

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท ไทยรับเบอร์ลาเท็กซ์กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ

ส่วนที่ 1

การควบคุมการเข้าออกห้องควบคุมปฏิบัติการระบบคอมพิวเตอร์

(Computing System Control Room)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้จะมีผลบังคับใช้กับผู้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

2. การควบคุมการเข้าออก

- 2.1 ภายในบริษัทมีการจำแนกและกำหนดพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมโดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอันอาจเกิดขึ้นได้
- 2.2 กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกันโดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ เป็นต้น
- 2.3 ต้องกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย
 - 2.3.1 จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ ที่ได้รับมอบหมาย
 - 2.3.2 กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออก ดังกล่าวโดยจัดทำเป็นเอกสาร “บันทึกการเข้า-ออกพื้นที่” (สแกนลายนิ้วมือ)
 - 2.3.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารปีละ 1 ครั้ง เป็นอย่างน้อย

- 2.4 บุคคลภายนอกเข้ามาติดต่อต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้อง และจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา
- 2.5 บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

ส่วนที่ 2

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของบริษัทและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทได้อย่างถูกต้อง

2. ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

2.1 ประเภทข้อมูลหรือรูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

2.1.1 รูปแบบเอกสารข้อความ (Text format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ปกติ เมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น

- TEXT format เป็น ไฟล์ที่เก็บเฉพาะตัวอักษร ไม่เก็บลักษณะ ที่ใช้เพื่อแสดงผลของเอกสาร
- Document format เป็นไฟล์ที่ผลิตจาก เวิร์ดโปรเซสเซอร์ เช่นไมโครซอฟต์เวิร์ด ปลาดาวออฟฟิศซึ่งไฟล์ประเภทนี้จะเก็บนายลักษณะของการแสดงผลของเอกสารไว้พร้อมกับ ตัวอักษร ซึ่งแต่ละโปรแกรมเวิร์ดโปรเซสเซอร์ จะเก็บนายลักษณะไว้แตกต่างกัน ทำให้บางครั้ง ไม่สามารถใช้โปรแกรมอื่น ๆ เปิดไฟล์นี้ได้ จึงก่อให้เกิดปัญหาในกรณี ที่ไฟล์ถูกผลิตไว้เป็นเวลานาน เมื่อต้องการนำกลับมาใช้จะไม่สามารถถ้าโปรแกรมเปิดเอกสารมาใช้งานได้
- PDF format (Portable Document Format) เป็นไฟล์เอกสารที่ถูกออกแบบให้สามารถเปิดใช้งานกับระบบคอมพิวเตอร์ต่างระบบกันได้ เช่น ระบบวินโดวส์ ระบบยูนิกซ์ จึงทำให้มีความสะดวกในการใช้งานสูง เป็นผลิตภัณฑ์ของบริษัท อโดเบ โดยต้องใช้

โปรแกรมอโครแบต รีเดอร์ (Acrobat Reader) ในการเปิด และต้องใช้โปรแกรมสร้างเอกสาร อโครแบตในการสร้างเป็นเอกสารรูปแบบ PDF

- XML (Extensible Markup Language) เป็นภาษาที่ใช้สำหรับการเขียนเอกสารมาร์คอัพ (Markup Document) โดยที่เอกสารมาร์คอัพ นั้นมีการใช้เมตาดาต้า (Metadata or Tags) เพื่อบอกหน้าที่และประเภทของข้อมูลของส่วนต่างๆ ในเอกสารนั้นได้ชัดเจน การเพิ่มเมตาดาต้าเข้าไปในเอกสารสามารถทำให้โครงสร้างของเอกสารชัดเจนขึ้น และทำให้การประมวลผลเอกสารเป็นไปโดยง่าย

2.1.2 รูปแบบเอกสารภาพ (Image) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์มีรูปแบบที่ใช้ งาน เช่น

- JPEG format เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพได้หลายสีมีการบีบอัดข้อมูล
- PNG or GIF formats เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพ มีการบีบอัดข้อมูลแบบ ไม่มีการสูญเสียของนายภาพ (Lossless compression) และสามารถใช้ได้กับภาพสี ภาพสีเทา และขาวดำ
- Bitmapping formats เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพในรูปแบบอื่น ๆ เป็นจุดของภาพ

2.2 การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางที่เหมาะสมที่ในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของ เอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

2.2.1 การกำหนดชั้นความลับ ตามความสำคัญของข้อมูลในเอกสาร กำหนดไว้ 3 ระดับ ได้แก่ลับ ลับมาก ลับที่สุด และมีการกำหนดความรับผิดชอบ ให้แก่ผู้มีอำนาจกำหนดชั้นความลับ เป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสาร และการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

2.2.2 การควบคุมเอกสาร โดยกำหนดให้มีมาตรการควบคุมต่าง ๆ คือ การจัดทำทะเบียนการตรวจสอบ การจัดทำเอกสาร การสำเนาและการแปล การโอน การส่งและการรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉิน เวลาสูญหาย รวมถึงการเปิดเผยข้อมูลในเอกสาร

3. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

3.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้า-ออก ที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

3.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยี

สารสนเทศ และการสื่อสารรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

- 3.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และระบบข้อมูลได้
- 3.4 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารของบริษัท และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ
- 3.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

4. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

- 4.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน และมีการจัดทำบัญชีผู้ใช้งานให้สอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้นั้น
- 4.2 เจ้าของข้อมูลหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น ต้องรู้ตามหน้าที่งานเท่านั้นเนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งาน เกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น เช่น กำหนดสิทธิการเข้าถึงระบบสารสนเทศตามภารกิจที่รับผิดชอบของแต่ละหน่วยงาน โดยหน่วยงานที่เป็นผู้รับผิดชอบตามภารกิจสามารถเข้าถึงปรับปรุงแก้ไขข้อมูลได้ ส่วนหน่วยงานที่ไม่ได้เป็นผู้รับผิดชอบโดยตรงจะสามารถเข้าถึงข้อมูลได้เพียงอย่างเดียว ไม่สามารถปรับปรุงข้อมูลได้
- 4.3 ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

5. การบริหารจัดการการเข้าถึงของผู้ใช้

- 5.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของบริษัทกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการตามความจำเป็น โดยผู้ใช้งานเป็นผู้ร้องขอเพื่อเข้าใช้ระบบงาน ผู้บังคับบัญชาเป็นผู้อนุมัติและผู้ดูแลระบบเป็นผู้บริหารจัดการบัญชีผู้ใช้งาน
- 5.2 ขั้นตอนปฏิบัติในการยกเลิกสิทธิการใช้งาน เช่น เมื่อได้รับแจ้งการลาออก ให้เพิกถอนภายใน 24 ชั่วโมงหรือ เมื่อโยกย้ายตำแหน่งงานภายใน ต้องทำภายใน 7 วัน
- 5.3 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ

- อินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- 5.4 ผู้ใช้ต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด รวมทั้งเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- 5.5 วิธีการบริหารจัดการรหัสผ่านของผู้ใช้ให้มีความมั่นคงปลอดภัย
- 5.5.1 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษร ที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)
- 5.5.2 ไม่ควรกำหนดรหัสผ่าน ส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- 5.5.3 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- 5.5.4 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองอยู่
- 5.5.5 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- 5.5.6 กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้ต้องเป็นไปอย่างปลอดภัย
- 5.6 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่
- 5.6.1 ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร “ส่วนที่ 3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน”
- 5.6.2 การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตาม “ส่วนที่ 3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน”
- 5.6.3 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
- 5.6.3.1 ต้องได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ
- 5.6.3.2 ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่เป็นเท่านั้น

- 5.6.3.3 ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- 5.6.3.4 ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 6 เดือน เป็นต้น
- 5.7 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
 - 5.7.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึง ผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
 - 5.7.2 เจ้าของข้อมูลต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน เหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม
 - 5.7.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและ การเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และ รหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
 - 5.7.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
 - 5.7.5 มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสาร “ส่วนที่ 3 การบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้งาน”
 - 5.7.6 มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

6. การบริหารจัดการการเข้าถึงระบบเครือข่าย

- 6.1 ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้การควบคุมและป้องกันการบุกรุกได้อย่าง เป็นระบบ
- 6.2 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
- 6.3 ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

- 6.4 ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้ กำหนดบุคคลที่รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบ
- 6.5 การป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
- 6.6 ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกบริษัทต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย
- 6.7 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบริษัทในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- 6.8 การเข้าสู่ระบบงานเครือข่ายภายในบริษัทโดยผ่านทางอินเทอร์เน็ต จำเป็นต้องมีการล็อกอิน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
- 6.9 IP Address ภายในของระบบงาน เครือข่ายภายในของบริษัท จำเป็นต้องมีการป้องกันมิให้หน่วยงาน ภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูล เกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย
- 6.10 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- 6.11 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
- 6.12 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศของบริษัทเท่านั้น

7. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

- 7.1 ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน
- 7.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่มีพบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

- 7.3 ต้องเปิดให้บริการ (Service) เท่าที่จำเป็นเท่านั้นเช่น Telnet FTP หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย
- 7.4 ต้องดำเนินการติดตั้งอัปเดตระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น
- 7.5 ต้องมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
- 7.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีและสารสนเทศเท่านั้น

8. การบริหารจัดการการบันทึกและตรวจสอบ

- 8.1 ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบบันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน
- 8.2 ต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- 8.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆและจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

9. การควบคุมการเข้าใช้งานระบบจากภายนอก

- 9.1 ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กรเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้
- 9.2 การเข้าสู่ระบบระยะไกล (Remote Access) ผู้ระบบเครือข่ายของบริษัท ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของบริษัท จากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
- 9.3 วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของบริษัท ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
- 9.4 การทำให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ
- 9.5 ต้องมีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

- 9.6 การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและ
ไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็นช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะ
เปิดให้ใช้ได้ เมื่อมีการร้องขอที่จำเป็นเท่านั้น

10. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

- 10.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กรดังนี้
- 10.1.1 แสดงชื่อผู้ใช้งาน (Username)
 - 10.1.2 ใส่รหัสผ่าน (Password)

ส่วนที่ 3

การบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้งาน

(User Access Data Management)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มี
หน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศ และเครือข่ายภายในโดยไม่ได้รับอนุญาต
รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัว
บุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

2. การลงทะเบียนผู้ใช้งาน (User Registration)

- 2.1 จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของบริษัท
- 2.2 ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน
- 2.3 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
- 2.4 ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อ
แสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้ง
ทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว
- 2.5 ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อ
ผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน
- 2.6 การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อ
ป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

3. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

- 3.1 ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติ งาน
ในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

- 3.2 ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ
- 3.3 ผู้ดูแลระบบต้องมอบหมายสิทธิควรมีความสอดคล้องกับนโยบายควบคุมการเข้าถึงข้อมูลของผู้ใช้งาน
- 3.4 ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน
- 3.5 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

4. ระบบบริหารจัดการรหัสผ่าน (Password Management System)

- 4.1 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้
- 4.2 ระบบบริหารจัดการรหัสผ่านต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่ที่ตั้ง
- 4.3 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น เช่น ไม่ใช่ชื่อพ่อแม่ ญาติพี่น้อง ไม่ใช่คำจากพจนานุกรม เป็นต้น
- 4.4 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ 6 เดือน
- 4.5 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชี ผู้ใช้งาน และ ทำการล็อกอินเข้าใช้งานระบบงานเป็นครั้งแรก
- 4.6 ระบบบริหารจัดการรหัสผ่านต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งาน นั้นกำลังใส่ข้อมูลล็อกอิน เช่น ให้แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอ เป็นต้น
- 4.7 ระบบบริหารจัดการรหัสผ่านควรป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ และที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น โดยการเข้ารหัสข้อมูลการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

5. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

- 5.1 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท
- 5.2 ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
- 5.3 ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

- 5.4 ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และควรกำหนดรหัสผ่านที่แตกต่างกัน
- 5.5 ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมลเป็นช่องทางในการส่งและกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

6. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

- 6.1 ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน 1 ครั้ง / ปีเป็นอย่างน้อย
- 6.2 ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป
- 6.3 ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน
- 6.4 ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ 4

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้ระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

2. การใช้งานรหัสผ่าน (Password Use)

- 2.1 ผู้ใช้งานระบบเทคโนโลยีสารสนเทศควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้
- 2.2 ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
- 2.3 ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง
- 2.4 ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
- 2.5 ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น
- 2.6 ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำที่กำหนดไว้
- 2.7 ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ
- 2.8 ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรมบริษัท

- 2.9 ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123, abcd หรือกลุ่มของตัวอักษรที่เหมือนกัน เช่น 111, aaa เป็นต้น
- 2.10 ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด
- 2.11 ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว
- 2.12 ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกๆ 3 เดือนสำหรับผู้ดูแลและ 6 เดือน สำหรับผู้ใช้งานระบบ
- 2.13 ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน
- 2.14 ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกหรือจดจำรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง
- 2.15 ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น
- 2.16 ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ใช้งาน

3. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

- 3.1 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน้ตบุ๊ก
- 3.2 ผู้ใช้งานควรล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว
- 3.3 ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

ส่วนที่ 5

การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูล และระบบสารสนเทศของบริษัทโดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

2. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

- 2.1 การใช้งานบริการเครือข่าย

- 2.1.1 ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของบริษัท
- 2.1.2 บริษัทไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และ เครือข่ายเช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร
- 2.1.3 ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มีชื่อของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่นการเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพ หรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว บริษัทฯ ไม่มีส่วนร่วมรับผิดชอบต่อความเสียหายดังกล่าว
- 2.1.4 ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าการพยายามรุกรานล่าเซตหวงห้ามของทางบริษัท
- 2.1.5 บริษัทให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกสิทธินี้ให้กับผู้อื่นไม่ได้
- 2.1.6 บัญชีผู้ใช้งาน (User Account) ที่บริษัทฯ ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบ ผลต่าง ๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- 2.1.7 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา
- 2.1.8 ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิงในระหว่างปฏิบัติงาน
- 2.2 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่บริษัทมีแนวทางปฏิบัติดังนี้
 - 2.2.1 ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น
 - 2.2.2 สิทธิในการเข้าออกห้องต่างๆภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากฝ่ายเทคโนโลยีและสารสนเทศ เป็นลายลักษณ์อักษรโดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

- 2.2.3 ต้องจัดทำระบบเก็บบันทึกการเข้าออกบริษัทตามกระบวนการที่ระบุไว้ในเอกสาร “แบบฟอร์มการ เข้า-ออกพื้นที่”
- 2.2.4 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบ เครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม
- 2.2.5 การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”
- 2.3 ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้
 - 2.3.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”
 - 2.3.2 ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน ภายในบริษัท มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่ายต้องลงบันทึกรายการอุปกรณ์ใน แบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน
 - 2.3.3 เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน
- 2.4 การระบุอุปกรณ์บนเครือข่าย
 - 2.4.1 ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
 - 2.4.2 กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่า สามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
 - 2.4.3 อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
 - 2.4.4 ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”
- 2.5 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ
 - 2.5.1 ผู้ดูแลระบบต้องกำหนดการเปิด – ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อ พอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบ เครือข่าย
 - 2.5.2 บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องควบคุมระบบคอมพิวเตอร์ จะต้อง ลงชื่ออนุญาตการเข้าออกใน “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มา ติดต่อตลอดเวลา
 - 2.5.3 บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษาบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือ บริหารจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น
 - 2.5.4 ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

2.6 การแบ่งแยกเครือข่าย

- 2.6.1 บริษัทแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
- 2.6.2 บริษัทจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ โดยหน่วยงานของบริษัทสามารถใช้งานระบบสารสนเทศผ่านระบบเครือข่ายภายใน แต่ไม่สามารถใช้ระบบดังกล่าวผ่านเครือข่ายภายนอกได้ เพื่อความปลอดภัยของฐานข้อมูล
- 2.6.3 บริษัทติดตั้ง Firewall เพื่อป้องกันทางเข้าเครือข่ายของบริษัทจากผู้ไม่หวังดี

ส่วนที่ 6

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงาน ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

- 2.1 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- 2.2 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อ ไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
- 2.3 ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง
- 2.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
- 2.5 ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- 2.6 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

- 2.7 ซอฟต์แวร์ที่บริษัท ใช้มีลิขสิทธิ์ผู้ใช้งานสามารถใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว
- 2.8 ซอฟต์แวร์ที่บริษัทจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
- 2.9 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัท เพื่อประโยชน์ทางการค้า
- 2.10 ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์
- 2.11 ห้ามผู้ใช้งานระบบสารสนเทศของบริษัท เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

3. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

- 3.1 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข
- 3.2 ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่า ผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- 3.3 ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
- 3.4 ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

4. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)

- 4.1 มีการกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ระดับสิทธิของผู้ขออนุมัติและการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้เพื่อจำกัดและควบคุมการใช้งาน
- 4.2 ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน
- 4.3 มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้
- 4.4 ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ส่วนที่ 7

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของบริษัท และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ได้อย่างถูกต้อง

2. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

- 2.1 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของบริษัท ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการทำงานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น
- 2.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- 2.3 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation Of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่า 10 นาทีระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Log in เข้าระบบสารสนเทศอีกครั้ง
- 2.4 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้
 - 2.4.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
 - 2.4.2 ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ให้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
 - 2.4.3 กำหนดให้ผู้ให้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

- 2.4.4 กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- 2.4.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- 2.4.6 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ
- 2.5 เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ บริษัทได้กำหนดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่บริษัทพัฒนาในรูปแบบของ WebBase Application โดยเข้าถึงได้ผ่าน ระบบเครือข่ายภายในของบริษัท ซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายดังกล่าว
- 2.6 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้
- 2.6.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- 2.6.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
- 2.6.3 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น
- 2.6.4 กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
- 2.6.5 กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น
- 3. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection time)**
- 3.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ 1 ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงานตามปกติเท่านั้น

- 3.2 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ
- 3.3 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและ พิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุก ๆ 1 ชั่วโมง

4. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

- 4.1 ต้องมีการกำหนดมาตรการและการเตรียมการต่างๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
- 4.2 ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
- 4.3 ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงาน ของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี เพื่อเข้าสู่ระบบงานของบริษัท
- 4.4 ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท รวมทั้งมาตรการควบคุมการใช้บริหารเครือข่ายไร้สายสายที่บ้าน
- 4.5 ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท จากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ ตามที่องค์กรต้องการ
- 4.6 ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสาร ไว้ให้กับผู้ปฏิบัติงานจากระยะไกล
- 4.7 บริษัทไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัว หรือเว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยบริษัท
- 4.8 บริษัทต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่างๆ ของบริษัทที่อนุญาตให้เข้าถึงได้จากระยะไกล
- 4.9 บริษัทต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

ส่วนที่ 8

นโยบายและขั้นตอนการปฏิบัติงานสำหรับการจัดหา พัฒนาและแก้ไขระบบ

(Policies and Procedures for Procurement System Solutions Development)

1. วัตถุประสงค์

เพื่อกำหนดนโยบายและขั้นตอนการปฏิบัติงานในด้านการจัดหา พัฒนาและแก้ไขระบบ ภายใต้การควบคุมการปฏิบัติงานอย่างถูกต้องของผู้ดูแลระบบคอมพิวเตอร์

2. แนวปฏิบัติการจัดการ พัฒนาโปรแกรมสำเร็จรูป

- 2.1 การจัดหาโปรแกรมสำเร็จรูป เพื่อมาใช้งานผู้ดูแลระบบคอมพิวเตอร์จะต้องมีส่วนร่วมในการพิจารณาจัดหาโปรแกรมต่าง ๆ ควรมีการวิเคราะห์ถึงเหตุผลที่เลือกใช้โปรแกรมดังกล่าว และโปรแกรมดังกล่าวสามารถรองรับการทำงานของระบบองค์กรในอนาคตได้
- 2.2 การพิจารณาเลือกซื้อโปรแกรม ต้องผ่านการเห็นชอบจากผู้ดูแลระบบคอมพิวเตอร์ ซึ่ง
- 2.3 สามารถทำได้หลายวิธี คือ การจัดหาโปรแกรมแบบสำเร็จรูป (Packaged) การจัดหาโปรแกรมแบบว่าจ้างทำ (Customized) หรือโปรแกรมแบบพัฒนาเอง (Development)
- 2.4 การทดสอบโปรแกรมที่ได้จัดหา หรือการพัฒนาโปรแกรม จะต้องมีการทดสอบโปรแกรมโดยผู้ใช้งานและผู้ดูแลระบบคอมพิวเตอร์ เพื่อหาข้อผิดพลาด หรือความเหมาะสมกับการใช้งานจริง โดยมีการประเมินรายละเอียดออกเป็นข้อ ๆ
- 2.5 ก่อนการพิจารณาอนุมัติจัดหา พัฒนาโปรแกรมควรสำรวจผลกระทบที่จะเกิดขึ้นจากการเปลี่ยนแปลง เพิ่มเติมทั้ง ฮาร์ดแวร์ ซอฟต์แวร์ และผู้ใช้งานโปรแกรมด้วย
- 2.6 หากมีการพิจารณาอนุมัติจัดหา พัฒนาโปรแกรมแล้ว การติดตั้งโปรแกรมต่าง ๆ ต้องผ่านผู้ดูแลระบบคอมพิวเตอร์เท่านั้นไม่ว่าจะเป็น Testing, Upgrade Program ก็ตาม

3. แนวปฏิบัติการปรับปรุงแก้ไขระบบ หรือรายงาน

- 3.1 การปรับปรุงแก้ไขระบบ บริษัทกำหนดขั้นตอนปฏิบัติสำหรับการขอปรับปรุงแก้ไขระบบ หรือรายงานต่าง ๆ จากแบบฟอร์มที่กำหนด
- 3.2 กำหนดผู้รับผิดชอบในการติดตั้งระบบ หรือรายงานที่มีการปรับปรุง ซึ่งรายงานนั้นจะต้องผ่านการตรวจสอบโดยผู้ใช้งานมาก่อนแล้วเท่านั้น
- 3.3 ควรสำรองระบบหรือรายงานต่าง ๆ ไว้ก่อน ทำการปรับปรุงระบบใหม่
- 3.4 การปรับปรุงแก้ไขระบบ หรือรายงานต่าง ๆ ต้องไม่กระทบกับระบบ หรือรายงานอื่น ๆ

ส่วนที่ 9

การจัดทำระบบสำรองข้อมูล (Backup System)

1. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์ และเครือข่ายสามารถดำเนินการสำรองข้อมูล ได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีจำเป็น

2. แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

- 2.1 ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของบริษัท
- 2.2 การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก
- 2.3 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
- 2.4 การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย
- 2.5 ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้
- 2.6 ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหา และรายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ
- 2.7 ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง ๆ (Incremental Backup)
- 2.8 การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
- 2.9 นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

3. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

- 3.1 ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
Mail Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลในเมลบ็อกซ์	1 ครั้งต่อเดือน
Web Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลเผยแพร่บนเว็บไซต์	1 ครั้งต่อเดือน
Database Server	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	1 ครั้งต่อเดือน
Firewall	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูล Rule ของ Firewall	1 ครั้งต่อเดือน
Server อื่น ๆ เช่น ระบบงานต่าง ๆ	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
	ข้อมูลบนเซิร์ฟเวอร์อื่น ๆ	1 ครั้งต่อเดือน
หมายเหตุ ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบคอัพแบบ Full Backup		

- 3.2 ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพ ตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

4. การกู้คืนระบบ

- 4.1 ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ
- 4.2 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ
- 4.3 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์
- 4.4 ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง

5. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูล และสารสนเทศ (IT Contingency Plan)

นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการ ดังต่อไปนี้

- 5.1 กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง
- 5.2 กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ
- 5.3 ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้ อันเป็นผลจากภัยพิบัติที่กำหนดไว้
- 5.4 จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง
- 5.5 ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 10

การตรวจสอบและประเมินความเสี่ยง (Monitoring and Risk Assessment)

1. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

2. แนวปฏิบัติการประเมินความเสี่ยง

- 2.1 กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ให้ปฏิบัติตามกระบวนการ PDCA ดังต่อไปนี้
 - 2.1.1 การกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

- กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาจากลักษณะการดำเนินงานบริษัท สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยีที่บริษัทใช้งาน
- กำหนดนโยบายความมั่นคงปลอดภัยเพื่อให้ครอบคลุมตามขอบเขตที่กำหนดไว้
- กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศของบริษัท
- ประเมินความเสี่ยง กำหนดทางเลือกในการจัดการกับความเสี่ยง และกำหนดมาตรฐานการลดความเสี่ยง (ซึ่งสามารถนำมาตรการต่าง ๆ ในมาตรฐาน ISO/IEC 27001 มาใช้ในการลดความเสี่ยง)

- นำเสนอภาพความเสี่ยงโดยรวม และขออนุมัติสำหรับความเสี่ยงที่ยังหลงเหลืออยู่
- จัดทำเอกสาร Statement of Applicability

2.1.2 การดำเนินการกับระบบบริหารจัดการความมั่นคงปลอดภัย (Do)

- จัดทำแผนการลดความเสี่ยง
- ปฏิบัติตามแผนการลดความเสี่ยงที่ได้กำหนดไว้
- กำหนดแผนการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยเพื่อใช้ในการติดตามภาพรวมของการบริหารจัดการความมั่นคงปลอดภัยของบริษัท
- จัดทำและดำเนินการตามแผนการอบรม และสร้างความตระหนักเพื่อให้ความรู้และสร้างความตระหนักแก่บุคลากรทั้งหมดที่อยู่ในขอบเขตเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพประสิทธิผล รวมทั้งมีความมั่นคงปลอดภัย
- บริหารจัดการการดำเนินงานและการใช้ทรัพยากรต่าง ๆ ภายในขอบเขตเพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของบริษัท
- จัดทำขั้นตอนปฏิบัติ และ/หรือ กำหนดมาตรการที่จำเป็นสำหรับการติดตาม และบริหาร จัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Management Procedures and Controls) รวมทั้งกำหนดให้ผู้ที่เกี่ยวข้องให้ปฏิบัติตามโดยเคร่งครัด

2.1.3 การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check)

- ดำเนินการตามขั้นตอนปฏิบัติและมาตรการในการเฝ้าระวังและติดตาม (ที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย) เพื่อตรวจหาข้อผิดพลาดจากการประมวลผล, ตรวจหาการ ละเมิดหรือความพยายามในการละเมิดความมั่นคงปลอดภัย, ตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น, ตรวจสอบว่าการดำเนินการจัดการกับเหตุการณ์การละเมิดความ มั่นคงปลอดภัยที่ได้ดำเนินการไปแล้วได้ผลหรือไม่ เป็นต้น
- ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอโดยอย่างน้อย นำสิ่งต่างๆ ดังนี้มาทบทวนด้วย เช่น ผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย, เหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น, ผลจากการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความ มั่นคงปลอดภัย, คำแนะนำและผลตอบกลับ (Feedback) จากผู้ที่เกี่ยวข้อง
- ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอโดยดูว่าแผนการวัดความสัมฤทธิ์ผลฯ เป็นไปตามเป้าหมายหรือตัวชี้วัดที่กำหนดไว้ในแผน
- ทบทวนผลการประเมินความเสี่ยงอย่างเป็นระยะๆ (เช่น ทุกๆ 3-6 เดือน) ทบทวนระดับความเสี่ยงที่ยังเหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ ตามการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับบริษัท, เทคโนโลยีที่บริษัทใช้งาน, วัตถุประสงค์และกระบวนการทางธุรกิจของ

บริษัท, ภัยคุกคามที่มีการระบุเพิ่มเติมหรือเปลี่ยนแปลง, ความสัมพันธ์ของมาตรการต่าง ๆ ที่บริษัทใช้งาน, เหตุการณ์ภายนอกต่าง ๆ เช่น การเปลี่ยนแปลงด้านกฎหมายระเบียบ ข้อบังคับ หรือสิ่งที่อยู่ในสัญญาจ้าง และการเปลี่ยนแปลงด้านสังคม เป็นต้น

- ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้
- บันทึกข้อมูลการดำเนินการและเหตุการณ์ต่างๆ ซึ่งอาจมีผลกระทบต่อความสัมพันธ์หรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งประกอบด้วย การประชุมทบทวนด้านความมั่นคงปลอดภัยโดยผู้บริหาร ให้จัดทำรายงานการประชุมและแจ้งเวียนมติให้ผู้ที่เกี่ยวข้องได้รับทราบและปฏิบัติตาม การปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่าง ๆ ในนโยบายความมั่นคงปลอดภัยของบริษัท ให้ผู้รับผิดชอบบันทึกหลักฐานการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเหล่านั้นไว้เพื่อให้สามารถตรวจสอบได้ในภายหลัง

2.1.4 การทบทวนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (Act)

- ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามผลของการเฝ้าระวัง ติดตามและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย เช่น การปฏิบัติตามมติการประชุมทบทวนโดยผู้บริหาร การปรับปรุงนโยบายความมั่นคงปลอดภัย การจัดการหรือแก้ไขความไม่สอดคล้องกับนโยบายความมั่นคงปลอดภัย การกำหนดมาตรการเพิ่มเติมเพื่อลดการเกิดขึ้นของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เคยเกิดขึ้นแล้ว การปฏิบัติตามแผนการลดความเสี่ยง การปฏิบัติตามแผนด้านความมั่นคงปลอดภัย การปฏิบัติตามคำแนะนำและผลตอบกลับจากผู้ที่เกี่ยวข้อง เป็นต้น
- แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องทราบ โดยให้รายละเอียดที่เพียงพอและเหมาะสมตรวจสอบว่าการปรับปรุงที่ได้ดำเนินการไปแล้ว ว่าบรรลุผลตามที่ต้องการหรือไม่

2.2 การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ต้องดำเนินการดังต่อไปนี้

- 2.2.1 มีการบริหารความเสี่ยง เพื่อกำจัดการป้องกัน/ลดการเกิดความเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ การสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup & Recovery)
- 2.2.2 มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)
- 2.2.3 มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง เป็นต้น
- 2.2.4 มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights)

- 2.3 ต้องมีการทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี อย่างน้อย ปีละ 1 ครั้ง
- 2.4 ต้องมีการตรวจสอบและประเมินความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี มีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ กำหนดให้บริษัทต้องดำเนินการ ดังนี้
- 2.4.1 แสดงการทบทวนนโยบายความมั่นคง
 - 2.4.2 แสดงผลการจัดทำนโยบายความมั่นคงปลอดภัยขององค์การอย่างเป็นลายลักษณ์อักษรโดย CIO หรือ CEO เป็นผู้อนุมัติ
 - 2.4.3 แสดงผลการกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศองค์การ
 - 2.4.4 แสดงระบบสารสนเทศที่มีทั้งหมดในองค์การ
 - 2.4.5 แสดงระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูลและสารสนเทศ
 - 2.4.6 แสดงรายละเอียดแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)
 - 2.4.7 แสดงผลการปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)
 - 2.4.8 แสดง Access Rights ที่ถูกต้องและทันสมัยได้อย่างน้อย 1 ระบบ

ส่วนที่ 11

นโยบายความมั่นคงปลอดภัยของการทำงานอินเทอร์เน็ต (Internet Security Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของบริษัทถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

- 2.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่บริษัทจัดสรรไว้เท่านั้นเช่น Proxy, Firewall, PS-

- IDS เป็นต้น ห้ามผู้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผล
ความจำเป็นและทำการขออนุญาตจากกลุ่มเทคโนโลยีและสารสนเทศเป็นลายลักษณ์อักษร
- 2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราว์เซอร์
- 2.3 ผู้ใช้หมั้น Update Patch และ Hotfix อย่างสม่ำเสมอ โดยสามารถ Download patch และ Hotfix ต่างๆ จาก Microsoft web site เพื่อแก้ปัญหาช่องโหว่
- 2.4 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
- 2.5 ผู้ใช้ต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของบริษัทเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่นเว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคมเป็นต้น
- 2.6 ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท
- 2.7 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัท
- 2.8 ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
- 2.9 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอันใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย
- 2.10 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ 12

แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

1. วัตถุประสงค์

- 1.1 เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของบริษัท สามารถสนับสนุนการปฏิบัติงานของบริษัท ไทยรับเบอร์ลาเท็กซ์กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือและการบริหารงานของบริษัท ไทยรับเบอร์ลาเท็กซ์กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือเป็นไปอย่างถูกต้องสะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผล
- 1.2 เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สำหรับบุคลากรของบริษัทและหน่วยงาน เป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับของบริษัท ไทยรับเบอร์ลาเท็กซ์กรุ๊ป จำกัด (มหาชน)

2. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

- 2.1 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัทให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
- 2.2 ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้อย่างใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท
- 2.3 สำหรับผู้ใช้อย่างใหม่จะได้รับรหัสผ่านครั้งแรก (default password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
- 2.4 รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น 'x' หรือ '*' ในการพิมพ์แต่ละตัวอักษร
- 2.5 ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง
- 2.6 ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการล็อกเอาท์ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
- 2.7 ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
- 2.8 ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน

- 2.9 ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัท หรือ ละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์หรือ อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ ผ่านระบบเครือข่าย ของบริษัท

ส่วนที่ 13

ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

(Terms of Use and Disclaimer)

1. วัตถุประสงค์

- 1.1 เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของบริษัท สามารถสนับสนุนการปฏิบัติงานของบริษัทเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์มีประสิทธิภาพ
- 1.2 เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของบริษัท และหน่วยงาน เป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัท ไทยรับเบอร์ลาเท็กซ์กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ

2. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท

- 2.1 ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ อย่างน้อยดังต่อไปนี้
 - 2.1.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
 - 2.1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
 - 2.1.3 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551
 - 2.1.4 ระเบียบการใช้งานคอมพิวเตอร์ที่บริษัทกำหนด

3. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท

- 3.1 หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อผลประโยชน์ของบริษัท
- 3.2 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อการประกอบธุรกิจ หรือแสวงหาผลประโยชน์ส่วนตัว
- 3.3 ห้ามใช้บริการนี้ไปในการเผยแพร่อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบันชาติ ศาสนา และ พระมหากษัตริย์

- 3.4 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท ในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยของข้อมูล ข่าวสาร ความลับของบริษัท
- 3.5 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพเสียง ข้อความที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น
- 3.6 ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบต่อทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือบริษัท
- 3.7 ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)
- 3.8 ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น
- (1) การสร้างจดหมายลูกโซ่ (Chain mail)
 - (2) การส่งจดหมายจำนวนมาก (Spam mail)
 - (3) การส่งจดหมายต่อเนื่อง (Letter bomb)
 - (4) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์
- 3.9 ห้ามผู้ให้บริการกระทำการใดๆ ที่อาจจะนำมาซึ่งความเสื่อมเสีย หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของบริษัท
- 3.10 ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคล หรือหน่วยงานของจดหมายอิเล็กทรอนิกส์เป็นไว้เป็นความลับ
- 3.11 ห้ามส่งข้อมูลข่าวสาร อันเป็นความลับของบริษัทให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับบริษัท
- 3.12 การส่งข้อมูลข่าวสารที่เป็นความลับของบริษัทให้กับบุคคลหรือหน่วยงานนอกบริษัท จะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติ และมาตรการรักษาความปลอดภัยข้อมูล ข่าวสารตามที่บริษัทกำหนด
- 3.13 ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน(Password) ของหน่วยหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันทีโดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)
- 3.14 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์บริษัทหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน และระเบียบปฏิบัติคำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของบริษัทได้อย่างถูกต้อง
- 3.15 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับบริการแก่สมาชิกนั้น ๆ เป็นการชั่วคราวเพื่อทำการสอบสวน และตรวจสอบหาสาเหตุของมูลเหตุนั้น ๆ

- 3.16 การกระทำใด ๆ ที่เกี่ยวกับการเผยแพร่ ทั้งในรูปแบบของอีเมลและ/หรือโฮมเพจของผู้ให้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ให้บริการกลุ่มเทคโนโลยีและสารสนเทศไม่มีส่วนเกี่ยวข้องใด ๆ

ส่วนที่ 14

การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Third party access control)

1. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้เช่นความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้องและการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่นการพัฒนาระบบการให้บริการของที่ปรึกษาการให้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

2. แนวทางปฏิบัติ

2.1 หัวหน้าฝ่ายเทคโนโลยีและสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสารได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

2.2.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ

2.2.2 จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำ เป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

■ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

- 2.2.3 หน่วยงานภายนอกที่ทำงานให้กับบริษัท ทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในบริษัทหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของบริษัท โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ
- 2.2.4 บริษัทควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน
- 2.2.5 เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล
- 2.2.6 สำหรับโครงการขนาดใหญ่หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของบริษัท ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆให้มีความมั่นคงปลอดภัยทั้ง 5 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และการปฏิบัติให้สอดคล้องกับกฎระเบียบ หรือกฎหมายที่เกี่ยวข้อง (Compliance)
- 2.2.7 บริษัทมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจได้ว่าบริษัทสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น
- 2.2.8 ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวดเพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ 15

การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของ ระบบเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

2. แนวปฏิบัติสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

- 2.1 จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
- 2.2 เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการอบรมพนักงานทั้งเก่าและเข้าใหม่ โดยมีแผนการดำเนินงานปีละอย่างน้อย 1 ครั้ง โดยจะจัดอบรมเกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และอาจมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้
- 2.3 ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
- 2.4 ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ส่วนที่ 16

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ให้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

2. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

- 2.1 ให้ฝ่ายเทคโนโลยีสารสนเทศสำนักงานใหญ่ เป็นผู้กำหนดพื้นที่ผู้ให้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายพื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น
- 2.2 ฝ่ายเทคโนโลยีสารสนเทศสำนักงานใหญ่ เป็นผู้กำหนดสิทธิ์การเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.3 ฝ่ายเทคโนโลยีสารสนเทศสำนักงานใหญ่ กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

3. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากกระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

3.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)

- 3.1.1 มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในบริษัท
- 3.1.2 มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง

- 3.1.3 ผนังล้อมรอบของสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในควรสร้างเป็นผนังทึบ
- 3.1.4 ประตูหรือทางเข้าสำนักงานหรืออาคารออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ
- 3.1.5 ประตูหรือทางเข้าของห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อกได้เพื่อป้องกันการบุกรุกทางกายภาพ
- 3.1.6 บุคลากรที่ปฏิบัติงานภายในกลุ่มเทคโนโลยีสารสนเทศ ต้องปิดประตูและหน้าต่างให้ล็อกอยู่เสมอภายหลังเลิกงาน และนอกเวลาบริษัท
- 3.1.7 มีการจัดระบบการรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัย (รปภ.) และมีการติดตั้งกล้องวงจรปิด เพื่อควบคุมการเข้าถึงของบุคคลภายนอก
- 3.1.8 ประตูหนีไฟและผนังในบริเวณข้างเคียงต้องมีการก่อสร้างให้มีความทนทานต่อความร้อนอย่างเพียงพอ
- 3.1.9 ต้องแยกพื้นที่สำหรับระบบเทคโนโลยีสารสนเทศของบริษัทออกจากพื้นที่ที่มีการดูแลหรือบริหารจัดการโดยผู้ให้บริการภายนอก
- 3.2 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Deliver, and Loading Areas)
 - 3.2.1 จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
 - 3.2.2 จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น
 - 3.2.3 จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในบริษัท
 - 3.2.4 ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน
 - 3.2.5 กำหนดให้มีการลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกโดย ให้สอดคล้องกับระเบียบพัสดุหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของบริษัท
- 3.3 การจัดวางและการป้องกันอุปกรณ์ (Equipment Siting and Protection)
 - 3.3.1 ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในสำนักงานให้น้อยที่สุด
 - 3.3.2 ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญในระบบนั้น โดยบุคคลภายนอก เช่น การหันหน้าจอเข้ามาภายในโดยไม่ให้ลูกค้าสามารถมองเห็นหน้าจอได้นั้นได้

- 3.3.3 ต้องแยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย โดยเฉพาะสำหรับอุปกรณ์นี้
- 3.3.4 ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ห้องควบคุมระบบ คอมพิวเตอร์
- 3.3.5 ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบ คอมพิวเตอร์เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การ ตรวจสอบว่า ระดับอุณหภูมิอยู่ในระดับปกติหรือไม่
- 3.3.6 มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน หรือไฟฟ้า กระชาก
- 3.4 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)
 - 3.4.1 ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของบริษัทที่เพียงพอต่อ ความต้องการใช้งาน เช่น ระบบปรับอากาศ ระบบระบายอากาศ ระบบกระแสไฟฟ้าสำรอง เป็นต้น และต้องมีการตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอเพื่อให้ มั่นใจได้ว่า ระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของ ระบบ
 - 3.4.2 ต้องมีการใช้ระบบยูทิลิตี้กับระบบเทคโนโลยีสารสนเทศเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหาย จากความไม่สม่ำเสมอของกระแสไฟฟ้าและต้องทดสอบระบบยูทิลิตี้อย่างสม่ำเสมอโดย ทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้ ต่อสัญญาการซ่อมบำรุงกับบริษัท ดังต่อไปนี้
- 3.5 การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงาน และทรัพย์สินอื่นๆ
 - 3.5.1 เจ้าหน้าที่ทุกคนต้องปฏิบัติตามการป้องกันทรัพย์สิน
 - 3.5.2 เจ้าหน้าที่ต้องออกจากระบบทันทีเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
 - 3.5.3 ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อก และไม่ให้เอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของทรัพย์สินของบริษัท
 - 3.5.4 ต้องป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน และป้องกันขั้นต้นหรือบริเวณที่ใช้ในการรับส่ง เอกสารไปรษณีย์ เพื่อความปลอดภัยของข้อมูล
 - 3.5.5 ต้องไม่ให้ผู้ที่มิได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่างๆ เช่น เครื่องคอมพิวเตอร์ กล้อง ดิจิตอล เครื่องพิมพ์เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น โดยไม่ได้รับอนุญาต
 - 3.5.6 นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

ส่วนที่ 17

แนวปฏิบัติในการติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

1. การปรับปรุงระบบปฏิบัติการ Operating System Update

- 1.1 ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ
- 1.2 ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน
- 1.3 กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator) และชื่อผู้ใช้ (User)
- 1.4 กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name)/ IP Address
- 1.5 ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่มีระบบปฏิบัติการที่มี Service Patch Update)
- 1.6 ติดตั้งโปรแกรม Antivirus/ ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกน และปรับปรุงโปรแกรม

2. การบริหารบัญชีผู้ใช้/ สิทธิการเข้าถึงและการใช้งานระบบ (User Account Management)

- 2.1 กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)
- 2.2 กำหนดชื่อผู้ใช้ (User) และรหัสผ่าน (Password)
- 2.3 บันทึกบัญชีผู้ใช้และสิทธิการเข้าใช้ระบบ

3. การปรับปรุงการรักษาความปลอดภัย/ Antivirus (System Security & Antivirus Update)

- 3.1 ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์การเข้าใช้ระบบ เช่น Log File หรือตรวจสอบ Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง
- 3.2 ปรับปรุง/ กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา
- 3.3 ปรับปรุงโปรแกรม Antivirus และ definition ให้ทันสมัยเป็นประจำทุกสัปดาห์ดำเนินการ Scan ตรวจสอบไวรัสคอมพิวเตอร์ เป็นประจำ

4. ติดตั้ง/ ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

- 4.1 ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้หรือรองรับงานบริการ
- 4.2 กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด
- 4.3 สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้และสิทธิการใช้
- 4.4 ปรับปรุง/ กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

5. ติดตั้งฐานข้อมูล โปรแกรมบริการ/ โปรแกรมระบบงานต่างๆ/ กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

- 5.1 ติดตั้งโปรแกรมการให้บริการ หรือโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา
- 5.2 กำหนดค่าหรือโปรแกรมหรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมบริการ หรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ
- 5.3 ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด
- 5.4 แจ้งผู้ใช้หรือเจ้าของระบบงาน ให้สามารถเริ่มใช้งานได้โดยแจ้งรายชื่อ รหัสผ่าน และสิทธิการเข้าใช้ระบบ และฐานข้อมูลตามระบบกำหนด
- 5.5 ระบุเกณฑ์การสำรอง/ สำเนา/ ทดสอบกู้คืน (Restore Test)
- 5.6 บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้แต่ละระดับของระบบทุกครั้งที่มีการสร้าง/ ปรับปรุง

6. ปฏิบัติการระบบฐานข้อมูล การสำรอง/ สำเนาฐานข้อมูล (Database Backup) และการกู้คืนฐานข้อมูล (Database Restore)

- 6.1 ตรวจสอบการทำงานโปรแกรมการให้บริการ/ โปรแกรมระบบงาน ที่ใช้ฐานข้อมูล
- 6.2 ตรวจสอบการทำงานของฐานข้อมูลในระบบ Database System และขนาดความจุตามระยะเวลาที่กำหนดแต่ละระบบ (ทุกวัน หรือ รายสัปดาห์)
- 6.3 ตรวจสอบการทำงานและขนาดของ Device ที่จัดเก็บฐานข้อมูลด้านการทำงานและรองรับบริการได้ปกติหรือไม่
- 6.4 ทำการสำรองข้อมูล Backup ฐานข้อมูลบันทึกสิ่งที่กำหนดไว้
- 6.5 ระบุชื่อ Backup โดยระบุชื่อฐานข้อมูล + วันที่ Backup
- 6.6 ทำการสำเนา Backup ฐานข้อมูลตามระบบกำหนด และส่งให้หน่วยงานจัดเก็บสำเนาที่ระบุ
- 6.7 ทดสอบการกู้คืนฐานข้อมูลจาก Backup ตามกำหนด
- 6.8 ปฏิบัติการกู้คืนจาก Backup ล่าสุด ในกรณีมีความเสียหายของระบบฐานข้อมูล
- 6.9 บันทึกการปฏิบัติการทุกครั้ง ตามชื่อฐานข้อมูล (ชื่อ Backup/ Restore Test หรือ การกู้คืน)/ ระดับปฏิบัติการ/ วันที่ปฏิบัติการ/ ปัญหาหรือผลสำเร็จ/ ชื่อผู้ปฏิบัติการ/ การทำสำเนาระบบ/ Destination Area
- 6.10 แจ้งผู้ควบคุมกำกับ ผู้รับผิดชอบระบบ และผู้ใช้ระบบฐานข้อมูลถึงความเสียหาย การแก้ไข การกู้คืนและการใช้งาน

7. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ

- 7.1 ตรวจสอบการทำงานส่วนประกอบของเครื่องแม่ข่าย ได้แก่สถานภาพการทำงานของเครื่อง โดยรวม Hard disk/ System Fan/ System Led/ จอภาพ และอุปกรณ์อื่นๆ

- 7.2 ทำความสะอาดเครื่อง อุปกรณ์ เป็นระยะตามกำหนด
- 7.3 ตรวจสอบการทำงานของอุปกรณ์สำรองไฟฟ้า หากมีการติดตั้ง
- 7.4 ตรวจสอบสถานการณ์ทำงาน ประสิทธิภาพของระบบ จาก Device Monitor และ Performance Monitor ของ Operating System ได้แก่ สถานการณ์ทำงานของ CPU/ Memory/ หน่วย Hard drive ขนาดความจุที่เหลือ
- 7.5 แจ้งผลตรวจสอบ/ ปัญหา ให้ผู้บริหารระบบ System Administrator ทราบ
- 7.6 บันทึกการตรวจสอบ/ แก้ไข และดูแลบำรุงรักษาทุกครั้ง

ส่วนที่ 18

การกำหนดขอบเขตอำนาจหน้าที่ผู้รับผิดชอบ

การกำหนดแบ่งอำนาจหน้าที่มีวัตถุประสงค์เพื่อลดความเสี่ยงด้านโครงสร้างพื้นฐาน ซึ่งมีแนวทางปฏิบัติดังนี้คือ ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงานออกจากบุคลากรที่ทำหน้าที่บริหารระบบ ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริงและต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายเทคโนโลยีสารสนเทศ อย่างชัดเจนเป็นลายลักษณ์อักษร ซึ่งมีการจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ ในกรณีจำเป็น โดยกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ รายละเอียดดังนี้

1. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบ คอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

2. ระดับปฏิบัติ

- 2.1 รับผิดชอบกำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษาทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความมั่นคงปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่ประสานงานเทคโนโลยีสารสนเทศ เจ้าหน้าที่เทคโนโลยีสารสนเทศ โปรแกรมเมอร์

- 2.2 รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่ประสานงานเทคโนโลยีสารสนเทศ เจ้าหน้าที่เทคโนโลยีสารสนเทศ โปรแกรมเมอร์ มีหน้าที่รับผิดชอบ ดังนี้
- 2.2.1 ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนที่ 2 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Access Control) และ ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
- 2.2.2 ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัย ของ ฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
- 2.3 รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบเครื่องคอมพิวเตอร์ระบบ เครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย รวมทั้งการสำเนา ฐานข้อมูลผู้รับผิดชอบ ได้แก่ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เจ้าหน้าที่เทคโนโลยี สารสนเทศ มีหน้าที่รับผิดชอบ ดังนี้
- 2.3.1 ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนที่ 5 การควบคุมการเข้าถึงและใช้ระบบเครือข่าย
- 2.3.2 ควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์ตามการกำหนดสิทธิการเข้าถึง ห้องควบคุมระบบคอมพิวเตอร์
- 2.3.3 ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และ อุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมด
- 2.3.4 ควบคุม ติดตาม ตรวจสอบ (Monitor) การใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ
- 2.3.5 ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่ กำหนด
- 2.3.6 ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคล ภายนอก (Hacker) โดยไม่ได้รับอนุญาต
- 2.3.7 ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก
- 2.4 รับผิดชอบในการรักษาความปลอดภัยระบบอินเทอร์เน็ต
- ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- เจ้าหน้าที่เทคโนโลยีสารสนเทศ
- 2.5 รับผิดชอบความปลอดภัยทั่วไป
- เจ้าหน้าที่ประสานงานเทคโนโลยีสารสนเทศ
- เจ้าหน้าที่เทคโนโลยีสารสนเทศ
- โปรแกรมเมอร์

การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

1. ระบบป้องกันผู้บุกรุกแผนดำเนินการรายวัน

- 1.1 ดำเนินการตรวจสอบไฟล์ล็อกหรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำตรวจสอบมีดังต่อไปนี้
 - 1.1.1 การโจมตีเกิดขึ้นมากน้อยเพียงใด การโจมตีประเภทใดเกิดขึ้นเป็นจำนวนมาก
 - 1.1.2 ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
 - 1.1.3 ระดับความรุนแรงมากน้อยเพียงใด
 - 1.1.4 หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

2. ระบบไฟร์วอลล์

- 2.1 ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละ 1 ครั้ง
- 2.2 ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟร์วอลล์สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้
 - 2.2.1 Packet ที่ไฟร์วอลล์ได้ทำการ Block
 - 2.2.2 ลักษณะของ Packet ที่ถูก Block
 - 2.2.3 Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก
- 2.3 กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

3. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต

ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์ แผนดำเนินการรายวัน/ รายสัปดาห์ /รายเดือน

- 3.1 ดำเนินการตรวจสอบไฟล์ล็อกและรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้
 - 3.1.1 มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
 - 3.1.2 มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
 - 3.1.3 มีการส่งมัลแวร์จากเครือข่ายภายในบริษัทไปยังภายนอกหรือไม่
- 3.2 ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของบริษัท
- 3.3 ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอกควรระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

4. การปรับปรุงระบบปฏิบัติการให้มีการอัปเดตอย่างสม่ำเสมอ

มีการเช็คการอัปเดตของ Server ทุกเครื่อง เพื่อการปิดช่องโหว่ ของเซิร์ฟเวอร์ เพื่อความปลอดภัย

เบอร์โทรติดต่อกรณีเกิดเหตุฉุกเฉิน

1. เบอร์โทรติดต่อฝ่ายเทคโนโลยีสารสนเทศ กรณีที่เกิดเหตุฉุกเฉินเกี่ยวกับระบบคอมพิวเตอร์
 - ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
 - เจ้าหน้าที่ประสานงานเทคโนโลยีสารสนเทศ
 - เจ้าหน้าที่เทคโนโลยีสารสนเทศ
 - โปรแกรมเมอร์
2. เบอร์โทรติดต่อผู้บริหาร ที่รับฝากข้อมูลของบริษัทไว้
 - กรรมการผู้จัดการสายตรวจสอบภายในและกำกับกิจการ
 - กรรมการ
 - ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
3. เบอร์โทรติดต่อคณะกรรมการความปลอดภัย อาชีวอนามัย กรณีเกิดเหตุฉุกเฉินด้านภัยพิบัติ
 - ประธานกรรมการ/ผู้แทนนายจ้าง
 - กรรมการผู้แทนระดับบังคับบัญชา
 - เลขานุการ
 - กรรมการผู้แทนลูกจ้าง
4. เบอร์โทรติดต่อ รปภ. ฝ้าอาคาร/แม่บ้าน กรณีเกิดเหตุฉุกเฉินทางกายภาพ
 - รปภ.
 - แม่บ้าน