการกำหนดขอบเขตการบริหารจัดการบริษัท มีการควบคุมการปฏิบัติงาน และมีการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศในบริษัท รวมทั้งการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกล และของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

นโยบาย

๒.๑ โครงสร้างภายในบริษัท (Internal Organization)

๒.๑.๑ บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities) หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและมอบหมายความรับผิดชอบ

๒.๑.๒ การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties) หน้าที่และส่วนงานที่รับผิดชอบที่จะทำให้เกิดการขัดต่อการปฏิบัติงานโดยการทำให้มีการเปลี่ยนแปลงทรัพย์สินของบริษัท หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกัน เพื่อลดโอกาสเกิดขึ้นของเหตุการณ์ความเสี่ยงนั้น ๆ

๒.๑.๓ การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with Authorities) การติดต่อกับหน่วยงานผู้มีอำนาจต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

๒.๑.๔ การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน(Contact with Special Interest Groups) การติดต่อกับกลุ่มที่มีความสนใจเรื่องเดียวกัน กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมอาชีพ ต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

๒.๑.๕ ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information Security in Project Management) การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตาม ต้องมีการระบุความมั่นคงปลอดภัยสารสนเทศของโครงการนั้น

๒.๒ อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Device and Teleworking)

๒.๒.๑ อุปกรณ์ประมวลผลและอุปกรณ์เคลื่อนที่ (Computing Device and Mobile Device) เพื่อเป็นมาตรการในการควบคุมบริหารจัดการความเสี่ยงสำหรับการใช้งานอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัท และเครื่องที่เป็นของส่วนตัวต้องปฏิบัติดังนี้

การใช้งานทั่วไปและการดูแลรักษา

๒.๒.๑.๑ อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัทถือเป็นสินทรัพย์ของบริษัทโดยใช้เพื่อการดำเนินงานของบริษัทเท่านั้น

๒.๒.๑.๒ การคืน หรือส่งซ่อมอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของบริษัท ให้ทำการสำรองข้อมูลหรือลบข้อมูลอย่างปลอดภัยตามระดับความลับของข้อมูลที่อยู่ในอุปกรณ์นั้นไปไว้ในที่เตรียมไว้

๒.๒.๑.๓ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไข Configuration หรือส่วนประกอบของอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัทโดยไม่ได้รับอนุญาต

๒.๒.๑.๔ ไม่ใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัทผิดวัตถุประสงค์และหลีกเลี่ยงการใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ในสภาวะแวดล้อมที่มีผลกระทบต่ออุปกรณ์

๒.๒.๑.๕ หากมีความจำเป็นต้องใช้งานอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ส่วนตัวมาใช้เชื่อมต่อเครือข่ายภายในของบริษัท รวมทั้งเข้าถึงระบบงานภายในต้องได้รับการอนุญาตจากผู้บังคับบัญชา และทำการชี้แจงเหตุผลต่อผู้บังคับบัญชาให้ทราบถึงสาเหตุที่ต้องนำอุปกรณ์ส่วนตัวนำมาใช้งานด้วยเหตุผลใด และนำอุปกรณ์ดังกล่าวไปขึ้นทะเบียนกับบริษัท เพื่อทำการตรวจสอบและติดตั้งในส่วนของโปรแกรมที่จำเป็นต่อการใช้งานรวมถึงโปรแกรมป้องกันไวรัสที่บริษัทได้ทำการซื้อและใช้งานภายในและต้องปฏิบัติตามขั้นตอนการใช้งานที่บริษัทกำหนด

๒.๒.๑.๖ ใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ส่วนตัว ในการเข้าถึงระบบงานทั่วไปของบริษัทเท่านั้น

๒.๒.๑.๗ ไม่ใช้อุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ส่วนตัว ในการเข้าถึงระบบบริหารจัดการบริการของบริษัท

๒.๒.๒ ความปลอดภัยทางด้านกายภาพของอุปกรณ์ประมวลผลและอุปกรณ์เสริมของบริษัท

๒.๒.๒.๑ ต้องจัดเก็บในที่ปลอดภัย ไม่วางทิ้งไว้ในที่เสี่ยงต่อการสูญหาย

๒.๒.๒.๒ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ในกรณีที่อุปกรณ์ประมวลผลสูญหายหรือเสียหาย ผู้ใช้งานต้องแจ้งไปยังฝ่ายเทคโนโลยีสารสนเทศโดยเร็วที่สุดตามความสำคัญ

๒.๒.๒.๓ หากผู้ใช้งานพ้นสภาพจากการเป็นพนักงานผู้ปฏิบัติงาน พ้นจากสภาพการฝึกงาน พ้นจากการสิ้นสุดสัญญาในการจ้าง ผู้เป็นเจ้าของอุปกรณ์นั้น ๆ ต้องดำเนินการนำส่งอุปกรณ์ประมวลผลและอุปกรณ์เสริมทั้งหมดที่เคยได้รับคืนให้บริษัทและปฏิบัติตามกระบวนการในการส่งอุปกรณ์คืน ให้กับทางบริษัท

๒.๒.๓ การบริหารจัดการข้อมูล

๒.๒.๓.๑ ข้อมูลของบริษัทที่มีชั้นความลับซึ่งถูกจัดเก็บไว้ในอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ทั้งของบริษัท และอุปกรณ์เคลื่อนที่ส่วนตัว ต้องบริหารจัดการตามระดับชั้นความลับของข้อมูล

๒.๒.๔ การบริหารจัดการรหัสผ่าน (Password)

๒.๒.๔.๑ ผู้ใช้งานต้องปฏิบัติตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy) สำหรับอุปกรณ์ประมวลผล ผู้ใช้งานต้องตั้งค่า Lock screen ด้วย PIN ที่เป็นรหัสที่เดาสุ่มได้ยาก ความยาว อย่างน้อย ๘ ตัว โดยใช้เป็นตัวเลข ตัวอักษรภาษาอังกฤษ อักขระพิเศษ หรือใช้วิธีการยืนยันตัวตนก่อนใช้งานเครื่องที่ดีกว่าเช่น Pattern, Password หรือ Fingerprint เป็นต้นสำหรับอุปกรณ์เคลื่อนที่ และกำหนดค่า Automatically Lock Screen Timeout ไม่มากกว่า ๑๕ นาที

๒.๒.๔.๒ ระบบกำหนดให้มีการจำกัดจำนวนครั้งของการพยายามเข้าสู่ระบบ ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง และหลังจากการเข้าสู่ระบบผิดพลาดให้บังคับระยะเวลาทิ้งช่วง เป็นเวลา ๕ นาทีก่อนที่จะยอมให้เข้าสู่ระบบอีกครั้ง และกำหนดให้เหมาะสมกับระบบสารสนเทศนั้น ๆ ตามแต่ความจำเป็นและความสำคัญของระบบ

๒.๒.๕ การเก็บข้อมูลสำรอง

๒.๒.๕.๑ ผู้ใช้งานต้องปฏิบัติตามนโยบายการสำรองข้อมูล (Back up Policy)

๒.๒.๕.๒. ผู้ที่ต้องการขอกู้ข้อมูลหรือการ สำรองข้อมูลจะต้องดำเนินการตามกรอบกระบวนในการขอกู้ข้อมูล

๒.๒.๕.๓. เมื่อทำการขอกู้คืนข้อมูลหรือ สำรองข้อมูลแล้วควรจะดำเนินการตรวจสอบตามกรอบกระบวนการตรวจสอบข้อมูลหลังการขอกู้ข้อมูล

๒.๒.๖ การป้องกันซอฟต์แวร์ที่ไม่พึงประสงค์ (Malware)

๒.๒.๖.๑ ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัท ร่วมไปถึงอุปกรณ์ส่วนตัวที่ผู้ใช้งานนำมาลงทะเบียนกับทางบริษัทโดยผู้ใช้งานต้องรับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับอุปกรณ์ส่วนตัวด้วยตนเอง

๒.๒.๖.๒ ห้ามผู้ใช้งานทำการปิด ยกเลิก กระทำการใด ๆ ที่อาจส่งผลต่อระบบการป้องกันไวรัสหรือระบบป้องกันมัลแวร์อื่นใด ที่ติดตั้งอยู่บนอุปกรณ์ประมวลผลและ/หรืออุปกรณ์เคลื่อนที่ของบริษัท

๒.๒.๖.๓ หากพบว่าโปรแกรมป้องกันไวรัสในอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ทำงานผิดพลาดหรือไม่ทำงาน หรือสงสัยว่าอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัท ติด Malware หรือพบข้อมูลภัยคุกคามผู้ใช้งานต้องยุติการเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายและให้แจ้งฝ่ายเทคโนโลยีสารสนเทศเพื่อดำเนินการทันที หากพบว่าอุปกรณ์ของผู้ใช้ประสบกับปัญหาดังกล่าวโดยเจ้าหน้าที่รักษาความมั่นคงปอลดภัยสารสนเทศ ทางเจ้าหน้าที่จะทำการตัดการเชื่อมต่อผู้ใช้งานออกจากเครือข่ายโดยทันที โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบก่อน

๒.๒.๖.๔ ต้องตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลต่าง ๆ ได้แก่ External Hard disk, Flash Drive ก่อนนำมาใช้งานทุกครั้งและต้องปฏิบัติอย่างเคร่งครัด

๒.๒.๖.๕ ต้องตรวจสอบไฟล์ที่แนบมากับ E-mail หรือไฟล์ที่ Download มาจากอินเทอร์เน็ต ด้วยโปรแกรมตรวจสอบไวรัสก่อนใช้งาน

๒.๒.๖.๖ ไม่ครอบครอง หรือพัฒนาโปรแกรมไวรัส หรือโปรแกรมที่ก่อกวน หรือโปรแกรมที่ส่งผลต่อระบบของบริษัทหรือองค์กรอื่น ๆ โดยไม่ได้รับอนุญาต

๒.๒.๖.๗ ไม่ติดตั้ง หรือใช้งานโปรแกรมเพิ่มเติม โดยไม่ได้รับอนุญาตในอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ของบริษัท และไม่ติดตั้งหรือใช้งานโปรแกรมที่สุ่มเสี่ยงกับการกระทำผิดกฎหมาย และละเมิดลิขสิทธิ์ในอุปกรณ์ประมวลผล และ/หรือ อุปกรณ์เคลื่อนที่ส่วนตัวที่นำมาใช้งานภายในเครือข่ายของบริษัท

๒.๓ การปฏิบัติงานจากภายนอกบริษัท (Teleworking)

๒.๓.๑ การควบคุมการเข้าถึงการปฏิบัติงานภายนอกบริษัท ในกรณีที่ผู้ให้บริการภายนอก (Third Party) มีการ Remote Access เพื่อ ปฏิบัติงานชั่วคราว ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Third Party Relationship Policy) โดยควบคุมและตรวจสอบการใช้งาน หรือการเข้าถึงระบบตามสิทธิ์ที่ได้รับอย่างเคร่งครัด

๒.๓.๒ การเชื่อมต่อจากภายนอกบริษัท จะต้องมีการดำเนินการที่ได้รับการอนุมัติและเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ที่บริษัทอนุญาตและจัดหาให้เท่านั้น ห้ามมิให้ผู้ใช้งานเปลี่ยนแปลงโปรแกรมที่ใช้ในการเชื่อมต่อเป็นอันขาด

๒.๓.๓ สิทธิ์ในการใช้งาน Remote Access เพื่อปฏิบัติงานชั่วคราวเป็นสิทธิ์ที่บริษัทจะให้เฉพาะผู้ใช้งาน ผู้ให้บริการภายนอกเป็นการชั่วคราวเท่านั้น ไม่สามารถถ่ายโอนกันได้

๒.๓.๔ ผู้ใช้งานระบบ Remote Access จะต้องทำการขออนุมัติจากผู้บังคับบัญชาก่อนเข้ามาใช้งาน Remote Access การเข้าสู่ระบบสารสนเทศ ผู้ใช้งานจะต้องระบุวัตถุประสงค์ วิธีการเข้าถึง และ ขอบข่ายของการเข้าถึงที่แน่ชัด และจะต้องทำการอนุมัติให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น

๒.๓.๕ บริษัทมีสิทธิ์เรียกร้องค่าเสียหายจากผู้ใช้งาน หรือผู้ให้บริการภายนอก หากระบบคอมพิวเตอร์ของบริษัทได้รับความเสียหาย โดยการติดไวรัสคอมพิวเตอร์จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

๓. การควบคุม ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (HUMAN RESOURCE SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่าพนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา มีความตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเองเพื่อลดความเสี่ยงจากความผิดพลาด และการนำไปใช้งานในทางที่ไม่เหมาะสมของพนักงาน และเพื่อให้มั่นใจในกระบวนการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงานไม่กระทบกับความปลอดภัยสารสนเทศ

นโยบาย

๓.๑ ก่อนการจ้างงาน (Prior to employment)

๓.๑.๑ การคัดเลือก (Screening) การตรวจสอบภูมิหลังของผู้สมัครงาน ต้องมีการดำเนินการ โดยมีความสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

๓.๑.๒ บริษัทต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศในคุณสมบัติของบุคลากรตามหน้าที่งานที่ได้รับมอบหมาย

๓.๑.๓ ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นบุคลากรของบริษัท จะต้องมีการตรวจสอบประวัติอาชญากรรม หรืออื่น ๆ ตามเงื่อนไขที่เกี่ยวข้อง

๓.๑.๔ ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง "พนักงาน" และบริษัท ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement : NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้น ๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องตามนโยบายการเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (SKY ICT Data Retention Policy) ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

๓.๑.๕ ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) ข้อตกลงและเงื่อนไขในสัญญาจ้างกับพนักงาน และผู้ที่ทำสัญญาต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน ของผู้ที่ทำสัญญาจ้าง และของบริษัทฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องกำหนดเงื่อนไขการจ้างงาน ที่รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท

๓.๑.๕.๑ ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องเตรียมข้อมูลที่เกี่ยวข้องกับ นโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท เพื่อให้พนักงานและผู้ใช้งานที่เข้ามาใหม่ได้ศึกษาและลงนามรับทราบ รวมถึงยอมรับสัญญาในการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายเหล่านั้นอย่างเคร่งครัด

๓.๑.๕.๒ เพื่อให้การบริหารจัดการ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุดฝ่ายบริหารและพัฒนาทรัพยากรบุคคล ต้องแจ้งให้หน่วยงานที่รับผิดชอบทราบทันทีเมื่อมีการดำเนินการดังต่อไปนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงานและลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

๓.๑.๕.๓ คณะกรรมการ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่าย พนักงาน และลูกจ้างใหม่ทุกคน ที่เข้ามาปฏิบัติงานในบริษัท ต้องลงนามรับทราบและยินยอมปฏิบัติตามสัญญาการรักษาข้อมูลที่เป็นความลับของบริษัท และเอกสารอื่น ๆ ที่เกี่ยวข้อง ก่อนอนุญาตให้เริ่มงานหรือเข้าถึงและใช้งานข้อมูลสารสนเทศของบริษัท

๓.๒ ระหว่างการจ้างงาน (During employment)

๓.๒.๑ หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities) ผู้บริหารต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาว่าจ้างทั้งหมดรักษาความมั่นคงปลอดภัยสารสนเทศโดยปฏิบัติให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติตามที่บริษัทกำหนดไว้อย่างเคร่งครัด

๓.๒.๒ การสร้างความตระหนัก การให้ความรู้ บุคลากรฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training) พนักงานของบริษัททั้งหมดและผู้ที่ทำสัญญาต่าง ๆ ที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก ให้ความรู้ และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการเรียนรู้ และทบทวนเพิ่มเติมในนโยบายและขั้นตอนปฏิบัติของบริษัทที่เกี่ยวข้องกับงานที่ตนเองปฏิบัติ

๓.๒.๒.๑ พนักงานของบริษัททุกคนต้องได้รับการอบรมให้ความรู้โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล เพื่อเป็นการสร้างความตระหนัก และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๒.๒.๒ ต้องจัดอบรมให้ความรู้แก่พนักงาน เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยและการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒.๒.๓ พนักงานใหม่ทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อนหรืออย่างน้อยภายใน ๙๐ วันนับจากเข้าทำงานในหน่วยงาน โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย

๓.๒.๒.๔ ฝ่ายบริหารและพัฒนาทรัพยากรบุคคล มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของ ให้แก่บุคลากรด้วย

๓.๒.๓ กระบวนการทางวินัย (Disciplinary process) กระบวนการทางวินัยต้องกำหนดอย่างเป็นทางการ และมีการสื่อสารให้พนักงานได้รับทราบและพนักงานต้องยินยอมทำตามเงื่อนไขที่กำหนด เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศของบริษัท

บริษัทจัดให้มีมาตรการดำเนินการกับผู้ฝ่าฝืนหรือละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทที่เป็นความผิดทางวินัยภายใต้ระเบียบ ข้อบังคับของบริษัทกรณีดำเนินกิจกรรมที่เกี่ยวกับการทดสอบระบบสารสนเทศ เพื่อตรวจสอบหรือส่งเสริมความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย ได้แก่ การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัส การตรวจสอบ Network Traffic เป็นต้น แต่หากปฏิบัติโดยได้รับอนุญาตหรือเป็นหน้าที่ต้องดูแลในส่วนนี้ของบริษัท ถือเป็นข้อยกเว้น

๓.๓ การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

๓.๓.๑ การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities) เมื่อมีการสิ้นสุดหรือการเปลี่ยนแปลงต้องแจ้งถึงส่วนที่เกี่ยวข้องทั้งหมด ว่าด้วยเรื่องของพนักงานมีการเปลี่ยนแปลง หรือ ออกจากหน้าที่

๓.๓.๒ ต้องมีการถอดถอนสิทธิ์ในการเข้าถึงข้อมูล และระบบสารสนเทศทันทีที่ถึงกำหนดในการคงไว้ซึ่งข้อมูลและหน้าที่หน้าที่ความรับผิดชอบ

๓.๓.๓ ด้านความมั่นคงปลอดภัยสารสนเทศที่ยังต้องคงไว้หลังการสิ้นสุดหรือเปลี่ยนการจ้างงาน ต้องมีการกำหนดและสื่อสารให้ได้รับทราบต่อพนักงานหรือผู้ที่ทำสัญญาจ้าง รวมทั้งควบคุมให้ปฏิบัติตามอย่างสอดคล้อง

๓.๓.๔ พนักงานต้องทำการคืนอุปกรณ์ของบริษัท ที่อยู่ในความดูแลของพนักงาน ให้กับทางบริษัทในสภาพที่สมบูรณ์ ถ้าตรวจสอบแล้วพบว่ามีสภาพที่ไม่สมบูรณ์จะถือว่าพนักงานต้องรับผิดชอบในส่วนที่ไม่สบบูรณ์ โดยให้เป็นไปตามกรอบการปฏิเสธการรับผิดในส่วนนั้น ๆ

๓.๓.๕ พนักงานที่สิ้นสุดหรือเปลี่ยนแปลงหน้าที่จะต้องไม่นำข้อมูลที่เป็นความลับของ บริษัทฯ ไปเปิดเผยโดยมิชอบหลังจากที่สิ้นสุดการเป็นพนักงาน ถ้าพบว่ามีการละเมิดข้อบังคับดังกล่าว ต้องมีการ ใช้บทลงโทษตามที่บริษัทกำหนดไว้ และจะดำเนินการให้ถึงที่สุด

๔. การควบคุม การบริหารจัดการทรัพย์สิน (ASSET MANAGEMENT)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการระบุทรัพย์สินของบริษัท และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม สารสนเทศได้รับการยกระดับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อบริษัท มีการป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

นโยบาย

๔.๑ หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

๔.๑.๑ บัญชีทรัพย์สิน (Inventory of assets)

๔.๑.๑.๑ ต้องจัดทำและเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ (Software Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ของบริษัท โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการบริหารจัดการสินทรัพย์สาร สนเทศของบริษัท

๔.๑.๑.๒ ต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภทตามระยะเวลาที่กำหนดไว้ เช่น ปีละ ๑ ครั้ง หรือภายใน ๑ เดือน เมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เป็นต้น

๔.๑.๑.๓ ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

๔.๑.๒ ผู้ถือครองทรัพย์สิน (Ownership of assets) จะต้องกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบข้อมูลและสินทรัพย์ทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท อย่างชัดเจน

๔.๑.๓ การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets) จะต้องกำหนด แสดง บันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลและสินทรัพย์จะต้องถูกใช้

๔.๑.๓.๑ การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมด ที่บริษัท เป็นผู้จัดหามานั้นมีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของบริษัท การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสมซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
- เจ้าหน้าที่ ตลอดจนหน่วยงานภายนอก ที่ได้รับการว่าจ้างโดยบริษัท จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้องโดยหมายรวมถึงข้อมูลและระบบสารสนเทศของบริษัทฯ
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของบริษัท อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน

- เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของบริษัท ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งานและต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง

- ต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท ก่อนได้รับอนุญาต

- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท อาทิการติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนำที่ระบุไว้ใน เอกสารขั้นตอนการปฏิบัติงานเรื่องการใช้เครื่องคอมพิวเตอร์ประเภทพกพาในการปฏิบัติงานนอกสถานที่

- อุปกรณ์คอมพิวเตอร์ของบริษัท ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด

๔.๑.๓.๒ การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้

- ห้ามพนักงานทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท

- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยพนักงาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และ

อนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัท

- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของบริษัท มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัท เท่านั้น

๔.๑.๓.๓ การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้

- บริษัท จัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำวิจัย การค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่ม

ประสิทธิภาพในการทำงานและการให้บริการของบริษัท

- ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัท และบุคคลผู้ที่เกี่ยวข้องกับบริษัท เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้บริษัท ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

- บริษัท ไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด หรือบล็อก) ของพนักงานทั้งนี้ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของพนักงานผู้นั้น

๔.๑.๓.๔ การอนุญาตให้ใช้งานจดหมายอิเล็กทรอนิกส์ (E–Mail) มีดังนี้

- ผู้ใช้งาน E-mail ทั้งหมดของบริษัท ต้องมี E-mail Account เป็นของตนเอง
- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำ E-mail ไปใช้ในทางที่ผิด
- E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น It-system@skyict.co.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของฝ่ายเพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-mail Account นั้น
- E-mail Account ทั้งหมด และ E-mail ทุกฉบับ (รวมถึง E-mail ส่วนตัว) ที่ถูกสร้างและเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นสินทรัพย์ของบริษัท
- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบ E-mail ของบริษัท
- พื้นที่เก็บ E-mail บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัดทั้งนี้เมื่อปริมาณของ E-mail มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของ E-mail มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับส่ง E-mail ได้ตามปกติอีกต่อไป
- ขนาดของ E-mail และไฟล์แนบได้รับการจำกัดไว้ โดยหาก E-mail และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับ E-mail ตีกลับแจ้งว่าไม่สามารถส่ง E-mail ดังกล่าวได้
- ผู้ใช้งานต้องลบ E-mail ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บ E-mail ให้เป็นไปตามขนาดที่บริษัทกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษา E-mail ที่เกี่ยวข้องกับการทำงานและ E-mail ตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-mail Account ของบริษัท เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมายตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
- ห้ามใช้ E-mail Account ของบริษัท ในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับบริษัท
- ซอฟต์แวร์สำหรับใช้งาน E-mail ต้องได้รับการตั้งค่าให้ E-mail ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน บริษัท และเบอร์โทรศัพท์ติดต่อ
- ห้ามผู้ใช้งานทำสำเนาข้อความ หรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจาก E-mail ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของ E-mail ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออก E-mail นั้นในนามตัวแทนของบริษัท
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความใน E-mail หัวจดหมาย E-mail ลายเซ็นใน E-mail หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่ง E-mail โดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

- ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง “Reply with History” ซึ่งเป็นการตอบกลับ E-mail พร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคำสั่ง “Reply with History” ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่ง E-mail

- ผู้ใช้งานต้องทำการส่ง E-mail ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง “Reply All” ถ้าหาก E-mail ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน

- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่าง ๆ (Spam Mail) เป็นต้น

- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด

- ห้ามผู้ใช้งานส่งหรือส่งต่อ E-mail ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้ายทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และ E-mail ที่กระทบต่อความมั่นคงของชาติหรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

- ห้ามผู้ใช้งานส่ง E-mail ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัท

- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จักซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)

- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัสผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

๔.๑.๓.๕ การอนุญาตให้ใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้

- ผู้ใช้งานต้องปกปูองความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่ เมื่อจำเป็นต้องส่งข้อมูลนั้นผ่านเครื่องโทรสาร

- ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิด หมายเลข ผิดส่วนงานเป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น

- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น

- ห้ามผู้ใช้งานบันทึกหรือฝากข้อความที่มีข้อมูลลับในเครื่องตอบรับโทรศัพท์อัตโนมัติหรือ ระบบวอยซ์เมล์โดยเด็ดขาด

- ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่น Voice Over IP หรือในระหว่างการประชุมทางไกล เว้นแต่ผู้เข้าร่วมการประชุมทุกหน่วยงานได้รับการพิสูจน์ตัวตนแล้วว่าเป็นผู้ที่เกี่ยวข้องและมีสิทธิ์รับทราบข้อมูล

- ตรวจสอบจนมั่นใจแล้วว่าไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลลับที่สนทนาอยู่

- การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสมสามารถป้องกันเสียงลอดออกมาได้ เป็นต้น

- ผู้ใช้งานต้องสนทนาโทรศัพท์ด้วยความระมัดระวัง เพื่อป้องกันข้อมูลลับถูกแอบฟังโดยบุคคลที่ไม่ได้รับอนุญาต

- ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใด ๆ ทางโทรศัพท์ ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้นเป็นผู้ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าว ก่อนที่จะเปิดเผยข้อมูล

- ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสารที่มีข้อมูลลับ โดยสำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับ

- พนักงานต้องไม่เปิดเผยสถานที่ตั้งของห้องเครื่องคอมพิวเตอร์แม่ข่ายต่อบุคคลภายนอกโดยเด็ดขาดเว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน

๔.๑.๔ การคืนทรัพย์สิน (Return of assets) พนักงานและลูกจ้างซึ่งพ้นสภาพจากการจ้างงานต้องคืนสินทรัพย์ทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน โดยปฏิบัติตามระเบียบปฏิบัติ

๔.๒ การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ (Information classification)

๔.๒.๑ การกำหนดชั้นความลับของสารสนเทศ (Classification of Information)

๔.๒.๑.๑ การจัดระดับชั้นความลับต้องพิจารณาถึงข้อกำหนดทางด้านกฎหมาย คุณค่าระดับความสำคัญและระดับความอ่อนไหว เพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต โดยให้ปฏิบัติอย่างเหมาะสมตามระดับชั้นความลับของข้อมูล

๔.๒.๑.๒ ผู้จัดการฝ่ายต้องกำหนดประเภทของข้อมูล ระดับความสำคัญ ลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง และช่องทางการเข้าถึง เป็นลายลักษณ์อักษรและมีการสื่อสารให้ผู้ ที่เกี่ยวข้องรับทราบ ดังนี้

- มีการการจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines) แบ่งเป็น
    - ฮาร์ดแวร์
    - ซอฟต์แวร์
    - ข้อมูลสารสนเทศ
    - ผู้ใช้
- หน่วยงานกำหนดชั้นความลับสารสนเทศ ได้แก่
    - ปกติ ไม่กำหนดชั้นความลับ
    - ลับ
    - ลับมาก
    - ลับที่สุด
- มีการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ
    - ไม่ลับ คือ สามารถเผยแพร่ได้
    - ลับ คือ ผู้ที่เกี่ยวข้องกับงาน
    - ลับมาก คือ หัวหน้าฝ่าย/กลุ่ม
    - ลับที่สุด คือ ผู้บริหารระดับสูง
- มีการกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ เช่นกำหนดให้มีการใส่รหัสผ่านก่อนการใช้อุปกรณ์ อุปกรณ์เหล่านั้นต้องลงทะเบียนก่อนเข้าสู่ระบบ

๔.๒.๒ การบ่งชี้สารสนเทศ (Labeling of information)

๔.๒.๒.๑ ต้องจัดให้มีวิธีการจัดทำและจัดการปูายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์ทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๒.๒.๒ ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

๔.๒.๓ การจัดการทรัพย์สิน (Handling of assets) ขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สินต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้

๔.๒.๓.๑ ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

๔.๒.๓.๒ ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม

๔.๒.๓.๓ ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน

๔.๒.๓.๔ ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสารฯลฯ โดยทันที

๔.๒.๓.๕ เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

๔.๒.๓.๖ เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับของบริษัท ในพื้นที่สาธารณะ เช่น ลิฟท์ ร้านอาหารฯลฯ

๔.๒.๓.๗ สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น PDA, USB-Drive, CD-ROM เป็นต้น) ที่มีข้อมูลลับของบริษัท บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

๔.๒.๔ การบริหารจัดการสื่อบันทึกข้อมูล (Media Handling) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัท โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

๔.๒.๔.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media) การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์หรือความเสียหายในระหว่างนี้ที่นาส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น ต้องกำหนดวิธีปฏิบัติและสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูลโดยปฏิบัติตามเอกสารระเบียบปฏิบัติ

๔.๒.๔.๒ บริษัท จัดทำระเบียบระเบียบปฏิบัติสำหรับการทำลายสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร ดังนี้

ประเภทสื่อบันทึกข้อมูล	**นำสื่อบันทึกกลับมาใช้ใหม่**	**ข้อมูลที่มีชั้นความลับและนำสื่อกลับมาใช้ใหม่**	**วิธีทำลาย**
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse	ห้ามนำกลับมาใช้ใหม่	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive, ฮาร์ดดิสก์	ใช้การ Format	ใช้การ Format แบบ Zero - Filling	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
เทป		ใช้การ Format แบบ Zero - Filling	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
แผ่น CD/DVD	ห้ามนำกลับมาใช้ใหม่		
สื่อบันทึกข้อมูลแบบมีระบบปฏิบัติการ	ใช้การ Format Data Reset	ห้ามนำกลับมาใช้ใหม่	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย

๔.๒.๕ การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)ต้องมีวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศหรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย โดยปฏิบัติตามระเบียบปฏิบัติ

๔.๒.๕.๑ ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้และมีกระบวนการตรวจสอบพนักงานส่งของ

๔.๒.๕.๒ บรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการส่งโดยเป็นไปตามความเหมาะสม

๔.๒.๕.๓ ต้องมีการควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต เช่น การเข้ารหัสให้สอดคล้องตามชั้นความลับ

๔.๒.๕.๔ ส่งด้วยตนเองหรือเจ้าหน้าที่ของบริษัทและลงบันทึกการรับ-ส่ง เพื่อสามารถตรวจสอบได้

๔.๒.๕.๕ บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลายส่วนและหลายเส้นทางเพื่อกระจายความเสี่ยง

๕. การควบคุม การเข้าถึง (ASSET CONTROL)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ขององค์การ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การได้อย่างถูกต้อง

เพื่อให้มั่นใจว่ามีการจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต มีการกำหนดสิทธิ์ในการเข้าถึงระดับบของข้อมูลหรือสารสนเทศเพื่อป้องกันการเข้าถึงข้อมูลที่เป็นความลับทั้งหมด

นโยบาย

๕.๑ นโยบายควบคุมการเข้าถึง (Access Control Policy)

๕.๑.๑ มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึง ให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๕.๑.๒ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยปฏิบัติตามระเบียบปฏิบัติ ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน

๕.๑.๓ ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

๕.๑.๔ ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทและเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

๕.๑.๕ ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๕.๑.๖ ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ

๕.๑.๗ การเข้าถึงข้อมูลและระบบสารสนเทศของบริษัทจะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น ๆ เท่านั้น ความปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึงการให้สิทธิ์และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูลและการกู้ข้อมูลที่เสียหายกลับคืนมา

๕.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

๕.๒.๑ การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration)

การลงทะเบียนผู้ใช้งานใหม่ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่นเมื่อลาออกไป หรือ

เมื่อเปลี่ยนตำแหน่งงานภายใน เป็นต้น โดยปฏิบัติตามระเบียบปฏิบัติ โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณาอนุมัติตามขั้นตอนอย่างเคร่งครัด

๕.๒.๒ การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึง ทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท

๕.๒.๓ การบริหารจัดการสิทธิ์ตามระดับสิทธิ์การเข้าถึง (Management of Privileged Access Right)

๕.๒.๓.๑ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย

๕.๒.๓.๒ ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อมีการ Log-on เข้าสู่ระบบสารสนเทศ

๕.๒.๔ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

๕.๒.๔.๑ ต้องมีกระบวนการจัดการที่ช่วยป้องกันข้อมูลในการส่งมอบให้แก่ผู้ใช้งานเพื่อพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นความลับ และการเก็บรักษาข้อมูลความลับของตัวเอง การส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ

๕.๒.๔.๒ พนักงานบริษัท สกายไอซีที จำกัด(มหาชน) ต้องปฏิบัติตามระเบียบปฏิบัติเรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ

๕.๒.๕ การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕.๒.๖ การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights)

๕.๒.๖.๑ สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ

๕.๒.๖.๒ ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ตามระเบียบปฏิบัติ

๕.๓ การควบคุมการเข้าถึงระบบ (System and application access control)

๕.๓.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๕.๓.๑.๑ ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๕.๓.๑.๒ บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๕.๓.๑.๓ บุคคลภายนอกต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของบริษัท สกายไอซีที จำกัด (มหาชน) อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ

๕.๓.๒ ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure) ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบมีการหน่วงเวลาการให้บริการเป็นเวลา ๕ นาที หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง และต้องวิเคราะห์ทบทวนว่าเป็นการโจมตีหรือไม่อย่างน้อยเดือนละ ๑ ครั้ง

๕.๓.๓ ระบบบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

๕.๓.๔ การใช้โปรแกรมอรรถประโยชน์(Use of Privileged Utility Programs)

๕.๓.๔.๑ การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

๕.๓.๔.๒ ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อปูองกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้เช่น ผู้ใช้งานระบบ เป็นต้น

๕.๓.๕ การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)

ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริงหรือให้บริการเช่น

- ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
- ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

๕.๔ การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services) ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

๕.๔.๑ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”

๕.๔.๒ การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

๕.๔.๓ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๕.๔.๔ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพดังต่อไปนี้

- ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
- ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
- ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
- ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย(Malware) ด้วย
- ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

- การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication)ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

- ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

- การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

- อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

- ผู้ดูแลระบบต้องจากัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” ผ่าน Inception หรือ ติดต่อฝ่ายเทคโนโลยีสารสนเทศของบริษัท

- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๕.๔.๕ กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อ

- เว้นว่างจากการใช้งานไม่เกินกว่า ๓ ชั่วโมง

๕.๔.๖ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๕.๔.๗ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

๕.๔.๘ กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๕.๔.๙ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ คอมพิวเตอร์พุทธศักราช ๒๕๕๐

๕.๔.๑๐ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

- บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน

- มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

- วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

- การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

- การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๕.๔.๑๑ กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

- Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

- Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

๕.๔.๑๒ กำหนดการปูองกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๔.๑๓ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ปูองกันการบุกรุกหรือโปรแกรมในการท า Packet filtering เช่น การใช้ไฟร์วอลล์(Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์(Malware) ด้วย

๕.๔.๑๔ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติโดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕.๔.๑๕ IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการปูองกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการปูองกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๕.๔.๑๖ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๖. การควบคุม การเข้ารหัสข้อมูล (CRYPTOGRAPHY)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม เข้าใจในกระบวนการเข้ารหัสลับ ซึ่งเป็นกระบวนการสำหรับแปรรูปข้อมูลธรรมดาให้อยู่ในรูปที่บุคคลทั่วไปไม่สามารถอ่านได้ถ้าจะอ่านต้องเข้าใจในวิธีการอ่าน รู้ช่องทางในการรับเข้า ในการถอดรหัสที่ตรงกันจึงจะสามารถถอดรหัสได้ และได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

เพื่อกำหนดแนวทางการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และ/หรือป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและความเหมาะสม

นโยบาย

๖.๑มาตรการการเข้ารหัสลับข้อมูล (Cryptographic Controls)

๖.๑.๑ มาตรการการเข้ารหัสลับข้อมูล

ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดมาตรการการเข้ารหัสลับข้อมูล และแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยกำหนดกลุ่มผู้ใช้งานอย่างเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ แต่กรณีที่ไม่สามารถเข้ารหัสได้ ต้องควบคุมการเข้าถึงอย่างเหมาะสมตามหน้าที่และความรับผิดชอบ

๖.๑.๒ การบริหารจัดการกุญแจเข้ารหัสลับข้อมูลฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล ซึ่งประกอบไปด้วย

๖.๑.๒.๑ การพิจารณาประเภทกลุ่มข้อมูลที่นำมาใช้เข้ารหัสว่าสอดคล้องกับการจัดระดับชั้นความลับของข้อมูล และแนวทางการดำเนินการกำกับข้อมูล

๖.๑.๒.๒ การเลือกใช้การเข้ารหัสข้อมูลให้สามารถดำเนินการได้ ๒ แบบ ดังนี้

- แบบ Symmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสเดียวกัน (Secret Key)
- แบบ Asymmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคู่ (Public/Private Key)

โดยพิจารณาวิธีการเข้ารหัสแต่ละรูปแบบ อ้างอิง “รูปแบบการเข้ารหัสข้อมูล” รวมทั้ง ใช้อัลกอริทึมที่เหมาะสม

๖.๑.๓ ดำเนินการสร้างกุญแจรหัสจากโปรแกรมที่น่าเชื่อถือ โดยแนวทางการสร้างกุญแจรหัส และการบริหารจัดการกุญแจรหัส (Key Management)

๖.๑.๔ ดำเนินการนำข้อมูลผ่านกระบวนการเข้ารหัส เพื่อนำข้อมูลที่เข้ารหัสไปใช้ตามจุดประสงค์ต่อไป

๗. การควบคุม ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (PHYSICAL AND ENVIRONMENTAL SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีผลต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัท มีการป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินงานของบริษัท

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับกับผู้ใช้งานและผู้ให้บริการภายนอก

นโยบาย

๗.๑ พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

๗.๑.๑ ข้อกำหนดทั่วไป

- ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน
- ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย ประกอบด้วยกล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกัน ภัยคุกคามจากผู้บุกรุก เป็นต้นในพื้นที่ใช้งานระบบสารสนเทศของบริษัทได้แก่ ห้อง Server/Data Center เพื่อให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัย หน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศใน “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” ให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ
- ต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน

๗.๑.๒ การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)

หน่วยงานที่เกี่ยวข้องกับการบริหารจัดการอาคารและสถานที่ต้องจัดให้มีการควบคุมการเข้าออกในบริเวณ“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะ “พนักงานบริษัท สกายไอซีที จำกัด (มหาชน)” ที่มีสิทธิ์เท่านั้น และมีแนวทางปฏิบัติดังนี้

๗.๑.๒.๑ ต้องกำหนด “พนักงานบริษัท สกายไอซีที จำกัด (มหาชน) และ บริษัท ในเครือ” ที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน

๗.๑.๒.๒ “พนักงานบริษัท สกายไอซีที จำกัด (มหาชน) และ บริษัท ในเครือ” จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๗.๑.๒.๓ หากมีบุคคลอื่นใดที่ไม่ใช่ “พนักงานบริษัท สกายไอซีที จำกัด (มหาชน) และ บริษัท ในเครือ” ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่

อนุญาตให้เข้าพื้นที่) และต้องมีการบันทึกข้อมูลการเข้าออกศูนย์ปฏิบัติการ ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย ๑ ปี

๗.๑.๒.๔ บุคคลภายนอกต้องทำการแลกบัตรประจำตัวของตนที่ออกให้โดยหน่วยงานของรัฐ ตัวอย่างเช่น บัตรประชาชน ใบขับขี่ พาสปอร์ต ฯลฯ กับบัตรผู้มาติดต่อของหน่วยงาน ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่

๗.๑.๒.๕ พนักงานบริษัท สกายไอซีที จำกัด (มหาชน) และ บริษัท ในเครือและบุคคลภายนอก ต้องติดบัตรเจ้าหน้าที่หรือบัตรผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่บริษัท ทั้งนี้บัตรประจำตัวและบัตรผู้มาติดต่อ ไม่อนุญาตให้โอนกรรมสิทธิ์หรือหยิบยืมกันใช้งาน

๗.๑.๒.๖ พนักงานบริษัท สกายไอซีที จำกัด (มหาชน) และ บริษัท ในเครือ ต้องไม่เปิดประตูบริษัททิ้งไว้หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่โดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้เพื่อเป็นการป้องกันการเข้าถึงพื้นที่บริษัท และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๗.๑.๒.๗ ผู้ใช้งานต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยทันทีเมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่แขวนบัตรเจ้าหน้าที่หรือบัตรผู้มาติดต่อในพื้นที่

๗.๑.๒.๘ พนักงานบริษัท สกายไอซีที จำกัด (มหาชน) และ บริษัท ในเครือ ควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่

๗.๑.๓ การรักษาความมั่นคงปลอดภัยบริษัท ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

๗.๑.๓.๑ ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับบริษัท ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก บริษัทหรือห้องจะต้อง ไม่มีป้าย หรือ สัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าวประตูหน้าต่างของบริษัท หรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

๗.๑.๓.๒ เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๗.๑.๓.๓ ข้อมูล สื่อบันทึก วัสดุและอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุมหรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๗.๑.๓.๔ ข้อมูล สื่อบันทึก วัสดุและอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม วิธีการทำลายข้อมูล สื่อบันทึก วัสดุและอุปกรณ์เหล่านี้โดยปฏิบัติตามเอกสารระเบียบปฏิบัติเรื่องการทำลาย

๗.๑.๓.๕ เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๗.๑.๔ การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environmental threats) การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ ดังนี้

มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม้ น้ำท่วม

- มีอุปกรณ์ดับเพลิงตามมาตรฐาน
- มีระบบปรับอากาศและความคุมความชื้น

- แผน คู่มือ การซักซ้อม และการสรุปผล การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม

- มีแผนการใช้งานด้าน Disaster Recovery Site หรือระบบคอมพิวเตอร์สำรองเมื่อมีเหตุการณ์ด้านภัยพิบัติของสภาพแวดล้อมขึ้น

๗.๑.๕ การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working in secure areas) ขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย

- ต้องรายงานการปฏิบัติงานและการตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่กำหนดไว้ นอกจากนี้ ในกรณีที่ได้ใช้บริการงานสนับสนุนด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกบริษัท ต้องมีระบบการตรวจสอบการปฏิบัติงานของบุคคลภายนอกอย่างรอบคอบและรัดกุมเพียงพอ เช่น มีการตรวจสอบบันทึกการทำงาน (log files) ของบุคคลภายนอก และกำหนดให้บุคคลภายนอกรายงานการปฏิบัติงาน เป็นต้น

- แต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น

- หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ”และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

๗.๑.๖ พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

๗.๑.๖.๑ หน่วยงานต้องมีการจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทำงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น บริเวณเก็บและจัดส่งสินค้าจะต้องไม่อยู่ในพื้นที่ ๆ บุคคลภายนอกเข้าถึงได้

๗.๑.๖.๒ เจ้าหน้าที่และเจ้าหน้าที่ของหน่วยงานภายนอก (Third Party) ต้องติดบัตรประจำตัวตลอดเวลาขณะปฏิบัติหน้าที่ในบริเวณ และหากผู้ใดพบเห็นผู้ที่ไม่ติดบัตรประจำตัวถือเป็นหน้าที่ที่จะต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยโดยทันที

๗.๒ ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security) เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

๗.๒.๑ การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิตปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำจัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลังจัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗.๒.๑.๑ จัดสรรพื้นที่ในการติดตั้งอุปกรณ์ที่มีความสำคัญให้เข้าถึงยาก

๗.๒.๑.๒ การติดตั้งอุปกรณ์ต้องติดตั้งในตู้เก็บอุปรกรณ์ให้มิดชิด

๗.๒.๒ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ กำหนดให้มีการดูแลรักษาอุปกรณ์Utilities ที่เกี่ยวข้อง เช่น Uninterruptible Power Supply (UPS) อุปกรณ์ตรวจจับความชื้น อุปกรณ์ตรวจจับควัน เป็นต้น มีการตรวจสอบการให้บริการของอุปกรณ์อย่างน้อยปีละ ๒ ครั้ง ยกตัวอย่างการแบ่งระดับความเสี่ยง ดังนี้

๗.๒.๒.๑ ความเสี่ยงสูง ต้องมีระบบสำรองไฟฟ้าทั้ง UPS และ เครื่องกำเนิดไฟฟ้า

๗.๒.๒.๒ ความเสี่ยงปานกลาง ต้องมีระบบสำรองไฟฟ้า UPS

๗.๒.๒.๓ ความเสี่ยงต่ำมีระบบสำรองไฟฟ้าหรือไม่ก็ได้

๗.๒.๓ ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

มีการป้องกันการเดินสายไฟฟ้า หรือสายเคเบิ้ลเข้ามาภายในอาคารบริษัท บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารบริษัท และมีการติดตั้งตู้พักสาย ต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะพนักงานที่หรือบุคคลที่มีสิทธิ์เท่านั้น

๗.๒.๓.๑ ความเสี่ยงสูง การเดินสายต้องใช้สายป้องกันการรบกวนสัญญาณและการเข้าถึงสายสัญญาณ

๗.๒.๓.๒ ความเสี่ยงปานกลาง การเดินสายต้องป้องกันการเข้าถึงสายสัญญาณ

๗.๒.๓.๓ ความเสี่ยงต่ำใช้สายสัญญาณธรรมดา

๗.๒.๓.๔ ต้องมีแผนการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร

๗.๒.๔ การบำรุงรักษาอุปกรณ์ (Equipment maintenance) อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มีสภาพความพร้อมใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง โดยจะแบ่งเป็นระดับของความเสี่ยง ดังนี้

๗.๒.๔.๑ ระบบที่มีความเสี่ยงสูงต้องบำรุงรักษาทุก ๑ เดือน

๗.๒.๔.๒ ระบบที่มีความเสี่ยงปานกลางต้องบำรุงรักษาทุก ๓ เดือน

๗.๒.๔.๓ ระบบที่มีความเสี่ยงต่ำต้องบำรุงรักษาทุก ๑๒ เดือน

๗.๒.๕ การนำทรัพย์สินของบริษัทออกนอกบริษัท (Removal of assets) อุปกรณ์สารสนเทศหรือซอฟต์แวร์ต้องไม่มีการนำออกนอกบริษัท โดยไม่ได้รับอนุญาต หากมีความประสงค์จะนำออกจากพื้นที่ต้องแจ้งต่อผู้บังคับบัญชาหรือผู้มีอำนาจในการอนุญาต โดยต้องปฏิบัติตามระเบียบปฏิบัติ

๗.๒.๖ ความมั่นคงปลอดภัยของอุปกรณ์ และทรัพย์สินที่ใช้งานอยู่ภายนอกบริษัท (Security of equipment and assets off premises) ทรัพย์สินที่ใช้งานอยู่ภายนอกบริษัทต้องมีการรักษาความมั่นคงปลอดภัย โดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกบริษัท

๗.๒.๗ ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or reuse of equipment) อุปกรณ์ที่มีสื่อบันทึกข้อมูล ต้องมีการตรวจสอบเพื่อให้มั่นใจว่า ข้อมูลสำคัญของซอฟต์แวร์ที่มีใบอนุญาต มีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์หรือก่อนการนำอุปกรณ์ไปใช้งานอย่างอื่น

๗.๒.๘ อุปกรณ์ของผู้ใช้งานที่ ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment) ผู้ใช้งานต้องมีการป้องกันอุปกรณ์อย่างเหมาะสม ซึ่งเป็นอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล

๗.๒.๙ นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

เอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ เมื่อมีการนำมาใช้งาน ต้องทำเรื่องขออนุญาตการนำไปใช้งานงานและกำหนดระยะเวลาเริ่มใช้งาน ระบุระยะเวลาในการนำส่งคืน ระบุถึงการจัดเก็บในระยะเวลาการใช้งาน

๘. การควบคุม ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (OPERATION SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่าการปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย สารสนเทสและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี มีการป้องกันการสูญหายของข้อมูล มีการบันทึกเหตุการณ์และจัดทำหลักฐาน และมีการป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

นโยบาย

๘.๑ ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

๘.๑.๑ มีการแบ่งมอบหมายและจัดแบ่งหน้าที่ความรับผิดชอบอย่างชัดเจนรวมทั้งมีขั้นตอนคู่มือการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures) และสามารถเข้าถึงได้โดยผู้ที่จำเป็นต้องใช้งานและมีระบบการควบคุมกำกับ ติดตามประเมินผลการปฏิบัติงานตามหน้าที่ความรับผิดชอบอย่างต่อเนื่อง

๘.๑.๒ การบริหารจัดการเปลี่ยนแปลง (Change management)

เพื่อควบคุมการเปลี่ยนแปลงระบบสารสนเทศ และบริการของบริษัทให้มั่นใจว่าการเปลี่ยนแปลงปรับปรุง แก้ไขระบบสารสนเทศ และบริการได้รับการควบคุมตลอดระยะเวลาที่มีการเปลี่ยนแปลงรวมถึงลดความเสี่ยงที่อาจเกิดความเสียหายจากการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบสารสนเทศและบริการ

๘.๑.๒.๑ ต้องมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ทุกครั้ง โดยปฏิบัติตามวิธีการปฏิบัติงานเรื่องการจัดการการเปลี่ยนแปลงสารสนเทศ (Change Management)

๘.๑.๒.๒ เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ เช่น ระบบปรับอากาศ น้ำ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ

๘.๑.๒.๓ เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง

๘.๑.๒.๔ ตาราง และ/หรือ แผนการเปลี่ยนแปลงทุกครั้งต้องได้รับความเห็นชอบจากผู้มีอำนาจในการาอนุมัติก่อนจะทำการเปลี่ยนแปลง

๘.๑.๒.๕ บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบโดยบันทึกฯ ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- วันที่ รับเรื่อง และวันที่ ทำการเปลี่ยนแปลง
- เจ้าของข้อมูล และผู้ดูแลระบบ
- วิธีการเปลี่ยนแปลง
- ผลของการเปลี่ยนแปลง (สำเร็จ หรือ ล้มเหลว)

๘.๑.๓ การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

เพื่อเป็นแนวทางในการบริหารจัดการทรัพยากรระบบของบริการให้เพียงพอตามข้อตกลงระดับการให้บริการ และต่อการให้บริการผู้มาติดต่อบริษัท หรือผู้ใช้งานทั้งในปัจจุบันและในอนาคต

๘.๑.๓.๑ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ดูแลข้อมูล

๘.๑.๓.๒ มีการวางแผนการตรวจสอบประเมินขีดความสามารถของระบบและกำหนดค่าสูงสุดที่ยอมรับได้ของขีดความสามารถของระบบทั้งทางด้านอุปกรณ์ระบบคอมพิวเตอร์ และระบบเครือข่าย อย่างน้อยการประเมินค่า CPU, RAM, Storage, Network Utilization

๘.๑.๓.๓ ดำเนินการตรวจสอบประเมินขีดความสามารถของระบบดังระบุข้างต้น

๘.๑.๓.๔ ดำเนินการวิเคราะห์ ประมวลผล ขีดสมรรถนะของระบบเพื่อค้นหาสาเหตุและปัญหารวมทั้งแนวทางการแก้ไขอย่างเป็นระบบ รวมทั้ง ติดตาม ปรับปรุง และคาดการความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพ

๘.๑.๓.๕ สรุปผลการบริหารจัดการขีดสมรรถนะของระบบ

๘.๑.๔ การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments)

ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบ ออกจากกับเครื่องที่ใช้งานจริงหากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย

๘.๒ การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

๘.๒.๑ มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

๘.๒.๑.๑ เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุดที่ได้รับการอนุมัติจาก บริษัท และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

๘.๒.๑.๒ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

๘.๒.๑.๓ เอกสารการติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก ๖ เดือน และต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย

๘.๒.๑.๔ ห้ามพนักงานทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติ หลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน

๘.๒.๑.๕ ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส

๘.๒.๑.๖ ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใด ๆ ตัวอย่างเช่น ไวรัส หนอนอินเทอร์เน็ตโปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ของบริษัท

๘.๒.๑.๗ ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๘.๒.๑.๘ ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับ - ส่งผ่านระบบเครือข่ายของบริษัท ได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก และจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสของบริษัท ก่อนเปิดใช้งานเสมอ

๘.๒.๑.๙ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ตยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

๘.๒.๑ มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware) มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

๘.๒.๒ ตั้งค่าให้ซอฟต์แวร์ Anti-malware อัปเดตซอฟต์แวร์ และปรับปรุงค่า Signature ทุกวัน

๘.๓ การสำรองข้อมูล (Backup)

เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัยธรรมชาติ ระบบเสียหาย ฯลฯ

๘.๓.๑ การสำรองข้อมูล (Information Backup)

๘.๓.๑.๑ ต้องกำหนดความถี่ในการทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล

๘.๓.๑.๒ ต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา

๘.๓.๑.๓ ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการปูองกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

๘.๓.๑.๔ ต้องกำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง

๘.๓.๑.๕ ต้องมีกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบเป็นระยะ ๆ

๘.๓.๑.๖ ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง

๘.๓.๑.๗ ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

๘.๓.๑.๘ ต้องลงบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูล ต้องได้รับการตรวจสอบเป็นประจำทุกปี

๘.๓.๑.๙ กระบวนการในการเก็บข้อมูลระหว่างสถานที่ระบบคอมพิวเตอร์และสถานที่เก็บข้อมูลต้องได้รับการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง

๘.๓.๑.๑๐ สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- ชื่อระบบ
- วันสร้าง
- ระดับความสำคัญของข้อมูล
- รายละเอียดติดต่อผู้ดูแลข้อมูล
- วิธีการเก็บรักษาสื่อบันทึก เช่น สำรอง online /Hard copy

๘.๔ การบันทึกข้อมูลการใช้งาน และการเฝ้าระวัง (Logging and Monitoring)

๘.๔.๑ การบันทึกข้อมูลเหตุการณ์ (Event logging)

มีการบันทึกการทำงานของระบบที่ไม่เป็นไปตามปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บและทบทวนอย่างสม่ำเสมอ รวมทั้งกำหนดวิธีการและระยะเวลาในการจัดเก็บให้สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๘.๕ การป้องกันข้อมูลล็อก (Protection of log information)

๘.๕.๑ อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต

๘.๕.๒ ต้องมีการตรวจสอบติดตามประเมินผลระบบการป้องกันข้อมูลล็อกที่มีประสิทธิภาพ

๘.๖ ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ(Administrator and operator logs)

๘.๖.๑ กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อกข้อมูลดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ

๘.๗ การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

๘.๗.๑ ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในหน่วยงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ถูกบุกรุกตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๘.๘ การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operation software)

๘.๘.๑ การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operation systems)

๘.๘.๑.๑ วิเคราะห์วางแผนการติดตั้งซอฟต์แวร์บนระบบการให้บริการเพื่อป้องกันความเสี่ยงต่อผลกระทบในการติดตั้งซอฟต์แวร์ระบบให้บริการที่อาจเกิดความล้มเหลว

๘.๘.๑.๒ มีขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมีการปฏิบัติตามให้สอดคล้อง

๘.๘.๑.๓ สรุปวิเคราะห์ประเมินผล การติดตั้งซอฟต์แวร์ เพื่อนำไปสู่การปรับปรุงวางแผนการติดตั้งซอฟต์แวร์

๘.๙ การบริการจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

๘.๙.๑ การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

๘.๙.๑.๑ มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

๘.๑๐ การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation)

๘.๑๐.๑ บริษัท ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

๘.๑๐.๒ บริษัท ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด(Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

๘.๑๐.๓ ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท โดยเด็ดขาด

๘.๑๐.๔ เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่บริษัท มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอจึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัท เพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตและในขณะเดียวกันไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

๘.๑๐.๕ บริษัท กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ ๒ ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าบริษัท มีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น สำนักงานอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

๙. การควบคุม ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (COMMUNICATIONS SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการป้องกันสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในบริษัท และภายนอกบริษัท

นโยบาย

๙.๑ การควบคุมการเข้าถึงเครือข่าย (Network Control)

๙.๑.๑ ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

๙.๑.๒ การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย

๙.๑.๓ ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่หน่วยงานนั้นรับผิดชอบ

๙.๑.๔ ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

๙.๑.๕ บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทด้วย

๙.๒ การรักษาความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

๙.๒.๑ ระบบเครือข่ายทั้งหมดของบริษัท ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

๙.๒.๒ ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดเฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์ และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานได้จริงของบริษัท ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายบริษัทได้

๙.๒.๓ ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตนเอง หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัทโดยไม่ได้รับอนุญาต

๙.๒.๔ ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทโดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

๙.๒.๕ ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด

๙.๒.๖ ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัททำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัทโดยเด็ดขาด

๙.๓ การจัดแบ่งเครือข่ายภายในบริษัท (Segregation in Network)

๙.๓.๑ ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๙.๓.๒ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๙.๔ การถ่ายโอนสารสนเทศ (Information transfer)

๙.๔.๑ นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

๙.๔.๑.๑ กำหนดนโยบาย ขั้นตอนการปฏิบัติงาน และมาตรการรองรับ โดยผ่านช่องทางการสื่อสารทุกชนิด

๙.๔.๒ ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

๙.๔.๒.๑ กำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น

๙.๔.๒.๒ กำหนดข้อตกลง แนวทาง วิธีปฏิบัติ ระยะเวลา ของการถ่ายโอนสารสนเทศ

๙.๔.๒.๓ มีการบันทึก วันเวลาที่มีการถ่ายโอนสารสนเทศในระหว่างบริษัท

๙.๔.๒.๔ จำกัดการเข้าถึงสารสนเทศเมื่อมีการโอนย้ายเสร็จสิ้นแล้ว

๙.๔.๓ การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic massaging)

๙.๔.๓.๑ กำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

๙.๔.๔ ข้อตกลงการรักษาความลับหรือไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

๙.๔.๔.๑ ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) ซึ่งเป็นไปตามความต้องการด้านการป้องกันข้อมูลของบริษัทและมีการทบทวนอย่างสม่ำเสมอ

๙.๔.๔.๒ พนักงาน บุคคล หรือผู้ติดต่อจากหน่วยงานอื่น ที่มีส่วนต้องเข้าถึงสารสนเทศของบริษัท ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และ “ผู้ติดต่อ” ว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement: NDA)

๑๐. การควบคุม การจัดหา การพัฒนา และการบำรุงรักษาระบบ (SYSTEM ACQUISITION,DEVELOPMENT AND MAINTENANCE)

วัตถุประสงค์

เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการใช้บริการผ่านเครือข่ายสาธารณะด้วย เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบ และดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

นโยบาย

๑๐.๑ ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

๑๐.๑.๑ การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ(Information security requirements analysis and specification)

๑๐.๑.๑.๑ ระบบสารสนเทศใหม่ ต้องมีการรักษาความปลอดภัย ที่สอดคล้องและสามารถเชื่อมโยงกับระบบเดิมได้ ระบบสารสนเทศเก่า จะต้องมีการป้องกันการเข้าใช้ server โดยอนุญาตให้เฉพาะบุคคลที่มีหน้าที่การทeงานโดยใช้การ login ด้วย user name และ password ของบุคคลนั้น และการยืนยันการเข้าใช้ว่าเป็นบุคคลไม่ใช่ program การ update ต่าง ๆ ต้องเป็นแบบ manual เท่านั้น

๑๐.๑.๑.๒ ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกัน

- จากการเปลี่ยนแปลงข้อมูลบนเครือข่ายสาธารณะโดยการกำหนด user name และpassword ของผู้เข้าถึงข้อมูล
- ข้อมูลต้องระบุได้ว่าบุคคลใดเป็นผู้สร้างข้อมูลและมีการ สำเนา/สำรอง ข้อมูลทุกครั้งเพื่อสามารถย้อนดูข้อมูลเก่า ณ เวลานั้นได้
- การเปิดเผยข้อมูลบนเครือข่ายสาธารณะ ต้องได้รับการอนุญาตของผู้ดูแลระบบเท่านั้น
- ไม่อนุญาตให้แก้ไขข้อมูลใด ๆ ที่ถูกสร้างขึ้น

๑๐.๑.๑.๓ การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ให้มีการตั้งระบบตอบกลับการส่งข้อมูลพร้อมทั้งมีการเข้ารหัสข้อมูลและมีการยืนยันตัวบุคคล

๑๐.๒ ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

๑๐.๒.๑ นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

- ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบายหรือข้อกำหนดที่บริษัทกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

๑๐.๒.๒ ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

- แต่งตั้งคณะทำงานดูแลการเข้าใช้งานระบบ และตั้งข้อปฏิบัติในการเข้าใช้งาน

- ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น

- คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์

- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ

- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข

- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ

- ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

๑๐.๒.๓ การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ(Technical review of applications after operating platform changes)

- ทำการทดสอบระบบทุกครั้งเมื่อมีการเปลี่ยนแปลงโครงสร้าง เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ต่าง ๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

๑๐.๒.๔ การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

การใช้ซอฟต์แวร์ของผู้ผลิตจะใช้การแก้ไขโดยผ่านทาง firewall และกำหนดให้มีการ Update firewall ต่าง ๆ ให้เป็นแบบ Manual เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

๑๐.๒.๕ หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

- มีคำสั่งจัดตั้งคณะกรรมการระบบด้านความมั่นคงปลอดภัย เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ

- จัดทำแบบแปลนโครงสร้างทางวิศวกรรมและสามารถรองรับการแก้ไขเพิ่มเติมในอนาคตได้

- ตรวจทาน ปรับปรุง แก้ไขและทดสอบระบบทุก ๆ จุดและกระจายการออกแบบไปยังส่วนกลาง

๑๐.๒.๖ สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

- แต่งตั้งคณะกรรมการเพื่อศึกษาสภาพแวดล้อมของการพัฒนาระบบ

- จ้างบริษัทที่มีมาตรฐานเพื่อเข้ามาจัดทำระบบ

๑๐.๒.๗ การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

- จัดบุคลากรสุ่มตรวจสอบซอฟต์แวร์

- การทำสัญญาว่าจ้างการพัฒนาระบบของบริษัท ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

๑๐.๒.๘ การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

- มีการกำหนดผลลัพธ์ที่ต้องการในการทดสอบด้านความมั่นคงปลอดภัย

๑๐.๒.๙ การทดสอบเพื่อรับรองระบบ (System acceptance testing)

- มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่ และระบบที่ปรับปรุง

- ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มีการเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ

๑๐.๓ ข้อมูลสำหรับการทดสอบ (Test data)

๑๐.๓.๑ การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

- ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อนเมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

๑๑. การควบคุม ความสัมพันธ์กับผู้ให้บริการภายนอก (SUPPLIER RELATIONSHIPS)

วัตถุประสงค์

การใช้บริการจากผู้ให้บริการภายนอก อาจก่อให้เกิดความเสี่ยงได้ ได้แก่ ความเสี่ยงต่อการเข้าถึงข้อมูลความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้นจึงจำเป็นต้องมีการควบคุมผู้ให้บริการภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางการคัดเลือก ควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก

นโยบาย

๑๑.๑ ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)

๑๑.๑.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships) ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินของบริษัทโดยผู้ให้บริการภายนอก ต้องมีการกำหนดตกลงกับผู้ให้บริการภายใน และจัดทำเป็นลายลักษณ์อักษร

- บริษัทต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณา หรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้ผู้ให้บริการภายนอก หรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของบริษัท
- ผู้ดูแลระบบและฝ่ายต่าง ๆ ที่รับผิดชอบในการประสานงานกับผู้ให้บริการภายนอก ต้องกำกับให้มีการดูแลให้บุคคลหรือผู้ให้บริการภายนอกแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

๑๑.๑.๒ การควบคุมการเข้าใช้งานของผู้ให้บริการภายนอก (Third Party)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผล และมีมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบได้
- ผู้ให้บริการภายนอก (Third Party) ที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของบริษัทจะต้องทำเรื่องขออนุมัติจากผู้จัดการฝ่ายและสำนักเจ้าของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าวเป็นลายลักษณ์อักษร ซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

  เหตุผลในการขอใช้

  ระยะเวลาในการใช้

  การตรวจสอบความปลอดภัยของอุปกรณ์เชื่อมต่อเครือข่าย

  การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล
- ผู้ให้บริการภายนอก (Third Party) ไม่ว่าจะปฏิบัติงานอยู่ภายในบริษัทหรือนอกบริษัทต้องลงนามในสัญญาการรักษาข้อมูลที่เป็นความลับของบริษัท
- เจ้าของระบบมีหน้าที่กำหนดและทบทวนสิทธิของการเข้าใช้งานระบบสารสนเทศเฉพาะบุคคลที่จำเป็นเท่านั้น และมีการทบทวนสิทธิให้เป็นปัจจุบัน

- บริษัทต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของผู้ให้บริการภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศ

- บริษัทมีสิทธิในการตรวจสอบตามสัญญาจ้างเพื่อให้มั่นใจได้ว่าบริษัทสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

- ในกรณีที่มีการเปลี่ยนแปลงการดำเนินงาน ผู้ให้บริการจากภายนอกต้องแจ้งให้บริษัทรับทราบและอนุมัติการเปลี่ยนแปลงนั้น ก่อนการดำเนินงาน เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

- เมื่อสิ้นสุดระยะเวลาการใช้งาน บริษัทต้องดำเนินการยกเลิกสิทธิในการเข้าถึงแหล่งข้อมูล และแจ้งผู้จัดการฝ่ายและสำนักเจ้าของข้อมูล

- หากพบเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศให้แจ้งไปยังเจ้าของระบบ

- ต้องดำเนินการตามนโยบายความมั่นคงปลอดภัยสารสนเทศที่บริษัทประกาศไว้อย่างเคร่งครัด

๑๑.๑.๓ การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการผู้ให้บริการภายนอก (Assessing security within supplier agreements) ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนด และตกลงกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการ โครงสร้างพื้นฐานของระบบสำหรับสารสนเทศของบริษัท โดยผู้ให้บริการภายนอก

- บริษัทต้องแสดงนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่ผู้ให้บริการภายนอกที่เกี่ยวกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการสารสนเทศของบริษัท

- ผู้ให้บริการภายนอกต้องยอมรับนโยบาย กฎหมายที่เกี่ยวข้องและการควบคุมด้านความมั่นคงปลอดภัยของบริษัท

- บริษัทมีสิทธิที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของผู้ให้บริการภายนอก

๑๑.๑.๔ ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศ และการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain) ข้อตกลงกับผู้ให้บริการภายนอกต้องรวมความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

- ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร

- ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูล และระบบสารสนเทศหรืออุปกรณ์ดังกล่าวได้

๑๑.๒ การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ ของผู้ให้บริการภายนอก

๑๑.๒.๑ การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

- บริษัท ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับบริษัท ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก

- ต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๑๑.๒.๒ การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

- การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของบริษัท ทุกครั้ง ต้องเป็นไปตามเอกสาร

- การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

๑๒. การควบคุม การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY INCIEDNT MANAGEMENT)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และมีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของบริษัท

นโยบาย

๑๒.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และการปรับปรุง (Management of information security incidents and improvements)

๑๒.๑.๑ บริษัทต้องมีการกำหนดหน้าที่ความรับผิดชอบ และกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับเหตุละเมิดด้านความมั่นคงปลอดภัยอย่างทันท่วงที

๑๒.๑.๒ บริษัทต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดออกจากเหตุการณ์ด้านการปฏิบัติงานทั่วไปเพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม

๑๒.๑.๓ บริษัทต้องกำหนดช่องทาง และเกณฑ์ในการรายงานเหตุการณ์ หรือจุดอ่อนหรือเหตุการณ์ความมั่นคงสารสนเทศ หรือสื่อสารให้บุคลากรในองค์กร และหน่วยงานภายนอกรับทราบ

๑๒.๒ การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องมีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสม และรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

๑๒.๒.๑ ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท โดยผ่านช่องทางรายงานที่กำหนดไว้จะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ โดยปฏิบัติตามเอกสารวิธีปฏิบัติงานเรื่องการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๑๒.๒.๒ ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในบริษัท ต่อผู้บังคับบัญชาหรือหน่วยงานจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

๑๒.๒.๓ ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อ IT-Security officer ทันที

๑๒.๒.๔ ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงาน IT-Security officer ทันที

๑๒.๒.๕ ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในบริษัทต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย IT-Security officer และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

๑๒.๒.๖ การกระทำอื่น ๆ ที่ถือเป็นข้อห้ามของบริษัท มีดังนี้

- การกระทำใด ๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่น ๆ ที่กล่าวถึงด้านล่างนี้ถือเป็นข้อห้ามของบริษัท ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาดทั้งนี้บริษัท มิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น

หมายเหตุ: พนักงานบางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงระบบเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ

- การใช้งานทรัพยากรของบริษัท เพื่อการจัดหาหรือส่งต่อ วัสดุ เอกสาร หรือรูปภาพลามกอนาจาร หรือที่ขัดต่อกฎหมาย

- การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่บริษัทกำหนดให้ เพื่อเสนอขายสินค้าหรือบริการใด ๆ

- การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่ายตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ Sniffing, Pinged Floods, Pack Spoofing, Denial of Service และForged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น

- การใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing

- การทำ Port Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย

- การดักฟังหรือดักจับข้อมูลที่พนักงานไม่ได้รับอนุญาตให้รับรู้ด้วยวิธีการใด ๆ เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย

- การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

- การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ระบบเครือข่ายใด ๆ

- การใช้โปรแกรม/สคริปต์/คำสั่ง หรือการส่งข้อความใด ๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่าง ๆ

- การให้ข้อมูลลับเกี่ยวกับรายชื่อพนักงาน รายชื่อลูกค้า ความลับของบริษัท และข้อมูลลับอื่น ๆ แก่บุคคลภายนอก

- การข่มขู่คุกคามทุกรูปแบบผ่านอีเมล์ โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษา ความถี่ หรือขนาดของข้อความการแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)

- การละเมิดสิทธิ์ส่วนบุคคล ลิขสิทธิ์ของบริษัท ความลับของบริษัท สิทธิบัตร ทรัพย์สินทางปัญญา หรือกฎหมายอื่นใด

๑๒.๓ การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)

พนักงานและผู้ที่ทำสัญญาจ้าง ซึ่งใช้ระบบและบริการสารสนเทศของบริษัท ต้องสังเกตและรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศในระบบหรือบริการที่สังเกตพบหรือที่สงสัย แบ่งเป็นระดับเหตุการณ์ได้ดังนี้

- เกณฑ์เหตุการณ์อยู่ในระดับต่ำ

ผู้ดูแลระบบสารสนเทศของฝ่ายสามารถแก้ไขเหตุการณ์ที่เกิดขึ้นเองได้ เช่นการติดไวรัส เป็นต้น และทำการรายงานเหตุการณ์ที่เกิดขึ้น ทุก ๆ ๑ เดือน

- เกณฑ์เหตุการณ์อยู่ในระดับกลาง

ผู้ดูแลระบบสารสนเทศฝ่ายแจ้งให้ผู้บังคับบัญชา ทราบถึงเหตุการณ์ที่เกิดขึ้น หากเหตุการณ์ที่เกิดขึ้นฝ่าย ประเมินความเสี่ยงแล้ว ให้ฝ่ายแจ้งเป็นลายลักษณ์อักษร แจ้งไปยังฝ่ายเทคโนโลยีสารนสนเทศของบริษัท เพื่อเข้ามาแก้ไขเหตุการณ์ที่เกิดขึ้น

- เกณฑ์เหตุการณ์อยู่ในระดับสูง

ผู้ดูแลระบบสารสนเทศของฝ่ายต้องทำการแจ้งฝ่ายเทคโนโลยีสารนสนเทศของบริษัทอย่างเร่งด่วนหากเหตุการณ์ที่เกิดขึ้น เป็นเหตุการณ์ร้ายแรง และเร่งด่วน เพื่อหาแนวทางในการแก้ไขปัญหา จากนั้นทำการสรุปปัญหาที่เกิดขึ้นกับระบบสารสนเทศฝ่ายให้ผู้บริหารระดับสูงทราบ

๑๒.๔ การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องมีการประเมินและต้องมีการตัดสินใจว่า สถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่ จากกระบวนการดังนี้

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ : ต้องกำหนดนโยบายให้กับบุคลากรและผู้ดูแลระบบในหน่วยงาน นั้น ๆ ปฏิบัติตามนโยบายที่วางไว้

- ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติและการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ จะถูกทำการวิเคราะห์ และหาสาเหตุของการบุกรุก ในระบบสารสนเทศของบริษัท เพื่อเป็นเครื่องมือสืบสวน หาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด

ผู้ดูแลระบบ : ต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติและการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ

- ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกหรือโจมตีกรม เป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟวอลล์เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตราย ที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ hacker รวมทั้ง ไวรัสประเภทต่าง ๆ

ผู้ดูแลระบบ : ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับบริษัท

- ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับบริษัท และจัดทำวิธีปฏิบัติที่ถูกต้อง ให้กับบริษัทเพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ

๑๒.๕ การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents) เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

๑๒.๕.๑ มีการกำหนดขั้นตอนไว้รองรับกรณีเกิดเหตุการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัย

๑๒.๕.๒ เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

๑๒.๕.๓ โดยได้จัดทำแยกประเภทตามระบบต่าง ๆ ดังนี้

๑๒.๕.๓.๑ ระบบป้องกันผู้บุกรุก

ดำเนินการตรวจสอบ Log File หรือรายงานของระบบปูองกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

๑๒.๕.๓.๒ ระบบไฟร์วอลล์

ดำเนินการตรวจระบบปูองกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีของเครือข่ายใดถูก Block เป็นจำนวนมาก

<u>หมายเหตุ</u> กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๑๒.๕.๓.๓ ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในบริษัทไปยังภายนอกหรือไม่

ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของบริษัท

ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

๑๒.๖.๑ การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องถูกนำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

๑๒.๖.๑.๑ ผู้ดูแลระบบต้องบันทึกเหตุละเมิดด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคามหรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขจากเหตุการณ์ที่เกิดขึ้นเพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๑๒.๖.๑.๒ หน่วยงานที่รับผิดชอบ ต้องจัดทำสรุปรายงานการแจ้งเหตุละเมิดความมั่นคงปลอดภัยให้ผู้บังคับบัญชาอย่างน้อยเดือนละ ๑ ครั้ง

๑๒.๖.๑.๓ ต้องมีการทบทวนเหตุละเมิดความมั่นคงปลอดภัย เพื่อป้องกันการเกิดปัญหาเดิมซ้ำ

๑๒.๖.๑.๔ ต้องมีการวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๑๒.๗ การเก็บรวบรวมหลักฐาน (Collection of evidence)

บริษัทต้องกำหนดและประยุกต์ขั้นตอนปฏิบัติสำหรับการระบุ การรวบรวม การจัดหา และจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐานได้

๑๒.๗.๑ หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องดำเนินการให้หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์สืบสวนหรือเป็นหลักฐานในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

๑๒.๗.๒ หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบ บริษัท สกายไอซีที จำกัด (มหาชน) และกฎหมาย (เช่น ๙๐ วัน หรือ ๑ ปีเป็นต้น)

๑๒.๗.๓ หัวหน้าหน่วยงานดูแลรับผิดชอบด้านกฎหมายและหน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษากฎเกณฑ์ที่เกี่ยวข้อง เช่น ถ่อยแถลงในกฎหมายแพ่งหรืออาญา ซึ่งระบุถึงลักษณะของหลักฐานที่ต้องเก็บรวบรวมมา เพื่อใช้ในการดำเนินการทางกฎหมายกับผู้กระทำผิด เป็นต้น

๑๒.๗.๔ หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

๑๓. การควบคุม ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการความต่อเนื่องทางธุรกิจ (INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT)

วัตถุประสงค์

เพื่อเป็นแนวทางในการบริหารจัดการความต่อเนื่องในการดำเนินงานของบริษัท เมื่ออยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ของบริษัทที่สำคัญ มีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP)และแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม เพื่อให้การดำเนินงานของบริษัท เป็นไปอย่างต่อเนื่อง

นโยบาย

๑๓.๑ ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

๑๓.๑.๑ การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

๑๓.๑.๑.๑ บริษัทต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ

๑๓.๑.๑.๒ ต้องจัดทำแนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน ของระบบเทคโนโลยีสารสนเทศควรพิจารณา ดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานของบริษัทและการให้บริการด้านเทคโนโลยีสารสนเทศบริษัท
- การตอบสนองต่อสถานการณ์ฉุกเฉินเพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุมการแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
- การดำเนินการเพื่อให้บริษัทสามารถดำเนินงานเป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญการกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานปกติเพื่อให้การดำเนินงานของบริษัทกลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

๑๓.๑.๒ การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)

บริษัทต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุง กระบวนการขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

๑๓.๑.๒.๑ ต้องจัดตั้ง ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ของระบบเทคโนโลยีสารสนเทศซึ่งประกอบไปด้วย ตัวแทนจากหน่วยงาน เจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลข้อมูล เป็นต้น

๑๓.๑.๒.๒ ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอรวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

๑๓.๑.๓ การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

บริษัทต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมไว้ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้อง และได้ผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น

๑๓.๑.๓.๑ ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่

๑๓.๑.๓.๒ ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย

๑๓.๑.๓.๓ ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรองเพื่อให้สามารถค้นหาได้โดยเร็ว, เพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

๑๓.๑.๓.๔ มีการขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจและควรจัดทำทะเบียนควบคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง

๑๓.๑.๓.๕ ต้องกำหนดขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่ง รวมถึงข้อมูลสำคัญต่าง ๆ ในฮาร์ดดิสก์

๑๓.๒ การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

๑๓.๒.๑ สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

๑๓.๒.๑.๑ มีการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงานด้วยการประเมินความเสี่ยง (Risk Assessment) และ/หรือ การประเมินผลกระทบของกระบวนงานหลัก

๑๓.๒.๑.๒ มีการกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

๑๓.๒.๑.๓ มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

๑๓.๒.๑.๔ มีการกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

๑๓.๒.๑.๕ มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน

๑๓.๒.๑.๖ หน่วยงานที่เป็นหน่วยสำรองข้อมูลหรือจัดเก็บข้อมูลก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน

๑๓.๒.๑.๗ มีการทบทวนหรือปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ (ทุก ๔ เดือน) และเก็บแผนฉุกเฉินไว้ในสถานที่มั่นคงปลอดภัย

๑๓.๒.๑.๘ ทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ ๒ ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง

๑๓.๒.๑.๙ ต้องสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทุกระดับได้รับทราบเฉพาะเท่าที่จำเป็นและควรป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ

๑๓.๒.๑.๑๐ กรณีที่เกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

๑๔. การควบคุม ความสอดคล้อง (COMPLIANCE)

วัตถุประสงค์

เพื่อป้องกันการละเมิดที่เกี่ยวข้องกับการปฏิบัติงาน ระเบียบ ข้อบังคับ เงื่อนไขในสัญญา และข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติงานของบริษัท ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบาย

๑๔.๑ การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

๑๔.๑.๑ การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

๑๔.๑.๑.๑ บริษัท ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๑๔.๑.๑.๒ พนักงาน ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด และมีรายการดังต่อไปนี้เป็นอย่างน้อย

- นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศ
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ลิขสิทธิ์

๑๔.๑.๑.๓ ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นสินทรัพย์ของบริษัท (ยกเว้น ข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตรหรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

๑๔.๑.๑.๔ เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของบริษัท กำหนดไว้

๑๔.๑.๑.๕ บริษัท ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามบริษัท จะดำเนินการตรวจสอบ ดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้นและจะไม่เปิดเผย ข้อมูลใด ๆ ของผู้ใช้งานเว้น แต่เป็น การเปิดเผยตามคำสั่งศาลตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

๑๔.๑.๑.๖ ห้ามพนักงานในบริษัท ใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

๑๔.๑.๑.๗ การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศ ไม่ขัดต่อข้อกฎหมายใด ๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชาและผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

๑๔.๑.๒ สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

สิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ที่มีกรรมสิทธิ์ต้องทำตามขั้นตอนกฎหมาย ข้อบังคับ และสัญญาจ้างเอกชน

๑๔.๑.๒.๑ บริษัทต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด

๑๔.๑.๒.๒ บริษัทต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง

๑๔.๑.๒.๓ ห้ามผู้ใช้งานดำเนินการทำซ้ำหรือเผยแพร่รูปภาพ บทเพลง บทความ หนังสือหรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัท โดยเด็ดขาด

๑๔.๑.๒.๔ เพื่อที่จะให้เกิดความแน่ใจว่าพนักงานในบริษัท มิได้ละเมิด ลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือ พลั้งเผลอจึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัทเพื่อจุดประสงค์ใด ๆ ก็ตามโดยที่ไม่ได้รับอนุญาต และในขณะเดียวกันพนักงานในบริษัทไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

๑๔.๑.๒.๕ บริษัท กำหนดให้มีการตรวจ สอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ ๒ ครั้งเพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าบริษัทมีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์ เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็นบริษัทอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

๑๔.๑.๓ การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

๑๔.๑.๓.๑ บริษัทต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบ หรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูลระเบียบหน่วยงานว่าด้วยงานสารบรรณและกฎหมาย

๑๔.๑.๔ ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

๑๔.๑.๔.๑ บริษัทต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญาที่เกี่ยวกับบริษัท

๑๔.๑.๕ การป้องกันข้อมูลสำคัญของบริษัท (Protection of Organizational Records)

๑๔.๑.๕.๑ ข้อมูลสำคัญของบริษัท ต้องได้รับการป้องกันจากการสูญหาย การถูกทำลายการปลอมแปลง การเข้าถึงและการเผยแพร่โดยไม่ได้รับอนุญาต

๑๔.๑.๕.๒ ผู้ใช้งานจากข้อมูลสำคัญของบริษัทต้องดำเนินการให้สอดคล้องกับกฎหมาย นโยบายระเบียบ ข้อบังคับของบริษัท

๑๔.๑.๖ การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

๑๔.๑.๖.๑ บริษัทต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

๑๔.๑.๗ การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities)

๑๔.๑.๗.๑ อุปกรณ์ประมวลผลสารสนเทศของบริษัทมีไว้เพื่อใช้ในกิจการของบริษัทเท่านั้นยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บังคับบัญชาที่มีอำนาจ

๑๔.๑.๗.๒ ต้องกำหนดให้มีผู้รับผิดชอบ รวมถึงการจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่ซื้อหรือเช่ามาใช้งาน

๑๔.๑.๗.๓ ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของบริษัท

๑๔.๑.๗.๔ การดำเนินการใด ๆ ที่เป็นการติดตั้งซอฟต์แวร์หรืออุปกรณ์เพิ่มเติมต้องได้รับการอนุมัติจากผู้บังคับบัญชาที่มีอำนาจเป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

๑๔.๑.๗.๕ อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนเป็นอย่างน้อย ก่อนการเข้าใช้งานด้วยวิธีการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน

๑๔.๒ การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

นโยบาย

๑๔.๒.๑ การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

๑๔.๒.๑.๑ ผู้จัดการฝ่ายต้องกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยของบริษัท

๑๔.๒.๑.๒ วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย วัตถุประสงค์ มาตรการ นโยบาย กระบวนการ ขั้นตอนการปฏิบัติ การประเมินความเสี่ยง ต้องมีการทบทวนอย่างน้อยปีละ ๑ ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๑๔.๒.๑.๓ ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องมีการทบทวนความสอดคล้องทางเทคนิคของระบบอย่างสม่ำเสมอเพื่อพิจารณาความสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

๑๔.๒.๒ การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

๑๔.๒.๒.๑ ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้อย่างน้อยปีละ ๑ ครั้ง

๑๔.๒.๒.๒ ต้องมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

๑๔.๒.๓ การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review) จัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วอย่างน้อยปีละ ๑ ครั้ง ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และ/หรือ ทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

๑๕. การควบคุม การใช้อุปกรณ์ส่วนตัวในการทำงาน

วัตถุประสงค์

เพื่อให้มั่นใจว่าบริษัทมีการพิจารณาดำเนินการ การใช้อุปกรณ์ส่วนตัวในการทำงาน ให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนการปฏิบัติของบริษัท

นโยบาย

ให้มีการพิจารณาและควบคุมการนำคอมพิวเตอร์แบบพกพา สื่อบันทึกอิเล็กทรอนิกส์แบบพกพา (เช่น USB) โทรศัพท์มือถือ หรือ iPad ที่เป็นทรัพย์สินส่วนตัวมาใช้ในการทำงาน เว้นแต่ ได้ลงทะเบียนการใช้อุปกรณ์ดังกล่าวไว้กับฝ่ายเทคโนโลยีสารสนเทศแล้ว ทั้งนี้ เมื่อฝ่ายเทคโนโลยีสารสนเทศ ได้ดำเนินการตั้งค่าเครื่องอุปกรณ์ดังกล่าว เพื่อความปลอดภัยของข้อมูล และอยู่ภายใต้การควบคุม กำกับดูแลของฝ่ายเทคโนโลยีสารสนเทศแล้ว การนำเครื่องอุปกรณ์ดังกล่าวไปใช้งาน ให้คำนึงถึงระดับความเสี่ยง และดำเนินการ ดังนี้

ระดับความเสี่ยงต่ำ	ตัวอย่างเช่น - การใช้งานมีข้อมูลที่ใช้ระบุตัวบุคคลได้ เช่น อีเมล์ หรือแอพพลิเคชั่นอื่น แต่ไม่ได้อ่อนไหวมากจนจัดอยู่ในระดับที่ถ้ามีการเปิดเผย หรือนำไปใช้ในทางที่ผิดแล้ว จะส่งผลเสียต่อเจ้าของข้อมูลหรือบริษัท - การใช้งานมีข้อมูลอันเป็นที่เปิดเผยแก่สาธารณะ หรือสามารถค้นหาได้จากแหล่งข้อมูลอื่นโดยง่าย
ระดับความเสี่ยงสูง	ตัวอย่างเช่น - ข้อมูลของพนักงานตั้งแต่ ๑๐ คนขึ้นไปที่เกี่ยวกับการประเมินผลการทำงาน การพัฒนาการศักยภาพในการทำงาน หรือข้อมูลที่เกี่ยวกับชีวิตส่วนตัว หรือครอบครัวของพนักงาน - บันทึกข้อมูลสุขภาพที่ใช้ระบุตัวบุคคลได้ - กลุ่มข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลมากกว่า ๑๐ คนขึ้นไปที่สามารถระบุตัวได้ และสามารถนำข้อมูลกลุ่มนี้ไปปลอมแปลงหรือแอบอ้าง ตัวอย่างเช่น ข้อมูลบัญชีหรือบัตรเครดิต หมายเลขประกันสังคม ข้อมูลติดต่อ วันเกิด เงินเดือน เป็นต้น

เมื่อพนักงานที่ใช้เครื่องอุปกรณ์ส่วนตัวในการใช้งานได้ประเมินระดับความเสี่ยงตามตัวอย่างข้างต้นแล้ว ในการปฏิบัติงานด้วยอุปกรณ์ส่วนตัวดังกล่าว นอกจากจะต้องปฏิบัติตามนโยบายของบริษัทที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการใช้งานเครื่องคอมพิวเตอร์แบบพกพา หรือ สื่อบันทึกพกพา และอุปกรณ์เคลื่อนที่ประเภทต่าง ๆ แล้ว ให้ดำเนินการดังต่อไปนี้เป็นการเพิ่มเติม

การปฏิบัติงานที่มีระดับความเสี่ยงต่ำ	- ตั้งรหัสผ่าน (เช่น PIN หรือ password) เพื่อใช้อุปกรณ์ และไม่เปิดเผยรหัสดังกล่าวกับผู้อื่น - ตั้งค่าให้อุปกรณ์ล็อคอัตโนมัติเมื่อไม่มีการใช้งานเป็นเวลา ๑๐ นาที - เฝ้าระวังอุปกรณ์อย่างเหมาะสม ไม่ทิ้งอุปกรณ์ไว้โดยไม่ดูแล - อัพเดตโปรแกรมสม่ำเสมอด้วยตนเองหรือกำหนดค่าในระบบให้อัปเดตโดยอัตโนมัติ - ตั้งค่าไม่ให้อุปกรณ์เชื่อมต่อโดยอัตโนมัติกับสัญญาณไร้สายที่มีความเสี่ยง และควรพิจารณาก่อนจะตัดสินใจเชื่อมต่อสัญญาณ - ให้ติดตั้งระบบล้างข้อมูลที่สามารถสั่งได้จากระยะไกล ในกรณีที่สูญหาย - ถ้าอุปกรณ์ของผู้ใช้งานเป็นอุปกรณ์มือสอง(ไม่ใช้ของใหม่ที่นำมาใช้หลังจากทำการจัดซื้อ) ให้ตั้งค่าให้อุปกรณ์กลับไปที่สภาพเครื่องจากโรงงานก่อนเริ่มใช้
การปฏิบัติงานที่มีระดับความเสี่ยงสูง	- ให้ดำเนินการตามแนวทางการปฏิบัติงานที่อยู่ในระดับความเสี่ยงต่ำทุกข้อ - ในกรณีที่คนในครอบครัวใช้อุปกรณ์ที่ลงทะเบียนไว้กับบริษัทด้วย พนักงานต้องไม่ให้คนในครอบครัวเข้าถึงข้อมูลของบริษัทได้ เช่น ให้มีรหัสผ่านป้องกัน account ของตนเพิ่มขึ้นมา (ทั้งนี้บริษัทขอความร่วมมือไม่ให้แบ่งปันอุปกรณ์ส่วนตัวที่ลงทะเบียนไว้กับบริษัทให้ผู้อื่นใช้ทุกกรณี) - จัดการและตรวจสอบข้อมูลภายในเครื่องอยู่เสมอ ทำลายข้อมูลที่ไม่จำเป็น - เมื่อพนักงานไม่ใช้อุปกรณ์นี้ต่อไปแล้ว (เช่น กรณีที่นำเครื่องอื่นมาใช้แทน) หรือเมื่อลาออกจากการเป็นพนักงาน ให้ทำการลบข้อมูลในอุปกรณ์ของผู้ใช้ออกให้หมด(ทำการติดตั้งระบบปฏิบัติการใหม่ อาจจะให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ) - เข้ารหัสอุปกรณ์ (เพื่อป้องกันการเข้าถึงข้อมูล แม้หน่วยเก็บข้อมูล (storage chips) หรือดิสก์จะถูกถอดออกไปใส่ในอุปกรณ์อื่น) - ให้ติดตั้งระบบติดตามไว้กับอุปกรณ์ในกรณีที่สูญหายหรือถูกขโมย ให้ติดตั้งระบบล้างข้อมูลที่สามารถสั่งได้จากระยะไกลให้ล้างข้อมูลภายใน ๒๔ ชม. หรือเร็วกว่านั้น - ต้องแจ้งให้เจ้าหน้าที่ด้านความปลอดภัยสารสนเทศทราบทันทีหากเกิดการรั่วไหลของข้อมูล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบทันทีที่เกิดเหตุการณ์ - ปรับและตั้งค่าอุปกรณ์ให้มีระบบการป้องกันที่มีประสิทธิภาพสูงสุด ใช้เวลาศึกษาและทำความเข้าใจการตั้งค่าต่าง ๆ - ถ้ามีการเข้าถึงข้อมูลของบริษัทจากสถานที่อื่น ให้ทำการออกจากระบบและหยุดการเชื่อมต่อสัญญาณทุกครั้งหลักเลิกใช้ หรือตั้งค่าให้หยุดการเชื่อมต่อโดยใช้ Session Time - เปิดใช้งานโหมดสูญหาย เช่น ระบบตามหาพิกัด หรือระบบสั่งล้างข้อมูลทางไกล - ดาวน์โหลดแอพลิเคชันจากแหล่งที่มีความน่าเชื่อถือเท่านั้น - ในกรณีของ iPhone หรือ iPad อุปกรณ์จะถูกเข้ารหัส (encrypt) เอาไว้ โดยให้กำหนดการป้องกันโดยการตั้ง PIN - ในกรณีของแอนดรอยด์ สามารถเลือกได้ให้อุปกรณ์เข้ารหัสในลักษณะ whole-device ได้ที่ “การตั้งค่า” ของอุปกรณ์ อุปกรณ์ประเภทอื่น ๆ อาจสามารถหรือไม่สามารถตั้งค่า ให้ทำการเข้ารหัสได้

การนำคอมพิวเตอร์แบบพกพา สื่อบันทึกอิเล็กทรอนิกส์แบบพกพา โทรศัพท์มือถือ หรือ iPad ออกไปใช้นอกสถานที่ให้ทำได้เท่าที่จำเป็น และต้องดำเนินการตามนโยบายนี้อย่างเคร่งครัด

คู่มือปฏิบัติสำหรับพนักงานและผู้ใช้งาน

นโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลบริษัทได้จัดทำขึ้นในลักษณะที่ทำให้พนักงานอ่านและทำความเข้าใจได้อย่างง่ายและสะดวกมากขึ้น ดังนั้นพนักงานสามารถค้นหาในส่วนที่เกี่ยวข้องกับพนักงานเองโดยดูจากกลุ่มของพนักงาน โครงสร้างของนโยบายฉบับนี้จึงได้แบ่งออกตามกลุ่มของพนักงาน ดังต่อไปนี้

๑. กลุ่มพนักงานและผู้ใช้งานทั่วไป: กลุ่มนี้หมายรวมคือ พนักงานทุกกลุ่มซึ่งหมายถึงพนักงานจากทุก ๆ ฝ่ายในบริษัท นโยบาย หน้าที่และความรับผิดชอบที่เกี่ยวข้องกับพนักงานจะถูกจัดลำดับตามกลุ่มของพนักงานไว้พนักงานที่มีหน้าที่รับผิดชอบในแต่ละกลุ่มต้องมีความเข้าใจและปฏิบัติตามนโยบายที่กำหนดไว้อย่างเคร่งครัด

๒. กลุ่มพนักงานส่วนงานบริหารและพัฒนาทรัพยากรบุคคล (PD): รวมถึงพนักงานที่ปฏิบัติงานในส่วนงานที่เกี่ยวข้องกับทรัพยากรบุคคล

๓. กลุ่มพนักงานว่าจ้างชั่วคราวหรือพนักงานว่าจ้างจากภายนอก: พนักงานกลุ่มนี้รวมถึง พนักงานทุกคนที่ทำงานให้กับบริษัท ทั้งในแบบระยะสั้นหรือระยะยาว แต่ไม่ใช่พนักงานประจำ ตัวอย่างของพนักงานที่อยู่ในกลุ่มนี้ เช่น ผู้ขาย (vendor) หรือ พนักงานว่าจ้างจากภายนอกมาทำงานในบริษัท

๔. กลุ่มพนักงานส่วนงานฝ่ายเทคโนโลยีสารสนเทศ (IT): เป็นพนักงานทุกคนที่อยู่ในฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายไอที

กลุ่มพนักงานและผู้ใช้ทั่วไป

การเปิดเผยข้อมูลกับบุคคลภายนอกบริษัท

๑. ข้อมูลของบริษัท ที่ไม่ได้กำหนดให้เป็นข้อมูลที่สามารถเปิดเผยได้ ต้องมีวิธีป้องกันไม่ให้บุคคลภายนอกเข้าถึงได้

๒. การอนุญาตให้บุคคลภายนอกเข้าถึงข้อมูลของบริษัทได้นั้น ต้องมีหลักฐานยืนยันเพื่อแสดงว่า ข้อมูลเหล่านั้นได้รับการอนุญาตให้เข้าถึงได้จากบริษัท จริง ซึ่งบุคคลภายนอกนั้นจำเป็นต้องมีการลงนามในสัญญาเรื่องการไม่เปิดเผยข้อมูลกับบริษัท และการเข้าถึงข้อมูลนั้น ๆ ต้องได้รับสิทธิ์หรือการอนุญาตจากเจ้าของข้อมูลก่อนเท่านั้น

๓. ถ้ามีเหตุการณ์เกี่ยวกับการเสียหายหรือสงสัยเกี่ยวกับการละเมิดการรุกล้ำสิทธิ์ในการเข้าถึงข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ควรเปิดเผย ต้องแจ้งให้เจ้าของข้อมูลหรือผู้รับผิดชอบข้อมูลนั้น ๆ และทีมงานความปลอดภัยข้อมูลรับทราบโดยด่วน

การขอข้อมูลของบริษัทจากบุคคลภายนอก

๑. การร้องขอเกี่ยวกับใบสอบถาม เอกสารทางด้านการเงิน เอกสารนโยบายภายในบริษัท ขั้นตอนปฏิบัติของการทำงานในบริษัท หรือสำหรับสำรวจตรวจสอบ และการขอสัมภาษณ์กับพนักงานภายในบริษัทถูกควบคุมโดยนโยบายฉบับนี้

๒. นโยบายฉบับนี้ไม่ได้ครอบคลุมถึงข้อมูลที่เกี่ยวเนื่องกับผลิตภัณฑ์และบริการของบริษัท ถ้าบุคคลภายนอกหรือคู่ค้าของบริษัทที่ทำการส่งข้อมูลที่เป็นความลับให้พนักงานของบริษัทเป็นการส่วนตัวนั้น ทางบริษัทจะถือว่าไม่มีส่วนรับผิดชอบใด ๆ กับข้อมูลเหล่านี้

การคัดลอกข้อมูลของบริษัท

๑. ไม่อนุญาตให้พนักงานที่ไม่มีสิทธิ์ทำการคัดลอกข้อมูลหรือโปรแกรม ซอฟต์แวร์ของบริษัท โดยไม่จำเป็นหรือไม่มีเหตุผลสมควร

๒. ถ้าหากผู้ที่ไม่ได้รับอนุญาตให้มีสิทธิ์ในข้อมูลนั้น ๆ กระทำการส่งต่อข้อมูลให้กับบุคคลภายนอกหรือคู่ค้าจะมีความผิดตามระเบียบของบริษัท

การป้องกันข้อมูลสำคัญจากภายนอก

ข้อมูลที่เกี่ยวข้องกับมาตรการความปลอดภัยข้อมูล ไม่ว่าจะเป็นข้อมูลที่ใช้ทำงานอยู่ในระบบต่าง ๆ และในระบบเครือข่ายของบริษัท ถือว่าเป็นข้อมูลลับ และห้ามเปิดเผยให้กับพนักงานหรือบุคคลอื่นที่ไม่มีสิทธิ์เข้าถึงข้อมูลนั้น ๆ โดยไม่ได้รับการเห็นชอบจากหน่วยงานความปลอดภัยข้อมูลของบริษัทก่อน ตัวอย่างเช่น ห้ามเปิดเผยข้อมูลเบอร์โทรศัพท์บ้านของพนักงานแก่คู่แข่งทางการค้าโดยเด็ดขาด

การจัดประเภทของข้อมูล (สี่ประเภท)

๑. การแบ่งประเภทของข้อมูลนั้นพิจารณาจากความสำคัญทางด้านความเสี่ยงของข้อมูล ซึ่งอาจจะดูได้จากความต้องการใช้งานของข้อมูลนั้น ๆ ความสำคัญหรือระดับของการป้องกันข้อมูลที่จำเป็นสำหรับข้อมูลประเภทนั้น ๆ

๒. บริษัท ได้จัดแบ่งกลุ่มข้อมูลโดยแบ่งเป็นประเภทต่าง ๆ และทำการกำหนดระดับความเหมาะสมในการป้องกันข้อมูลแต่ละประเภท และมาตรการการป้องกันและรับผิดชอบในข้อมูลนั้น ๆ รวมถึงวิธีการเก็บรักษาข้อมูล

๓. ข้อมูลต่าง ๆ ในบริษัทต้องถูกจัดให้อยู่ในประเภทดังต่อไปนี้

- ลับสุดยอด (ห้ามเปิดเผยโดยเด็ดขาด)
- เป็นความลับ
- ใช้ภายในเท่านั้น
- ทั่วไป (สามารถเปิดเผยได้)

เพื่อให้แน่ใจว่าข้อมูลได้รับการป้องกันเป็นอย่างดี พนักงานทุกคนต้องทำความคุ้นเคย และเข้าใจความหมายของประเภทของข้อมูลให้ถูกต้องและเล็งเห็นความสำคัญในการจัดประเภทของข้อมูลนี้ด้วย

การติดป้ายข้อมูล

๑. บริษัท ต้องมีการติดป้ายประเภทของข้อมูลอย่างเหมาะสม ตามขั้นตอนที่ได้กำหนดไว้เบื้องต้น

๒. ข้อมูลที่เป็นความลับ ไม่สามารถเปิดเผยได้ ไม่ว่าจะอยู่ในสถานะใด (ตั้งแต่ขั้นแรกเริ่มจนถึงขั้นทำลาย) ต้องระบุประเภทข้อมูลให้ชัดเจน

๓. การติดป้ายต้องระบุประเภทของข้อมูล วันหมดอายุหรือระยะเวลา ของข้อมูลที่ต้องเก็บรักษาไว้ วิธีการหรือขั้นตอนในการใช้งานข้อมูลนั้น ๆ และที่ตั้งในการเก็บข้อมูล ถ้ามีแล้วแต่ความจำเป็นของ

เอกสารส่วนใหญ่อยู่ในประเภท “ใช้ภายในเท่านั้น” ไม่จำเป็นต้องติดป้ายบอกประเภทไว้ ดังนั้นเอกสารที่ไม่ได้ติดป้ายบอกประเภทจะ ถือว่าเป็นเอกสารที่ใช้สำหรับภายในเท่านั้น

การส่งข้อมูลและการถือครองข้อมูล

๑. ข้อมูลที่เป็นความลับต้องมีการควบคุมเรื่องสิทธิ์ในการเข้าถึงโดยคณะทำงานความปลอดภัยข้อมูลของบริษัท

๒. ผลหรือข้อมูลที่ได้จากระบบคอมพิวเตอร์ที่เป็นความลับต้องมีการส่งถึงผู้รับไว้ด้วยเป็นการส่วนตัว ต้องได้รับการเห็นชอบและอนุญาตจากเจ้าของข้อมูลก่อนนำข้อมูลที่เป็นความลับออกนอกพื้นที่ของบริษัท ข้อมูลความลับที่อยู่ในรูปแบบเอกสารต้องเก็บไว้อย่างดีเมื่อยังไม่นำออกมาใช้งาน

๓. ข้อมูลที่เป็นความลับและเปิดเผยไม่ได้ที่อาจจะอยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ที่อ่านออกได้ และรูปแบบเสียงที่สามารถได้ยินและฟังได้ เพื่อใช้ในการสื่อสารระหว่างกันต้องมีการเข้ารหัสด้วย

การยกเลิกการจัดประเภทและการลดระดับความสำคัญของข้อมูล

ข้อมูลที่ถูกยกเลิกการจัดอยู่ในประเภท “เป็นความลับ ” และ “ลับสุดยอด ” แล้วนั้นต้องมีการระบุและแจ้งให้บุคคลที่เกี่ยวข้องทราบ จำเป็นต้องมีการทบทวนจัดประเภทข้อมูลให้ถูกต้องอย่างน้อยปีละหนึ่งครั้ง

การทำลายข้อมูล

ข้อมูลของบริษัท ต้องทำลายเมื่อไม่มีความจำเป็นต้องใช้อีกต่อไปในทางธุรกิจ หากข้อมูลที่เป็นความลับหรือไม่สามารถเปิดเผยได้นั้นไม่มีความจำเป็นในการใช้งานอีก จะต้องเก็บไว้ในที่ปลอดภัยและล็อคป้องกันการเข้าถึงได้จนกว่าจะมอบให้กับผู้ที่มีสิทธิ์ของบริษัทเป็นผู้จัดการต่อไป พนักงานต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนทำลายเอกสารหรือบันทึกต่าง ๆ ที่สำคัญของบริษัท

การยินยอมจากพนักงาน

พนักงานทุกคนทั้งพนักงานประจำและพนักงานว่าจ้างชั่วคราว ต้องยินยอมในการเซ็นยอมรับในเอกสารข้อตกลงที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล หรือเอกสารข้อตกลงที่เกี่ยวข้องกับการไม่เปิดเผยข้อมูลของบริษัทตั้งแต่วันที่พนักงานเข้าทำงานในบริษัท

การควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกต่าง ๆ

๑. การเข้าพื้นที่ทำงาน ห้องเก็บเครื่องมือสื่อสารโทรคมนาคม ห้องเซิร์ฟเวอร์ หรือพื้นที่ของสถานที่ทำงานที่มีการเก็บข้อมูลที่ไม่สามารถเปิดเผยได้หรือมีข้อมูลที่เป็นความลับจะต้องจำกัดสิทธิ์เฉพาะพนักงานที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้

๒. ข้อมูลที่เป็นความลับต้องป้องกันจากบุคคลที่ไม่มีสิทธิ์ในการเข้าถึง

๓. เอกสารที่อยู่ในรูปแบบสิ่งพิมพ์และเก็บข้อมูลที่เป็นความลับต้องถูกเก็บไว้ในตู้เอกสารที่ปิดล็อคได้

๔. ข้อมูลที่เป็นความลับต้องถูกเก็บไว้ในที่ ๆ ปลอดภัยและสามารถปิดล็อคได้ระหว่างที่ไม่ได้อยู่ในช่วงเวลาทำงาน

๕. แนะนำให้มีการทำนโยบายการรักษาระเบียบและความสะอาดโต๊ะทำงานเพื่อป้องกันการเข้าถึงเอกสารสำคัญ

๖ หน้าจอคอมพิวเตอร์ควรจะมีการตั้งค่าของภาพที่แสดงให้เหมาะสม โดยไม่ควรแสดงหรือกำหนดภาพและเนื้อหาที่ไม่เหมาะสมบนหน้าจอคอมพิวเตอร์

การถือครองข้อมูลระหว่างการเข้ากะทำงาน

ข้อมูลที่เป็นความลับของบริษัทต้องถูกเก็บไว้ในพื้นที่ ๆ จัดไว้อย่างปลอดภัย และต้องไม่ละเลยหรือทิ้งข้อมูลเหล่านั้นไว้ในที่ ที่ไม่ปลอดภัยในช่วงของกะทำงานเวลาถัดไป

การตรวจสอบทรัพย์สินก่อนนำออก

ต้องมีการตรวจสอบหรือได้รับอนุญาตให้นำอุปกรณ์คอมพิวเตอร์หรือชิ้นส่วนคอมพิวเตอร์ก่อนจะนำออกจากพื้นที่ของบริษัทได้

สิทธิ์ในการตรวจสอบและระวังภัย

๑. ผู้จัดการหรือหัวหน้างานมีสิทธิ์ในการตรวจสอบหรือตรวจตราการใช้งานระบบที่เกี่ยวข้องกับข้อมูลของบริษัททุกเวลา

๒. การตรวจสอบในลักษณะนี้อาจจะได้รับการยินยอมหรือไม่ยินยอมจากพนักงานคนนั้น ๆ ก็ตาม

๓. ระบบข้อมูลต่าง ๆ ของบริษัทสามารถตรวจสอบโดยดูจาก การใช้งานการทำงานของพนักงานที่บันทึกไว้ จากข้อมูลไฟล์ที่อยู่ในฮาร์ดดิสก์ และข้อมูลจากอีเมลหรือจดหมายอิเล็กทรอนิกส์ทั้งนี้เอกสารต่าง ๆ ที่ถูกพิมพ์ หรือข้อมูลที่อยู่ในลิ้นชักโต๊ะและพื้นที่ที่ใช้เก็บข้อมูลก็สามารถถูกตรวจสอบได้เช่นกัน

๔. การตรวจสอบในลักษณะนี้ต้องได้รับการอนุญาตจากหน่วยงานกฎหมายและความปลอดภัยข้อมูลก่อน

๕. ผู้จัดการหรือหัวหน้างานมีสิทธิ์ที่จะริบหรือยึดสิ่งของที่ผิดต่อระเบียบนโยบายบริษัทหรือผิดต่อกฎหมาย เพื่อทำการตรวจสอบและส่งคืนเมื่อทำการตรวจสอบเรียบร้อยแล้ว

ความเป็นเจ้าของในทรัพย์สิน

๑. บริษัท ถือเป็นเจ้าของกรรมสิทธิ์ในเรื่องสิทธิบัตร ลิขสิทธิ์ สิ่งประดิษฐ์คิดค้นหรือทรัพย์สินทางปัญญาที่สร้างหรือทำขึ้นโดยพนักงานของบริษัท

๒. โปรแกรมและเอกสารทุกอย่างที่จัดทำหรือสร้างขึ้นเพื่อใช้ประโยชน์ในบริษัทโดยพนักงานของบริษัท ถือว่าเป็นกรรมสิทธิ์และทรัพย์สินของบริษัททั้งหมด และบริษัทสามารถกำหนดสิทธิ์ในการเข้าถึงหรือใช้งานข้อมูลเหล่านั้นได้ตามเห็นสมควร

การเข้าถึงอินเทอร์เน็ต

๑. บริษัท กำหนดว่าพนักงานทุกคนสามารถเข้าอินเทอร์เน็ตได้จากเครื่องคอมพิวเตอร์ตั้งโต๊ะที่จัดไว้ให้ซึ่งการเข้าถึงนี้สามารถยกเลิกได้ทุกเมื่อตามแต่ความเห็นชอบของผู้บริหาร

๒. การเข้าถึงอินเทอร์เน็ตจะถูกตรวจสอบการใช้งานให้เป็นไปอย่างเหมาะสมตามสมควร และปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลของบริษัท

๓. ห้ามมีการแสดงถึงความเป็นบริษัทหรือกลุ่มในบริษัทในที่สาธารณะโดยไม่ได้รับการอนุมัติหรือเห็นชอบจากผู้บริหารที่รับผิดชอบก่อน

๔. ข้อมูลต่าง ๆ ที่ได้รับผ่านทางอินเทอร์เน็ตควรจะมีการตรวจสอบก่อนว่าได้รับมาจากแหล่งที่เชื่อถือได้จริง

๕. ห้ามมีการนำสิ่งของหรือสัญลักษณ์ที่แสดงถึงตัวบริษัทหรือข้อมูลของบริษัทไปแสดงในระบบประมวลผลข้อมูลสาธารณะโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลและฝ่ายความปลอดภัยข้อมูลก่อน

๖. ข้อมูลที่เป็นความลับ ไม่สามารถเปิดเผยได้ เช่น รหัสผ่านและเลขบัตรเครดิต ไม่ควรส่งผ่านทางอินเทอร์เน็ตโดยวิธีใด ๆ โดยไม่ได้ทำการเข้ารหัสก่อน

จดหมายอิเล็กทรอนิกส์หรืออีเมล

๑. บริษัท ให้พนักงานในบริษัททุกคนมีการใช้จดหมายอิเล็กทรอนิกส์โดยมีบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์และให้บริการในการรับส่งอีเมล เพื่อประโยชน์และเพิ่มความสะดวกในการการทำงานของพนักงานเอง

๒. การสื่อสารที่เกี่ยวข้องกับธุรกิจของบริษัทต้องรับส่งกันโดยใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของ บริษัท

๓. การใช้งานบัญชีผู้ใช้ส่วนตัว เช่น Yahoo, Hotmail ไม่อนุญาตให้นำมาใช้กับธุรกิจของบริษัท

๔. ไม่อนุญาตให้มีการส่งจดหมายอิเล็กทรอนิกส์ที่เข้าข่ายล่อลวง หรือไม่มีสาระสำคัญทางธุรกิจให้กับลูกค้า

๕. ทุกคนในบริษัทต้องใช้ลายเซ็นกำกับด้านล่างของจดหมายอิเล็กทรอนิกส์ให้เป็นมาตรฐาน ซึ่งประกอบไปด้วย ชื่อจริง นามสกุล ตำแหน่งการทำงาน ที่อยู่บริษัทและเบอร์โทรศัพท์ให้ชัดเจน

การเจาะข้อมูลในระบบ

พนักงานต้องไม่กระทำการเจาะข้อมูลในระบบของบริษัท หรือกระทำพฤติกรรมที่คล้ายคลึงกับการตั้งใจเจาะข้อมูลในระบบ ซึ่งรวมถึงการพยายามเข้าถึงข้อมูลทั้ง ๆ ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลนั้น ๆ แม้กระทั่งพยายามสร้างความเสียหาย พยายามเปลี่ยนแปลงให้กับข้อมูล หรือสร้างความยุ่งยากให้เกิดขึ้นภายในระบบที่ใช้งานจริง และการพยายามสืบหาใช้รหัสผ่านของบุคคลอื่นหรือพยายามถอดรหัสกุญแจของระบบ และไม่ว่าการจะใช้วิธีการเข้าถึงหรือควบคุมระบบโดยไม่ได้รับอนุญาตและไม่ได้รับสิทธิ์ ทั้งหมดถือว่าเป็นการพยายามเจาะข้อมูลในระบบทั้งสิ้น

จัดระเบียบการใช้ซอฟต์แวร์

ทุกซอฟต์แวร์ที่ทำการติดตั้งในระบบของบริษัท และมีจัดให้พนักงานใช้หลายคนในเวลาเดียวกันต้องมีการจัดระเบียบการใช้งานและกำหนดสิทธิ์ในการเข้าถึงของพนักงานก่อนที่จะมีการเข้าถึงซอฟต์แวร์นั้น ๆ ได้จริง

สิทธิ์เริ่มต้นในการเข้าถึงไฟล์และระบบงานต่าง ๆ

เพื่อเป็นการควบคุมสิทธิ์ในการเข้าถึงข้อมูล จากผู้ที่ไม่มีสิทธิ์ในการเข้าถึงระบบเครือข่ายของ บริษัท ต้องมีการกำหนดค่าเริ่มต้นเป็นผู้ที่ไม่มีสิทธิ์เข้าถึงเสมอ

การควบคุมการเข้าถึงผิดพลาด

ถ้าคอมพิวเตอร์หรือระบบการควบคุมการเข้าถึงข้อมูลทำงานผิดพลาดหรือไม่สามารถทำงานได้ตามปกติ ระบบต้องมีการตั้งค่าเริ่มต้นเป็นปฏิเสธการเข้าถึงจากผู้ใช้งานทั้งหมดทันที

การกำหนดและรับรองการเป็นตัวตนของผู้ใช้งาน (User ID and password [ID Management Security Policy])

๑. บริษัท ต้องกำหนดให้พนักงานทุกคนเข้าถึงระบบที่เกี่ยวข้องกับข้อมูลบริษัทด้วยการใช้บัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ของพนักงานเองเท่านั้น

๒. บัญชีผู้ใช้งาน (User ID) ถูกใช้เพื่อกำหนดเรื่องของสิทธิ์ในการเข้าถึงระบบต่าง ๆ ขึ้นอยู่กับหน้าที่รับผิดชอบลักษณะการทำงานของพนักงานแต่ละคน

๓. พนักงานทุกคนในบริษัทต้องรับผิดชอบที่จะปกป้องบัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ของตัวเอง

๔. การจัดเก็บรหัสผ่านของผู้ใช้งานในระบบ บริษัทฯ ใช้วิธีการแฮช (Hash) โดยใช้ Algorithm ที่ปลอดภัย

วิธีการตั้งรหัสผ่าน

ผู้ใช้งานระบบทุกคนต้องตั้งรหัสผ่านของตัวเอง โดยรหัสผ่านนั้นควรจะยากต่อการคาดเดา และไม่ควรมีข้อมูลส่วนตัวประกอบในรหัสผ่านนั้น ตัวอย่างเช่น เลขรหัสพนักงาน เลขบัตรประชาชน เลขบัตรสุขภาพ PIN code เบอร์โทรศัพท์ ชื่อคู่ครอง ชื่อแฟน รหัสไปรษณีย์ ชื่อสถานที่ต่าง ๆ หรือศัพท์เทคนิค ศัพท์ในพจนานุกรม ไม่ควรนำมาใช้เป็นรหัสผ่านการตั้งรหัสผ่านที่ดี มีเทคนิคดังนี้:

๑. ใช้คำบางคำเป็นส่วนประกอบ

๒. ใช้ตัวหนังสือภาษาอังกฤษตัวเล็กหรือตัวใหญ่ หรือใช้ตัวเลขคั่นสลับกัน

๓. เปลี่ยนคำธรรมดาให้เป็นคำที่มีตัวอักษรอื่นแอบแฝง

๔. สามารถสร้างเป็นตัวย่อจากคำเต็มได้เอง เช่น CEGEP โดยไม่มีใครรู้ความหมาย

๕. ใช้คำที่สะกดผิดเป็นส่วนประกอบ

๖. ใช้เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:”;'<>?,./)

การใช้รหัสผ่านที่คล้ายคลึงรหัสเดิม

ผู้ใช้งานไม่ควรจะตั้งรหัสผ่านที่เหมือนกับรหัสผ่านเดิม หรือตั้งรหัสซ้ำสำหรับการเข้าถึงระบบใด ๆ ก็ตาม และไม่ควรคล้ายคลึงกับรหัสผ่านเดิมที่เคยใช้งานมาก่อนแล้ว

ข้อบังคับในการตั้งรหัสผ่าน

๑. รหัสผ่านต้องมีอย่างน้อย ๘ ตัวและต้องมีการเปลี่ยนรหัสผ่านทุก ๆ ๑๘๐ วันหรืออาจจะน้อยกว่านี้

๒. ระบบการจัดการเรื่องรหัสผ่านต้องมีการกำหนดให้ผู้ใช้งานตั้งรหัสผ่านโดยใช้ตัวอักษร ตัวเลขและอักขระพิเศษเป็นอย่างน้อยและต้องไม่อนุญาตให้มีการใช้รหัสผ่านซ้ำจากเดิมที่เคยตั้งมาแล้วหรืออย่างน้อยต้องเว้นไประยะหนึ่งถึงจะอนุญาตให้ใช้ซ้ำได้

การเก็บรักษารหัสผ่าน

๑. รหัสผ่านไม่ควรเก็บไว้ในเอกสารหรือที่ ๆ เก็บแล้วสามารถนำออกมาอ่านได้ ไม่ว่าจะเป็นการเก็บเข้าแฟ้ม มาโครในซอฟต์แวร์ต่าง ๆ ในคอมพิวเตอร์ของผู้ใช้งานเอง โดยไม่มีการควบคุมการเข้าถึงเป็นอย่างดี หรือทำให้มีบุคคลที่ไม่มีสิทธิ์สามารถเข้าถึงสถานที่เก็บรหัสผ่านได้

๒. รหัสผ่านควรจะไม่จดออกมาใส่กระดาษและไม่ทิ้งไว้ในที่โล่งแจ้งหรือในที่ ๆ สามารถมองเห็นได้โดยทั่วไป เช่น แปะไว้ที่หน้าจอคอมพิวเตอร์ หรือที่โต๊ะทำงาน เป็นต้น

การร่วมใช้รหัสผ่าน

๑. ถ้าข้อมูลที่มีความจำเป็นต้องมีการใช้งานร่วมกัน พนักงานสามารถทำได้โดยใช้อีเมลของบริษัทหรือจดหมายอิเล็กทรอนิกส์ฐานข้อมูล ไดเร็กทรอรีสาธารณะ ที่เก็บอยู่ในเซิร์ฟเวอร์ของบริษัท หรืออยู่ในอุปกรณ์บันทึกข้อมูลหรืออุปกรณ์ที่ใช้ในการส่งต่อหรือแลกเปลี่ยนข้อมูลกัน

๒. รหัสผ่านต้องไม่มีบอกผู้อื่นที่ไม่ใช่เจ้าของ ห้ามเปิดเผยให้ผู้อื่นทราบ

๓ เจ้าหน้าที่ดูแลระบบหรือเจ้าหน้าที่ ทางเทคนิค ไม่ควรสอบถามรหัสผ่านหรือเปิดเผยรหัสผ่านของพนักงานคนอื่น ๆ ยกเว้นแต่จะมีการใช้รหัสผ่านนั้นชั่วคราวเพื่อจุดประสงค์ในการทำงาน และต้องมีการเปลี่ยนรหัสผ่านนั้นทันทีหลังจากที่มีการเข้าใหม่อีกครั้งของพนักงานคนนั้น

๔. ถ้าผู้ใช้งานสงสัยว่ามีบุคคลอื่นกำลังใช้บัญชีผู้ใช้ (User ID) และรหัสผ่าน (Password) ของตัวเองอยู่ จะต้องแจ้งให้เจ้าหน้าที่ที่รับผิดชอบทราบโดยด่วน

การกำจัดไวรัสคอมพิวเตอร์

๑. เมื่อพนักงานได้พบเจอไวรัสที่เครื่องคอมพิวเตอร์ของตัวเอง ต้องทำการหยุดไวรัสตัวนั้นทันทีเพื่อไม่ให้ระบบหรือเครื่องคอมพิวเตอร์อื่นได้รับไวรัสด้วย และทำการแจ้งหน่วยงาน IT ทันที

๒. ถ้าหากแผ่นบันทึกข้อมูล หรืออุปกรณ์เครื่องบันทึกข้อมูลที่มีการใช้งานกับเครื่องคอมพิวเตอร์ที่ติดไวรัสแล้ว ไม่ควรนำมาใช้กับเครื่องคอมพิวเตอร์เครื่องอื่นโดยเด็ดขาด จนกว่าจะมีการลบไวรัสออกเรียบร้อยแล้ว

๓. เครื่องคอมพิวเตอร์ที่ติดไวรัสต้องถูกกักกัน หรือแยกออกจากระบบเครือข่ายของบริษัท โดยทำการดึงสาย LAN ออกจากเครื่อง หรือปิด Wi-Fi

๔. ผู้ใช้งานต้องไม่พยายามลบไวรัสด้วยตัวท่านเอง

๕. พนักงาน IT หรือเจ้าหน้าที่รับผิดชอบมีหน้าที่ในการนำไวรัสออกจากเครื่อง อย่างเป็นขั้นตอนเพื่อให้เครื่องคอมพิวเตอร์เกิดความเสียหายน้อยที่สุด

การป้องกันไวรัส

ปัจจุบันได้มีการติดตั้งโปรแกรมตรวจจับไวรัสไว้ที่เครื่องเซิร์ฟเวอร์ทุกเครื่องและมีการทำงานตลอดเวลา เครื่องคอมพิวเตอร์ที่ไม่ได้ทำการอัพเดตเวอร์ชันในการให้รู้จักไวรัสในปัจจุบัน ไม่อนุญาตให้เชื่อมต่อกับระบบของบริษัท โดยเด็ดขาด ผู้ใช้งานต้องไม่ทำการดาวน์โหลดโปรแกรมหรือซอฟต์แวร์จากเว็บไซต์หรือที่อื่น ๆ ในอินเทอร์เน็ต ยกเว้นแต่เว็บไซต์นั้นจะเป็นเว็บไซต์ที่เชื่อถือได้และได้รับการอนุญาตจากหน่วยงานความปลอดภัยข้อมูลของบริษัทก่อน

การให้ความรู้แก่พนักงานในบริษัท

๑. พนักงานในบริษัททุกคนต้องได้รับการให้ความรู้และความเข้าใจพื้นฐานในนโยบายต่าง ๆ มาตรฐาน และขั้นตอนการดำเนินงานของบริษัท ทั้งนี้พนักงานทุกคนต้องได้รับความรู้เกี่ยวกับข้อมูลความปลอดภัยในปัจจุบันผ่านจากสื่อต่าง ๆ เช่น จากการทำอบรมภายในบริษัท จากทางอีเมลหรือจดหมายอิเล็กทรอนิกส์หรือจากการประกาศบนหน้าเว็บภายในของบริษัทหรือตามป้ายติดภายในบริษัทเอง

๒. เนื่องจากพนักงานควรจะได้รับความรู้ในรูปแบบที่แตกต่างกัน โดยแยกตามระดับการทำงานได้ ๓ ระดับดังนี้

- ระดับผู้บริหาร
- ระดับพนักงานเทคนิค
- ระดับพนักงานทั่วไป

กลุ่มพนักงานส่วนงานบริหารและพัฒนาทรัพยากรบุคคล (PD)

ความปลอดภัยที่เกี่ยวเนื่องกับขอบเขตการทำงานและพัฒนาทรัพยากรบุคคล

๑. กำหนดขอบเขตและลักษณะงานของแต่ละตำแหน่งต่าง ซึ่งหมายถึงงานที่รับผิดชอบหลักงานที่เกี่ยวข้องกับส่วนงานหรือหน่วยงานอื่น และทักษะความสามารถ ประสบการณ์ที่จำเป็นสำหรับความรับผิดชอบต่อตำแหน่งงานนั้นขอบเขตและลักษณะงานนี้ต้องมีการทบทวนและแก้ไขหน้าที่ความรับผิดชอบให้ถูกต้องตามตำแหน่งงานที่เปลี่ยนแปลงไป

๒. ขั้นตอนการว่าจ้างพนักงานใหม่ในตำแหน่งใด ๆ ต้องมีหลักฐานเอกสารให้ตรวจสอบได้ชัดเจน ขั้นตอนการตรวจสอบเรื่องของคุณสมบัติ แหล่งอ้างอิง การศึกษา ประวัติทางคดีการเงินและอาชญากรจำเป็นต้องมีการทบทวนและตรวจสอบเป็นอย่างดี

๓. จัดให้มี Code of conduct สำหรับกำหนดพนักงานผู้มีสิทธิ์เข้าถึงข้อมูลและวิธีการเข้าถึงข้อมูล

๔. จัดให้มีขั้นตอนการตรวจสอบและจัดทำ ความยินยอม (Consent Form) ให้กับพนักงาน

๑. PD Employee Consent Form ๑

๒. PD Employee Consent Form ๒

๓. PD Employee Consent Form ๓

๔. PD Applicant Consent Form

กลุ่มพนักงานว่าจ้างชั่วคราว หรือพนักงานว่าจากภายนอก

การใช้บัญชีเข้าระบบของพนักงานชั่วคราวหรือจ้างจากภายนอก

บุคคลใด ๆ ที่ไม่ใช่พนักงานประจำหรือพนักงานว่าจ้างตามสัญญา หรือที่ปรึกษาของบริษัท ไม่มีสิทธิ์ในการใช้บัญชีใช้งานเข้าระบบ (User ID) หรือไม่มีสิทธิ์ในการใช้ระบบคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์ของบริษัท จนกว่าจะได้รับการอนุญาตจากหน่วยงานที่เกี่ยวข้องเป็นลายลักษณ์อักษรก่อน

การควบคุมการเข้าถึงระบบ

การเข้าถึงระบบภายในหรือข้อมูลของบริษัทโดยบุคคลภายนอกในแบบที่ไม่เป็นทางการต้องได้รับอนุญาตจากผู้ประสานงานหรือผู้รับผิดชอบของหน่วยงานความปลอดภัยข้อมูลก่อนล่วงหน้า ก่อนที่บุคคลภายนอกจะทำการติดต่อหรือเชื่อมต่อกับระบบของบริษัทผ่านทางเครือข่ายคอมพิวเตอร์แบบ Real-time ต้องได้รับอนุญาตจากหน่วยงานความปลอดภัยข้อมูลก่อน

ข้อเสนอและเงื่อนไขสำหรับการทำสัญญากับบริษัทคู่ค้า

การทำสัญญากับบริษัทคู่ค้าหรือบุคคลภายนอกต้องระบุในเรื่องของข้อเสนอและเงื่อนไขต่าง ๆ เกี่ยวกับการเข้าถึงระบบของบริษัท และมีการเซ็นรับรองจากระดับผู้จัดการของบริษัทคู่ค้าบริษัทนั้นด้วย และมีการเห็นชอบจากหน่วยงานความปลอดภัยข้อมูลและฝ่ายกฎหมายของบริษัท

การปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูล

ที่ปรึกษา คู่สัญญา และพนักงานว่าจ้างชั่วคราวต้องปฏิบัติตามข้อกำหนดและนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลของบริษัท และมีหน้าที่ความรับผิดชอบเสมือนเป็นพนักงานของบริษัท

ข้อตกลงในการไม่เปิดเผยข้อมูลของ บริษัท สกาย ไอซีที จำกัด (มหาชน)

การสื่อสารที่ต้องเปิดเผยข้อมูลภายในของบริษัทกับบุคคลภายนอกหรือคู่ค้าบริษัทอื่น ต้องมีการเซ็นข้อตกลงในการไม่เปิดเผยข้อมูลของบริษัท จากบริษัทหรือบุคคลภายนอกก่อน ข้อมูลที่ให้กับบุคคลภายนอกหรือบริษัทคู่ค้าอื่น ต้องมีการจำกัดเรื่องของขอบเขตให้อยู่ในส่วนงานหรือเกี่ยวข้องกับส่วนงานที่ทำเท่านั้น และการเปิดเผยข้อมูลหรือให้ข้อมูลนี้ต้องได้รับการอนุญาตจากเจ้าข้อมูลก่อนเสมอ

ข้อตกลงในการไม่เปิดเผยข้อมูลของบริษัทคู่ค้า

ในกรณีที่ทางบริษัทคู่ค้ามีนโยบายให้พนักงานของบริษัท เซ็นลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูลของบริษัทคู่ค้านั้น ผู้ที่ได้รับเอกสารฉบับนั้นต้องส่งต่อให้ทางฝ่ายกฎหมายตรวจสอบซึ่งทางพนักงานของฝ่ายกฎหมายจะเป็นผู้ลงนามในเอกสารนั้นเอง

รายการการควบคุมการใช้งานระบบจัดจ้างภายนอก

ข้อตกลงที่ระบุในสัญญาทุกฉบับกับทางบริษัทจัดทำระบบจัดจ้างภายนอก ต้องมีการกำหนดเงื่อนไขให้ บริษัท สกาย ไอซีที จำกัด (มหาชน) ได้รับรายการความคิดเห็นเกี่ยวกับผลจากการควบคุมการทำงานของบริษัทที่จัดทำระบบจัดจ้างภายนอกนั้นเป็นประจำทุกปี

ผู้ให้บริการใช้ซอฟต์แวร์แอปพลิเคชัน

ทุกแอปพลิเคชันใช้ในงานจริงและมีข้อมูลของบริษัท อยู่ต้องมีใบอนุญาตในการใช้งานซอฟต์แวร์นั้นอย่างถูกต้องจากผู้ให้บริการหรือเจ้าของซอฟต์แวร์นั้น และต้องมีการให้ซอร์สโค้ดเวอร์ชันล่าสุดกับบริษัทรวมถึงเอกสารรายละเอียดขั้นตอนต่าง ๆ เกี่ยวกับแอปพลิเคชันนั้น ๆ ด้วย

ผู้ให้บริการสำรอง

ถ้าเกิดกรณีฉุกเฉินเกี่ยวกับระบบการทำงานข้อมูลของบริษัท ผู้ให้บริการสำรองต้องพร้อมในการรับมือกับเหตุการณ์ลักษณะนี้เสมอ โดยเฉพาะในกรณีบริษัทจัดจ้างภายนอกที่ใช้บริการอยู่ไม่สามารถทำงานหรือส่งงานตามกำหนดได้

แผนสำรองในการให้บริการของผู้ให้บริการ

สัญญาทุกฉบับที่ทำกับบริษัทให้เช่าเว็บไซต์ ผู้ให้บริการการจัดการระบบต่าง ๆ และบริษัทจัดจ้างภายนอกเกี่ยวกับระบบข้อมูลต่าง ๆ ของบริษัท ต้องมีการจัดทำแผนสำรองเป็นเอกสารอย่างชัดเจนและมีการทดสอบใช้ระบบสำรองนั้นจริงเป็นประจำตามแผนที่กำหนด

กลุ่มพนักงานส่วนงานฝ่ายเทคโนโลยีสารสนเทศ (IT)

การกำหนดสิทธิ์การใช้งานแอปพลิเคชันและการเข้าถึงข้อมูล

๑. การเข้าถึงในพื้นที่สงวนหรือเขตรักษาความปลอดภัยไม่ว่าเป็นทางกายภาพ (Physical access) หรือไม่ใช่ทางกายภาพ (Logical Access) และการเข้าถึงจากทางไกล (Remote access) ต้องมีวิธีการควบคุมโดยใช้วิธีการให้แสดงตัวตนของผู้เข้าถึงอย่างเข้มงวด (Identification method) และวิธีการตรวจสอบความเป็นตัวตนจริง (Authentication method) ของการเข้าถึงนั้น วิธีการตรวจสอบความเป็นตัวตนต้องถูกกำหนดโดยวิธีการเข้าถึงที่เป็นมาตรฐาน ซึ่งอาจจะต้องใช้วิธีการเข้ารหัสลับในการป้องกันผู้อื่นล่วงรู้

๒. พนักงานทุกคนต้องได้รับระดับและสิทธิ์ในการใช้งาน (Authorization) เพื่อเข้าถึงแอปพลิเคชันและระบบต่าง ๆ ในบริษัทอย่างเหมาะสม ทุกระดับและสิทธิ์ในการใช้งานต้องได้รับการอนุมัติจากเจ้าของข้อมูลหรือผู้มีอำนาจในการให้เข้าถึง หรือผู้จัดการโปรเจคนั้น ๆ ก่อนเสมอ

๓. วิธีการตรวจสอบความเป็นตัวตน (Authentication method) และวิธีการกำหนดสิทธิ์ (Authorization method)ในทุก ๆ แอปพลิเคชันและระบบต่าง ๆ ในบริษัทเหล่านี้ ต้องมีการทบทวนการใช้งานสิทธิ์อย่างเป็นประจำ

๔. ต้องมีการบันทึกล็อก (Log) การตรวจสอบความเป็นตัวตนของผู้ใช้งานระบบและเก็บไว้ในที่ ๆ ปลอดภัย

วิธีการป้องกันการขโมย

๑. อุปกรณ์เกี่ยวกับระบบการใช้งานและเครือข่าย ที่ติดตั้งอยู่ในที่โล่งแจ้ง ต้องมีการป้องกันการขโมยทางด้านกายภาพเป็นอย่างดี

๒. เซิร์ฟเวอร์ในระบบเครือข่าย (LAN) และระบบสำหรับใช้งานได้หลายคนต้องถูกติดตั้งและเก็บไว้ในห้องที่สามารถปิดล็อคได้

อุปกรณ์คอมพิวเตอร์และการควบคุมคอมพิวเตอร์

อุปกรณ์คอมพิวเตอร์และเครื่องคอมพิวเตอร์ที่ใช้งานกับระบบจริงต้องถูกเก็บและติดตั้งในพื้นที่สงวนหรือพื้นที่ ๆ มีความปลอดภัย ที่มีทั้งความปลอดภัยในแง่เครือข่าย ความปลอดภัยในระบบและความปลอดภัยในการพิมพ์งาน

การสร้างศูนย์คอมพิวเตอร์

การสร้างศูนย์คอมพิวเตอร์ใหม่หรือการปรับปรุงนั้น ต้องคำนึงถึงการป้องกันความเสียหายที่เกิดขึ้นจากไฟไหม้จากน้ำ จากการบุกรุกหรือทำลายทรัพย์สินจากบุคคลภายนอก และจากภัยต่าง ๆ ที่คาดว่าจะเกิดขึ้น หรืออาจจะเกิดขึ้นกับสถานที่ใกล้เคียงหรือที่เกี่ยวข้องได้

การจ่ายไฟฟ้า

คอมพิวเตอร์ทุกเครื่องที่ใช้ในการบริการลูกค้าโดยตรงต้องมีการใช้ไฟสำรองจากระบบจ่ายไฟฟ้าที่ดี ฟิลเตอร์ หรือตัวระงับการกระชากไฟ ที่ได้รับการเห็นชอบจากฝ่ายเทคโนโลยีสารสนเทศ

ความชื้นและการควบคุมอุณหภูมิ

เครื่องปรับอากาศทุกเครื่องในศูนย์คอมพิวเตอร์ต้องมีตัวอุปกรณ์ปรับอุณหภูมิให้คงที่และควบคุมความชื้นตลอด ๒๔ ชั่วโมงต่อวัน

การป้องกันความเสียหายที่เกิดจากน้ำ

ศูนย์คอมพิวเตอร์ต้องสร้างมาเพื่อป้องกันความเสียหายที่เกิดจากน้ำ ซึ่งจะต้องมีสัญญาณเตือนภัยเป็นขั้นต่ำและกำหนดโดยหน่วยงานความปลอดภัยข้อมูล ศูนย์คอมพิวเตอร์ต้องยกพื้นให้สูงกว่าพื้นราบปกติและสูงกว่าระดับน้ำที่จะสามารถท่วมถึง (กรณีที่มีวิธีการระบายน้ำ) และต้องตั้งให้อยู่สูงกว่าท่อน้ำ หรือไม่ตั้งอยู่ใกล้กับถังเก็บกักน้ำโดดเด็ดขาด

การใช้สอยอย่างปลอดภัยหรือการนำมาใช้ใหม่ของอุปกรณ์

หน่วยงานความปลอดภัยข้อมูลต้องทำการแยกข้อมูลสำคัญหรือข้อมูลลับของบริษัทออกจากส่วนงานของระบบที่ใช้กับทางธุรกิจก่อนที่จะนำออกสู่ภายนอกหรือ ติดต่อกับทางบริษัทคู่ค้า ผู้จัดการฝ่ายมีหน้าที่จัดการทรัพยากรที่ไม่เป็นประโยชน์ต่อกิจกรรมทางธุรกิจโดยเป็นไปตามขั้นตอนที่ทางหน่วยงานความปลอดภัยข้อมูลจัดทำไว้ รวมถึงการย้ายข้อมูลหรือซอฟต์แวร์ที่ไม่สามารถนำมาใช้งานได้อีกด้วย

ความปลอดภัยในการสื่อสารผ่านระบบเครือข่าย

๑. การเชื่อมต่อระบบเครือข่ายทั้งหมดจะถูกออกแบบหรือจัดทำโดยฝ่ายเทคโนโลยีสารสนเทศ (IT) บุคคลใดที่ต้องการเปลี่ยนค่าการติดตั้งเชื่อมต่อสายในการส่งข้อมูล ต้องมีการขออนุญาตจากหน่วยงาน IT ก่อนเริ่มต้นการทำงานนั้น ๆ

๒. การเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับข้อมูลที่เป็นความลับของบริษัท ต้องมีการเข้ารหัสเสมอผู้ใช้งานในระบบเครือข่ายที่ไม่สิทธิ์ในการเข้าถึงระบบข้อมูลหรือเครือข่ายใด ๆ ต้องไม่ได้รับสิทธิ์ในการเข้าถึงนั้นหรือได้รับสิทธิ์มากกว่าที่มีอยู่โดยเด็ดขาด

สิทธิ์พิเศษในการติดต่อสื่อสาร

เครื่องคอมพิวเตอร์ทุกเครื่องไม่ว่าจะเป็นเครื่องที่ใช้งานประจำหรือว่าติดตั้งแบบชั่วคราว และมีการเชื่อมต่อไปยังเครือข่ายภายนอกได้เพื่อทำการเข้าถึงโดยมีสิทธิ์พิเศษ ต้องมีการควบคุมและเห็นชอบจากหน่วยงานความปลอดภัยข้อมูลก่อน ผู้ใช้งานทั่วไปไม่สามารถทำการค้นหาระบบหรือเครือข่ายได้โดยไม่รับอนุญาต

ข้อมูลที่ถูกต้องครบถ้วน

ข้อมูลจากอินเทอร์เน็ตต้องถูกแยกออกจากข้อมูลที่มาจากแหล่งอื่น และมีการตรวจสอบในไวรัสก่อนโดยซอฟต์แวร์ป้องกันไวรัสเวอร์ชันปัจจุบัน ผู้ใช้งานทั่วไปต้องไม่ลงซอฟต์แวร์ใด ๆ บนเครื่องด้วยตัวเอง ห้ามเปิดไฟล์แนบมากับจดหมายอิเล็กทรอนิกส์หรืออีเมลถ้าหากจดหมายหรืออีเมลนั้นไม่ได้มาจากแหล่งที่เชื่อถือได้หรือบุคคลที่ที่รู้จัก

การรายงานเหตุการณ์

๑. ถ้าข้อมูลสำคัญหรือข้อมูลลับของบริษัทเกิดสูญหาย ถูกเปิดเผยแก่บุคคลภายนอก หรือสงสัยว่าจะมีเหตุการณ์ลักษณะนี้เกิดขึ้น ต้องมีการแจ้งให้กับทางหัวหน้าหน่วยงานความปลอดภัยข้อมูลรับทราบโดยทันที ผู้ใช้งานทั่วไปที่ได้รับข้อมูลเกี่ยวกับช่องโหว่ของระบบที่ใช้งานอยู่ต้องทำการส่งต่อให้กับหน่วยงานความปลอดภัยข้อมูล

๒. ผู้ใช้งานทั่วไป ต้องไม่ทำการทดสอบหรือทดลองการใช้งานวิธีการที่มีผลต่อระบบการใช้งานจริง ไม่ว่าจะภายในบริษัทหรือส่งผลต่อที่อื่นในอินเทอร์เน็ต ถ้าหากไม่ได้รับการเห็นชอบหรือ อนุญาตจากหน่วยงานความปลอดภัยข้อมูลก่อน

การสำรองข้อมูลและการนำข้อมูลกลับเข้าระบบ

๑. ข้อมูลในระบบต่าง ๆ ควรมีการทำการสำรองข้อมูลลงบนสื่อบันทึกข้อมูลเป็นประจำ

๒. ระบบการติดต่อสื่อสารหรือมีการใช้งานหลาย ๆ คนทางผู้ดูแลระบบมีหน้าที่ทำการสำรองข้อมูลเป็นระยะอย่างต่อเนื่อง

๓. เมื่อมีการร้องขอ ฝ่ายเทคโนโลยีสารสนเทศ (IT) ต้องให้ความช่วยเหลือในการติดตั้งฮาร์ดแวร์อุปกรณ์หรือซอฟต์แวร์ในการสำรองข้อมูล

๔. การสำรองข้อมูล สำหรับข้อมูลที่เป็นความลับมาก ต้องมีการเก็บไว้ในที่ ๆ ปลอดภัยและถูกควบคุมการเข้าถึงอย่างเป็นระบบ

๕. การสำรองข้อมูลลงอุปกรณ์จะต้องเก็บไว้ในที่ลับเฉพาะเพื่อจะนำมาใช้ใหม่เมื่อมีการนำข้อมูลกลับเข้าสู่ระบบ เมื่อเกิดเหตุการณ์ เช่น ระบบคอมพิวเตอร์ติดไวรัสและมีความเสียหายต้องมีการกู้ข้อมูล มีการติดไวรัสที่ฮาร์ดดิสก์ หรือเกิดปัญหาอื่น ๆ ที่เครื่องคอมพิวเตอร์ขึ้นเป็นต้น

๖. มีการทำติดตามสถานะของการสำรองข้อมูลว่าสามารถสำรองข้อมูลได้อย่างสมบูรณ์ ทุก ๆ ไตรมาสเพื่อให้มั่นใจว่าบริษัทจะสามารถนำสื่อบันทึกข้อมูลที่สำรองกลับมาใช้งานในกรณีฉุกเฉินได้

๗. ต้องมีการจัดทำแผนสำรองฉุกเฉินไว้สำหรับแอปพลิเคชันต่าง ๆ ที่มีการจัดการเกี่ยวกับการใช้งานข้อมูลในระบบที่มีความสำคัญต่อธุรกิจ เจ้าของข้อมูลต้องแน่ใจว่าแผนที่จัดทำสามารถรองรับกับการใช้งานจริง มีการปรับปรุงแก้ไขให้ทันสมัยที่สุด และมีการทบทวนแผนอย่างต่อเนื่อง

๘. พิจารณาให้มีการเข้ารหัสข้อมูลที่สำรองไว้ และจัดเก็บข้อมูลในลักษณะออฟไลน์

แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

เหตุการณ์	การวางแผน	การดำเนินการ	การตรวจสอบ	การปรับปรุงเพิ่มเติม
ปัญหาจากการบุกรุกพื้นที่	กำหนดสิทธิ์การเข้าถึงพื้นที่ต่าง ๆ ของพนักงานและบุคคลภายนอก	ติดตั้ง Access Control และให้สิทธิ์การเข้าถึงพื้นที่ตามความเหมาะสม	ตรวจสอบการเข้าถึงพื้นที่ของพนักงานและบุคคลภายนอก	ทำการปรับตั้งค่าให้เหมาะสม, เพิ่ม – ลบ ข้อมูลของพนักงานใหม่ และพนักงานที่พ้นสภาพ
ปัญหาจากการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	ทำการบันทึกการเข้าใช้งานระบบ (Log) ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	จัดเก็บข้อมูลการใช้งานระบบไม่น้อยกว่าเก้าสิบวันตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	ตรวจสอบการบันทึกข้อมูลในอุปกรณ์บันทึกข้อมูล พร้อมประมาณการบันทึกข้อมูลตามการใช้งานระบบ	เพื่อสื่อบันทึกข้อมูล กรณีพื้นที่บันทึกข้อมูลไม่เพียงพอต่อจำนวนวันที่ต้องบันทึก
ปัญหาจากการติดต่อสื่อสารจากระบบเทคโนโลยีสารสนเทศ	พนักงานใช้งานระบบตามชื่อบัญชีของตน	พนักงานเข้าใช้งานระบบของตนตามที่ได้ส่งมอบให้	ตรวจสอบระบบการทำงาน จาก Log ระบบที่ได้บันทึกไว้	หากไม่สามารถใช้งานได้สามารถติดต่อเจ้าหน้าที่ไอที เพื่อดำเนินการแก้ไขปัญหา

เหตุการณ์	การวางแผน	การดำเนินการ	การตรวจสอบ	การปรับปรุงเพิ่มเติม
ปัญหาจากการกำหนดสิทธิ์การใช้งาน	พนักงานต้องใช้งานระบบด้วยชื่อบัญชีของพนักงานเท่านั้น	พนักงานเข้าใช้ระบบด้วยชื่อบัญชีของตน	ตรวจสอบระบบการทำงาน จาก Log ระบบที่ได้บันทึกไว้	จัดทำระบบเฝ้าระวังการใช้งานชื่อบัญชีของพนักงานแบบไม่พึงประสงค์
ปัญหาจากการใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	ตรวจสอบการใช้งานซอฟต์แวร์ของบริษัท	จัดหาซอฟต์แวร์ที่ใช้งานภายในบริษัท จัดซื้อซอฟต์แวร์ที่จำเป็นและจัดหาซอฟต์แวร์โอเพ่นซอร์สเพื่อใช้งานทดแทน	ตรวจสอบการใช้งานซอฟต์แวร์ในเครื่องพนักงาน	รับแจ้งความต้องการใช้งานซอฟต์แวร์เพิ่มเติมพร้อมตรวจสอบจำนวนอุปกรณ์ที่ใช้งานภายในบริษัท
ปัญหาจากไวรัสคอมพิวเตอร์และการโจมตีทางไซเบอร์	ป้องกันไวรัสและการโจมตีทางไซเบอร์ผ่านระบบเครือข่ายและอินเตอร์เน็ต	ทำการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์ที่ใช้งานและเปิดความสามารถป้องกันไวรัสและป้องกันการโจมตีทางไซเบอร์ที่ไฟล์วอล	ตั้งค่าแจ้งเตือนเมื่อพบไวรัส หรือการโจมตีต่าง ๆ มายังเจ้าหน้าที่ไอที	อัพเดตรายชื่อไวรัสและการโจมตีต่าง ๆ ในระบบที่ใช้งาน ติดตามข่าวสารและทำการตรวจสอบปรับปรุงระบบ และปิดช่องโหว่ ต่าง ๆ ที่มีประกาศออกมาก
ปัญหาจากการเข้าถึงข้อมูลจากบุคคลที่ไม่มีสิทธิ์จากภายนอกบริษัท	จัดทำระบบเครือข่ายส่วนตัวแบบเสมือน (VPN) ให้ใช้งานกรณีต้องใช้งานระบบจากภายนอกบริษัท	พนักงานใช้งานระบบดังกล่าวในการดำเนินการ	ตรวจสอบ Log การใช้งานตรวจสอบหาความผิดปกติในการใช้งานและติดตั้งระบบแจ้งเตือน เมื่อมีการใช้งานแบบผิดปกติ	ตรวจสอบการใช้งาน ว่าเพียงพอกับความต้องการหรือไม่
ปัญหาจากการกระแสไฟฟ้า	มีกระแสไฟฟ้าจ่ายให้ระบบอย่างต่อเนื่อง	ทำการติดตั้งระบบสำรองไฟฟ้าในระบบที่ให้บริการ	ทดสอบการทำงานผ่านระบบที่มีในเครื่องสำรองไฟฟ้า	ตรวจสอบการทำงานว่าสามารถสำรองไฟฟ้าได้ เป็นระยะเวลาที่กำหนดหรือไม่ หากมีการทำงานไม่ตรงกับข้อกำหนดให้ดำเนินการปรับปรุง เช่นลดการใช้กระแสไฟฟ้า เพิ่มระบบสำรองไฟฟ้า
ปัญหาจากระบบอินเตอร์เน็ต	ระบบสามารถใช้งานอินเตอร์เน็ตได้อย่างต่อเนื่อง	ติดตั้งอินเตอร์เน็ตเพื่อให้ระบบใช้งาน	จัดทำระบบตรวจสอบการทำงานของอินเตอร์เน็ต	ทำระบบตรวจจับการทำงานของอินเตอร์เน็ต, ขอติดตั้งอินเตอร์สำรอง ป้องกันปัญหาผู้ให้บริการไม่สามารถให้บริการได้
ปัญหาจากอุปกรณ์ระบบเครือข่ายและเครื่องแม่ข่าย	อุปกรณ์พร้อมใช้งานเสมอ	เมื่อเกิดปัญหาให้ดำเนินการแก้ไขให้ระบบกลับมาใช้งานได้	ทำการตรวจสอบการทำงานทุกวันว่า ระบบพร้อมทำงาน ตรวจสอบการทำงาน หลังจากทำการแก้ไขปัญหา	ทำการซื้อการสนับสนุนจากผู้ผลิตและตัวแทนจำหน่าย ปรับเปลี่ยนอุปกรณ์ตามอายุการใช้งาน, วางแผนป้องกันสาเหตุที่พบปัญหา

เหตุการณ์	การวางแผน	การดำเนินการ	การตรวจสอบ	การปรับปรุงเพิ่มเติม
ปัญหาข้อมูลสูญหายจากระบบ	พนักงานสามารถใช้งานระบบและข้อมูลได้	เมื่อได้รับแจ้ง เจ้าหน้าที่ไอที จะทำการตรวจสอบและกู้คืนระบบตามที่ได้รับแจ้ง	ทำการตรวจสอบระบบสำรองข้อมูล, ทำการบันทึกผลข้อมูล และจัดเก็บสื่อบันทึกข้อมูลพร้อมทำป้ายกำกับอย่างเหมาะสม	เพิ่มสื่อบันทึกข้อมูลตามความเหมาะสม
ปัญหาจากซอฟต์แวร์และโปรแกรมที่ใช้งาน	ระบบสามารถให้บริการต่าง ๆ ได้	เมื่อรับแจ้งปัญหาเจ้าหน้าที่ไอทีทำการตรวจสอบระบบและดำเนินการแก้ไขปัญหา	ทำการตรวจสอบการทำงานของระบบ, ซอฟต์แวร์ และโปรแกรมที่ใช้งานพร้อมบันทึกผล	ทำการตรวจสอบ Patch, และทำการ Update ที่เหมาะสมกับระบบ
ปัญหาจากการไม่สามารถเข้าถึงพื้นที่บริษัท	เมื่อพนักงานไม่สามารถเข้าถึงพื้นที่บริษัทเพื่อปฏิบัติงานได้	พนักงานสามารถเข้าถึงระบบไอทีจาก Internet ผ่าน VPN	ตรวจสอบว่า VPN พร้อมใช้งาน	ขยายช่องสัญญาณให้เหมาะสมตามการใช้งาน
ปัญหาจากอัคคีภัย	มีระบบแจ้งเตือนอัคคีภัย และระบบดับเพลิงในห้องศูนย์ข้อมูลเบื้องต้น	เมื่อพบเหตุผู้ประสบเหตุสามารถแจ้ง เจ้าหน้าที่ไอที เพื่อเปิดห้องและดำเนินการดับเพลิงด้วยอุปกรณ์ที่จัดเตรียมไว้ หากสามารถดับเพลิงได้ ให้ทำการแจ้งเจ้าหน้าที่ที่เกี่ยวข้อง หากไม่สามารถดับเพลิงได้ ให้ทำการอพยพตามแผนดับเพลิง ของอาคาร	ทำการตรวจสอบผลกระทบจากเพลิงไหม้ว่าระบบสามารถทำงานต่อได้หรือไม่ ถ้าสามารถดำเนินการต่อได้ ให้ทำบันทึกข้อมูล ก่อนเปิดระบบ และตรวจสอบการทำงานของระบบ หากไม่สามารถเปิดระบบที่ประสบเหตุได้ ให้ทำการจัดหาอุปกรณ์เพื่อทำการกู้คืนระบบ	ติดตั้งอุปกรณ์ป้องกันเพลิงไหม้ที่ทำงานแบบอัตโนมัติ, ทำการสำรองข้อมูลและจัดเก็บสื่อบันทึกข้อมูลในสถานที่ อื่น, จัดให้พนักงานไอทีที่เกี่ยวข้องอบรมการใช้งาน เครื่องดับเพลิงสำหรับศูนย์คอมพิวเตอร์
ปัญหาจากความไม่สงบเรียบร้อยในบ้านเมือง	ระบบไอทีสามารถทำงานได้	ให้พนักงานใช้งานระบบผ่าน VPN	ตรวจสอบการใช้งานและช่องสัญญาณให้เพียงพอต่อการใช้งาน	ขยายช่องสัญญาณหากมีการใช้งานปริมาณสูง หรือย้ายขึ้นระบบ Cloud หรือทำศูนย์ข้อมูลสำรอง หากมีปัญหาไม่สามารถ ใช้บริการศูนย์ข้อมูลหลักได้
ปัญหาจากภัยพิบัติเป็นผลให้ระบบเดิมไม่สามารถให้บริการได้	ระบบไอทีสามารถทำงานได้	ทำการจัดหาอุปกรณ์และโครงสร้างพื้นฐานที่จำเป็นสำหรับระบบทั้งหมด และดำเนินการ กู้ข้อมูลจากสื่อบันทึกข้อมูลจากแหล่งที่จัดเก็บ สื่อข้อมูลสำรอง เมื่อดำเนินการแล้วเสร็จจะทำการตรวจสอบการทำงานของระบบตามการตรวจสอบประจำวัน	ตรวจสอบการใช้งานว่าสามารถให้บริการได้ตามปกติ	ในการจัดหาโครงสร้างพื้นฐานสำหรับระบบทั้งหมดอาจใช้เวลานาน ซึ่งอาจนำระบบ Cloud มาร่วมในการกู้คืนระบบได้

การจัดการกับการเปลี่ยนแปลง (CHANGE MANAGEMENT)

๑. ระบบคอมพิวเตอร์และระบบการติดต่อสื่อสารของบริษัทที่ใช้สำหรับการดำเนินการทางธุรกิจต้องมีเอกสารซึ่งบอกถึงขั้นตอนในจัดการกับการเปลี่ยนแปลงในระบบอย่างชัดเจน เพื่อให้แน่ใจว่าบุคคลที่กระทำการเปลี่ยนแปลงข้อมูลต่าง ๆ ในระบบเป็นผู้ที่ได้อนุญาตและมีสิทธิ์ในการเปลี่ยนแปลงนั้น ๆ จริง

๒. ต้องมีการปฏิบัติตามระเบียบขั้นตอนของการจัดการที่กำหนดไว้ทุกครั้ง ในกรณีที่มีการเปลี่ยนแปลงค่าต่าง ๆ ที่มีผลกระทบกับระบบการทำงานจริง อุปกรณ์ การเชื่อมต่อ หรือขั้นตอนปฏิบัติงาน

๓. นโยบายนี้รวมไปถึงคอมพิวเตอร์ที่ใช้ทำงานในระบบปฏิบัติงานจริงและระบบการใช้งานที่เข้าถึงได้จากพนักงานหลายคนด้วย

การพัฒนาและปรับปรุงรักษาระบบ

๑. การพัฒนาและการปรับปรุงรักษาซอฟต์แวร์สำหรับการใช้งานจริงในระบบโดยพนักงานของบริษัทต้องปฏิบัติตามนโยบายของฝ่ายเทคโนโลยีสารสนเทศ มาตรฐาน ขั้นตอนและระเบียบต่าง ๆ ของบริษัท

๒. ระเบียบต่าง ๆ ที่กล่าวถึงนี้รวมไปถึงการทดสอบ การฝึกอบบรม และเอกสารอ้างอิงที่จัดทำไว้

๓. การเปลี่ยนแปลงไฟล์หรือซอฟต์แวร์ต่าง ๆ ก็ต้องปฏิบัติตามระเบียบข้อกำหนดของการควบคุมการจัดการการเปลี่ยนแปลงระบบด้วย (Change management)

การจัดการเกี่ยวกับใบอนุญาตซอฟต์แวร์

๑. ผู้บริหารต้องต่อรองข้อตกลงอย่างเหมาะสมกับทางผู้ให้บริการซอฟต์แวร์โดยคำนึงถึงความจำเป็นในการใช้ใบอนุญาตซอฟต์แวร์หรือ License เพิ่มเติม

๒. จะมีการซื้อซอฟต์แวร์ที่มีความจำเป็นต่อการใช้งานจริงในบริษัท

การเข้าถึงข้อมูลที่เป็นความลับโดยสิทธิ์อ่านได้อย่างเดียว

ผู้ใช้งานที่มีสิทธิ์ในการเข้าถึงข้อมูลที่เป็นความลับโดยการอ่านได้อย่างเดียว ต้องได้รับอนุญาตในการเข้าถึงเพียงข้อมูลระดับนี้หรือน้อยกว่าระดับนี้เท่านั้น

การเข้าถึงข้อมูลที่เป็นความลับโดยมีสิทธิ์การแก้ไขได้

ผู้ใช้งานต้องไม่ทำการเคลื่อนย้ายข้อมูลที่อยู่ในระดับนี้ไปยังระดับที่อยู่น้อยกว่า เว้นแต่จะมีการทำการยกเลิกข้อมูลชนิดนี้ออกจากระดับข้อมูลนี้ ตามขั้นตอนที่ถูกต้อง

การจัดการบัญชีผู้ใช้งาน

พนักงานแต่ละคนจะได้รับบัญชีผู้ใช้งาน (User Id) ของตัวเองซึ่งจะเป็นข้อมูลการใช้งานของพนักงานคนนั้น ๆ โดยเฉพาะ ผู้จัดการต้องมีการแจ้งให้หน่วยงานที่รับผิดชอบในการตั้งค่าบัญชีผู้ใช้งาน เมื่อพนักงานคนนั้นมีการเปลี่ยนแปลงในเรื่องของหน้าที่การทำงาน สิทธิ์ในการเข้าถึง และอื่น ๆ ที่เกี่ยวข้องกับการทำงานของพนักงานทันที บัญชีผู้ใช้งานต้องไม่สามารถใช้งานได้อีกต่อไปเมื่อเจ้าของบัญชีผู้ใช้งานนั้นลาออกจากบริษัทหรือไม่มีสิทธิ์ในการเข้าถึงงานหรือระบบที่เกี่ยวข้องกับบัญชีการใช้งานนั้นในบริษัทอีกต่อไป

การจัดการสิทธิพิเศษ

สิทธิพิเศษในเรื่องเกี่ยวกับคอมพิวเตอร์และระบบการติดต่อสื่อสารของผู้ใช้งาน ระบบ โปรแกรมทั้งหมด ต้องถูกกำหนดให้ขึ้นอยู่กับความจำเป็นในการใช้งาน ในกรณีที่มีการร้องขอพิเศษ จะขึ้นอยู่กับความรับผิดชอบโดยตรงที่เกี่ยวข้องกับการบริหารจัดการระบบหรือความปลอดภัยข้อมูล และต้องทำการยกเลิกทันที เมื่อไม่ได้มีการใช้งานแล้ว

การควบคุมการเข้าถึงโดยใช้รหัสผ่าน

ระบบที่มีขนาดเล็ก แต่มีการจัดการเกี่ยวกับข้อมูลที่เป็นความลับหรือข้อมูลสำคัญ ต้องมีการกำหนดให้ใช้ระบบการเข้าถึงโดยใช้รหัสผ่าน

ซอฟต์แวร์อันตราย

ซอฟต์แวร์ตรวจสอบไวรัส (Virus Detection Software)

๑. ผู้ใช้งานระบบคอมพิวเตอร์ไม่ควรจะยกเลิกหรือปิดขั้นตอนการอัปเดตเวอร์ชันไวรัสที่ทำงานขึ้นเองโดยอัตโนมัติ

๒. ไฟล์ของระบบทุกไฟล์ควรจะมีการสแกนหรือตรวจสอบโดยซอฟต์แวร์ที่ใช้ตรวจสอบไวรัส

๓. ต้องมีการสแกนไวรัสก่อนที่จะเปิดไฟล์ใหม่ ๆ หรือก่อนที่จะทำการเปิดหรือติดตั้งซอฟต์แวร์ตัวใหม่ก่อน

ความปลอดภัยของระบบเครือข่าย

การเชื่อมต่อระบบเครือข่ายภายใน

๑. คอมพิวเตอร์ทุกเครื่องที่ทำหน้าที่เก็บข้อมูลที่เป็นความลับหรือมีการเชื่อมต่อกับระบบคอมพิวเตอร์เครือข่ายของบริษัทเพื่อใช้งานเป็นประจำ หรือชั่วคราวต้องได้รับการอนุญาตในการเข้าถึงระบบจากหน่วยงานความปลอดภัยข้อมูลก่อน

๒. ระบบการจัดการประมวลผลข้อมูลทุกชนิดต้องติดตั้งรหัสผ่านหรือมีการล็อคหน้าจอหลังจากที่ไม่มีการใช้งานอัตโนมัติภายในระยะเวลาที่กำหนดไว้ และเมื่อต้องการใช้งานอีกครั้ง ก็ต้องมีการร้องขอให้ใส่รหัสผ่าน

๓ ระบบที่ใช้งานหลายคนต้องใช้วิธีการปิดการเชื่อมต่ออัตโนมัติเมื่อไม่มีการใช้งานของผู้ใช้งานเกิดขึ้นในระยะเวลาหนึ่งหรือภายในระยะเวลาที่กำหนดไว้

การเชื่อมต่อระบบเครือข่ายภายนอก

๑. การเชื่อมต่อระบบจากภายนอกเข้าสู่ระบบข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการป้องกันโดยระบบการเข้าถึงโดยการใช้รหัสผ่านแบบเปลี่ยนแปลงได้ (dynamic password) หรือใช้รหัสผ่านแบบตรวจสอบความเป็นตัวตนจากจุดเดียว (Single sign-on user and password) การใช้งานรหัสผ่านแบบเปลี่ยนแปลงได้ในแต่ละครั้งที่มีการใช้งาน สามารถป้องกันการขโมยรหัสผ่านได้

๒. พนักงานบริษัทไม่ควรจะเชื่อมต่อหรือสร้างการเชื่อมต่อออกไปยังเครือข่ายภายนอกหรืออินเทอร์เน็ตเอง โดยใช้ระบบของบริษัท โดยไม่ได้รับอนุญาตจากหน่วยงานความปลอดภัยข้อมูลก่อน

การเปลี่ยนแปลงระบบเครือข่าย

๑. การเปลี่ยนแปลงระบบคอมพิวเตอร์ของบริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการบันทึกลงในแบบฟอร์มการขอเปลี่ยนแปลง (change request form) และต้องได้รับการอนุมัติจากผู้มีอำนาจในขั้นตอนการควบคุมการเปลี่ยนแปลงนั้น ยกเว้นได้ในกรณีฉุกเฉินเท่านั้น

๒. การเปลี่ยนแปลงต่าง ๆ ที่มีผลมายังระบบเครือข่ายภายในต้องมีการแจ้งให้กับผู้มีอำนาจหรือผู้รับผิดชอบในส่วนงานเทคโนโลยีสารสนเทศรับทราบก่อน

๓. ขั้นตอนนี้สามารถลดความเสี่ยงที่เกิดจากผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลและการเปลี่ยนแปลงนี้อาจจะทำให้เกิดผลร้ายแรงได้จากผู้ที่รู้เท่าไม่ถึงการณ์ถึงแม้ว่าจะมีสิทธิ์ในฝ่ายเทคโนโลยีสารสนเทศได้

๔. ขั้นตอนนี้กำหนดใช้กับพนักงานบริษัทสกาย ไอซีทีและกลุ่มบริษัทในเครือ และรวมไปถึงผู้ที่ให้บริการด้วย

การทำงานทางไกล

๑. พนักงานในบางหน่วยงานสามารถมีสิทธิ์ในการทำงานจากที่บ้านได้

๒. การอนุญาตเพื่อให้ทำงานจากทางไกลได้นั้น ส่วนหนึ่งขึ้นอยู่กับนโยบายและมาตรฐานความปลอดภัยข้อมูล

การจัดการความเสี่ยง

เพื่อให้การปฏิบัติงานของระบบคอมพิวเตอร์และระบบเครือข่ายเป็นไปอย่างต่อเนื่องด้วยดี บริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการจัดทำแผนการดำเนินงานทางธุรกิจให้ต่อเนื่อง (Business continuity plan) ซึ่งประกอบไปด้วย:

๑. การประเมินความเสี่ยงทางธุรกิจ

๒. ลักษณะของการบริหารความเสี่ยง

๓. การระบุความเสี่ยงที่จะเกิดขึ้น

๔. การวัดค่าความเสี่ยง

๕. แผนการรับมือกับความเสี่ยงที่จะเกิดขึ้น

๖. ความเสี่ยงที่สามารถยอมรับได้

๗. การเลือกวิธีหรือเครื่องมือป้องกัน

๘. การพิจารณาผลการประเมินความเสี่ยง

แผนการดำเนินงานทางธุรกิจให้ต่อเนื่อง (BCP)

บริษัทต้องมีการตั้งทีมงานเพื่อทำแผนการจัดการเกี่ยวกับการบริหารความเสี่ยงและอบรมให้ความรู้แก่ผู้ใช้งานถึงเรื่องแผนการดำเนินงานทางธุรกิจให้ต่อเนื่องเป็นประจำทุกปี รวมถึงการปรับปรุงแผนการและต้องมีการอัปเดตให้ใหม่เข้ากับสถานการณ์ของบริษัทปัจจุบัน และทำการอัปเดตในความเป็นไปได้ทุกเหตุการณ์ที่อาจจะเกิดขึ้น ซึ่งจะต้องประกอบไปด้วยลักษณะอาการต่าง ๆ สาเหตุที่ทำให้เกิด และวิธีการแก้ไข

การบันทึกการจราจรข้อมูลทางอินเทอร์เน็ต

อ้างถึงมาตรฐานการเก็บบันทึกการจราจรข้อมูลหรือล็อก (Log) กำหนดโดยกระทรวงเทคโนโลยีสารสนเทศของประเทศไทย ปีพุทธศักราช ๒๕๕๐ ซึ่งมีชนิดของข้อมูล หรือล็อกที่ต้องได้รับการบันทึกและเก็บไว้ดังนี้

๑. Log ของระบบเครือข่าย

- ข้อมูลการเข้าถึงระบบระบุถึงบุคคลที่สามารถเข้าถึงและสิทธิ์ในการเข้าถึงระบบเครือข่าย
- ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
- ข้อมูลของบัญชีผู้ใช้งานระบุตัวตนผู้ใช้งาน
- ข้อมูลเลขหมายหรือ IP Address ที่กำหนดให้เครื่องลูกข่าย
- ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา

๒. Log ของการใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล ทางบริษัท ใช้บริการ จดหมายอิเล็กทรอนิกส์ Microsoft Exchange / Microsoft Office ๓๖๕ suite อาจจะมีข้อมูลหลาย ๆ ข้อนี้

- ข้อมูลหมายเลขของข้อความที่ระบุในอีเมล (Message ID)
- ข้อมูลชื่อที่อยู่อีเมลของผู้ส่ง
- ข้อมูลชื่อที่อยู่อีเมลของผู้รับ
- ข้อมูลที่บ่งบอกสถานะของอีเมล เช่น ส่งล่าช้า ส่งสำเร็จ ปฏิเสธการส่ง หรือส่งคืนผู้ส่ง เป็นต้น
- ข้อมูลเลขหมาย หรือ IP address ที่กำหนดให้เครื่องลูกข่าย
- ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
- ชุดข้อมูลเลขหมาย หรือ IP address ของเครื่องผู้ส่งอีเมล
- บัญชีชื่อผู้ใช้งาน
- ข้อมูลที่มีการบันทึกการเข้า ออก ของอีเมล ผ่านโปรแกรมการจัดการจากเครื่องของสมาชิกหรือการเข้าถึงเพื่อเรียกข้อมูลอีเมลไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลอีเมลที่ดึงไปนั้นไว้ที่เครื่องให้บริการหรือเครื่องเซิร์ฟเวอร์ (POP3 or IMAP4 log)

๓. Log โอนไฟล์หรือข้อมูล

- ข้อมูลทุกอย่างเมื่อมีการเข้าถึงเครื่องให้บริการโอนไฟล์ข้อมูล
- ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
- ข้อมูลหมายเลขของเครื่องคอมพิวเตอร์ที่เข้ามาทำการเชื่อมต่ออยู่ในขณะนั้น
- บัญชีชื่อผู้ใช้งาน
- ข้อมูลตำแหน่งและชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป
- ข้อมูลการเข้าถึง แก้ไข หรือเปลี่ยนแปลงข้อมูล รวมถึงการเปลี่ยนแปลงสิทธิของผู้ใช้งาน

๔. Log การเข้าถึงอินเทอร์เน็ต

- ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
- ข้อมูลหมายเลขหรือ IP address ของเครื่องที่ทำการเชื่อมต่อไปยังเครื่องให้บริการหรือเครื่องเซิร์ฟเวอร์และคำสั่งการใช้งาน

ข้อปฏิบัติและข้อบังคับตามกฎหมาย

บริษัท มีการจัดทำการตรวจสอบความปลอดภัยข้อมูลเพื่อให้ถูกต้องและตรงกับนโยบาย ระเบียบและกฎหมายอย่างต่อเนื่อง

การปฏิบัติตามนโยบายและระเบียบ

พนักงานทุกคนต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลและเอกสารที่เกี่ยวข้องกับนโยบายนี้ รวมถึงนโยบายอื่น ๆ ที่เกี่ยวข้อง อย่างเคร่งครัด เช่น นโยบายการคุ้มครองข้อมูลส่วนบุคคล พนักงานท่านใดที่ละเลย หรือมีเจตนาที่จะไม่ปฏิบัติตาม ถือว่ามีการละเมิดนโยบายดังกล่าว จะได้รับบทลงโทษหรืออาจจะร้ายแรงถึงขั้นไล่ออก

การปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ

นโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลจะต้องเป็นไปตามข้อบังคับทางกฎหมาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช ๒๕๖๒ (PDPA) กฎหมายที่เกี่ยวกับการป้องกันข้อมูล การเข้าถึงข้อมูล การป้องกันข้อมูลส่วนตัวและเอกสารอิเล็กทรอนิกส์ต่าง ๆ เป็นต้น

ตามระเบียบข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช ๒๕๕๐ นั้นถือว่าบริษัท สกาย ไอซีที จำกัด (มหาชน) เป็นผู้ให้บริการเข้าถึงอินเทอร์เน็ต ซึ่งต้องมีการบันทึกและเก็บการบันทึกข้อมูลจราจรทางอินเทอร์เน็ตทั้งหมดตามวันและเวลาที่เข้าถึง ย้อนหลังอย่างน้อย ๙๐ หรือมากกว่านั้น

ระเบียบและบทลงโทษ

๑. การกระทำที่สงสัยว่าจะละเมิดนโยบายการรักษาความปลอดภัย (การเจาะข้อมูล, การทำลายข้อมูลของไวรัสคอมพิวเตอร์) หรือสงสัยว่ามีการล่วงละเมิดหรือแทรกแซงระบบข้อมูล ต้องแจ้งให้กับผู้บริหาร และเจ้าหน้าที่รักษาความปลอดภัยข้อมูลทราบทันที

๒. การกระทำที่สงสัยว่าจะละเมิดข้อมูลส่วนบุคคล ต้องดำเนินการแจ้งให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทันทีโดยอ้างอิงจาก "**นโยบายการคุ้มครองข้อมูลส่วนบุคคล**"

๓. การละเมิดหรือการไม่ปฏิบัติตามนโยบายการรักษาความปลอดภัยของข้อมูล มีบทลงโทษต่อผู้ละเมิดอย่างร้ายแรง ระเบียบการลงโทษมีความรุนแรงขึ้นอยู่กับการกระทำ และสามารถรุนแรงถึงขั้นไล่ออก

๔. การทำตามระเบียบของพนักงานทั้งหมดที่อยู่ภายใต้การดูแลของหัวหน้าฝ่ายหรือผู้มีระดับที่สูงกว่า เมื่อพนักงานทำผิดหรือละเมิดกฎหัวหน้าฝ่ายหรือผู้มีระดับที่สูงกว่าจะเป็นผู้พิจารณาลงโทษ

๕. การกระทำที่ถือว่าเป็นการละเมิดกฎมีดังนี้

๕.๑ การเปลี่ยนแปลงแก้ไขข้อมูลภายในระบบโดยไม่ได้รับอนุญาตจากผู้มีอำนาจหรือหัวหน้างานก่อน

๕.๒. การปลอมแปลง ขโมย ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าใช้งานในระบบแอปพลิเคชันใด ๆ โดยตั้งใจหรือไม่ตั้งใจก็ตาม

๕.๓ การใช้บัญชีผู้ใช้งานและรหัสผ่านของผู้อื่นในการเข้าใช้งานระบบคอมพิวเตอร์เพื่ออ่าน คัดลอกหรือทำสำเนา เปลี่ยนแปลงหรือลบข้อมูลไม่ว่าจะด้วยเหตุผลใด ๆ ก็ตาม

๕.๔ การละเลยและอนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้งานและรหัสผ่านของตัวเองในการเข้าใช้งานระบบคอมพิวเตอร์รวมถึงให้ใช้สิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์นั้น ๆ ด้วย

๕.๕ ทำการพยายามเปิดเผย ขาย และกระจายข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน)

๕.๖ การพยายามเข้าใช้งานระบบและแอพลิเคชันใด ๆ โดยไม่มีสิทธิ์ในการใช้งาน

๕.๗ การติดตั้ง ตรวจสอบ เฝ้าดู และใช้เครื่องมือหรือซอฟต์แวร์ในการเจาะข้อมูล (hacking tools) หรือโปรแกรมที่เกี่ยวกับตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์ ยกเว้นผู้ที่มีหน้าที่รับผิดชอบในด้านในการทำการดังกล่าวเท่านั้น

๕.๘ ติดตั้งและทำการเปลี่ยนแปลงหมายเลขของเครื่องคอมพิวเตอร์ (IP address) โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ (IT) ก่อน

๕.๙ การเปลี่ยนแปลง โอนย้าย หรือติดตั้ง ส่วนใดส่วนหนึ่งในระบบคอมพิวเตอร์โดยไม่ได้รับการอนุญาตจากฝ่าย IT ก่อน

๕.๑๐ การร่วมมือกับบุคคลภายนอกเพื่อให้เข้ามาใช้งานระบบคอมพิวเตอร์หรือโปรแกรมแอปพลิเคชันใด ๆ หรือทำลายการรักษาความปลอดภัยของข้อมูลหรือระบบของบริษัท สกาย ไอซีที จำกัด (มหาชน)

๖. บทลงโทษการฝ่าฝืนและละเลย

๖.๑ การกล่าวตักเตือน

๖.๒ ออกจดหมายเตือน

๖.๓ ได้รับการพักงานชั่วคราว

๖.๔ พ้นสภาพจากการเป็นพนักงานของบริษัท

๖.๕ บริษัทฯ จะพิจารณาและใช้ความละเอียดรอบคอบในการลงโทษพนักงานที่ทำผิดหรือละเมิดนโยบาย

บทสรุป

บริษัท สกาย ไอซีที จำกัด (มหาชน) จำเป็นต้องมีการพัฒนานโยบาย ระเบียบขั้นตอน ข้อแนะนำ และมาตรฐานต่าง ๆ ขึ้นมา เพื่อให้การสนับสนุนการทำงานในส่วนนโยบายความมั่นคงปลอดภัยสารสนเทศข้อมูลนี้ ซึ่งมีการประกาศใช้อย่างเป็นทางการให้ได้รับทราบภายในบริษัท คู่มือของนโยบายการรักษาความปลอดภัย สามารถใช้อ้างอิงถึงมาตรฐานหรือนโยบายย่อยที่ใช้ควบคุมระบบต่าง ๆ ภายในบริษัทและมีการปรับปรุงอย่างต่อเนื่อง

มีผลตั้งแต่วันที่ 14 พฤศจิกายน 2568 เป็นต้นไป

-สมคิด เลิศไพฑูรย์

(ศ.ดร. สมคิด เลิศไพฑูรย์)

ประธานกรรมการ

อนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 9/2568

เมื่อวันที่ 13 พฤศจิกายน 2568