นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท ดิทโต้ (ประเทศไทย) จำกัด (มหาชน)

1. หลักการและเหตุผล

กลุ่มบริษัท ดิทโต้ (ประเทศไทย) จำกัด (มหาชน) กำหนดให้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัทเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ กลุ่มบริษัท จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ

2. วัตถุประสงค์

2.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยมีการปรับปรุงอย่างต่อเนื่อง

2.3 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่จะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย 1 ครั้ง ต่อปี

3. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1 ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

3.2 มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือ ฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

3.3 เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

3.4 เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

3.5 ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

4. องค์ประกอบของนโยบาย

4.1. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

4.2. การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

4.3. การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

4.4. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

4.5. การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

4.6. การรักษาความมั่นคงปลอดภัยของอีเมล์ (E-mail Policy)

4.7. การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Internet Cyber Security Policy)

4.8. การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

4.9. ความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

4.10. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Organizational of Information Security)

4.11. การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)

4.12. การบริหารจัดการสินทรัพย์ (Asset Management)

4.13. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

4.14. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

4.15. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

4.16. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security - aspects of business continuity management)

4.17. การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

4.18. การเข้ารหัสข้อมูล (Cryptography)

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย)

รองประธาน เจ้าหน้าที่บริหารด้านปฏิบัติการ หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย) ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย)

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย) และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย)

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย)

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งกลุ่มบริษัทบมจ. ดิทโต้ (ประเทศไทย) กำหนดไว้ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) เช่น ประธาน / รองประธานบริษัท เป็นต้น

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

เจ้าหน้าที่ หมายถึง พนักงานกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย)

หน่วยงานภายนอก หมายถึง องค์กรหรือบริษัทในเครือ อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)

พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

โปรแกรมประยุกต์ หมายถึง โปรแกรม SAP Business One , Fix Assets ,Rental , Sales Force เป็นต้น

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

2.1 ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจนและจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

2.2 ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.3 ให้ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงานจะต้องลงบันทึกในแบบฟอร์ม “ใบคำร้องขอเข้าใช้งานจากผู้ใช้งานภายนอก” (FM-IT-DT-07)

การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

(Access Control Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) มีดังนี้

2.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.1.1 กลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) กำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องลงบันทึกในแบบฟอร์ม “ใบคำร้องขอเข้าใช้งานจากผู้ใช้งานภายนอก”(FM-IT-DT-07)

2.1.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

2.1.3 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบลงในแบบฟอร์ม “ตารางบันทึกบุคคลเข้าออกห้องคอมพิวเตอร์”(FM-IT-DT-09) ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

2.2 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.2.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของเจ้าหน้าที่ กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้ระบบเทคโนโลยีสารสนเทศ ตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

2.2.2 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2.2.3 ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

2.2.3.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

2.2.3.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

2.2.3.3 ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

2.2.3.4 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2.2.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

2.2.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างลงในแบบฟอร์มขอดำเนินการด้านระบบสารสนเทศ (FM-IT-DT-08)

2.2.4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

2.2.4.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

2.2.4.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

2.2.4.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.2.4.4 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

2.2.4.5 ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดตามมาตรฐาน “QP-DT-IT-01”

2.2.4.6 ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2.3 การควบคุมการเข้าถึงระบบปฏิบัติการ

2.3.1 ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

2.3.2 ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

2.3.3 ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

2.3.4 ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

1. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

กลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

2.1 ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2 ผู้ใช้บริการจากภายนอกจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของบริษัท ต้องทำการลงทะเบียนในแบบฟอร์ม “ใบคำร้องขอเข้าใช้งานจากผู้ใช้งานภายนอก” (FM-IT-DT-07) และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

2.3 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทำการกรอกแบบฟอร์ม ”ขอดำเนินการด้านระบบสารสนเทศ ”(FM-IT-DT-08) ต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่น ๆ

2.4 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

2.5 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

2.5.1 ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

2.5.2 ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

2.5.3 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

2.5.4 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

2.5.5 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

2.5.6 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

2.5.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.5.8 การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.5.9 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

2.6 กลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

2.6.1 ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

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

2.6.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

2.6.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

2.7 กลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

2.7.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรโดยต้องกรอกแบบฟอร์ม แบบฟอร์ม “ขอดำเนินการด้านระบบสารสนเทศ” FM-IT-DT-08 เพื่อขออนุญาตจากรองประธาน เจ้าหน้าที่บริหารด้านปฏิบัติการ หรือ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

2.7.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

2.7.3 วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลโดยต้องกรอกแบบฟอร์ม “ขอดำเนินการด้านระบบสารสนเทศ” FM-IT-DT-08 เพื่อขออนุญาตจากรองประธาน เจ้าหน้าที่บริหารด้านปฏิบัติการ หรือ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

2.7.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

2.7.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

(Wireless Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) หน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

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

2.2 ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

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

2.4 กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

2.4.1 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริง ๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

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

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

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

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

2.4.6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

2.4.6.1 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

(Firewall Policy)

1. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอล์ โดยการกำหนดค่าต่าง ๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

2. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอทั้งหมดของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย)

2.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

2.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

2.4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

2.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

2.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

2.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

2.8 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากรองประธาน เจ้าหน้าที่บริหารด้านปฏิบัติการ หรือ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ก่อน

2.9 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อรองประธาน เจ้าหน้าที่บริหารด้านปฏิบัติการ หรือ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ โดยต้องระบุข้อมูลดังนี้

2.9.1 หมายเลข Port ที่ต้องการขอให้เปิด

2.9.2 หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

2.9.3 วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้น ๆ

2.9.4 วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

2.10 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

2.11 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

2.12 กลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

2.13 ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศระเบียบ ของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) หรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางฝ่ายเทคโนโลยีสารสนเทศจะยกเลิกการให้บริการทันที

2.14 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตในแบบฟอร์ม “ขอดำเนินการด้านระบบสารสนเทศ” (FM-IT-DT-08) เพื่อดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากต่อรองประธาน เจ้าหน้าที่บริหารด้านปฏิบัติการ หรือ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อน

การรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์

(E-mail Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

2.1 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการแจ้งผ่านระบบ Help Desk โดยกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงาน

2.2 เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที

2.3 ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

2.4 ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน

2.5 ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

2.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

2.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

2.8 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) หรือก่อให้เกิดความเสียหายต่อกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย)

2.9 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) เพื่อเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย)

2.10 การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.11 การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน 5 เมกะไบท์

2.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(Internet Cyber Security Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเตอร์เน็ตของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเตอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้เครือข่ายอินเตอร์เน็ต

ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

2.1 การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการแจ้งไปยังระบบ Help Deskโดยกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตโดยผู้ใช้งานจะต้องเป็นบุคลากรของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) สำหรับบุคคลภายนอกจะต้องกรอกแบบฟอร์ม “ใบคำร้องขอเข้าใช้งานจากผู้ใช้งานภายนอก” (FM-IT-DT-07) ที่แผนกประชาสัมพันธ์

2.2 ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

2.3 ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

2.4 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

2.5 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

2.6 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

2.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

2.8 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจากการเครือข่ายอินเตอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

(Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

1. วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) ให้มีความมั่นคงปลอดภัย

2. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุกเครือข่าย เป็นดังนี้

2.1 IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

2.2 ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

2.3 โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

2.4 มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

2.5 มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

2.6 IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ

2.7 เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

2.8 พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

2.9 พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน 1 ชั่วโมงที่ตรวจพบ

2.10 การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

2.11 มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

2.12 กลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย) มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

2.13 ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย) การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของกลุ่มบริษัท บมจ.ดิทโต้ (ประเทศไทย) จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ความมั่นคงปลอดภัยของการสำรองข้อมูล

(Backup Policy)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

2. แนวทางปฏิบัติในการสำรองข้อมูล

2.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

2.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการตั้งชื่อของข้อมูลนั้นให้สามารถแสดงถึงวันที่ เวลาที่สำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

2.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ

(Organizational of Information Security)

1. วัตถุประสงค์

เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย

2. บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

2.1 รองประธาน เจ้าหน้าที่บริหารด้านปฏิบัติการ ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ ในการดำเนินงานทางด้านความมั่นคง ปลอดภัยสำหรับสารสนเทศของบริษัทฯ ไว้อย่างชัดเจน

2.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ผู้จัดการแผนกเทคโนโลยีสารสนเทศ ต้องแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน เพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงทรัพย์สินของสำนักงานฯ หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาติหรือโดยไม่ได้เจตนาก็ตาม

2.3 กำหนดรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with Authorities) ในกรณีที่เกิดปัญหา เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) เป็นต้น

2.4 การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management) ต้องมีการกำหนดระเบียบ ข้อบังคับ กฎเกณฑ์ต่าง ๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูล เพื่อให้มีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน เพื่อให้เกิดความมั่นคงปลอดภัยและลดผลกระทบจากความ เสี่ยงที่อาจเกิดขึ้น

การรักษาความปลอดภัยด้านทรัพยากรมนุษย์

(Human resource security)

1. วัตถุประสงค์

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความ เหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างของบริษัท

2. แนวทางปฏิบัติในการจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

2.1 การสรรหาบุคลากร (Screening) ฝ่ายบริหารทรัพยากรบุคคล ต้องทำการคัดเลือกและตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนเข้าสู่กระบวนการสรรหาและนัดสัมภาษณ์ผู้สมัครที่ผ่านการคัดเลือกจากการสัมภาษณ์จะต้องยินยอมให้บริษัทฯ ตรวจสอบประวัติและจะต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีมาก่อน

2.2 ฝ่ายบริหารทรัพยากรบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และบริษัทฯ ว่าจะไม่เปิดเผยข้อมูลความลับของหน่วยงานหรือบริษัทฯ (Non Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้าง ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 2 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

2.3 ฝ่ายบริหารทรัพยากรบุคคลและหน่วยงานต้นสังกัดต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงกำหนดหน้าที่ความรับผิดชอบ โดยฝ่ายบริหารทรัพยากรบุคคล ต้องแจ้งให้ ฝ่ายเทคโนโลยีสารสนเทศ ทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การโยกย้ายหน่วยงาน
- การสิ้นสุดสภาพการเป็นพนักงาน ด้วยลาออกจากงาน การถูกเลิกจ้าง การเกษียณอายุ หรือการถึงแก่กรรม
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

การบริหารจัดการสินทรัพย์

(Asset Management)

1. วัตถุประสงค์

เพื่อให้สินทรัพย์ของบริษัท ได้รับการป้องกันและปกป้องอย่างเหมาะสม

2. แนวทางปฏิบัติในการบริหารจัดการสินทรัพย์ (Asset Management)

2.1 ทะเบียนสินทรัพย์ (Inventory of assets) แผนกที่รับผิดชอบ การบริหารจัดการสินทรัพย์ ต้องจัดทำและเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูล และเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ (Software Asset) สินทรัพย์ อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset)และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อ สินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์บริษัท ต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) และต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภท ตามระยะเวลาที่กำหนดไว้ ปีละ 1 ครั้ง เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

2.2 ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets) แผนกที่รับผิดชอบ การบริหารจัดการสินทรัพย์ จะต้องกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบข้อมูลและสินทรัพย์ ทั้งหมดด้านเทคโนโลยีสารสนเทศและอื่น ๆ อย่างชัดเจน

2.3 การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets) แผนกที่รับผิดชอบ การบริหารจัดการสินทรัพย์จะต้องกำหนดการอนุญาตเจ้าหน้าที่ ให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมด ที่บริษัทเป็นผู้จัดหามานั้น เพื่อให้ใช้ในการดำเนินงานของบริษัท รวมไปถึงการใช้งานระบบและอุปกรณ์ต่าง ๆ
- เจ้าหน้าที่ตลอดจนหน่วยงานภายนอก ที่ได้รับการว่าจ้างโดยบริษัท จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้ มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูลและระบบสารสนเทศของบริษัท
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ อย่าง ระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
- เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของบริษัท ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของบริษัท รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทก่อนได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่อง คอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกัน สปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้อง อุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนำของฝ่ายเทคโนโลยีสารสนเทศ
- อุปกรณ์คอมพิวเตอร์ของบริษัท ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด

2.4 การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้

- ห้ามเจ้าหน้าที่ ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท
- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และ อนุมัติอย่างเหมาะสม โดยหน่วยงานเจ้าของระบบหรือข้อมูลก่อนนำมาติดตั้งใช้งานบนระบบ เทคโนโลยีสารสนเทศ
- บริษัทจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำงาน และการติดต่อสื่อสารกับบุคคลภายนอกเพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของบริษัท ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทและบุคคลผู้ที่เกี่ยวข้อง เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดี ตามกฎหมาย
- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ขอสงวนสิทธิ์ในการ ตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพหรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยแสปม เนื่องจาก เว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของ ผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิด กฎหมาย
- บริษัทไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บ บอร์ด หรือบล็อก) ของเจ้าหน้าที่ ทั้งนี้ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็น ดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

2.5 การอนุญาตให้ใช้งานอีเมล์มีดังนี้

- ผู้ใช้งานอีเมล์ทั้งหมดของบริษัท ต้องมี E-mail Account เป็นของตนเอง
- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ ไปใช้ในทางที่ผิด
- E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น everyone@dittothailand.com, everyone@siamtc.co.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลาง เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-mail Account นั้น
- E-mail Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นสินทรัพย์ของบริษัท
- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมล์ของบริษัท
- พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้ เมื่อปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะต้องบริหารจัดการพื้นที่ของอีเมล์ และถ้าหากปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับส่งอีเมล์ได้ตามปกติอีกต่อไป
- ขนาดของอีเมล์และไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่ กำหนดผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้

- ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ ให้เป็นไปตามขนาดกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-mail Account ของบริษัท เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
- ห้ามใช้ E-mail Account ของบริษัท ในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของ การทำงานให้กับบริษัท
- ซอฟต์แวร์สำหรับใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง แผนก สังกัดและเบอร์โทรศัพท์ติดต่อ
- ห้ามผู้ใช้งานทำสำเนาข้อความ หรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อน ได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัท
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา หรือบุคคลอื่นใดก็ตาม
- ผู้ใช้งานต้องทำการส่งอีเมล์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้ คำสั่ง “Reply All” ถ้าหากอีเมล์ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน
- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้า ต่าง ๆ (Spam Mail) เป็นต้น
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้ายทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มี เนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัท
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่ สภาพปกติ

2.6 การอนุญาตให้ใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้

- ผู้ใช้งานต้องปกป้องความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่ เมื่อจำเป็นต้องส่งข้อมูลนั้นผ่านเครื่องโทรสาร
- ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิด หมายเลข ผิด ส่วนงาน เป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น
- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น

- ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่อ อิเล็กทรอนิกส์ใด ๆ เช่น Voice Over IP หรือในระหว่างการประชุมทางไกล เว้นแต่ผู้เข้าร่วมการประชุมทุกหน่วยงานได้รับการพิสูจน์ตัวตนแล้วว่า เป็นผู้ที่เกี่ยวข้องและมีสิทธิ์รับทราบข้อมูล
- ผู้ที่เกี่ยวข้องตรวจสอบจนมั่นใจแล้วว่า ไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลลับที่สนทนาอยู่
- การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสม สามารถปูองกันเสียงลอดออกมาได้ เป็นต้น
- ผู้ใช้งานต้องสนทนาโทรศัพท์ด้วยความระมัดระวัง เพื่อป้องกันข้อมูลลับถูกแอบฟังโดยบุคคลที่ไม่ได้รับอนุญาต
- ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใด ๆ ทางโทรศัพท์ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้นเป็นผู้ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าว ก่อนที่จะเปิดเผยข้อมูล
- เจ้าหน้าที่ต้องไม่เปิดเผยสถานที่ตั้งของห้องเครื่องคอมพิวเตอร์แม่ข่ายต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน

2.7 การคืนสินทรัพย์ (Return on Assets) เจ้าหน้าที่ ซึ่งพ้นสภาพจากการจ้างงานต้องคืนสินทรัพย์ทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วงคู่มือและเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

ความมั่นคงปลอดภัยสำหรับการดำเนินงาน

(Operation Security)

1. วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

2. แนวทางนโยบายความมั่นคงปลอดภัยสำหรับการดำเนินงาน

2.1 การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

2.1.1 ต้องจัดทำคู่มือ และ/หรือ ขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียด ขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ

2.1.2 คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิดชอบการปฏิบัติงานนั้นๆ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง

2.1.3 มีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

2.2 การจัดการการเปลี่ยนแปลง (Change Management)

2.2.1 ต้องมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ทุกครั้งโดยปฏิบัติตามวิธีการปฏิบัติงานเรื่องการจัดการการเปลี่ยนแปลงสารสนเทศ (Change Management)

2.2.2 เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ เช่น ระบบปรับอากาศ น้ำ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ ฯลฯ เจ้าหน้าที่ต้องประสานงานให้ผู้เกี่ยวข้องรับทราบ

2.3 การจัดการขีดความสามารถ (Capacity Management)

2.3.1 ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมของทรัพยากรชนิดต่าง ๆ ต้องมีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากความ ต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต (อาทิ ความต้องการใน 1 ปี ที่จะถึง เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น) สภาพการใช้งานทรัพยากรใน ปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

2.3.2 แผนการจัดการขีดความสามารถของระบบต้องประกอบด้วยวิธีการจัดการขีดความสามารถ อาทิการ Tunning การจัดหาเพิ่มเติม

2.4 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบและสภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment)

2.4.1 ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบออกจากกับเครื่องที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย

ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

(Communications Security)

1. วัตถุประสงค์

เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัท

2. แนวทางนโยบายความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

2.1 การควบคุมการเข้าถึงเครือข่าย (Network Control)

2.1.1 ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัยและดำเนินการตรวจสอบผู้กระทำการละเมิด

2.1.2 การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย

2.1.3 ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่หน่วยงานนั้นรับผิดชอบ

2.1.4 ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

2.1.5 บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทด้วย

2.2 การความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

2.2.1 ระบบเครือข่ายทั้งหมดของบริษัท ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้ง ต้องมีความสามารถในการตรวจจับไวรัสด้วย

2.2.2 ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้ เฉพาะเท่านั้น

2.2.3 ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัทโดยไม่ได้รับอนุญาต

2.2.4 ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัท โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้อง ดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

2.2.5 ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด

2.2.6 ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัท ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัท โดยเด็ดขาด

2.3 การจัดแบ่งเครือข่ายภายในบริษัท (Segregation in Network)

2.3.1 ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และโซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

2.3.2 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ความสัมพันธ์กับผู้ให้บริการภายนอก

(Supplier relationships)

1. วัตถุประสงค์

เพื่อให้มีการป้องกันสินทรัพย์ขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

2. แนวทางการจัดการความสัมพันธ์กับผู้ให้บริการภายนอก

2.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

2.1.1 หน่วยงานจะต้องกำหนดให้มีการจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างหน่วยงานกับผู้ให้บริการภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร

2.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)

2.2.1 เจ้าหน้าที่ต้องระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่าง หน่วยงานกับผู้ให้บริการภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องปฏิบัติตามวิธีปฏิบัติงานเรื่องการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management) เมื่อมีความจำเป็นต้องให้ผู้ให้บริการภายนอกนั้น เข้าถึงสารสนเทศหรืออุปกรณ์ ประมวลผล สารสนเทศของบริษัท และก่อนที่จะอนุญาตให้สามารถเข้าถึงได้ ผู้ให้บริการต้องรับการอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศเสมอ

2.3 ห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

2.3.1 ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารที่เกี่ยวข้องขององค์กรด้วย

การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(Information Security Incident Management)

1. วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัท ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

2. แนวทางการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

2.1.1 ต้องกำหนดหน้าที่ความ รับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

2.2 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)

2.2.1 ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท โดยผ่าน ช่องทางรายงานที่กำหนดไว้

2.2.2 ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในบริษัท ต่อผู้บังคับบัญชาหรือฝ่ายเทคโนโลยีสารสนเทศทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

2.2.3 ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อฝ่ายเทคโนโลยีสารสนเทศทันที

2.2.4 ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานฝ่ายเทคโนโลยีสารสนเทศทันที

2.2.5 ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในบริษัท ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา ฝ่ายเทคโนโลยีสารสนเทศและห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้น ด้วยตนเอง

2.2.6 การกระทำอื่น ๆ ที่ถือเป็นข้อห้ามของบริษัท มีดังนี้

- การกระทำใด ๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่น ๆ ที่กล่าวถึงด้านล่างนี้ถือเป็นข้อห้ามของบริษัท ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาด ทั้งนี้ บริษัท มิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ ผู้ใช้งานได้รับทราบเท่านั้น หมายเหตุ: เจ้าหน้าที่บางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับ การเข้าถึงระบบเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ
- การใช้งานทรัพยากรของบริษัท เพื่อการจัดหาหรือส่งต่อ วัสดุ เอกสาร หรือรูปภาพ ลามกอนาจาร หรือที่ขัดต่อกฎหมาย
- การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่บริษัท กำหนดให้ เพื่อเสนอขายสินค้าหรือ บริการใดๆ
- การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่ายตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบ เครือข่ายได้แก่ Sniffing, Pinged Floods, Pack Spoofing, Denial of Service และ Forged 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 ไม่ว่าจะด้วยภาษาความถี่ หรือขนาดของข้อความการแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)
- การละเมิดสิทธิ์ส่วนบุคคล ลิขสิทธิ์ของบริษัท ความลับของบริษัทสิทธิบัตรทรัพย์สินทางปัญญาหรือกฎหมายอื่นใด

2.3 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

2.3.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องบันทึกและรายงาน จุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทที่สังเกตุพบหรือเกิดความสงสัยในระบบ หรือบริการที่ใช้งานอยู่

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

2.4.1 สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นถือเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

2.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

2.5.1 ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดขั้นตอนไว้รองรับกรณีเกิดเหตุการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัย

2.5.2 เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

2.6 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Information Security Incidents)

2.6.1 ฝ่ายเทคโนโลยีสารสนเทศต้องบันทึกเหตุการณ์ละเมิด ความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ปริมาณที่เกิดขึ้นและ ค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้วและเตรียมการป้องกันที่จำเป็นไว้

2.7 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

2.7.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องรวบรวมและจัดเก็บ หลักฐานตามกฎ หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ

(Information security - aspects of business continuity management)

1. วัตถุประสงค์

เพื่อป้องกันการหยุดชะงักในการดำเนินงานของบริษัท ที่เป็นผลมาจากความล้มเหลวหรือการ หยุดทำงานของระบบ

2. แนวทางการจัดการประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ

2.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

2.1.1 องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่อง ในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ

2.1.2 ฝ่ายเทคโนโลยีสารสนเทศต้อง จัดทำแนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดขึ้นที่ก่อให้เกิดความเสียหาย และมีผลกระทบต่อการดำเนินงานของบริษัท
- การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดของเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
- การดำเนินงานของฝ่ายเทคโนโลยีสารสนเทศ สามารถดำเนินงานเป็นได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานที่ปกติ เพื่อให้การดำเนินงานของบริษัท กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

2.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement information security continuity)

2.2.1 บริษัท ต้องจัดตั้งแผนสร้างความต่อเนื่อง ของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลข้อมูล เป็นต้น

2.2.2 ต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน (BCP) ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมไปถึงมีการจัดซ้อมแผนอย่างน้อยปีละ 1 ครั้ง

2.3 การตรวจสอบทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

2.3.1 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดการทดสอบแผนการที่ชัดเจน รวมไปถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่ เริ่มต้นถึงสิ้นสุดกระบวนการ

2.3.2 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดเหตุการณ์จำลองที่จะใช้ทดสอบและรายละเอียดในการกำหนดวัตถุประสงค์ ขอบเขตของระบบงานที่จะทำการทดสอบ

2.3.3 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบ กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุมประสานงาน รวมไปถึงสถานที่ และอุปกรณ์เครื่องมือต่าง ๆ

2.3.4 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดแผนงานแนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน และมีการทดสอบอย่างน้อยปีละ 1 ครั้ง

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย
และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
(Compliance)

1. วัตถุประสงค์

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ

2. แนวทางการปฏิบัติตามข้อกำาหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

2.1 การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

2.1.1 บริษัทต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือ สัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

2.1.2 เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตาม รายการของนโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยตรวจสอบกับกฎหมายและมีรายการดังต่อไปนี้เป็นอย่างน้อย

- นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- พ.ร.บ. ลิขสิทธิ์

2.1.3 ข้อมูลที่ถูกสร้างเก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นสินทรัพย์ของบริษัท (ยกเว้นข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

2.1.4 เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่างๆ ของบริษัทกำหนดไว้ บริษัทขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมล์ของผู้ใช้งาน โดยไม่จำเป็นต้อง แจ้งให้ทราบล่วงหน้าอย่างไรก็ตามบริษัทจะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้นและจะไม่เปิดเผยข้อมูลใดๆ ของผู้ใช้งานเว้นแต่มีการเปิดเผยตามคำสั่งตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

2.1.5 ห้ามเจ้าหน้าที่ ใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

2.1.6 การส่งซอฟต์แวร์ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศ ไม่ขัดต่อข้อกฎหมายใด ๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

2.2 สินทรัพย์ทางปัญญา (Intellectual Property Rights)

2.2.1 บริษัทต้องปฏิบัติตามข้อกาหนดทางลิขสิทธิ์ (Copyright) ในการ ใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด

2.2.2 บริษัทต้องปฏิบัติตามข้อกำหนดที่ ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วยได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

2.2.3 ห้ามผู้ใช้งานดำเนินการทำซ้ำหรือเผยแพร่รูปภาพ บทเพลง บทความ หนังสือหรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัทโดยเด็ดขาด

2.2.4 เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่บริษัทมิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอจึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของบริษัท เพื่อจุดประสงค์ใดๆ ก็ตามที่ไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ และในขณะเดียวกัน เจ้าหน้าที่ไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงเครื่องในเครื่องของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจ ว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

2.2.5 บริษัทกำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ เพื่อตรวจดูรายการของซอฟแวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่า บริษัทมีการใช้งานสำหรับผลิตภัณฑ์ ถ้าพบว่ามีซอฟแวร์ที่ไม่ได้รับอนุญาตเหล่านั้นจะถูกลบทิ้งมัน

2.3 การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

2.3.1 บริษัทต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบหรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล

2.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

2.4.1 บริษัทต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมายระเบียบสัญญาที่เกี่ยวกับบริษัท

2.5 การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

2.5.1 บริษัทต้องมีการควบคุมการเข้ารหัสข้อมูลตามข้อตกลงกฎหมาย และระเบียบที่เกี่ยวข้อง

การเข้ารหัสข้อมูล

(Cryptography)

1. วัตถุประสงค์

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลและเพื่อป้องการความลับการปลอมแปลง หรือความถูกต้องของสารสนเทศ

2. แนวทางการกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

2.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls) บริษัทต้องมีการควบคุมการเข้ารหัสไฟล์ข้อมูล รวมไปถึงการส่งข้อมูลไปยังบุคคลอื่นให้มีการทำรหัสผ่านในการเปิดใช้งาน โดยต้องประกอบด้วย ตัวอักษรภาษาอังกฤษตัวใหญ่, ตัวเล็ก, ตัวเลขและตัวอักษรพิเศษ อย่างน้อย 6 ตัวอักษร

2.2 ประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสม สำหรับข้อมูลที่จำเป็นต้องป้องกัน

2.3 เชื่อมต่อผ่านโพรโทคอล SSL สำหรับระบบสารสนเทศแบบเว็บแอพพลิเคชั่น (Web Application) เพื่อเป็นการเข้ารหัสข้อมูลที่ส่ง ระหว่างเว็บบราวเซอร์ (Web Browser) และเว็บเซิร์ฟเวอร์ (Web Server)

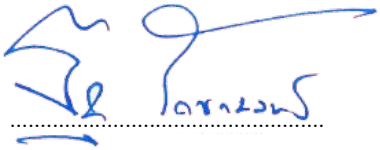
2.4 ห้ามเผยแพร่ไฟล์ข้อมูลลับของบริษัท โดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรโดยเด็ดขาด

2.5 ตรวจสอบการทำงานของระบบป้องกันมัลแวร์ (Malware) อย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลว่ามีการทำงานของระบบป้องกันมัลแวร์ตามปกติหรือไม่

2.6 ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติ หรือไม่

2.7 สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอตามความจำเป็นแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากผู้บริหารกลุ่มบริษัท บมจ. ดิทโต้ (ประเทศไทย) เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

นโยบายฉบับนี้ได้รับอนุมัติจากคณะกรรมการบริษัท ครั้งที่ 1/2567 เมื่อวันที่ 26 กุมภาพันธ์ 2567 โดยให้มีผลบังคับใช้ตั้งแต่วันที่ 26 กุมภาพันธ์ 2567 เป็นต้นไป



(นายฐกร รัตนกมลพร)

ประธานกลุ่มบริษัท