

องค์ประกอบของระเบียบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

องค์ประกอบระเบียบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วย 5 ส่วน ดังนี้

ส่วนที่ 1 ด้านการควบคุมการเข้าถึงและการทำงานของระบบเทคโนโลยีสารสนเทศ (Access Management Control)

ก. ระเบียบการควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

ข้อ 1 เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง

ข้อ 2 เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีในลักษณะที่ไม่ถูกต้องและการถูกคุกคามต่างๆ

ข้อ 3 เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง เช่น ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ข้อ 4 เพื่อสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างถูกต้อง

แนวทางปฏิบัติเกี่ยวกับการควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

ข้อ 1 การเข้าถึงหรือการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ สามารถแบ่งระดับการเข้าถึง ข้อมูล สิทธิ เวลา และช่องทางการเข้าถึงได้ดังนี้

1.1 กำหนดระดับการเข้าถึงข้อมูลแต่ละประเภท ประเภทผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูล ดังนี้

- ระดับการเข้าถึงข้อมูลสำหรับผู้บริหาร
- ระดับการเข้าถึงข้อมูลสำหรับผู้ใช้งาน
- ระดับการเข้าถึงข้อมูลสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย
- ระดับการเข้าถึงข้อมูลสำหรับบุคคลภายนอก

1.2 กำหนดประเภทสิทธิของผู้เข้าถึงข้อมูล ดังนี้

- สร้าง
- ปรับปรุง / แก้ไข
- อ่าน

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก้ไข หรือทำซ้ำโดยไม่ได้รับอนุญาต

- ลบ
- อนุมัติ
- ไม่มีสิทธิ

1.3 กำหนดเวลาที่สามารถเข้าถึงข้อมูลได้

- 7 วัน ตลอด 24 ชั่วโมง

1.4 กำหนดช่องทางในการเข้าถึงข้อมูล

ผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดได้นั้น จะต้องได้รับสิทธิจากทางผู้ดูแลระบบเทคโนโลยีสารสนเทศของบริษัท โดยมีการกำหนดข้อบัญญัติผู้เกี่ยวข้องตามระดับการเข้าถึงให้สามารถเข้าใช้งาน มีการแยกประเภทความรับผิดชอบ และพิสูจน์ตัวตนเพื่อตรวจสอบสิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงข้อมูลเฉพาะที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึงข้อมูล ดังนี้

- ระบบเครือข่ายภายใน (Intranet)
- ระบบเครือข่ายภายนอก (Remote Access)
- ระบบเครือข่ายอินเทอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)
- การเข้าถึงห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

1.5 กำหนดบัญชีชื่อผู้ใช้สำหรับการเข้าใช้งาน ดังนี้

- การตั้งชื่อบัญชีผู้ใช้งานและผู้ดูแลระบบโดยกำหนดตามวิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้ (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)¹

ข้อ 2 หลักในการควบคุมการเข้าถึงระบบ ดังนี้

2.1 เจ้าของข้อมูลและเจ้าของระบบ

- ต้องมีการควบคุมการเข้า ออกสถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญให้รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ และมีความจำเป็นต้องเข้าใช้งานเท่านั้น

- จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบ เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

2.2 ผู้ดูแลระบบ

- มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการเข้าสู่ระบบให้แก่ผู้ใช้งาน และในการขออนุญาตเข้าระบบงานของบริษัทนั้น จะต้องมีการขออนุมัติเป็นทางการ เพื่อเก็บหลักฐาน

- มีการบริหารจัดการระบบคอมพิวเตอร์แม่ข่ายต้องปฏิบัติโดยอยู่พื้นฐานตามหลักเกณฑ์ในหมวด 3 ส่วนที่ 1 ข.³

- การติดตั้งและการเชื่อมต่ออุปกรณ์ในระบบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเทคโนโลยีสารสนเทศและเจ้าของระบบเท่านั้น

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก๊ซ หรือทำซ้ำโดยไม่ได้รับอนุญาต

- การลงทะเบียนชื่อบัญชีผู้ใช้ ต้องเป็นไปตามเกณฑ์วิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้ (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)¹

- ต้องมีการบริหารจัดการบัญชีผู้ใช้งาน และรหัสผ่านตามหลักเกณฑ์ในหมวด 3 ส่วนที่ 1 ข.²

- กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่เท่านั้น และต้องได้รับความเห็นชอบจากผู้ดูแลระบบอย่างเป็นทางการ รวมถึงต้องทบทวนสิทธิอย่างสม่ำเสมอ

- ต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

- ต้องกำหนดให้มีการควบคุมการใช้งานระบบ ที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กรเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก

2.3 ผู้ใช้งาน

- จะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบ และระบบตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

- ต้องรับทราบถึงสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศที่ตนเองรับผิดชอบ และต้องปฏิบัติตามอย่างเคร่งครัด

- ผู้ใช้งานที่ต้องการเข้าระบบ หรือเข้าถึงข้อมูลจากภายนอก จะถูกควบคุมโดยอยู่บนพื้นฐานของหลักเกณฑ์ในหมวด 3 ส่วนที่ 1 ฉ.⁴ และข้อกำหนดเกี่ยวกับการเข้าถึงข้อมูลผ่านระบบเครือข่ายส่วนตัวเสมือน (VPN)⁵

¹ ระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ ส่วนที่ 2 วิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้งาน (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)

² ส่วนที่ 1 ข. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

³ ส่วนที่ 1 ข. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

⁴ ส่วนที่ 1 ฉ. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

⁵ ระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ ส่วนที่ 4 ข้อกำหนดเกี่ยวกับการเข้าถึงข้อมูลผ่านระบบเครือข่ายส่วนตัวเสมือน (VPN)

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก๊ซ หรือทำซ้ำโดยไม่ได้รับอนุญาต

ข. ระเบียบด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว โดยการกำหนดต้องคำนึงถึงการใช้งานและความปลอดภัย รวมถึงเพื่อป้องกันการเข้าถึงจากผู้ไม่ได้รับอนุญาต

แนวทางปฏิบัติเกี่ยวกับการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ 1 กำหนดให้มีการให้ฝึกอบรมและให้ความรู้ความเข้าใจ

1.1 ผู้ใช้งานต้องเข้าร่วมฝึกอบรมในหลักสูตรที่มีเนื้อหาเกี่ยวข้องกับการสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยด้านการใช้เทคโนโลยีสารสนเทศ (Information Security Awareness Training)

1.2 ผู้ดูแลระบบต้องจัดให้มีการเผยแพร่ประชาสัมพันธ์ความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงการกำหนดมาตรการในเชิงการป้องกันตามความเหมาะสม

ข้อ 2 กำหนดให้มีการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่องต่อไปนี้

2.1 กรณีที่เป็นพนักงานของบริษัท

- ชื่อบัญชีที่ได้รับการรองรับจากฝ่ายทรัพยากรบุคคลเท่านั้น¹
- การระบุชื่อบัญชีผู้ใช้ (User Name) แยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
- การกำหนดชื่อบัญชีผู้ใช้ จะกำหนดตามเกณฑ์วิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้ (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)²

2.2 กรณีที่ไม่เป็นพนักงานของบริษัท

- ผู้รับผิดชอบต้องจัดทำเอกสารขอใช้ระบบเทคโนโลยีสารสนเทศ³ และกรอกข้อมูลให้ครบถ้วน เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน โดยการลงทะเบียนผู้ใช้ในกรณีนี้จะอายุการใช้งานขึ้นกับข้อมูลที่ได้รับมอบหมาย แต่ต้องไม่เกิน 1 ปี นับจากวันที่ทำการลงทะเบียน

- การระบุชื่อบัญชีผู้ใช้ (User Name) แยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
- การกำหนดชื่อบัญชีผู้ใช้ จะกำหนดตามคำร้องขอในเอกสารขอใช้ระบบเทคโนโลยีสารสนเทศ

2.3 กรณีการลงทะเบียนผู้ใช้แบบกลุ่มภายใต้ชื่อบัญชีเดียวกัน

- การระบุชื่อบัญชีจะอ้างอิงจากหน่วยงาน และ/ หรือแผนก และ/ หรือส่วนงาน และ/ หรือฝ่าย และ/ หรือสายงาน และ/ หรือกลุ่มธุรกิจ ที่ได้รับการรองรับจากฝ่ายทรัพยากรบุคคลเท่านั้น¹ และไม่ซ้ำซ้อนกัน

2.4 กรณีพิเศษของการลงทะเบียนผู้ใช้แบบกลุ่มภายใต้ชื่อบัญชีเดียวกัน

- ผู้รับผิดชอบต้องจัดทำเอกสารขอใช้ระบบเทคโนโลยีสารสนเทศ¹ และกรอกข้อมูลให้ครบถ้วน เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน โดยการลงทะเบียนผู้ใช้ในกรณีนี้จะอายุการใช้งานขึ้นกับข้อมูลที่ได้รับมอบหมาย แต่ต้องไม่เกิน 1 ปี นับจากวันที่ทำการลงทะเบียน

- การระบุชื่อบัญชีตามข้อตกลงที่ผู้รับผิดชอบได้ระบุไว้ในเอกสารขอใช้ระบบเทคโนโลยีสารสนเทศ และไม่ซ้ำซ้อนกัน

ข้อ 3 การบริหารจัดการรหัสผ่าน (Password Management) ครอบคลุมในเรื่องต่อไปนี้

3.1 มีหลักเกณฑ์การปฏิบัติ สำหรับการกำหนดหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยที่ชัดเจน²

3.2 การส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการจัดส่งผ่านจดหมายอิเล็กทรอนิกส์ (E-mail) ในการจัดส่ง

ข้อ 4 การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมสิทธิเพื่อให้สามารถเข้าถึง และใช้งานระบบเทคโนโลยีสารสนเทศได้ตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง โดยครอบคลุมในเรื่องต่อไปนี้

4.1 การปรับปรุงและเพิกถอนการอนุญาตใช้งาน

- พนักงาน

- เมื่อมีการเปลี่ยนตำแหน่ง โอนย้ายงาน จะถูกปรับปรุงข้อมูลผู้ใช้งานในระบบ หลังจากได้รับเรื่องจากฝ่ายทรัพยากรบุคคล³

- เมื่อมีการลาออกหรือสิ้นสุดการจ้างงาน จะถูกเพิกถอนการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน หลังจากได้รับเรื่องจากฝ่ายทรัพยากรบุคคล³

- ไม่ใช่พนักงาน

- ชื่อบัญชีผู้ใช้ที่ไม่เป็นพนักงานของบริษัท เช่น บุคคลภายนอก นักศึกษาฝึกงาน และ/ หรือชื่อบัญชีผู้ใช้สำหรับทดสอบระบบชั่วคราว เป็นต้น เมื่อสิ้นสุดระยะเวลาที่ได้มีการตกลงไว้ หรือผู้รับผิดชอบในบัญชีผู้ใช้อย่างกล่าว มีการลาออกหรือสิ้นสุดการจ้างงาน จะถูกเพิกถอนการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน

- ชื่อบัญชีผู้ใช้แบบกลุ่มภายใต้ชื่อเดียวกัน จะถูกปรับปรุงข้อมูล เมื่อมีการเปลี่ยนแปลงชื่อหน่วยงาน แผนก ส่วนงาน ฝ่าย สายงาน กลุ่มธุรกิจ องค์การ ของบริษัท การปรับปรุงข้อมูลจะถูกดำเนินการหลังจากได้รับเรื่องจากฝ่ายทรัพยากรบุคคล

¹ เอกสารขอใช้ระบบเทคโนโลยีสารสนเทศ คือระบบ IT E-Helpdesk

² ระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ ส่วนที่ 2 วิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้งาน (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)

³ เอกสาร DDS Code, เอกสาร Organization Unit Chart , Workflow New Employee และ Workflow Resignation

- ชื่อบัญชีผู้ใช้แบบกลุ่มภายใต้ชื่อบัญชีเดียวกันที่ถูกลงทะเบียนในกรณีพิเศษ เมื่อสิ้นสุดระยะเวลาที่ได้มีการตกลงไว้ หรือผู้รับผิดชอบในบัญชีผู้ใช้ดังกล่าว มีการลาออกหรือสิ้นสุดการจ้างงาน จะถูกเพิกถอนการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน

4.2 การกำหนดสิทธิ

- ผู้ใช้งาน

- จะได้รับสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ที่เหมาะสมตามหน้าที่ ความรับผิดชอบ ความจำเป็นในการใช้งาน และ/ หรือความต้องการทางธุรกิจ ทั้งนี้ต้องได้รับการอนุญาตจากผู้มีอำนาจสูงสุดของฝ่าย สายงาน กลุ่มธุรกิจ หรือเจ้าของข้อมูล

- หากมีความจำเป็นต้องได้รับสิทธิสูงกว่าเดิมที่ได้รับ หรือสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากผู้มีอำนาจสูงสุดของหน่วยงาน แผนก ส่วนงาน ฝ่าย สายงาน กลุ่มธุรกิจ หรือเจ้าของข้อมูล และผู้มีอำนาจสูงสุดของฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศ เพื่อพิจารณาความเหมาะสม โดยมีการกำหนดระยะเวลาในการใช้งาน และระบุวันที่เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง ทั้งนี้ต้องมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง

- ผู้ดูแลระบบ

- จะได้รับสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ที่เหมาะสมตามหน้าที่ ความรับผิดชอบ ความจำเป็นในการใช้งาน และ/ หรือความต้องการทางธุรกิจ ทั้งนี้ต้องได้รับอนุญาตจากผู้มีอำนาจสูงสุดของฝ่าย หรือเจ้าของข้อมูล

- หากมีความจำเป็นต้องได้รับสิทธิสูงกว่าเดิมที่ได้รับ หรือสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากผู้มีอำนาจสูงสุดของฝ่าย สายงาน กลุ่มธุรกิจ หรือเจ้าของข้อมูล และผู้มีอำนาจสูงสุดของฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศ เพื่อพิจารณาความเหมาะสม โดยมีการกำหนดระยะเวลาในการใช้งาน และระบุวันที่เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง ทั้งนี้ต้องมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง

4.3 การทบทวนชื่อบัญชีผู้ใช้งาน และสิทธิของผู้ใช้งาน

- ทบทวนชื่อบัญชีผู้ใช้งานของพนักงาน และบุคคลภายนอก สม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

- ทบทวนชื่อบัญชีผู้ใช้แบบกลุ่มภายใต้ชื่อบัญชีเดียวกันสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

- ทบทวนสิทธิการใช้งานของพนักงาน สม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

- ทบทวนสิทธิผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป โดยอย่างน้อยปีละ 2 ครั้ง

ค. ระเบียบการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์

- ข้อ 1 เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย
- ข้อ 2 เพื่อบังคับใช้กับผู้ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท
- ข้อ 3 เพื่อป้องกันการเข้าถึง การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ โดยไม่ได้ อนุญาต

แนวทางปฏิบัติเกี่ยวกับการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ 1 การกำหนดวิธีปฏิบัติการใช้งานรหัสผ่านสำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนแปลงรหัสผ่านที่มีคุณภาพ ดังนี้

- 1.1 รหัสผ่านสำหรับเข้าใช้งานระบบของบริษัท ถือเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปัน หรือเปิดเผย รหัสผ่านให้บุคคลอื่นรับรู้
- 1.2 เปลี่ยนรหัสชั่วคราวทันทีที่ภายหลังจากที่ได้รับรหัสผ่านจากผู้ดูแลระบบ เพื่อป้องกันบุคคลอื่น ลักลอบใช้งาน
- 1.3 เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด
- 1.4 การตั้งรหัสผ่านที่ยากแก่การคาดเดาของผู้อื่น และควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ ตาม เกณฑ์วิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้ (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)¹
- 1.5 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ใน ระบบคอมพิวเตอร์
- 1.6 หลีกเลี่ยงการใช้รหัสผ่านเดียวกัน สำหรับการใช้งานระบบงานต่างๆ ที่ตนมีสิทธิใช้งาน
- 1.7 ผู้ใช้งานของบริษัททุกคน มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้ บุคคลอื่น เข้าใช้เครือข่ายจากชื่อบัญชีผู้ใช้ของตน
- 1.8 หากมีการกระทำผิดเกิดขึ้นจากชื่อบัญชีผู้ใช้ และรหัสผ่านของบุคคลใด บุคคลนั้นต้องเป็น ผู้รับผิดชอบต่อการกระทำผิดนั้นตามระเบียบ ข้อบังคับ กฎหมาย ที่เกี่ยวข้อง

ข้อ 2 การควบคุมสินทรัพย์ด้านสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen) ต้องควบคุมไม่ให้สินทรัพย์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูล สารสนเทศ อยู่ในสถานะซึ่งเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ ขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

¹ เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แกะไข หรือทำซ้ำโดยไม่ได้รับอนุญาต

- 2.1 จากระบบงาน(Log out) โดยทันทีเมื่อเสร็จสิ้นงาน
 - 2.2 มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้ามาใช้งาน
 - 2.3 ต้องจัดเก็บ และ/ หรือสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย
 - 2.4 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการ ที่ต้องใช้งานตลอด 24 ชั่วโมง
 - 2.5 การตั้งค่า Screen Server ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานหรือถือครอง ให้มีการล็อก (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ได้ใช้งานเกินกว่า 30 นาที
 - 2.6 ให้มีการขออนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายขึ้นไป กรณีที่ต้องการนำทรัพย์สินด้านสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกบริษัท ก่อนทุกครั้ง
 - 2.7 ระมัดระวัง และดูแลทรัพย์สินของบริษัท ที่ตนเองใช้งานหรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อต้องรับผิดชอบ หรือต้องชดเชยต่อความเสียหายนั้น
- ข้อ 3 ผู้ใช้งานอาจนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ โดยผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐาน เมื่อมีการรับส่งข้อมูลที่สำคัญ หรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

¹ ระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ ส่วนที่ 2 วิธีปฏิบัติในการใช้งานชื่อผู้ใช้ (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)

ง. ระเบียบการควบคุมการเข้าถึงโปรแกรมประยุกต์ (Application Access Control)

วัตถุประสงค์

ข้อ 1 เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงโปรแกรมประยุกต์ของบริษัท เช่น โปรแกรมจากระบบ ERP โปรแกรมจากระบบ Workflow เป็นต้น

ข้อ 2 เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายจากโปรแกรม และ/ หรือโปรแกรมชุดคำสั่งที่ไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือระบบเทคโนโลยีสารสนเทศ ให้หยุดชะงัก

ข้อ 3 เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวตนบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

แนวทางปฏิบัติเกี่ยวกับการควบคุมการเข้าถึงโปรแกรมประยุกต์ (Application Access Control)

ข้อ 1 การจำกัดการเข้าถึงโปรแกรมประยุกต์

1.1 ผู้ดูแลระบบ ต้องจัดให้มีการลงทะเบียนผู้ใช้งานและกำหนดสิทธิโดยใช้ตามหลักเกณฑ์ในหมวด 3 ส่วนที่ 1 ข.¹

1.2 ผู้ดูแลระบบ ต้องมีการทบทวนสิทธิในการใช้งานอย่างสม่ำเสมอ และ/ หรืออย่างน้อยปีละ 1 ครั้ง

1.3 ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทที่เป็นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

1.4 ผู้ดูแลระบบ ต้องมีการกำหนดให้มีการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลแต่ละระบบ

1.5 การรับส่งข้อมูลสำคัญผ่านระบบ ควรได้รับการเข้ารหัสที่เป็นมาตรฐานสากล เช่น SSL หรือ XML Encryption เป็นต้น

1.6 การนำอุปกรณ์คอมพิวเตอร์ หรือสื่อข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

ข้อ 2 การจัดการระบบฐานข้อมูลที่มีความสำคัญสูง จะต้องดำเนินการดังนี้

2.1 แยกระบบดังกล่าวออกจากระบบอื่นๆ ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องคอมพิวเตอร์แม่ข่ายเดียวกัน

2.2 ควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

2.3 ควบคุมการเข้ามาใช้งานจากเครือข่ายทั้งภายในและภายนอก โดยกำหนดสิทธิการใช้งาน ในการกำหนดค่าที่ระบบป้องกันความปลอดภัย (Firewall)

2.4 ควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน ที่เกี่ยวข้องกับระบบดังกล่าว

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก้ไข หรือทำซ้ำโดยไม่ได้รับอนุญาต

ข้อ 3 การปฏิบัติงานจากภายนอกบริษัท จะต้องดำเนินการดังนี้

3.1 ผู้ดูแลระบบ ต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกล รวมถึงการเตรียมระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

3.2 ผู้ใช้งาน จากระยะไกลต้องรักษาความลับของบริษัท ไม่อนุญาตให้บุคคลที่ไม่เกี่ยวข้องใดๆ เข้าถึงระบบเทคโนโลยีสารสนเทศ

3.3 การขออนุมัติ และ/ หรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิในการเข้าถึงระบบงานต้องปฏิบัติตามเกณฑ์ในหมวด 3 ส่วนที่ 1 ณ.²

¹ส่วนที่ 1 ข. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

²ส่วนที่ 1 ณ. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

จ. ระเบียบการควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

ข้อ 1 เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจ และปฏิบัติตามอย่างเคร่งครัด

ข้อ 2 เพื่อให้การใช้งานโปรแกรมคอมพิวเตอร์มีความมั่นคงปลอดภัย และให้สอดคล้องพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560

แนวทางปฏิบัติเกี่ยวกับการควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

ข้อ 1 ผู้ดูแลระบบ

1.1 มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัท

1.2 มีหน้าที่รับผิดชอบในการติดตั้ง และอัปเดตโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย

1.3 ทำการถอด และยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัทยกเลิกการใช้งานโปรแกรมคอมพิวเตอร์

ข้อ 2 ผู้ใช้งาน

2.1 ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชนจะพึงใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท

2.2 โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3 ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมประเภทที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย

2.4 ห้ามมิให้นำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์อย่างเด็ดขาด

2.5 การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และ/ หรือโปรแกรมคอมพิวเตอร์ให้ผู้ใช้งาน ขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

2.6 การนำเครื่องคอมพิวเตอร์ส่วนตัวของพนักงานมาติดตั้งโปรแกรมคอมพิวเตอร์เพื่อการใช้งานในกิจกรรมของบริษัท จะต้องได้รับการอนุมัติจากผู้มีอำนาจระดับฝ่ายขึ้นไป และผู้ดูแลระบบจะทำการติดตั้งโปรแกรมคอมพิวเตอร์ลงบนเครื่องคอมพิวเตอร์ส่วนตัวของผู้ใช้งานที่ได้รับการอนุมัติแล้ว

2.7 หากผู้ใช้งาน นำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะเป็น License Software หรือ Freeware ก็ตาม ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

2.8 ผู้ใช้งาน โปรแกรมคอมพิวเตอร์เพื่อทำกิจการงานของบริษัทจะต้องปฏิบัติตามข้อกำหนดเกี่ยวกับการควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software Licensing)¹

¹ ประกาศ ข้อกำหนดเกี่ยวกับการควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software Licensing)

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก้ไข หรือทำซ้ำโดยไม่ได้รับอนุญาต

จ. ระเบียบการควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

(Computer and Peripheral Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติเกี่ยวกับการควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control)

ข้อ 1 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท

1.1 ไม่นำข้อมูลส่วนตัวที่ไม่เกี่ยวข้องกับงานบริษัทมาเก็บไว้ในเครื่องคอมพิวเตอร์ของบริษัท

1.2 ห้ามใช้ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัว และไม่มีส่วนเกี่ยวข้องกับหน่วยงานหรือบริษัท

1.3 กรณีส่งเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงเพื่อตรวจสอบ ผู้ดูแลระบบจะตรวจสอบในขั้นต้น และแจ้งสาเหตุให้ทราบ หากไม่สามารถซ่อมได้ ให้ผู้ใช้งานแจ้งผู้ดูแลทรัพย์สินของบริษัทต่อไป

1.4 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท ที่อยู่ในระบบ Domain เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน

1.5 ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบเรื่องทรัพยากรที่เป็นทรัพย์สินของบริษัท และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม

1.6 ผู้ใช้งานไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อนชื้น ฝุ่นละออง และต้องระวังการตกกระทบ

1.7 ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

1.8 ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ควรระมัดระวังอย่างวางของหนักทับ หรือการโยน

1.9 ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะที่เครื่องเปิดใช้งานอยู่

1.10 หลีกเลี้ยงของแข็งกดสัมผัสหน้าจocomพิวเตอร์ให้เป็นรอยขีดข่วน หรือทำให้แตกเสียหายได้ และควรเช็คทำความสะอาดหน้าจocomพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

1.11 ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ทุกชนิดให้กับเจ้าของรายใหม่ พร้อมทั้งต้องทำการปลดรหัสสำหรับเข้าใช้งานคอมพิวเตอร์ และต้องทำการแจ้งการเปลี่ยนแปลงให้กับหน่วยงานที่รับผิดชอบเรื่องทรัพยากรที่เป็นทรัพย์สินของบริษัททุกครั้ง

1.12 ห้ามกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่อทรัพยากรของบริษัทโดยพลการ นอกจากได้รับอนุญาตจากผู้รับผิดชอบ หรือหน่วยงานผู้รับผิดชอบ

1.13 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อกเครื่องคอมพิวเตอร์ขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

ข้อ 2 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ส่วนตัว

2.1 เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา และอุปกรณ์สื่อสารเคลื่อนที่ ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส ก่อนนำเข้ามาใช้งานหรือปฏิบัติงานของบริษัท

2.2 กรณีที่มีการนำเครื่องคอมพิวเตอร์ส่วนตัว มาเพื่อใช้งานในกิจการของบริษัท จะต้องได้รับอนุมัติจากผู้มีอำนาจสูงสุดในแต่ละหน่วยงาน รวมถึงต้องรับผิดชอบต่อความผิดอันอาจเกิดขึ้นจากเครื่องคอมพิวเตอร์ส่วนตัวนั้น

ข้อ 3 การป้องกันกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.1 ห้ามใช้ทรัพยากร และ/ หรือเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งผิดกฎหมาย หรือขัดต่อศีลธรรม เป็นต้น

3.2 ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้

3.3 ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูล ที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก

3.4 ห้ามเผยแพร่ข้อมูลของผู้ใช้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้นๆ

3.5 ห้ามก่อวินาศกรรม ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัท และระบบเครือข่ายอื่นให้เกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น

3.6 ห้ามลักลอบดักจับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์

3.7 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ ที่ขัดต่อนโยบาย ระเบียบ ข้อกำหนด ข้อบังคับ และประกาศของบริษัท

3.8 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

3.9 ผู้ใช้งานต้องตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

3.10 ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

3.11 การตั้งชื่อเครื่องคอมพิวเตอร์ของบริษัทที่อยู่ในระบบ Domain จะต้องกำหนดโดยผู้ดูแลระบบเทคโนโลยีสารสนเทศเท่านั้น

3.12 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องมีการ Update Service Pack และ Hot Fix เป็นเวอร์ชันล่าสุดเสมอ เพื่อความปลอดภัยจากการติดไวรัส

3.13 การเชื่อมต่อเพื่อใช้งานระบบงานจากภายนอกให้ปฏิบัติตามหลักเกณฑ์ในหมวด 3 ส่วนที่ 1 ก.¹ และ ณ.²

3.14 ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีความยากแก่การคาดเดาจากผู้ไม่ประสงค์ดี

3.15 ผู้ใช้งานต้องใช้โปรแกรม Screen Server โดยตั้งให้มีการล็อกหน้าจอแบบอัตโนมัติเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

3.16 ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.17 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งาน และรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.18 ผู้ใช้งานไม่ควรทำการบันทึกหรือรหัสผ่านในการเข้าใช้งานระบบ หรือการเข้าถึงข้อมูล

3.19 ฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ภายในบริษัท

ข้อ 4 การป้องกันกระทำผิดทางกฎหมาย และการกระทำที่เข้าข่ายผิดทางกฎหมาย

4.1 ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมประเภทที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย

4.2 ห้ามใช้ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของบริษัทเผยแพร่หรือเข้าถึงสื่อที่เกี่ยวข้องกับเรื่องลามกอนาจาร ผิดต่อศีลธรรม จริยธรรม การละเมิดทรัพย์สินทางปัญญา การหมิ่นพระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ หรือการทำให้บุคคลอื่นเสียชื่อเสียงหรือได้รับความอับอาย

4.3 ห้ามใช้คอมพิวเตอร์ของบริษัทส่งข้อมูล หรือส่งจดหมายอิเล็กทรอนิกส์ ในรูปแบบภาพนิ่ง ภาพเคลื่อนไหว ภาพที่เกิดจากการสร้างขึ้น การตัดต่อ ดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ รวมถึงข้อความลามกอนาจาร ผิดต่อศีลธรรม จริยธรรม การละเมิดทรัพย์สินทางปัญญา การหมิ่นพระบรมเดชานุภาพ การสร้างปัญหาความมั่นคงของประเทศ การทำให้บุคคลอื่นเสียชื่อเสียงหรืออับอาย การปลอมแปลงหรือแอบอ้างเพื่อสร้างความเข้าใจผิด การส่งจดหมายอิเล็กทรอนิกส์ในรูปแบบของ Spam จนทำให้เกิดความยุ่งยากในการใช้งานระบบเครือข่ายคอมพิวเตอร์

4.4 โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

4.5 ห้ามผู้ใช้งานทุกคนทำการปรับแต่งเวลาของเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา อุปกรณ์สื่อสารเคลื่อนที่ และอุปกรณ์ต่อพ่วง ทุกเครื่อง และหากมีการแก้ไขเวลาถือว่าผู้ใช้งานนั้นอาจจะกระทำการอันเป็นสุ่มเสี่ยงต่อกฎหมาย

¹ส่วนที่ 1 ก. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

²ส่วนที่ 1 ฉ. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข. ระเบียบการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail)

วัตถุประสงค์

ข้อ 1 เพื่อให้การรับ ส่งข้อมูลข่าวสารด้วยจดหมาย สามารถสนับสนุนการปฏิบัติงาน ให้เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ

ข้อ 2 เพื่อให้การติดต่อสื่อสารโดยการรับ ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์ เป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัท

ข้อ 3 เพื่อให้ผู้ใช้เข้าใจความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัย

แนวทางปฏิบัติเกี่ยวกับการใช้จดหมายอิเล็กทรอนิกส์ (Electronic Mail)

ข้อ 1 ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อกฎหมาย, พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560, พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และระเบียบการใช้งานระบบจดหมายอิเล็กทรอนิกส์ บริษัทกำหนด

ข้อ 2 หน่วยงาน และ/ หรือพนักงานผู้ให้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัท

ข้อ 3 พนักงานจะได้รับสิทธิในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ให้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อพนักงานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล

ข้อ 4 เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก ควรเปลี่ยนรหัสผ่านโดยทันที และควรเปลี่ยนรหัสผ่านทุก 90 วัน ตามวิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้ (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)¹

ข้อ 5 ไม่ควรบันทึก หรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้ หากมีการสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านควรจะกำหนดให้ยากแก่การคาดเดา

ข้อ 6 ไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน หรือรับ หรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ให้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

ข้อ 7 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งาน

ข้อ 8 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับการอนุญาตจากบังคับบัญชาแล้วเท่านั้น

ข้อ 9 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยุ่วยุเสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท

ข้อ 10 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของบริษัท

ข้อ 11 ห้ามผู้ให้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีกระทำความผิดดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ หรือเจ้าของผู้ให้บริการ เป็นผู้รับผิดชอบต่อการกระทำความผิดดังกล่าว

ข้อ 12 ห้ามกระทำการที่อันจะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น

12.1 การสร้างจดหมายลูกโซ่ (Chain mail)

12.2 การส่งจดหมายจำนวนมาก (Spam mail)

12.3 การส่งจดหมายต่อเนื่อง (Letter bomb)

12.4 การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

ข้อ 13 ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัท ให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัท

ข้อ 14 การส่งข้อมูลข่าวสารที่เป็นความลับของบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น และไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

ข้อ 15 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

ข้อ 16 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ และ/ หรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์ของหน่วยงาน จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ ตลอดจนข้อแนวทางปฏิบัติเกี่ยวกับการใช้จดหมายอิเล็กทรอนิกส์ของบริษัท ได้อย่างถูกต้อง

ข้อ 17 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่พนักงานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบหาสาเหตุ

ข้อ 18 หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด เกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท²

ข้อ 19 การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และ/ หรือ โสมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัท ไม่มีส่วนเกี่ยวข้องใดๆ

ข้อ 20 การสมัครสมาชิกหรือการทำการใดๆ เกี่ยวกับกระบวนการดำเนินงานกับเว็บไซต์ภายนอกในนามของบริษัทฯ เช่น เว็บไซต์การสั่งซื้อสินค้า เป็นต้น ต้องสมัครด้วย Email “@metrosystems.co.th” เท่านั้น ห้ามใช้อีเมลส่วนตัวในการสมัครสมาชิก และต้องปฏิบัติตาม ข้อ ข. ระเบียบด้านการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

¹ ระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ ส่วนที่ 2 วิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้ (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)

² ช่องทางการแจ้งเบาะแสของบริษัท ตามระเบียบขั้นตอนการแจ้งเบาะแสของบริษัท

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก้ไข หรือทำซ้ำโดยไม่ได้รับอนุญาต

ข. ระเบียบการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

วัตถุประสงค์

ข้อ 1 เพื่อเป็นแนวทางในการปฏิบัติในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

ข้อ 2 เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นกับระบบงานที่ให้บริการบนเครื่องคอมพิวเตอร์แม่ข่ายนั้นๆ
เกิดความเสียหายหรือการหยุดชะงัก

ข้อ 3 เพื่อป้องกันข้อมูลความลับขององค์กรรั่วออกไปนอกองค์กร

แนวทางปฏิบัติเกี่ยวกับการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

ข้อ 1 การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

1.1 กำหนดให้มีบัญชีผู้ใช้ และรหัสผ่านเฉพาะ ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย โดยให้แยกจากบัญชีผู้ใช้ของผู้ดูแลระบบ และต้องปฏิบัติตามหลักเกณฑ์ในหมวด 3 ส่วนที่ 1 ค.¹ ข้อ 1

1.2 กำหนดสิทธิตามหน้าที่ และความรับผิดชอบของผู้ดูแลระบบ และต้องได้รับการอนุมัติจากผู้มีอำนาจ

1.3 ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบต้องปฏิบัติตามหลักเกณฑ์ในหมวด 3 ส่วนที่ 1 จ.² ข้อ 3

ข้อ 2 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

2.1 การติดตั้ง หรือเปลี่ยนแปลง หรือปรับปรุง Software ของระบบงานต้องได้รับการอนุมัติก่อนดำเนินการ

2.2 ควบคุมการเปลี่ยนแปลงต่อระบบงานในช่วงเวลาปฏิบัติงาน เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

2.3 ก่อนดำเนินการติดตั้งระบบงานบนเครื่องให้บริการ ผู้ใช้งานต้องปฏิบัติ ดังนี้

- จัดทำแผนถอยหลังกลับ (Rollback) และเตรียมเครื่องหรือระบบทดสอบก่อน เพื่อป้องกันกรณีที่จะเกิดความผิดพลาดในการติดตั้ง หรือเปลี่ยนแปลง หรือปรับปรุง

- ตรวจสอบความมั่นคงปลอดภัยของระบบงานรวมถึงระบบปฏิบัติการอย่างครบถ้วน

- ทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ

ข้อ 3 การทบทวนการทำงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

3.1 แจ้งผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้ผู้ที่เกี่ยวข้องได้ดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

3.2 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่ต้องเปลี่ยนระบบปฏิบัติการใหม่

ข้อ 4 การพัฒนา และ/ หรือปรับปรุง และ/ หรือดูแลบำรุงรักษา Software และระบบเทคโนโลยีสารสนเทศ โดยหน่วยงานภายนอก

4.1 จัดให้มีการควบคุมโครงการการพัฒนา และ/ หรือปรับปรุง และ/ หรือดูแลบำรุงรักษาซอฟต์แวร์ และระบบเทคโนโลยีสารสนเทศ โดยผู้รับจ้างให้บริการจากหน่วยงานภายนอก

4.2 ให้กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการจากหน่วยงานภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการจากหน่วยงานภายนอก

4.3 ให้ตรวจสอบโปรแกรมที่ไม่พึงประสงค์ที่อาจจะติดมากับ Software ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

4.4 การดำเนินการพัฒนา Software และ/ หรือปรับปรุง และ/ หรือดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ดำเนินการโดยหน่วยงานภายนอกนั้น ซึ่งหน่วยงานภายนอกจะต้องมีการลงนามในสัญญารักษาความลับ รักษาข้อมูลของหน่วยงานก่อนมีการเริ่มดำเนินการใดๆ รวมทั้งจะต้องปฏิบัติตามนโยบาย และ/ หรือแนวปฏิบัติของหน่วยงาน หรือบริษัทอย่างเคร่งครัด

ข้อ 5 การกำหนดความเป็นเจ้าของ และความรับผิดชอบ

หน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย ต้องกำหนดระดับสิทธิการใช้งาน ให้กับผู้ที่ทำหน้าที่รับผิดชอบที่ได้รับการอนุมัติจากหัวหน้าฝ่าย เพื่อดูแลเครื่องคอมพิวเตอร์แม่ข่าย โดยทำการ Update Service pack หรือ Patch ต่างๆ ให้ทันสมัยอยู่เสมอ เพื่อปิดช่องโหว่ของตัวระบบปฏิบัติการ และตัวโปรแกรม

ข้อ 6 การติดตั้ง

6.1 ห้ามเปิด Service หรือ Application ใดๆ ที่ไม่เกี่ยวข้องกับการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย ที่ให้บริการนั้นๆ โดยเด็ดขาด

6.2 เมื่อมีการปรับแต่งหรือแก้ไขค่า ต้องมีการแจ้งผู้ดูแลรับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายนั้นๆ

ข้อ 7 การเฝ้าดูและการตรวจสอบ

7.1 ต้องดำเนินการเก็บ Log ของเหตุการณ์ละเมิดความมั่นคงปลอดภัยดังต่อไปนี้

- จัดเก็บ Log ที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยอย่างน้อยเป็นเวลา 90 วัน

- ระบบจัดเก็บ Log ต้องมีความปลอดภัยในการเข้าถึง และพร้อมเรียกใช้งานได้ เมื่อมีพนักงานที่ได้รับสิทธิต้องการข้อมูลนั้นๆ

7.2 ผู้ดูแลต้องตรวจสอบ Log และเหตุการณ์จะเมิตความมั่นคงปลอดภัย และรายงานให้กับผู้มีอำนาจของหน่วยงานทราบ เช่น

- การโจมตีในรูปแบบ Post-Scan หรือแบบ DDOS (Distributed Denial Of Service)
- การโจมตีของโปรแกรมที่ไม่พึงประสงค์
- การเข้าสู่ระบบของผู้ใช้งานที่ไม่ได้รับสิทธิในการใช้ระบบนั้น
- เหตุการณ์ผิดปกติที่เกิดขึ้นของเครื่องคอมพิวเตอร์แม่ข่าย

7.3 ต้องดำเนินการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำ

7.4 ต้องมีการประเมินความเสี่ยงของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการตามอย่างน้อยปีละ 1 ครั้ง พร้อมกับรายงานผลการประเมินความเสี่ยงกับผู้ที่มีอำนาจของหน่วยงานทราบ

¹ส่วนที่ 1 ค.การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

²ส่วนที่ 1 ข.การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

ณ. ระเบียบการควบคุมการเข้าถึงเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกันมิให้บุคคลอื่นที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท

แนวทางปฏิบัติเกี่ยวกับการควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ 1 การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

1.1 ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่ขัดต่อกฎหมาย หรือศีลธรรม ผู้ใช้งานนั้นจะต้องรับผิดชอบในการกระทำดังกล่าว ซึ่งถือว่าอยู่นอกเหนือจากความรับผิดชอบของบริษัท

1.2 ห้ามผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะแสวงหาผลประโยชน์ของตนเอง ผ่านระบบคอมพิวเตอร์ และระบบเครือข่ายของบริษัท เช่น การซื้อ หรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย แก่บุคคลอื่น

1.3 ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น ได้แก่

- ต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใดๆ ในส่วนที่ไม่ใช่ของตน โดยไม่ได้รับอนุญาต
- การบุกรุก เข้าสู่บัญชีผู้ใช้งานของผู้อื่น
- การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหาย เสื่อมเสียแก่ผู้อื่น
- การใช้ภาษาไม่สุภาพ หรือเขียนข้อความที่ทำให้ผู้อื่นเสียหาย

การกระทำเหล่านี้ ถือเป็นการละเมิดสิทธิของผู้อื่น ผู้ใช้งานจะต้องรับผิดชอบต่อแต่เพียงฝ่ายเดียว บริษัทไม่มีส่วนร่วมรับผิดชอบต่อความเสียหายดังกล่าว

1.4 กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตเท่านั้น

1.5 ผู้ใช้งานต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญตามข้อปฏิบัติที่บริษัทกำหนดเท่านั้น ได้แก่ ระบบจดหมายอิเล็กทรอนิกส์ ระบบเครือข่าย ระบบอินเทอร์เน็ต เป็นต้น โดยเฉพาะ สิทธิเฉพาะสำหรับการใช้ในการปฏิบัติหน้าที่และได้รับการอนุมัติจากผู้จัดการฝ่ายขึ้นไป

1.6 มีการกำหนดระบบเทคโนโลยีสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

1.7 มีข้อกำหนด และ/หรือข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก้ไข หรือทำซ้ำโดยไม่ได้รับอนุญาต

1.8 กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบ DMAS ระบบฐานข้อมูล เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับการอนุมัติจากผู้มีอำนาจของฝ่ายขึ้นไป รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

ข้อ 2 การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกบริษัท ต้องกำหนดให้มีการยืนยันตัวตนบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกบริษัทสามารถเข้าใช้งานเครือข่ายและระบบเทคโนโลยีสารสนเทศของบริษัทได้

2.1 การเข้าสู่เครือข่ายของบริษัทผ่านเครือข่ายภายนอก จะต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้ และรหัสผ่านทุกครั้ง

2.2 การอนุญาตให้ใช้บัญชีผู้ใช้และรหัสผ่าน ในการเข้าใช้งานต้องขึ้นอยู่กับความจำเป็นของการดำเนินงาน รวมทั้งต้องได้รับความเห็นชอบจากผู้มีอำนาจสูงสุดของหน่วยงาน ตามเกณฑ์การอนุมัติของฝ่าย ITS¹

2.3 หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอให้บัญชีผู้ใช้มีสิทธิใช้งาน จะต้องได้รับความเห็นชอบจากผู้มีอำนาจสูงสุดของหน่วยงานของตนเอง และจากฝ่ายเทคโนโลยีสารสนเทศก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

ข้อ 3 การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ในบริษัท ต้องกำหนดให้มีการยืนยันตัวตนบุคคลก่อนที่จะอนุญาตให้ผู้ใช้สามารถเข้าใช้งานเครือข่ายและระบบเทคโนโลยีสารสนเทศของบริษัทได้

3.1 การเข้าสู่เครือข่ายของบริษัทผ่านเครือข่ายภายในบริษัท จะต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้ และรหัสผ่านทุกครั้ง

3.2 การอนุญาตให้ใช้บัญชีผู้ใช้และรหัสผ่าน ในการเข้าใช้งานนอกเหนือจากหน้าที่รับผิดชอบ ต้องขึ้นอยู่กับความจำเป็นของการดำเนินงาน รวมทั้งต้องได้รับการอนุมัติจากหัวหน้าของฝ่ายขึ้นไป และจากฝ่ายเทคโนโลยีสารสนเทศก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

ข้อ 4 การระบุอุปกรณ์บนเครือข่าย ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

4.1 การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของบริษัทต้องได้รับอนุญาตจากทางฝ่ายเทคโนโลยีสารสนเทศก่อนจึงจะสามารถดำเนินการได้

4.2 ผู้ดูแลระบบมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด และสามารถระบุสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

4.3 จะต้องมีการจำกัดสิทธิการเข้าใช้งานอุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการใช้งานอุปกรณ์โดยใช้บัญชีผู้ใช้ เพื่อความปลอดภัยและความเหมาะสมในการเข้าถึง

4.4 จัดทำผังระบบเครือข่าย (Network Diagram) ซึ่งมีการระบุรายละเอียดอุปกรณ์บนเครือข่ายอุปกรณ์ที่ติดตั้งในเครือข่าย และข้อมูลอื่นๆ ที่จำเป็น

ข้อ 5 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

5.1 ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล็อกอินเข้ามาใช้งาน

5.2 ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า Configuration ไว้ในศูนย์ข้อมูลคอมพิวเตอร์ที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

5.3 ผู้ให้บริการภายนอกต้องขออนุมัติจากหัวหน้าฝ่ายขึ้นไป ก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

5.4 เปิดพอร์ตที่มีความจำเป็นใช้ในการใช้งานเท่านั้น และยกเลิกหรือปิดพอร์ต บริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

5.5 ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ

ข้อ 6 การแบ่งแยกเครือข่าย ต้องทำการแบ่งแยกระบบเครือข่าย ดังนี้

6.1 ต้องทำการแบ่งแยกเครือข่ายโดยใช้ VLAN แบ่งแยกเครือข่าย เช่นแบ่งแยกตามที่ตั้งอาคาร เป็นต้น ออกจากกันเพื่อป้องกันการละเมิดทรัพยากรเครือข่ายของแต่ละหน่วยงาน และเพื่อป้องกันการโจมตีการโปรแกรมหรือบุคคลที่ไม่หวังดี

6.2 ต้องแบ่งแยกเครือข่ายออกเป็นโซน เพื่อความมั่นคงปลอดภัยของระบบจากการบุกรุกเครือข่าย เช่น แบ่งเครือข่ายเป็น เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานนอก เป็นต้น

ข้อ 7 การควบคุมการเชื่อมต่อเครือข่าย ต้องควบคุมการเข้าถึง หรือใช้เครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างกัน ดังนี้

7.1 มีการตรวจสอบการเชื่อมต่อเครือข่าย

7.2 จำกัดสิทธิการเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตนเอง

7.3 มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับคอมพิวเตอร์แม่ข่าย

7.4 มีการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่าย

7.5 ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

ข้อ 8 การควบคุมการจัดเส้นทางบนเครือข่าย ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้เชื่อมต่อบริเวณคอมพิวเตอร์และการส่งผ่านข้อมูลหรือสารสนเทศ ดังนี้

8.1 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

8.2 กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

8.3 กำหนดมาตรการการบังคับใช้เส้นทาง สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ข้อ 9 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

9.1 การควบคุมระบบเครือข่ายไร้สาย สำหรับบุคคลภายนอก และ/ หรือผู้มาเยือน

- ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องสร้างระบบเครือข่ายไร้สายสำหรับบุคคลภายนอก และ/ หรือผู้มาเยือน แยกออกจากระบบเครือข่ายอื่นใดของบริษัท และไม่สามารถเข้าถึงระบบอื่นใดของบริษัทได้

- บุคคลภายนอก และ/ หรือผู้มาเยือนที่ต้องการเข้าถึงระบบเครือข่ายไร้สายต้องทำการลงทะเบียนกับผู้ดูแลระบบ หรือตัวแทนผู้รับผิดชอบของแต่ละหน่วยงาน

9.2 การควบคุมระบบเครือข่ายไร้สาย สำหรับบุคลากรของบริษัท

- ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับ ส่งสัญญาณจากภายนอกบริเวณพื้นที่ควบคุมได้

- ควรทำการเปลี่ยนค่า SSID ที่ถูกเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

- ผู้ดูแลระบบต้องกำหนด WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ

- ผู้ดูแลระบบเลือกใช้วิธีควบคุมข้อบัญญัติผู้ใช้ และรหัสผ่าน ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานเครือข่ายไร้สาย โดยอนุญาตเฉพาะข้อบัญญัติผู้ใช้งาน และรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายอย่างถูกต้อง

- จัดให้มีการติดตั้ง Firewall ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายอื่นภายในหน่วยงาน

- ควรใช้ Software หรือ Hardware ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างน้อยทุก 1 เดือน เพื่อคอยตรวจสอบเหตุการณ์ที่อาจทำให้ระบบเครือข่ายไร้สายไม่สามารถใช้งานได้ และเมื่อตรวจพบสิ่งผิดปกติให้รายงานต่อผู้มีอำนาจของหน่วยงานทราบโดยทันที

ข้อ 10 การใช้งานการควบคุมการเข้าใช้งานระบบจากภายนอก ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กรเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

10.1 การเข้าสู่ระบบระยะไกล (Remote access) ผู้ระบบเครือข่ายของบริษัท ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของบริษัท จากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

10.2 วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายของผู้ใช้งาน และหัวหน้าส่วนงานผู้ดูแลระบบเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของบริษัทอย่างเคร่งครัด

10.3 การให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับบริษัทอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

10.4 ต้องมีการควบคุมพอร์ตที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และปิดการเชื่อมต่อเมื่อไม่ได้ใช้งานโดยทันที

10.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบเทคโนโลยีสารสนเทศจากระยะไกลต้องอยู่บนพื้นฐานของข้อกำหนดเกี่ยวกับการเข้าถึงข้อมูลผ่านระบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN)²

10.6 ผู้ใช้งานจะต้องทำการพิสูจน์ตัวตนจากระบบของบริษัททุกครั้งที่มีการเข้าใช้งานจากภายนอก

ข้อ 11 การควบคุมการใช้งานหมายเลขเครือข่าย (IP Address)

11.1 ผู้ดูแลระบบเทคโนโลยีสารสนเทศมีหน้าที่ควบคุมและจัดสรรการใช้งาน Public IP Address ให้แก่หน่วยงานภายในบริษัท และให้จัดทำทะเบียนควบคุมการใช้งาน Public IP Address

11.2 การใช้งานระบบอินเทอร์เน็ตผ่าน Public IP Address กลาง

- ผู้ดูแลระบบเทคโนโลยีสารสนเทศมีหน้าที่ควบคุมดูแลการใช้งานระบบอินเทอร์เน็ตของพนักงาน ซึ่งเป็นการใช้บริการผ่าน Public IP Address กลาง ของบริษัท

- ผู้ดูแลระบบเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการจัดให้มีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ผ่าน Public IP Address กลางไว้ใน Centralized Log Server และจัดให้มีระบบการพิสูจน์ตัวตน (Identification and Authentication Systems) โดยจะต้องปฏิบัติตามกฎหมาย และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์ในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ (ฉบับ 2) พ.ศ. 2560 หรือกฎระเบียบอื่นใดที่จะมีขึ้น หรือจะมีการเปลี่ยนแปลงแก้ไขต่อไปในภายหน้าอย่างเคร่งครัด

- ผู้ดูแลระบบเทคโนโลยีสารสนเทศมีหน้าที่จัดทำทะเบียนควบคุมการใช้ Public IP Address กลาง

11.3 การใช้งานระบบอินเทอร์เน็ตผ่าน Public IP Address เฉพาะ

- ผู้ใช้งานในตำแหน่งผู้ช่วยผู้อำนวยการขึ้นไป ต้องเป็นผู้ควบคุมดูแลการใช้งานระบบอินเทอร์เน็ตของผู้ใช้งานได้บังคับบัญชาผ่าน Public IP Address เฉพาะดังกล่าว

- ผู้ใช้งานในตำแหน่งผู้ช่วยผู้อำนวยการขึ้นไป ดำเนินการให้มีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ผ่าน Public IP Address เฉพาะ ไว้ใน Centralized Log Server โดยให้ผู้ดูแลระบบเทคโนโลยี

สารสนเทศเป็นผู้กำหนดรายการของข้อมูลที่จะต้องจัดเก็บ และแจ้งให้แก่ผู้ช่วยผู้อำนวยการซึ่งเป็นผู้รับผิดชอบทราบ เพื่อดำเนินการ

- ผู้ใช้งานในตำแหน่งผู้ช่วยผู้อำนวยการขึ้นไป ต้องเป็นผู้รับผิดชอบควบคุมดูแลให้ผู้ใช้งานได้ บังคับบัญชา และ/ หรือเครื่องคอมพิวเตอร์ที่จะเชื่อมต่อเข้าระบบอินเทอร์เน็ตผ่าน Public IP Address เฉพาะ จะต้องมีการพิสูจน์ตัวตน (Identification and Authentication Systems) ไม่ว่าจะเป็นการเชื่อมต่อด้วยวิธีใดก็ตาม เพื่อระบุตัวบุคคลที่ใช้งานระบบอินเทอร์เน็ตในเวลานั้นๆ

- สำหรับผู้ใช้งานทั่วไป การขอ Public IP Address เฉพาะ เพื่อการใช้งานในแต่ละหน่วยงาน จะต้องได้รับการพิจารณาอนุมัติก่อนจากผู้มีอำนาจสูงสุดของหน่วยงาน และจากฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศ

- สำหรับผู้ใช้งานทั่วไป ให้หน่วยงานที่ได้รับการจัดสรร Public IP Address เฉพาะ แสดงสิทธิและความรับผิดชอบต่อ Public IP Address ที่ได้รับไปใช้งาน โดยจะต้องปฏิบัติตามกฎหมาย และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์ในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ (ฉบับ 2) พ.ศ. 2560 หรือกฎระเบียบอื่นใดที่จะมีการเปลี่ยนแปลงแก้ไขต่อไปในภายหน้าอย่างเคร่งครัด

- สำหรับผู้ใช้งานทั่วไป ห้ามมิให้มีการแก้ไข เพิ่มเติม หรือเปลี่ยนแปลง Public IP Address เฉพาะ นอกเหนือจากที่ได้รับไว้ไว้ในทะเบียนควบคุมการใช้งาน เว้นแต่จะได้รับอนุมัติจากฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศก่อนเท่านั้น

11.4 ให้ผู้ช่วยผู้อำนวยการซึ่งเป็นผู้บังคับบัญชาของหน่วยงาน จัดให้มีการควบคุมดูแลให้เครื่องคอมพิวเตอร์ที่จะเข้าสู่ระบบเครือข่ายอินเทอร์เน็ตตั้งเวลาของเครื่องให้ตรงกับเวลาอ้างอิงสากล (Stratum0) ซึ่งจะต้องผิดพลาดไม่เกิน 10 มิลลิวินาที โดยให้เทียบเวลากับ Network Time Protocol Server ที่ฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศจัดทำไว้ เพื่อให้เครื่องทุกเครื่องสามารถอ้างอิงเวลาที่ตรงกันก่อนเข้าสู่ระบบเครือข่ายอินเทอร์เน็ต

11.5 ในกรณีที่หน่วยงานนำ Public IP Address ไปให้ลูกค้าใช้งานตามสัญญาบริการ หรือข้อตกลง หรือสัญญาอื่นใดที่เกี่ยวข้องกับการขายหรือให้บริการ ให้ผู้ช่วยผู้อำนวยการซึ่งเป็นผู้มีอำนาจของหน่วยงานดังกล่าว เป็นผู้รับผิดชอบในการกำหนดแนวทางให้ลูกค้าปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับ 2) พ.ศ. 2560 และประกาศใดๆ ที่ออกตามกฎหมายดังกล่าว รวมตลอดจนการปฏิบัติตามกฎหมายอื่นๆ ที่เกี่ยวข้อง

ทั้งนี้ให้ผู้ช่วยผู้อำนวยการซึ่งเป็นผู้รับผิดชอบจัดให้มีการควบคุม หรือกำหนดให้ลูกค้า หรือผู้ให้บริการ และ/ หรือเครื่องคอมพิวเตอร์ที่จะเชื่อมต่อเข้าระบบอินเทอร์เน็ตผ่าน Public IP Address จะต้องมีการพิสูจน์ตัวตน (Identification and Authentication Systems) ไม่ว่าจะเป็นการเชื่อมต่อด้วยวิธีใดก็ตาม เพื่อระบุตัวบุคคลที่ใช้งานระบบอินเทอร์เน็ตในเวลานั้นๆ

ข้อ 12 การใช้งาน Bandwidth เครือข่ายที่เหมาะสม

12.1 ให้ผู้ใช้งานเครือข่ายใช้งานระบบจดหมายอิเล็กทรอนิกส์ที่ทางบริษัทจัดเตรียมให้เท่านั้น

12.2 ห้ามผู้ใช้งานเครือข่ายเข้าถึงเว็บไซต์ประเภทมุ่งเน้นด้านความบันเทิง หรือการดาวน์โหลดวิดีโอ คลิป เช่น YouTube ดูหนังออนไลน์ (TV Streaming) ฟังเพลงออนไลน์ (Radio Streaming) เป็นต้น ในช่วงเวลาปฏิบัติงาน

12.3 ห้ามผู้ใช้งานเครือข่ายเข้าถึงเว็บไซต์ประเภทสื่อสังคมออนไลน์ ที่ใช้เผยแพร่ข้อมูลและแสดงความคิดเห็นบนโลกออนไลน์ เช่น Facebook Twitter เป็นต้น ในช่วงเวลาปฏิบัติงาน

12.4 กรณีที่บริษัทตรวจสอบพบว่าบัญชีผู้ใช้งานในมีพฤติกรรมสุ่มเสี่ยง เช่น การดาวน์โหลด Bit Torrent³ เป็นต้น บริษัทขอสงวนสิทธิในการระงับ และ/ หรือหยุด และ/ หรือยกเลิกการให้บริการแก่ผู้ใช้งานนั้น

12.5 บริษัทขอสงวนสิทธิในการตรวจจับ Bandwidth ของแพ็กเก็ต ทั้งการจราจรขาเข้า (Inbound Traffic) และการจราจรขาออก (Outbound Traffic) ของบัญชีผู้ใช้งานโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

12.6 บริษัทขอสงวนสิทธิในการจัดสรร Bandwidth (Bandwidth Quota) ของผู้ใช้งาน เพื่อเป็นการจัดการทรัพยากร Bandwidth ที่เหมาะสม

¹ WI-IT-04 วิธีการปฏิบัติงานระดับการอนุมัติของฝ่าย ITS

² ระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ ส่วนที่ 4 ข้อกำหนดเกี่ยวกับการเข้าถึงข้อมูลผ่านระบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

³ การดาวน์โหลด Bit Torrent คือเป็นการดาวน์โหลดไฟล์คอมพิวเตอร์ เช่น ภาพยนต์ เพลงไทย เพลงสากล Software Game เป็นต้น จากเว็บไซต์ได้ดิน ผ่านเครือข่ายอินเทอร์เน็ต การดาวน์โหลด BitTorrent ใช้แบนด์วิดท์ที่วางอยู่ทั้งหมดไปใช้ในการดาวน์โหลด ซึ่งทำให้การใช้งานอื่นช้าลง และนอกจากนี้ ยังถือว่าการดาวน์โหลดประเภทนี้เป็นการละเมิดลิขสิทธิ์อย่างรุนแรงอีกด้วย

ญ. ระเบียบการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

วัตถุประสงค์

ข้อ 1 เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน และ/ หรือการเข้าถึงห้องศูนย์ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ตลอดจนระบบเทคโนโลยีสารสนเทศอื่นๆ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ

ข้อ 2 เพื่อบังคับใช้กับผู้ใช้งานซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท ทั้งนี้ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการปฏิบัติเกี่ยวกับการควบคุมและการเข้าใช้งานศูนย์ข้อมูลคอมพิวเตอร์¹

ข้อ 3 เพื่อกำหนดเป็นมาตรการควบคุมการเคลื่อนย้ายและติดตั้งอุปกรณ์ ของระบบเทคโนโลยีสารสนเทศ

ข้อ 4 เพื่อกำหนดเป็นมาตรการควบคุม สอดส่อง ดูแลความปลอดภัยในชีวิตและทรัพย์สิน ด้วยระบบกล้องวงจรปิด บริเวณพื้นที่ที่กำหนดภายในบริษัท

ข้อ 5 เพื่อเพิ่มประสิทธิภาพการรักษาความปลอดภัย บริเวณพื้นที่ที่ไม่มีเจ้าหน้าที่รักษาความปลอดภัยอยู่ประจำ

แนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

ข้อ 1 ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

1.1 ให้ฝ่ายผู้ดูแลเป็นผู้กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน

1.2 ให้ฝ่ายผู้ดูแลเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ในงานระบบเทคโนโลยีสารสนเทศ ตามระเบียบการปฏิบัติเกี่ยวกับการควบคุมการเข้าใช้งานศูนย์ข้อมูลคอมพิวเตอร์¹

1.3 ให้ฝ่ายผู้ดูแลกำหนดมาตรการ การควบคุมการเข้า - ออกพื้นที่ใช้ระบบเทคโนโลยีสารสนเทศ ตามระเบียบการปฏิบัติเกี่ยวกับการควบคุมการเข้าใช้งานศูนย์ข้อมูลคอมพิวเตอร์¹

1.4 บุคคลภายนอกที่จะเข้ามาปฏิบัติงานในศูนย์ข้อมูลคอมพิวเตอร์ต้องปฏิบัติตาม ตามระเบียบการปฏิบัติเกี่ยวกับการควบคุมการเข้าใช้งานศูนย์ข้อมูลคอมพิวเตอร์¹

1.5 บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

1.6 ระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง เครื่องแบตเตอรี่สำรอง เครื่องปรับอากาศ เครื่องดับเพลิง เครื่อง

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก๊ซ หรือทำซ้ำโดยไม่ได้รับอนุญาต

ควบคุมความชื้น และเครื่องวัดอุณหภูมิ รวมถึงให้มีการตรวจสอบ ระบบสนับสนุนเหล่านี้อย่างสม่ำเสมอ ให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการความล้มเหลวในการทำงานของระบบ

1.7 ติดตั้งระบบแจ้งเตือนกรณีจากระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูลคอมพิวเตอร์ ผิดปกติหรือหยุดทำงาน

1.8 มีการติดตั้งระบบกล้องวงจรปิด เพื่อเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งเฝ้าระวังความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

1.9 หากเกิดเหตุฉุกเฉินที่ไม่สามารถยับยั้งได้ตามระยะเวลาที่กำหนด ให้ปฏิบัติตามกระบวนการบริหารจัดการแผนรับมือเหตุฉุกเฉิน (DRP/BPC) เพื่อรองรับการบริหารความต่อเนื่องทางธุรกิจ

ข้อ 2 การเดินสายไฟ สายสัญญาณสื่อสาร และสายเคเบิลอื่นๆ

2.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึง

2.2 ให้มีการร้อยท่อสัญญาณต่างๆ เพื่อป้องกันการดักจับ หรือการตัดสายสัญญาณ

2.3 ให้เดินสายสัญญาณเครือข่ายและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณ

2.4 จัดทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการเกิดความสับสนในการใช้งาน

ข้อ 3 การบำรุงรักษาอุปกรณ์

3.1 ให้กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาการใช้งานของอุปกรณ์

3.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามการใช้งานของอุปกรณ์

3.3 จัดเก็บบันทึกการบำรุงรักษา ปัญหา และข้อบกพร่องของอุปกรณ์ ที่ให้บริการทุกครั้ง เพื่อประเมินและปรับปรุง และควรเก็บอย่างน้อย 1 ปี

3.4 ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน หรือในบริษัท ให้ปฏิบัติงานเป็นไปตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.5 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ 4 การนำทรัพย์สินเข้า – ออกศูนย์ข้อมูลคอมพิวเตอร์

4.1 ต้องได้รับการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นเข้า – ออกศูนย์ข้อมูลคอมพิวเตอร์

4.2 เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ พร้อมทั้งรายงานผู้เกี่ยวข้อง(ถ้ามี)

4.3 บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ 5 การป้องกันอุปกรณ์ที่ใช้งานอยู่ภายนอก

5.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของบริษัทออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

5.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของบริษัทไว้โดยไม่มีการควบคุมดูแลในที่สาธารณะ

ข้อ 6 การกำจัดหรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

6.1 ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

6.2 กำหนดมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ ก่อนนำอุปกรณ์นั้นไปใช้งานต่อ หรืออนุญาตให้ผู้อื่นนำไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ข้อ 7 การรักษาความปลอดภัยด้วยระบบกล้องวงจรปิด

7.1 ใช้ในงานควบคุมและจัดการเกี่ยวกับการรักษาความปลอดภัยในกับพนักงาน และทรัพย์สินของบริษัท

7.2 การติดตั้งกล้องวงจรปิด ต้องดำเนินการตามแบบ และตามตำแหน่งที่ทางบริษัทกำหนดไว้

7.3 การติดตั้งอุปกรณ์ระบบควบคุมและบันทึกภาพจากกล้องวงจรปิด ในพื้นที่ที่ทางบริษัทได้กำหนดไว้ และมีการจำกัดสิทธิการเข้าถึง

7.4 การติดตั้งอุปกรณ์ตรวจจับวัน ตามจุดเหมาะสมกับการใช้งานในพื้นที่ที่มีความสำคัญที่มีความเสี่ยงที่จะเกิดเพลิงไหม้ เช่น ศูนย์ข้อมูลคอมพิวเตอร์

7.5 ให้ทำการติดตั้งระบบสำรองไฟสำหรับกล้องวงจรปิด เครื่องควบคุม และบันทึก

7.6 ให้ทำการตั้งเวลาของเครื่องให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) ซึ่งจะต้องผิดพลาดไม่เกิน 10 มิลลิวินาที โดยให้เทียบเวลากับ Network Time Protocol Server ที่ฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศจัดทำไว้ เพื่อให้กล้องวงจรปิดทุกตัวสามารถอ้างอิงเวลาที่เป็นมาตรฐานตรงกัน

7.7 ต้องบันทึกเหตุการณ์ให้สามารถเรียกดูย้อนหลังได้ 30 วัน

7.8 กรณีที่ต้องการขอดูบันทึกเหตุการณ์ย้อนหลัง จะต้องปฏิบัติตาม WI-BLD-03²

¹ ระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ ส่วนที่ 1 ระเบียบการปฏิบัติเกี่ยวกับการควบคุมและเข้าใช้งานศูนย์ข้อมูลคอมพิวเตอร์

² WI-BLD-03 วิธีการปฏิบัติงานการขอดูกล้อง CCTV

ฎ. ระเบียบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File Management)

วัตถุประสงค์

ข้อ 1 เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560

ข้อ 2 เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้

แนวทางปฏิบัติเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ข้อ 1 กำหนดให้มีการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ อย่างน้อย 90 วัน

ข้อ 2 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดให้เป็นความลับในการเข้าถึง

ข้อ 3 ห้ามผู้ดูแลระบบแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ ที่เก็บรักษาไว้ หากมีกรณีนี้เกิดขึ้นบุคคลนั้นต้องรับโทษตามกฎหมาย และระเบียบของบริษัท

ข้อ 4 กำหนดวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงข้อมูลเหล่านั้นให้เฉพาะบุคคลที่มีหน้าที่รับผิดชอบ หรือได้รับมอบอำนาจเท่านั้น

ฎ. ระเบียบการเข้าถึงระบบแบบการยืนยันตัวตนสองชั้น

วัตถุประสงค์

- ข้อ 1 เพื่อเสริมความแข็งแกร่งให้กับบัญชีของผู้ใช้งาน ไม่ให้ถูกขโมยบัญชีผู้ใช้ไปในทางที่ผิด
- ข้อ 2 เพื่อป้องกันและลดความเสี่ยงจากการถูกโจรกรรมข้อมูล ในระบบการใช้ที่ต้องการความปลอดภัยเป็นพิเศษ

แนวทางปฏิบัติเกี่ยวกับการเข้าถึงระบบแบบการยืนยันตัวตนสองชั้น

- ข้อ 1 กำหนดให้การใช้งานกับระบบอีเมลและการใช้งาน VPN (เครือข่ายส่วนตัวเสมือน)
 - 1.1 การเข้าใช้งานอีเมลเมื่ออยู่ภายในบริษัทโดยใช้อินเทอร์เน็ตของบริษัทสามารถเข้าใช้งานโดยไม่ต้องผ่านการยืนยันตัวตนสองชั้น
 - 1.2 การลงทะเบียนสำหรับพนักงานที่ต้องการใช้งานอีเมลจะต้องลงโปรแกรมสำหรับยืนยันตัวตนแบบสองชั้นที่โทรศัพท์มือถือ โดยโปรแกรมจะสนับสนุนการใช้งานบนระบบ android 7 และ IOS 12 ขึ้นไป
 - 1.3 อีเมลที่ลงทะเบียนการใช้งานแบบสองชั้นเรียบร้อยแล้ว จะสามารถใช้งานได้กับโปรแกรม Outlook ทั้งบนโทรศัพท์มือถือและคอมพิวเตอร์เท่านั้น
- ข้อ 2 การใช้งาน VPN (เครือข่ายส่วนตัวเสมือน)
 - 2.1 การเข้าใช้งานอีเมล หรือ VPN ต้องทำการยืนยันตัวตนผ่านสองขั้นตอน ก่อนการเข้าใช้งาน โดยพนักงานทุกท่านที่ต้องการใช้งานในระบบดังกล่าวต้องลงโปรแกรมสำหรับการยืนยันตัวตนสองชั้นในมือถือของตนเองด้วยเสมอ

ส่วนที่ 2 ด้านการสำรองและกู้คืนข้อมูลสารสนเทศ (Backup and Recovery Policy)

ก. การจัดการสำรองข้อมูลสารสนเทศ (Information Backup)

วัตถุประสงค์

ข้อ 1 เพื่อกำหนดในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย ได้อย่างถูกต้อง

ข้อ 2 เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่องและเหมาะสม

แนวทางปฏิบัติการจัดการสำรองข้อมูลสารสนเทศ

ข้อ 1 จัดให้มีการสำรองข้อมูล โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

ข้อ 2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลอย่างถูกต้อง ทั้งระบบฐานข้อมูล ข้อมูลในระบบสารสนเทศ และซอฟต์แวร์ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ข้อ 3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

ข้อ 4 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

ข้อ 5 กำหนดเวลาในการจัดเก็บข้อมูลสำรองตามวิธีการใน WI-IT-09¹ , PM-MIS-052 และ WI-MIS-05

¹ WI-IT-09 วิธีการปฏิบัติงานการ Backup และ Restore ข้อมูล

² PM-MIS-05 ขั้นตอนการดำเนินงานการ Back up data และขั้นตอนการ Recovery data บนเครื่อง AS400 ของแผนก MIS

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก้ไข หรือทำซ้ำโดยไม่ได้รับอนุญาต

ข. ระเบียบการจัดการกู้คืนข้อมูลสารสนเทศ (Information Recovery)

วัตถุประสงค์

ข้อ 1 เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อข้อมูลระบบสารสนเทศ ให้สามารถกู้กลับคืนได้ในระยะเวลาที่เหมาะสม

ข้อ 2 เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่องและเหมาะสม

แนวทางปฏิบัติการจัดการกู้คืนข้อมูล

ข้อ 1 กรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ผู้ดูแลระบบจะต้องดำเนินการกู้คืนข้อมูลอย่างถูกต้อง โดยใช้ข้อมูลล่าสุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

ข้อ 2 ผู้ดูแลระบบต้องมีการจัดทำและฝึกซ้อมแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่บริษัทกำหนด

ส่วนที่ 3 ด้านการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment)

ก. ระเบียบการสร้างความรู้ ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศ

(Knowledge of Information Technology)

วัตถุประสงค์

- ข้อ 1 เพื่อสร้างความรู้ ความเข้าใจในการใช้งานระบบเทคโนโลยีสารสนเทศให้กับผู้ใช้งานของบริษัท
- ข้อ 2 เพื่อป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน
- ข้อ 3 เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย

แนวทางปฏิบัติเกี่ยวกับการสร้างความรู้ ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศ

- ข้อ 1 ควรจัดให้มีการฝึกอบรมการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่ปรับปรุงและเปลี่ยนแปลงการใช้งานระบบเทคโนโลยีสารสนเทศ
- ข้อ 2 ควรจัดทำคู่มือการใช้งานระบบเทคโนโลยีสารสนเทศ ให้ทันสมัยเสมอ โดยมีการทบทวนอย่างน้อย ปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลง
- ข้อ 3 ควรติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อมูล ระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย อย่างสม่ำเสมอ
- ข้อ 4 ควรประเมิน ติดตาม หรือสำรวจความต้องการของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง

ข. ระเบียบการปฏิบัติตามระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ

(Compliance Covenant Procedure and Advice of Corporation)

วัตถุประสงค์

เพื่อให้มีมาตรฐานและสอดคล้องในการใช้ระบบเทคโนโลยีสารสนเทศ ในการดำเนินธุรกิจของบริษัท

แนวทางปฏิบัติเกี่ยวกับการปฏิบัติตามระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ

ข้อ 1 เอกสารระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ จะถูกกำหนดขึ้นโดยผู้ดูแลระบบและส่วนงานที่เกี่ยวข้อง และได้รับการอนุมัติจากผู้มีอำนาจสูงสุดของฝ่าย

ข้อ 2 ผู้ใช้งานต้องตระหนักและปฏิบัติตามระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำในการใช้เทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งครัด

ข้อ 3 ทบทวนระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบเทคโนโลยีสารสนเทศ

ค. ระเบียบการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(Audit and Risk Assessment)

วัตถุประสงค์

ข้อ 1 เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 2 เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมาย ที่เกี่ยวข้องกับการดำเนินการของบริษัท

ข้อ 3 เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

แนวทางปฏิบัติเกี่ยวกับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ 1 ระบุความเสี่ยงและเหตุการณ์ความเสี่ยง เพื่อการประเมินความเสี่ยงนั้น เช่น ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย เนื่องจากพนักงาน (Human Error), ไวรัสมัลแวร์, ระบบไฟฟ้าขัดข้อง, การโจรกรรม, ความเสียหายจากเพลิงไหม้ และความเสียหายจากอุทกภัย เป็นต้น

ข้อ 2 การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

- 2.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
- 2.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
- 2.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

ข้อ 3 กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

ข้อ 4 กำหนดมาตรการจัดการความเสี่ยง

- 4.1 ดำเนินการทบทวนแผนแก้ไขปัญหามาจากเหตุการณ์ความไม่แน่นอน และภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ
- 4.2 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นอย่างน้อยปีละ 1 ครั้ง
- 4.3 ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 4 ด้านการรักษาความมั่นคงความปลอดภัยของไฟร์วอลล์ (Firewall Security Policy)

ก. ระเบียบการจัดการการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Security Controls)

วัตถุประสงค์

- ข้อ 1 เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์โดยการกำหนดค่าต่างๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน
- ข้อ 2 เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

แนวทางปฏิบัติเกี่ยวกับการปฏิบัติตามระเบียบ ข้อกำหนด วิธีปฏิบัติ และคำแนะนำ

- ข้อ 1 เจ้าหน้าที่ฝ่าย ITS มีหน้าที่ในการบริหารจัดการ และการกำหนดค่าของไฟร์วอลล์
- ข้อ 2 กำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็น Deny ทั้งหมด
- ข้อ 3 ทุกเส้นทางที่เชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามระเบียบ จะถูกบล็อก (Block) โดยไฟร์วอลล์
- ข้อ 4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User Account) และรหัสผ่าน (Password) ¹
- ข้อ 5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ ต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
- ข้อ 6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
- ข้อ 7 ข้อมูลการจราจรทางคอมพิวเตอร์ที่ผ่านไฟร์วอลล์ จะต้องถูกจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะจัดเก็บข้อมูลจราจรตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
- ข้อ 8 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย จะกำหนดเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น
- ข้อ 9 จะต้องมีการสำรองข้อมูลของอุปกรณ์ไฟร์วอลล์เป็นประจำเดือน

ข้อ 10 เจ้าหน้าที่ ITS จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของฝ่าย ITS หรือกฎหมาย ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศจนกว่าจะได้รับการแก้ไข

ข้อ 11 ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของฝ่าย ITS หรือกฎหมาย ที่จะทำให้เกิดความเสียหายด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ ทาง ITS จะยกเลิกการให้บริการทันที

ข้อ 12 ฝ่าย ITS จะไม่รับผิดชอบ กรณีที่ผู้ใช้งานไม่ปฏิบัติตามกฎหมาย นโยบาย ระเบียบ ข้อบังคับ หรือข้อกำหนดของบริษัท

¹ ประกาศ วิธีปฏิบัติในการใช้งานชื่อบัญชีผู้ใช้งาน (User Name) และเปลี่ยนแปลงรหัสผ่าน (Password)

ข. การควบคุมการเข้าถึงและการใช้งานระบบอินเทอร์เน็ต (Internet Access control)

วัตถุประสงค์

ข้อ 1 เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ต เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย

ข้อ 2 เพื่อให้ผู้ใช้งานตระหนักก่อนมีการใช้งานเว็บไซต์ต่างๆ ผ่านระบบอินเทอร์เน็ตของบริษัท

แนวทางปฏิบัติเกี่ยวกับการควบคุมการเข้าถึงและการใช้งานระบบอินเทอร์เน็ต (Internet Access Control)

ข้อ 1 ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Proxy, Firewall เป็นต้น

ข้อ 2 เครื่องคอมพิวเตอร์ของบริษัท เครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ ของระบบปฏิบัติการ

ข้อ 3 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ข้อ 4 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท

ข้อ 5 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท

ข้อ 6 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

ข้อ 7 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน

ข้อ 8 ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือเว็บไซต์ลามก อนาจาร เป็นต้น

ข้อ 9 ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560 หรือกฎหมายอื่นใดที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ต เพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด

ค. ระเบียบการใช้เครือข่ายสังคมออนไลน์ (Social Network)

วัตถุประสงค์

เพื่อให้พนักงานสามารถใช้สื่อสังคมออนไลน์ได้อย่างมีประสิทธิภาพ และเกิดประโยชน์สูงสุด โดยไม่ก่อให้เกิดความเสียหายทั้งต่อตนเอง ต่อผู้อื่น และต่อองค์กร

ความหมายและประเภท

สื่อสังคมออนไลน์ (Social Network) หมายถึง สื่อหรือช่องทางในการติดต่อในลักษณะของการสื่อสารผ่านระบบเครือข่ายอินเทอร์เน็ต เป็นสื่อรูปแบบใหม่ที่บุคคลทั่วไปสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่างๆ ซึ่งในปัจจุบันมีแหล่งให้บริการเครือข่ายทางสังคมเกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ตเป็นจำนวนมาก จึงได้มีการแบ่งแยกสื่อสังคมออนไลน์เป็น 2 ประเภท ตามลักษณะการใช้งาน ดังนี้

ข้อ 1 สื่อสังคมออนไลน์ภายในองค์กร ได้แก่ Slack, Microsoft Lync, Cisco Communication CUPC

ข้อ 2 สื่อสังคมออนไลน์ภายนอกองค์กร เช่น Facebook, Twitter, Instagram, Line, Skype, We Chat, YouTube, Blog, Wiki รวมทั้งเว็บไซต์ต่างๆทั้งในประเทศและต่างประเทศ ที่เปิดให้บริการ File Sharing, Photo Sharing, Video Sharing และกระดานข่าว (Web board) เป็นต้น

แนวทางปฏิบัติของการใช้เครือข่ายสังคมออนไลน์ (Social Network)

ข้อ 1 การป้องกันกระทำผิดทางกฎหมาย

1.1 ผู้ใช้บริการพึงตระหนักว่า ข้อความหรือความคิดเห็นที่เผยแพร่บนเครือข่ายสังคมออนไลน์เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคม และกฎหมาย นอกจากนี้ยังมีผลกระทบต่อชื่อเสียง การทำงานและอนาคตของวิชาชีพของตนได้

1.2 ผู้ใช้บริการควรใช้ความระมัดระวังอย่างยิ่ง ในการเผยแพร่ความคิดเห็นที่อาจจะกระตุ้นหรือนำไปสู่การโต้แย้งที่รุนแรง เช่น เรื่องเกี่ยวกับการเมือง หรือศาสนา

1.3 ผู้ใช้บริการพึงระลึกว่าการเผยแพร่ข้อมูลและความคิดเห็น บนเครือข่ายสังคมออนไลน์ อาจขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560 โดยสามารถศึกษาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560 และข้อกำหนดต่างๆ ได้ตามเอกสารแนบท้าย

ทั้งนี้ การละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560 และ/ หรือ ข้อกำหนดต่างๆ ที่กำหนดไว้ เช่น การเปิดเผยข้อมูลความลับของบริษัท และ/ หรือผู้รับบริการ และ/ หรือลูกค้า ที่ได้มาจากการปฏิบัติหน้าที่หรือความไว้วางใจ ที่ก่อให้เกิดความเสียหายแก่บริษัท และ/ หรือผู้รับบริการ และ/ หรือลูกค้า หรือการทำให้เกิดความเสียหายอย่างร้ายแรงแก่ทรัพย์สิน เกียรติ และชื่อเสียงของบริษัท และ/ หรือผู้รับบริการ และ/ หรือลูกค้า ถือเป็นความผิดอย่างร้ายแรง และผู้ที่ละเมิดจะต้องเป็นผู้รับผิดชอบ และถูกดำเนินการตามกฎหมาย โดยทางบริษัทจะไม่มีส่วนเกี่ยวข้องใดๆ

1.4 ผู้ใช้บริการต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรใช้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

ข้อ 2 การใช้บริการเครือข่ายสังคมออนไลน์ทั่วไป

2.1 ผู้ใช้บริการพึงตระหนักว่า หากประสงค์จะใช้เครือข่ายสังคมออนไลน์ เพื่อเผยแพร่ข้อมูลเกี่ยวกับเรื่องหน้าที่การงาน หรือข้อมูลเกี่ยวกับองค์กร ต้องแยกบัญชีผู้ใช้ (Account) ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน ยกตัวอย่างเช่น การใช้ Facebook ของผู้ที่ทำหน้าที่ประชาสัมพันธ์ของส่วนงาน ควรมีการแยก Facebook Profile ที่ใช้สำหรับติดต่อเครือข่ายของตนในเรื่องส่วนตัว ออกจาก Facebook Profile ที่ใช้ประชาสัมพันธ์ของส่วนงาน หรืออาจตั้งเป็น Facebook Page ประจำส่วนงานขึ้น แทนที่จะใช้ Profile ส่วนตัว

2.2 การเผยแพร่ข้อมูล และ/ หรือแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นจากบริษัท หรือส่วนงาน ต้องมีการแจ้งข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของบริษัท หรือส่วนงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของบริษัท หรือส่วนงานอย่างแท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้องแล้วแต่กรณี

2.3 ผู้ใช้บริการที่เป็นหัวหน้าหน่วยงาน และ/ หรือผู้มีอำนาจหน่วยงาน และ/ หรือผู้บริหารในระดับใดๆ พึงระมัดระวังในการเผยแพร่ข้อมูล และ/ หรือการแสดงความคิดเห็น เนื่องจากจะถูกมองว่าเป็นความเห็นของหน่วยงานของตนได้ และอาจมีผลกระทบต่อความเข้าใจของผู้ได้บังคับบัญชาได้ ทั้งนี้ควรให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจนเช่นเดียวกับข้อ 2.2

2.4 ระมัดระวังอย่างยิ่งในการใช้เครือข่ายสังคมออนไลน์ในการปฏิสัมพันธ์ในเรื่องงานกับลูกค้า และ/ หรือผู้รับบริการ และ/ หรือบุคคลทั่วไป โดยเฉพาะไม่ควรใช้บัญชีผู้ใช้ (Account) ที่ใช้สำหรับส่วนตัวเพื่อการนี้ เนื่องจากไม่มีวิธีที่ได้ผลสมบูรณ์ในการปกปิดความลับของลูกค้า และ/ หรือผู้รับบริการ และ/ หรือบุคคลทั่วไปบนเครือข่ายสังคมออนไลน์

2.5 ระมัดระวังอย่างยิ่งในการใช้เครือข่ายสังคมออนไลน์ในการปฏิสัมพันธ์ในเรื่องข้อกล่าวหา กับลูกค้า และ/ หรือผู้รับบริการ และ/ หรือบุคคลทั่วไป และไม่ควรใช้บัญชีผู้ใช้ (Account) ที่ใช้สำหรับของส่วนงาน และ/ หรือบริษัท ในกรณีที่เกิดพฤติกรรมไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับ ลูกค้า และ/ หรือผู้รับบริการ และ/ หรือบุคคลทั่วไป และ/ หรือส่วนงาน และ/ หรือบริษัท ผู้ใช้บริการจะต้องได้รับการตักเตือน หรือรับโทษในกรณีที่ร้ายแรง โดยผู้ดูแลระบบ และบริษัทจะไม่มีส่วนเกี่ยวข้องใดๆ กับการกระทำนั้น

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก๊ซ หรือทำซ้ำโดยไม่ได้รับอนุญาต

2.6 ผู้ให้บริการพึงปฏิบัติตามจริยธรรม ศีลธรรมอย่างเคร่งครัด

2.7 ผู้ให้บริการพึงเคารพและต้องไม่ละเมิดความเป็นส่วนตัว (Privacy) และความลับ (Confidentiality) ของผู้ให้บริการท่านอื่น

2.8 หากพบเพื่อนร่วมหน่วยงาน และ/ หรือบริษัท ใช้เครือข่ายสังคมออนไลน์อย่างไม่เหมาะสม ให้ตักเตือนโดยตรง หรือแจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท¹

2.9 ผู้ให้บริการควรศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Setting”² ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริษัท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสม นอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลกระทบต่อส่วนงานและบริษัทได้ด้วย

ข้อ 3 การใช้บริการเครือข่ายสังคมออนไลน์กับงานของบริษัท

3.1 หากผู้ให้บริการต้องการสร้าง Page และ/ หรือบัญชีผู้ใช้ (Account) ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการ

- กรณีที่เป็นเครือข่ายสังคมออนไลน์ภายในองค์กร ต้องทำการร้องขอจากผู้ดูแลระบบ และต้องได้รับการอนุมัติจากผู้มีอำนาจสูงสุดของฝ่าย

- กรณีที่เป็นเครือข่ายสังคมออนไลน์ภายนอกองค์กร ต้องแจ้งและต้องได้รับการอนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายขึ้นไป

- ทั้งสองกรณีต้องมีการแจ้งรายชื่อของผู้ดูแล Page (Admin) และ/ หรือเจ้าของบัญชีผู้ใช้ (Account) นั้น ให้ผู้ดูแลระบบ และ/ หรือผู้มีอำนาจสูงสุดของหน่วยงานทราบ และเมื่อผู้ดูแล Page (Admin) พ้นจากหน้าที่ หรือพ้นสภาพจากการเป็นพนักงาน ผู้ดูแล Page (Admin) ต้องมอบสิทธิ์ในการดูแล Page และบัญชีผู้ใช้ (Account) นั้นคืนแก่ส่วนงาน หรือบริษัท

3.2 ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของบริษัท และ/ หรือข้อมูลที่ใช้ภายในบริษัท ก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ

3.3 หากมีการใช้ตราสัญลักษณ์ (Logo) ของหน่วยงาน หรือบริษัท บนรูปประกอบ Profile ใช้เพื่อโฆษณา ประชาสัมพันธ์ สินค้า ผลิตภัณฑ์ หรือบริการใดๆ ของตน จะต้องได้รับการอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงานก่อนทุกครั้ง

3.4 บุคลากรที่ปฏิบัติงานให้กับบริษัท พึงตระหนักถึงความรับผิดชอบในการเผยแพร่ข้อมูลเกี่ยวกับลูกค้า และ/ หรือผู้รับบริการ เนื่องจากผลของการเผยแพร่ข้อมูล อาจมีผลกระทบต่อลูกค้า และ/ หรือผู้รับบริการ ส่วนงานบริษัท และวิชาชีพของตนได้

3.5 หากต้องการเผยแพร่ข้อมูลเพื่อการศึกษา เช่น รูปภาพ หรือสื่ออื่นๆ ที่มีจากกับลูกค้า และ/ หรือผู้รับบริการของหน่วยงาน หรือบริษัท ต้องขออนุญาตก่อนเสมอ และต้องลบข้อมูลที่จะทำให้เกิดการทราบถึงตัวคนของลูกค้า และ/ หรือผู้รับบริการนั้นให้หมด เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากลูกค้า และ/ หรือผู้รับบริการ ทั้งนี้ให้รวมถึงการเผยแพร่ข้อมูลในกลุ่มปิดเฉพาะด้วย

เอกสารนี้เป็นสมบัติของบริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน) ห้ามนำออกไปภายนอก แก๊ซ หรือทำซ้ำโดยไม่ได้รับอนุญาต

3.6 ควรแจ้งให้ผู้รับผิดชอบส่วนงาน หรือบริษัททราบ หากพบว่ามีความบนเครือข่ายสังคมออนไลน์ที่อาจทำให้เกิดความเสื่อมเสียชื่อเสียงต่อหน่วยงาน หรือบริษัทได้ สำหรับหน่วยงานควรมอบหมายให้มีผู้เฝ้าระวัง และตรวจตราข่าวสารในทุกช่องทางที่อาจส่งผลกระทบต่อชื่อเสียงของหน่วยงานได้

¹ ช่องทางการแจ้งเบาะแสของบริษัท ตามระเบียบขั้นตอนการแจ้งเบาะแสของบริษัท

² การตั้งค่าความเป็นส่วนตัว หรือ Privacy Setting สามารถหาข้อมูลที่เกี่ยวข้องได้ที่ www.google.com โดยพิมพ์ “Privacy Setting (แล้วตามด้วยชื่อ Application)”

หมวด 4 ด้านการตรวจสอบ

วัตถุประสงค์

เพื่อใช้ในการตรวจสอบ การใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทให้มีความมั่นคงปลอดภัย และเพื่อให้บริษัทดำเนินธุรกิจได้อย่างต่อเนื่อง

แนวทางการตรวจสอบ

ข้อ 1 ฝ่ายผู้ดูแลระบบมีอำนาจในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท ตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ 2 กรณีที่ฝ่ายผู้ดูแลระบบตรวจสอบพบว่า ผู้ใช้งานไม่ปฏิบัติ หรือกระทำการใดๆ อันเป็นการฝ่าฝืนนโยบาย ระเบียบ ข้อบังคับ หรือข้อกำหนดของบริษัท ให้แจ้งกับผู้ใช้งานทราบ เพื่อเปลี่ยนแปลงแก้ไขให้ถูกต้อง และให้ผู้ใช้งาน ปฏิบัติตามที่ได้รับแจ้งทันที โดยให้รายงานเหตุการณ์ดังกล่าวให้กับผู้มีอำนาจสูงสุดของฝ่ายผู้ดูแลระบบ และผู้มีอำนาจระดับหัวหน้าฝ่ายขึ้นไป ของต้นสังกัดผู้ใช้งานทราบด้วย

ข้อ 3 กรณีที่ผู้ใช้งานไม่ปฏิบัติตามการควบคุมข้อ 2 ให้ฝ่ายผู้ดูแลระบบ มีอำนาจถอดโปรแกรมคอมพิวเตอร์ที่ติดตั้งใช้งานบนระบบคอมพิวเตอร์ และ/ หรือระบบคอมพิวเตอร์แม่ข่าย และ/ หรือระบบเครือข่าย หรือลบข้อมูล หรือปิดการใช้งาน หรือกระทำการใดๆ แล้วแต่กรณี เพื่อป้องกันความเสียหายที่จะเกิดขึ้นกับการดำเนินงานของบริษัท และบริษัท โดยในการดำเนินการดังกล่าว ให้รายงานให้กับผู้มีอำนาจสูงสุดของฝ่ายผู้ดูแลระบบ และผู้มีอำนาจระดับหัวหน้าฝ่ายขึ้นไป ของต้นสังกัดผู้ใช้งาน ทราบถึงเหตุผลของการดำเนินการด้วย

ข้อ 4 กรณีที่ฝ่ายผู้ดูแลระบบ ตรวจสอบพบว่าการกระทำใดๆ ที่เข้าข่ายความผิดตามพระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 หรือความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (ฉบับ 2) พ.ศ.2560 หรือกฎหมายอื่นใดที่เกี่ยวข้อง ให้มีอำนาจถอดโปรแกรมคอมพิวเตอร์ที่ติดตั้งใช้งานบนระบบคอมพิวเตอร์ และ/ หรือระบบคอมพิวเตอร์แม่ข่าย และ/ หรือระบบเครือข่าย หรือลบข้อมูล หรือปิดการใช้งาน หรือกระทำการใดๆ แล้วแต่กรณี เพื่อป้องกันความเสียหายที่จะเกิดขึ้นกับการดำเนินงานของบริษัท โดยในการดำเนินการดังกล่าว ให้รายงานให้กับผู้มีอำนาจสูงสุดของฝ่ายผู้ดูแลระบบ และผู้มีอำนาจระดับหัวหน้าฝ่ายขึ้นไป ของต้นสังกัดผู้ใช้งาน ทราบถึงเหตุผลของการดำเนินการด้วย

ข้อ 5 เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท เป็นไปตามวัตถุประสงค์ของนโยบาย ระเบียบ ข้อบังคับ หรือข้อกำหนดของบริษัท ให้ฝ่ายผู้ดูแลระบบ โดยความเห็นชอบของผู้มีอำนาจสูงสุด และ/ หรือผู้อำนวยการของฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศ มีอำนาจกำหนดแนวทางปฏิบัติใดๆ ตามที่เห็นเป็นการสมควรก็ได้ ทั้งนี้เท่าที่ไม่เป็นอุปสรรคต่อการปฏิบัติงานตามหน้าที่ของผู้ใช้งาน

หมวด 5 ด้านบทลงโทษ

วัตถุประสงค์

เพื่อใช้เป็นมาตรการในการลงโทษผู้กระทำความผิด เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

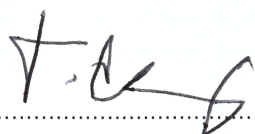
แนวทางเกี่ยวกับบทลงโทษ

ข้อ 1 หากผู้ใช้งานไม่ปฏิบัติตามนโยบาย ระเบียบ ข้อบังคับ หรือข้อกำหนดของบริษัท จะต้องได้รับโทษตามข้อบังคับเกี่ยวกับการทำงานของบริษัท กล่าวคือ ตักเตือนด้วยวาจาหรือลายลักษณ์อักษร ภาคทัณฑ์ หรือให้ทำทัณฑ์บน พักงาน ตัดโบนัส ปลดออก ไล่ออก แล้วแต่กรณี

การพิจารณาโทษสถานใด ให้อยู่ในดุลยพินิจของผู้มีอำนาจสูงสุด และ/ หรือผู้อำนวยการของฝ่ายผู้ดูแลระบบเทคโนโลยีสารสนเทศ หรือผู้มีอำนาจสูงสุด และ/ หรือผู้อำนวยการหน่วยงานต้นสังกัดของผู้กระทำความผิด โดยความเห็นชอบของกรรมการบริหารของบริษัท

ข้อ 2 หากผลแห่งการที่ผู้ใช้งานไม่ปฏิบัติตามนโยบาย ระเบียบ ข้อบังคับ หรือข้อกำหนดของบริษัท ก่อให้เกิดความเสียหายขึ้นกับบริษัท ผู้ใช้งานจะต้องรับผิดชอบค่าใช้จ่ายให้แกบริษัทได้รับความเสียหายจริง

ข้อ 3 นอกเหนือจากผู้ใช้งานจะต้องรับโทษตามข้อบังคับเกี่ยวกับการทำงานของบริษัทแล้ว หากการกระทำของผู้ใช้งานนั้นถือเป็นการละเมิดในทางแพ่ง หรือเข้าข่ายการกระทำผิดทางอาญา ผู้ใช้งานจะต้องรับผิดชอบในผลแห่งละเมิดทางแพ่ง และ/ หรือรับโทษทางอาญาตามที่กฎหมายกำหนด

ลงชื่อ 

(นายธวิษ จารูจนะ)

ประธานเจ้าหน้าที่บริหาร

บริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน)

1 วัตถุประสงค์

เพื่อใช้เป็นแนวนโยบาย การควบคุมการเข้าถึงทางกายภาพ โดยไม่ได้รับอนุญาต อีกทั้งเพื่อป้องกันทรัพย์สินขององค์กร จากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือสารสนเทศถูกเปิดเผยโดยไม่ได้รับอนุญาต โดยจัดทำขึ้นตามข้อกำหนดของมาตรฐานระบบจัดการ ISO 27001:2013 ของสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ข้อกำหนดจัดการ ISO 27001:2013 ที่เกี่ยวข้อง ประกอบด้วย

- A.11 นโยบายความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security Policy)

2 ขอบเขตการบังคับใช้

สำหรับเป็นขั้นตอนการปฏิบัติเฉพาะภายในสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

3 การกำหนดบริเวณที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Area) (Annex A: A.11.1)

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้ เกิดความเสียหาย และการก่อวินาศกรรมหรือแทรกแซงต่อทรัพย์สินขององค์กร อีกทั้งเพื่อป้องกันทรัพย์สินขององค์กร จากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือสารสนเทศถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมการดำเนินงาน

3.1 การจัดทำขอบเขตหรือบริเวณโดยรอบพื้นที่ควบคุม (Physical Security Perimeter)

หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้ มีการควบคุมห้อง Data Center ดังต่อไปนี้

1. ห้อง Data Center ต้องอยู่ในอาคารซึ่งอยู่ในพื้นที่ที่มีรั้วล้อมรอบ
2. ผนังของอาคาร ต้องมีโครงสร้างที่แข็งแรง ประตูชั้นนอกทั้งหมดต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอย่างแน่นหนา ด้วยกลไกควบคุมและมีระบบที่สามารถล็อกได้ เพื่อป้องกันการบุกรุกทางกายภาพ
3. ภายในห้อง Data Center อาคารที่มีห้อง Data Center ตั้งอยู่ และบริเวณล้อมรอบ ต้องมีการติดตั้งกล้องวงจรปิดให้ครอบคลุมพื้นที่ที่สำคัญทั้งหมด โดยต้องเก็บข้อมูลบันทึกภาพไว้ อย่างน้อยเป็นเวลา 90 วัน

3.2 การควบคุมการเข้า-ออกทางกายภาพ (Physical Entry Controls)

การเข้า-ออกของห้อง Data Center ต้องมีการควบคุม ดังต่อไปนี้

1. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการรักษาความปลอดภัยบริเวณทางเข้า – ออกของห้อง Data Center (ผ่านทาง Access card หรือ เจ้าหน้าที่รักษาความปลอดภัย) เพื่อเฝ้าระวังและรักษาความปลอดภัย
2. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องกำหนดสิทธิ์พนักงานและลูกจ้างหน่วยงานภายนอก และบุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานในห้องฯ ตามสิทธิ์การเข้าถึงที่ระบุโดยส่วนงานที่เป็นเจ้าของทรัพย์สิน และตามช่วงเวลาที่มีสิทธิ์ผ่านเข้า – ออกห้อง Data Center อย่างเป็นลายลักษณ์อักษร
3. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องทบทวนสิทธิ์ผ่านเข้า – ออกห้อง Data Center เป็นประจำอย่างน้อยทุก 6 เดือน หรือเมื่อมีการเปลี่ยนแปลง
4. ในการเข้า – ออกห้อง Data Center ทุกคนที่เข้า – ออกห้อง Data Center ต้องทำการลงบันทึกข้อมูลในแบบฟอร์มเข้า-ออกพื้นที่ (Physical Entry Control)
5. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องตรวจสอบความถูกต้องครบถ้วนของแบบฟอร์มเข้า-ออกพื้นที่ (Physical Entry Control) เป็นประจำทุกสัปดาห์และจัดเก็บบันทึกผู้มาติดต่อไว้อย่างน้อย 1 ปี
6. ประสิทธิภาพทางเข้า-ออกของห้อง Data Center ควรจะมีระบบควบคุมการเข้าออก ที่มีการรักษาความมั่นคงปลอดภัย เช่น การใช้บัตรผ่านเฉพาะบุคคล (Access Card) การใช้รหัสผ่านเฉพาะบุคคล (PIN) หรือระบบตรวจสอบลายนิ้วมือ เป็นต้น โดยหัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ควรตรวจสอบประสิทธิภาพ

เข้า-ออกของห้อง Data Center เป็นประจำอย่างน้อยทุก 3 เดือน เพื่อหาพฤติกรรมการเข้าออกที่ผิดปกติไปจากปกติ พร้อมทั้งควรมีการจัดเก็บประวัติ การเข้าออกห้อง Data Center ไว้ อย่างน้อย 1 ปี

3.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices, Rooms, and Facilities)

1. ส่วนงานที่รับผิดชอบด้านความปลอดภัยอาคารและสถานที่ หรือ หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีเจ้าหน้าที่หรือวิธีการรักษาความปลอดภัย เพื่อควบคุมให้เข้าสถานที่ทำงานได้เฉพาะบุคคลที่ได้รับอนุญาตจากเจ้าของพื้นที่เท่านั้น
2. พนักงาน ลูกจ้าง หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานในองค์กร และนักศึกษาฝึกงาน ควร มีวิธีการป้องกันการเข้าถึงสารสนเทศ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์ให้บริการโทรคมนาคม หรือ อุปกรณ์โทรคมนาคม ขององค์กร เมื่อไม่อยู่ภายในห้อง

3.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against External and Environmental Threats)

1. มีระบบป้องกันไฟไหม้ เช่น ระบบตรวจจับความร้อน ระบบตรวจจับควัน เป็นต้น
2. มีอุปกรณ์ดับเพลิงอย่างพอเพียงและติดตั้งอยู่ในจุดที่สะดวกแก่การใช้งาน ทั้งบริเวณอาคารที่ตั้งห้อง Data Center และภายในห้อง Data Center
3. มีระบบควบคุมอุณหภูมิและความชื้น โดยอุณหภูมิและความชื้นต้องอยู่ในระดับที่เหมาะสมกับอุปกรณ์ประมวลผลสารสนเทศที่จัดอยู่ในห้อง Data Center
4. มีการควบคุมมิให้มีวัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้ หรือวัสดุที่ติดไฟได้ง่าย ตั้งอยู่ในห้อง Data Center

3.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

ทุกคนที่ปฏิบัติงานภายในห้อง Data Center ต้องปฏิบัติตามข้อปฏิบัติ ดังต่อไปนี้

1. เมื่อพบเห็นผู้ที่มีพฤติกรรมน่าสงสัยอยู่ภายในห้อง Data Center ต้องแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้อง โดยทันที
2. ห้ามสูบบุหรี่ ภายในห้อง Data Center
3. ห้ามนำอาหารและเครื่องดื่ม เข้าไปในห้อง Data Center
4. ห้ามนำ อุปกรณ์ที่บันทึกภาพ วิดีทัศน์หรือเสียง และสื่อบันทึกชนิดเคลื่อนที่ เข้าไปภายในห้อง Data Center เว้นแต่ได้รับอนุมัติจากหัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่เท่านั้น

3.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas)

หัวหน้าส่วนงานที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการควบคุมสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกสำหรับห้อง Data Center ดังต่อไปนี้

1. มีบริเวณพักรอสำหรับบุคคลภายนอกที่ไม่สามารถเข้าถึงบริเวณอื่นๆ ของห้อง Data Center
2. มีบริเวณสำหรับการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อให้สามารถส่งมอบผลิตภัณฑ์โดยไม่จำเป็นต้องเข้าถึงในบริเวณอื่นๆ ของห้อง Data Center
3. มีการตรวจสอบว่าผลิตภัณฑ์ดังกล่าวอาจจะก่อให้เกิดความเสียหายต่อห้อง Data Centerหรือไม่ เช่น วัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้ หรือวัสดุที่ติดไฟได้ง่าย ก่อนจะเคลื่อนย้ายผลิตภัณฑ์จากบริเวณสำหรับการเข้าถึงหรือการ ส่งมอบไปยังจุดที่ติดตั้งใช้งานจริง

4 การสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์ (Equipment) (Annex A: A.11.2)

4.1 การจัดวางและป้องกันอุปกรณ์ (Equipment Siting and Protection)

มีการจัดวางและป้องกันอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม และอุปกรณ์สำนักงานขององค์กร เพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อม และอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยมิได้รับอนุญาต

ส่วนงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม และอุปกรณ์สำนักงานขององค์กร ดังต่อไปนี้

1. ต้องจัดวาง อยู่ในพื้นที่ที่ได้รับการจัดสรรไว้ เพื่อให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
2. ต้องจัดวางอยู่ในพื้นที่และสภาพแวดล้อมที่เหมาะสมตามคู่มือการใช้งานของเจ้าของผลิตภัณฑ์
3. ต้องจัดวางอยู่ในพื้นที่และสภาพแวดล้อมที่เหมาะสม เพื่อลดความเสี่ยงอันเกิดจากความเสียหายจากภัยธรรมชาติ เช่น อุทกภัย วาตภัย เป็นต้น
4. ต้องได้รับการป้องกันการสูญหายอย่างเหมาะสม เช่น การใช้สายล็อกอุปกรณ์ เป็นต้น
5. ต้องได้รับการป้องกันความเสียหายอันเกิดจากระบบไฟฟ้าอย่างเหมาะสม เช่น มีระบบกรองกระแส ไฟฟ้า (Stabilizer System) เป็นต้น
6. ต้องมีการประกันภัยเพียงพอตามความเหมาะสม

4.2 การบริหารจัดการอุปกรณ์สนับสนุนการประมวลผลสารสนเทศ (Supporting Utilities)

อุปกรณ์สนับสนุนการประมวลผลสารสนเทศสำหรับห้อง Data Center ต้องมีการควบคุม ดังต่อไปนี้

1. ผู้บริหารสารสนเทศระดับสูง ต้องจัดให้มีอุปกรณ์สนับสนุนการประมวลผลสารสนเทศอย่างเพียงพอ เพื่อสนับสนุนการทำงานของอุปกรณ์ประมวลผลสารสนเทศ
2. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการตรวจสอบการทำงานของอุปกรณ์สนับสนุนการประมวลผลสารสนเทศอย่างสม่ำเสมอ
3. หัวหน้าส่วนงานที่รับผิดชอบพื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีระบบหรือกระบวนการในการปิดการทำงานฉุกเฉินสำหรับอุปกรณ์ประมวลผลสารสนเทศเมื่อเกิดเหตุฉุกเฉินหรือระบบไฟฟ้าสำรองมีกระแสไฟฟ้าเหลืออยู่ในจำนวนจำกัดเพื่อป้องกันความเสียหายอันเกิดจากอุปกรณ์ประมวลผลสารสนเทศไม่ได้รับการปิดการทำงานได้ทันเวลาที่

4.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

กรณีภายในห้อง Data Center ภายในห้องคอมพิวเตอร์ส่วนงานที่รับผิดชอบระบบสารสนเทศ และ หัวหน้าส่วนงานที่รับผิดชอบพื้นที่หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีการควบคุมการ เดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ ดังต่อไปนี้

1. สายไฟฟ้า สายสื่อสารและสายเคเบิลอื่นๆ ต้องวางสายภายในท่อหรือรางร้อยสาย หรือได้รับการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อหลีกเลี่ยงจากการเกิดความเสียหาย หรือการดักจับข้อมูลโดยผู้ที่มีได้รับอนุญาต
2. ระบุสัญญาณหรือการให้บริการสำหรับ สายสื่อสารและสายเคเบิลอื่นๆ ที่ไม่มีความจำเป็นต้องใช้งาน
3. สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสมเพื่อป้องกันการรบกวนของสัญญาณ
4. สายสื่อสาร และสายเคเบิลอื่นๆ ต้องได้รับการทำสัญลักษณ์อย่างชัดเจน
5. สำหรับสายสื่อสาร และสายเคเบิลอื่นๆ ที่ใช้สำหรับส่งผ่านสารสนเทศ ควรพิจารณาให้มีการควบคุม ดังต่อไปนี้
 - 5.1 ติดตั้งท่อหุ้มสายชนิดพิเศษ (Armored Conduit)
 - 5.2 มีเส้นทางสำรอง
 - 5.3 ใช้สายใยแก้วนำแสง (Fiber Optic)
 - 5.4 ใช้อุปกรณ์ห่อหุ้มสายเพื่อป้องกันคลื่นแม่เหล็กไฟฟ้า
 - 5.5 ตรวจสอบระบบสายเพื่อตรวจจับอุปกรณ์แปลกปลอม
 - 5.6 ควบคุมการเข้าถึงแผงพักปลายสาย (Patch Panel)

4.4 การบำรุงรักษาและซ่อมบำรุงอุปกรณ์ (Equipment Maintenance)

1. มีการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ อย่างน้อยตามที่ได้รับอนุญาตในคู่มือการใช้งานของอุปกรณ์ และจัดให้มีการซ่อมบำรุงอย่างทันเวลาที่ตามความสำคัญของระบบ
2. มีการบันทึกประวัติการบำรุงรักษาและ ซ่อมบำรุงอุปกรณ์ ทั้งนี้บันทึกดังกล่าวต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้
 - 2.1 วันที่ในการบำรุงรักษาและซ่อมบำรุง
 - 2.2 ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุง
 - 2.3 รายละเอียดการบำรุงรักษาและซ่อมบำรุง
 - 2.4 สถานะของอุปกรณ์
 - 2.5 ปัญหาที่พบและการแก้ไข
 - 2.6 ลายมือชื่อผู้บำรุงรักษาและซ่อมบำรุง
3. ถ้ามีการว่าจ้างหน่วยงานภายนอกเพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์ ส่วนงานที่ว่าจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการว่าจ้าง โดยต้องกำหนดระยะเวลา ขอบเขต และระดับการให้บริการอย่างชัดเจน

4.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of Assets)

1. บุคคลผู้นำอุปกรณ์ออกนอกอาคารหรือองค์กร ต้องได้รับการอนุมัติจากหัวหน้าส่วนงานที่เป็นเจ้าของทรัพย์สินก่อนเท่านั้น
2. เจ้าหน้าที่รักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมาย ต้องตรวจสอบลักษณะของทรัพย์สินที่นำออก โดยเปรียบเทียบกับเอกสารการนำของออกอย่างละเอียดรอบคอบ
3. เจ้าหน้าที่รักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมาย ต้องเก็บเอกสารการนำของออก จัดทำบันทึกการอนุญาตการนำของออกนอกอาคารหรือนอกองค์กร และรายงานการนำทรัพย์สินออกไปยังส่วนงานที่เป็นเจ้าของทรัพย์สิน เพื่อตรวจสอบและยืนยันความถูกต้องตามระยะเวลาที่กำหนด อ้างอิง Asset management Policy

4.6 การควบคุมการกำจัดอุปกรณ์และการนำกลับมาใช้งาน (Secure Disposal or Re-use of Equipment)

ในการจำหน่ายอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ให้บริการโทรคมนาคม หรืออุปกรณ์โทรคมนาคม ขององค์กรออกนอกองค์กร ส่วนงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ก่อนการจำหน่าย เพื่อให้มั่นใจว่าข้อมูลและซอฟต์แวร์ลิขสิทธิ์จะไม่สามารถนำกลับมาได้ (Non-Retrieveable) โดยอ้างอิงจากเอกสาร Asset Management Policy

4.7 การป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งาน (Unattended User Equipment)

1. ส่วนงานที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการจัดวางอุปกรณ์อย่างเหมาะสม เพื่อป้องกันการเข้าถึงขณะที่ไม่มีผู้ใช้งาน
2. ส่วนงานที่รับผิดชอบระบบสารสนเทศ ต้องจัดให้มีการ Lock off จากระบบ หรือยกเลิกการเชื่อมต่อกับแอปพลิเคชันหรือเครือข่าย (Session Time-Out) อย่างอัตโนมัติ เมื่อไม่มีการใช้งาน โดยกำหนดระยะเวลาอย่างเหมาะสม ตามระดับความมั่นคงปลอดภัยของสารสนเทศ โดยให้ปฏิบัติตาม Asset Management Policy

4.8 นโยบายควบคุมการละทิ้งทรัพย์สิน (Clear Desk and Clear Screen Policy)

พนักงาน ลูกจ้าง หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานในองค์กร และนักศึกษาฝึกงาน ต้องมีการจัดเก็บเอกสารและสื่อบันทึกข้อมูลที่บันทึกสารสนเทศ ตามระดับความมั่นคงปลอดภัยของสารสนเทศ โดยให้ปฏิบัติตาม Asset Management Policy เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต เช่น ไม่วางเอกสารสำคัญทิ้งไว้บนโต๊ะทำงาน เก็บเอกสารไว้ในตู้หรือลิ้นชักที่มีกุญแจล็อก เป็นต้น

----- จบ -----