บริษัท เมืองไทย แคปปิตอล จำกัด

MUANGTHAI CAPITAL CO.,LTD

นโยบายความมั่นคงปลอดภัยสารสนเทศ

(Information Security Policy)

ลำดับการประกาศใช้เอกสาร

ครั้งที่	รายละเอียด	วันที่มีผลบังคับใช้
1	นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)	9 พฤษภาคม 2557

สารบัญ

1. นโยบายความมั่นคงปลอดภัย (Security Policy)

1.1 นโยบายความปลอดภัยสารสนเทศ (Information Security Policy)

จุดประสงค์และขอบเขต

เพื่ออธิบายถึงจุดประสงค์และขอบเขตของนโยบายความปลอดภัยสารสนเทศในภาพรวม โดยรวมถึงความรับผิดชอบในการดูแลและปรับปรุงนโยบาย

นโยบายความปลอดภัยสารสนเทศ จัดทำขึ้นเพื่อแสดงถึงทิศทางของผู้บริหารขององค์กร ด้านความปลอดภัยสารสนเทศที่ต้องการให้บุคคลที่เกี่ยวข้องกับข้อมูลขององค์กรยึดถือ และนำมาใช้ในการปฏิบัติงาน ไม่ว่าเป็นการนำไปพัฒนากระบวนการทำงานให้สอดคล้องกับนโยบาย หรือการใช้เป็นหลักเกณฑ์ด้านความปลอดภัยสารสนเทศประกอบการจัดซื้อจัดหาอุปกรณ์ หรือว่าจ้างบริการที่เกี่ยวข้องกับข้อมูล ขององค์กร โดยมีเป้าหมายคือการทำให้การปฏิบัติงานของพนักงานที่เกี่ยวข้องกับข้อมูล รวมถึงระบบ ที่เกี่ยวข้องกับข้อมูลให้มีความปลอดภัยสารสนเทศที่เพียงพอในการรองรับการดำเนินธุรกิจ ณ ปัจจุบัน และในอนาคตขององค์กร

นโยบายความปลอดภัยสารสนเทศในที่นี้ ครอบคลุมถึงการปกป้องข้อมูลขององค์กรเป็นหลัก เนื่องด้วยข้อมูล ถือได้ว่าเป็นทรัพย์สินที่มีความสำคัญเป็นอย่างมากในการดำเนินธุรกิจขององค์กร ซึ่งในกรณีที่ข้อมูลสำคัญขององค์กร ไม่มีความปลอดภัย ไม่สามารถรักษาความลับ ความถูกต้องและความพร้อมใช้ ของข้อมูลได้นั้น จะส่งผลกระทบต่อองค์กร ไม่ว่าจะเป็นด้านการเงิน ด้านความเชื่อถือ หรือชื่อเสียงขององค์กร ข้อมูลที่กล่าวถึงในนโยบายนั้น มิได้จำกัดอยู่แต่ในรูปอิเล็กทรอนิกส์เท่านั้น ข้อมูลอาจอยู่ในรูปอื่นๆ เช่น เอกสาร ฟิล์ม หรือแม้แต่ในรูปของการสนทนา อย่างไรก็ดี การปกป้องข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ จะกล่าวถึงเป็นส่วนใหญ่ เนื่องจากข้อมูลขององค์กรส่วนใหญ่นั้นจะอยู่ในรูปอิเล็กทรอนิกส์ ซึ่งในอนาคต จะมีแนวโน้มเพิ่มขึ้นตามลำดับ

เนื้อหานโยบาย

1.1.1 แนวนโยบายความปลอดภัยสารสนเทศ

1) นโยบายความปลอดภัยสารสนเทศ เป็นหลักเกณฑ์พื้นฐานด้านความปลอดภัยสารสนเทศ ของข้อมูลในการพัฒนากระบวนการทำงาน และระบบที่มีความปลอดภัยที่เหมาะสมกับการดำเนินธุรกิจขององค์กร โดยให้มีการจัดทำนโยบายความปลอดภัยเฉพาะด้านขึ้นตามความเหมาะสม เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ทั้งนี้ อาจมีการจัดทำมาตรฐาน และ/หรือขั้นตอนปฏิบัติที่เกี่ยวข้องเพื่อใช้เป็นเอกสารสนับสนุนในการปฏิบัติตามนโยบาย
2) ผู้บริหาร พนักงาน ขององค์กรรวมถึงบุคคลภายนอกที่เกี่ยวข้องกับข้อมูลขององค์กรต้องทำความเข้าใจ ยอมรับและปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ

3) คณะกรรมการความปลอดภัยสารสนเทศเป็นเจ้าของนโยบายนี้ มีหน้าที่ต้องรับผิดชอบในการดูแลและสอบทานเนื้อหาของนโยบายอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การเปลี่ยนแปลงกลยุทธ์หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างเทคโนโลยี เป็นต้น

4) คณะกรรมการความปลอดภัยสารสนเทศ ต้องประเมินประสิทธิผลของการนำนโยบายไปใช้ เพื่อนำมาปรับปรุงเนื้อหานโยบายหรือแผนกลยุทธ์ ในการนำนโยบายไปใช้ในองค์กรให้มีประสิทธิผลต่อไป

1.1.2 การบังคับใช้นโยบายความปลอดภัยสารสนเทศ

1) นโยบายความปลอดภัยสารสนเทศ ต้องจัดทำเป็นลายลักษณ์อักษรตามจุดประสงค์และขอบเขตต้องได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการ เพื่อประกาศใช้และถือปฏิบัติทั่วทั้งองค์กร โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นขององค์กรตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและทรัพย์สินสารสนเทศขององค์กร

2) ผู้บริหาร ผู้ดูแลและผู้ใช้งานในส่วนของข้อมูลรวมถึงทรัพย์สินอื่นที่เกี่ยวข้องกับสารสนเทศ มีหน้าที่โดยตรง ที่จะต้องสนับสนุน ดำเนินการ และปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้งานอื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลทรัพย์สินสารสนเทศ จะต้องให้ความร่วมมือในการดำเนินการตามนโยบายการฝ่าฝืนนโยบายนี้ ถือเป็นความผิดที่ร้ายแรง โดยมีบทลงโทษถึงขั้นสูงสุดตามระเบียบขององค์กร

3) ในกรณีที่ต้องปฏิบัติแตกต่าง หรือต้องยกเว้นการปฏิบัติ ตามนโยบายความปลอดภัยสารเทศนี้ จะต้องจัดทำเอกสารบันทึก ตามแบบฟอร์มขออนุมัติยกเว้นนโยบาย (Waiver Request Form) โดยระบุเหตุผลและความจำเป็น สำหรับการขอยกเว้นนโยบาย และเสนอคณะกรรมการ ความปลอดภัยสารสนเทศ เพื่อพิจารณาอนุมัติ ซึ่งมีข้อพิจารณาในการขอยกเว้นนโยบายดังนี้

   3.1) การขอยกเว้นนโยบายความปลอดภัยสารสนเทศนั้น ต้องมีเหตุผลอันควรทางธุรกิจ และมีเอกสารประกอบ ตลอดจนต้องได้รับอนุมัติก่อนจึงจะมีการยกเว้นได้

   3.2) ข้อยกเว้นต่างๆ ต้องได้รับอนุมัติจากคณะกรรมการความปลอดภัยสารสนเทศ

   3.3) คณะกรรมการความปลอดภัยสารสนเทศ ต้องตรวจทาน และประเมินข้อยกเว้น ของนโยบายต่างๆ อย่างน้อยปีละครั้ง

   3.4) เจ้าของเรื่องต้องขออนุมัติใหม่หากยังไม่สามารถแก้ไขให้เป็นไปตามนโยบาย ในระยะเวลา ที่กำหนด

3.5) หากข้อยกเว้นของนโยบายนั้น มีผลกระทบต่อการควบคุมภายในที่มีอยู่เดิม ต้องมีการสร้างมาตรการควบคุมชดเชยขึ้นมารองรับสำหรับข้อยกเว้นดังกล่าว โดยต้องปรึกษากับหน่วยงาน ความปลอดภัยสารสนเทศเพื่อให้มั่นใจได้ว่าความเสี่ยงที่เหลืออยู่ขององค์กรอยู่ในระดับ ที่สามารถยอมรับได้

3.6) หลังจากที่ได้พิจารณาใช้มาตรการควบคุมดังกล่าว ต้องถือปฏิบัติตามมาตรการควบคุมนั้น

3.7) การควบคุมชดเชยต้องได้รับการตรวจสอบ โดยหน่วยงานตรวจสอบภายใน

2. นโยบายโครงสร้างความปลอดภัยสารสนเทศ (Organization of Information Security Policy)

2.1 โครงสร้างด้านความปลอดภัยภายในองค์กร (Internal Organization)

จุดประสงค์และขอบเขต

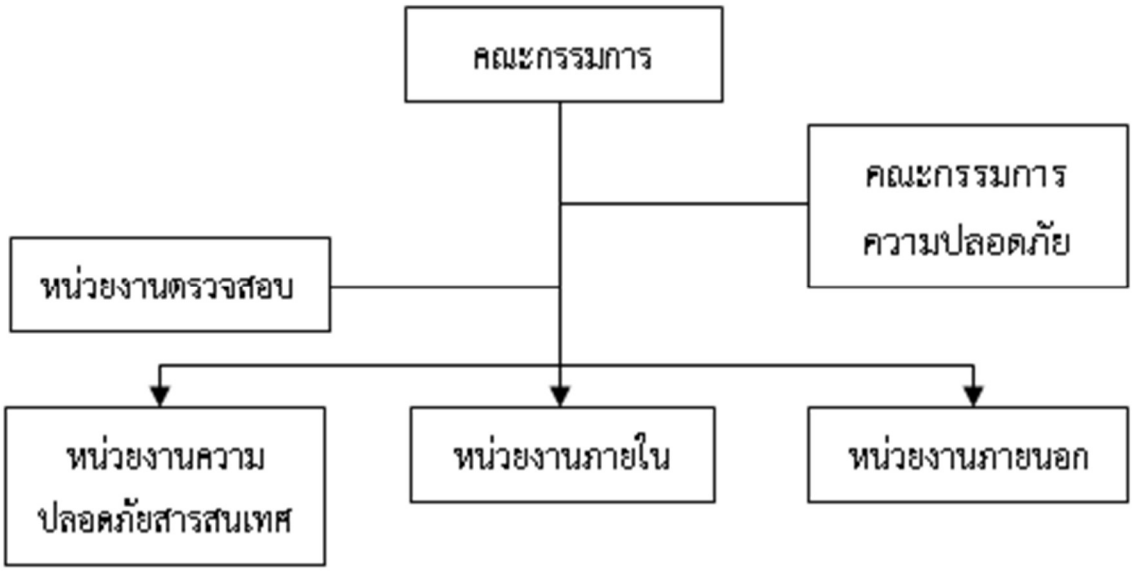
ในการจัดการความปลอดภัยสารสนเทศอย่างเป็นระบบนั้น องค์กรจำเป็นต้องมีการจัดโครงสร้างของหน่วยงานภายในที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม ตั้งแต่ระดับบริหารจนถึงหน่วยงานในระดับปฏิบัติการและรวมถึงการกำหนดบทบาทและหน้าที่ที่มีต่อข้อมูลของผู้ที่เกี่ยวข้องในฐานะต่างๆ ตลอดจนความเข้าใจและตระหนักถึงหน้าที่ด้านความปลอดภัยข้อมูล

เนื้อหานโยบาย

2.1.1 การให้ความสำคัญของผู้บริหารและกำหนดให้มีการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ

ผู้บริหารให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ โดยอนุมัติให้มีการจัดตั้งคณะกรรมการความปลอดภัยสารสนเทศ

1) ลักษณะโครงสร้างของคณะกรรมการความปลอดภัยสารสนเทศ



2) คณะกรรมการความปลอดภัยสารสนเทศ มีองค์ประกอบจากผู้บริหารของหน่วยงานดังนี้

2.1) ผู้บริหารจากหน่วยงานด้านธุรกิจหลักขององค์กร

2.2) ผู้บริหารจากหน่วยงานด้านเทคโนโลยีสารสนเทศ

2.3) ผู้บริหารจากหน่วยงานด้านสนับสนุนทั่วไป

2.4) ผู้บริหารจากหน่วยงานด้านทรัพยากรบุคคล

2.5) ผู้บริหารจากหน่วยงานด้านกฎหมาย

2.6) ผู้บริหารจากหน่วยงานด้านความปลอดภัยสารสนเทศ

3) คณะกรรมการความปลอดภัยสารสนเทศมีหน้าที่ดังนี้

3.1) กำหนดนโยบายเป้าหมายในเรื่องความปลอดภัยสารสนเทศและปกป้องข้อมูลขององค์กร

3.2) ประเมินและบริหารความปลอดภัยสารสนเทศของข้อมูลในภาพรวม

3.3) ตรวจสอบและให้ความเห็นชอบโครงการที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

3.4) ศึกษา พิจารณา ทบทวนและจัดทำร่างเอกสารนโยบาย

3.5) จัดทำแผนพัฒนา แผนการเผยแพร่ประชาสัมพันธ์ แผนการอบรมและแผนการดำเนินการ ด้านความปลอดภัยสารสนเทศ

3.6) ตรวจสอบและอนุมัตินโยบายความปลอดภัยสารสนเทศ ที่มีการเปลี่ยนแปลงหรือที่ได้เพิ่มเติม

3.7) สอบทานสถานภาพปัจจุบันของความปลอดภัยสารสนเทศ

3.8) สอบทานเหตุการณ์ที่กระทบด้านความปลอดภัยสารสนเทศ

3.9) อนุมัติข้อยกเว้นนโยบาย

4) บทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องตามโครงสร้างของคณะกรรมการความปลอดภัยสารสนเทศ

4.1) หน่วยงานด้านความปลอดภัยสารสนเทศ จัดตั้งขึ้นเพื่อป้องกันความเสียหายขององค์กรอันเกิดจากภัยคุกคามด้านข้อมูล เช่น การสูญหายของข้อมูล หรือการเจาะระบบสารสนเทศ เป็นต้น และทำให้การดำเนินการในส่วนที่เกี่ยวข้องกับข้อมูลมีความปลอดภัยในระดับที่สอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

4.2) หน่วยงานด้านตรวจสอบ รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศขององค์กร

4.3) หน่วยงานภายใน คือ พนักงานทุกคนขององค์กร ที่มีส่วนเกี่ยวข้องกับสารสนเทศไม่ว่าทางใดทางหนึ่ง มีหน้าที่รับผิดชอบ ดังนี้

4.3.1) ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ

4.3.2) รักษาความลับของข้อมูลและรหัสผ่านเข้าใช้ระบบ

4.3.3) รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัยเมื่อเกิดเหตุการณ์ดังกล่าว

4.3.4) ใช้งานข้อมูลและทรัพย์สินทางข้อมูลขององค์กรอย่างรับผิดชอบ ตามข้อกำหนดควบคุมที่เกี่ยวข้องและใช้ข้อมูลสำหรับงานที่ได้รับอนุญาตเท่านั้น

4.4) หน่วยงานภายนอก คือ บุคคลภายนอกที่เข้ามาปฏิบัติงานในองค์กรหรือทำงานให้กับองค์กร ซึ่งมีส่วนเกี่ยวข้องในการใช้ข้อมูลหรือทรัพย์สินสารสนเทศอื่นขององค์กร เช่น ผู้ให้บริการ/ผู้จำหน่าย ระบบคู่สัญญา หรือผู้ที่ได้รับอนุญาต โดยมีหน้าที่ความรับผิดชอบเช่นเดียวกับพนักงาน ขององค์กร

2.1.2 การประสานงานความปลอดภัยสารสนเทศในองค์กร

ผู้บริหารทุกหน่วยงาน มีหน้าที่ในการสนับสนุนและประสานงานในการประกาศใช้นโยบาย ความปลอดภัยสารสนเทศ เพื่อให้มีความร่วมมือและถือปฏิบัติทั่วทั้งองค์กร

2.1.3 ข้อตกลงมิให้เปิดเผยความลับขององค์กร

ข้อมูลขององค์กรต้องได้รับการปกป้องด้านความปลอดภัย โดยผู้บริหาร พนักงาน ตลอดจนหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับข้อมูลทุกคน ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูล ซึ่งเป็นข้อตกลงที่จะไม่เปิดเผยข้อมูลที่เป็นความลับขององค์กร

3. นโยบายการบริหารจัดการทรัพย์สิน (Asset Management Policy)

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

จุดประสงค์และขอบเขต

ในการดูแลรักษาและปกป้องทรัพย์สินขององค์กรได้อย่างเหมาะสมนั้น องค์กรควรทราบถึงการมีอยู่ของทรัพย์สิน ทรัพย์สินในที่นี้คือทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ข้อมูล ซอฟต์แวร์ หรือแม้แต่อุปกรณ์ ที่เกี่ยวข้องในการประมวลผล นอกจากนี้องค์กรควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน อย่างไรก็ดี เจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว

เนื้อหานโยบาย

3.1.1 การจัดทำบัญชีทรัพย์สิน

1) ทุกหน่วยงานขององค์กรที่เกี่ยวข้องกับข้อมูล จะต้องดำเนินการจัดทำบัญชีทรัพย์สินที่เกี่ยวข้อง กับข้อมูลขององค์กร สามารถจัดประเภทได้ดังนี้
   1.1) ทรัพย์สินด้านฮาร์ดแวร์ เช่น เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่างๆ อุปกรณ์สื่อสาร เป็นต้น
   1.2) ทรัพย์สินด้านข้อมูลทั้งที่อยู่ในรูปอิเล็กทรอนิกส์และรูปเอกสาร เช่น ฐานข้อมูล, แฟ้มข้อมูล ในระบบที่ใช้งานจริง ข้อมูลสำรอง คู่มือการใช้งานระบบ เอกสารประกอบการพัฒนาระบบ และสัญญาต่างๆ เป็นต้น ทั้งนี้ ให้พิจารณาจัดทำบัญชีทรัพย์สินเฉพาะในส่วนของที่เป็นข้อมูลหลัก และมีความสำคัญ
   1.3) ทรัพย์สินด้านซอฟต์แวร์ เช่น ระบบปฏิบัติการ โปรแกรมประยุกต์ เครื่องมือต่างๆ ในการพัฒนาระบบ และโปรแกรมอรรถประโยชน์ เป็นต้น
2) ผู้ดูแลทรัพย์สินต้องตรวจทาน และปรับปรุงบัญชีทรัพย์สินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน

1) ในการจัดทำทะเบียนทรัพย์สิน แต่ละหน่วยงานจะต้องกำหนดเจ้าของทรัพย์สินที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น สำหรับในกรณีที่เป็นทรัพย์สินด้านข้อมูล ซึ่งอาจมีเจ้าของข้อมูลได้หลายคน ผู้บริหารระดับสูงขึ้นไป ต้องมอบหมายความรับผิดชอบความเป็นเจ้าของข้อมูลให้กับบุคคลที่ใช้หรือเกี่ยวข้องกับข้อมูลนั้นมากที่สุด
2) เจ้าของทรัพย์สิน ต้องสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สินตลอดจนการแจ้งถึงการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินทราบ

3.1.3 การใช้งานทรัพย์สินที่เหมาะสม

1) ข้อมูลเกี่ยวกับบัญชีทรัพย์สินถือว่าเป็นข้อมูลลับที่อาจอนุญาตให้เปิดเผย หรือเข้าใช้งานได้ เฉพาะบุคคลที่เกี่ยวข้องและมีความจำเป็นต้องทราบเท่านั้น
2) ผู้ใช้งาน พนักงาน หน่วยงานภายนอกต้องยินยอมทำตามข้อกำหนดในการใช้งานข้อมูลและทรัพย์สินสารสนเทศ

3.2 การจัดหมวดหมู่สารสนเทศ (Information Classification)

จุดประสงค์และขอบเขต

นโยบายได้กำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้น และได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้นโยบายยังได้กำหนดถึงบทบาทของเจ้าของข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้องกับการจัดลำดับชั้นของข้อมูล

เนื้อหานโยบาย

3.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ

1) กำหนดลำดับชั้นข้อมูลขององค์กรเป็น 5 ลำดับชั้น ดังนี้
   1.1) ชั้นที่ 1 ข้อมูลเปิดเผยได้

   ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น ซึ่งเป็นข้อมูลที่ไม่มีผล ต่อการปฏิบัติงาน สามารถนำเสนอต่อสาธารณะชน และไม่เป็นประโยชน์โดยตรงในเชิงการค้าต่อคู่แข่ง หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย

   1.2) ชั้นที่ 2 ข้อมูลใช้ภายในองค์กรเท่านั้น

   เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้พนักงานทุกคนภายในองค์กรทราบได้ แต่ไม่สามารถเปิดเผยต่อบุคคลภายนอกองค์กรได้ เนื่องจากอาจสร้างความเสียหายให้กับองค์กรได้ หากมีการร้องของบุคคลภายนอก เจ้าของข้อมูลต้องใช้ดุลยพินิจในการเปิดเผย โดยยึดหลักความจำเป็นในการใช้งาน

   1.3) ชั้นที่ 3 ข้อมูลลับ

   เป็นข้อมูลใช้ภายในองค์กรที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงาน ทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน

   1.4) ชั้นที่ 4 ข้อมูลลับมาก

เป็นข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้ใช้บางกลุ่มขององค์กร (ส่วนใหญ่เป็นผู้บริหารเท่านั้น) และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูลประเภทนี้ มีความจำเป็นต่อการปฏิบัติงานขององค์กร และจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือ ทำให้เกิดผลเสียหายร้ายแรงต่อองค์กร

1.5) ชั้นที่ 5 ข้อมูลลับที่สุด

ข้อมูลใช้ภายในองค์กร แต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้บริหารระดับสูงขององค์กรเท่านั้น และเป็นการใช้เพื่อการวินิจฉัยและตัดสินใจที่สำคัญขององค์กร ไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เลย เนื่องจากข้อมูลประเภทนี้มีความจำเป็นต่อการปฏิบัติงานขององค์กรจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือทำให้เกิดผลเสียหายร้ายแรงต่อองค์กร การนำข้อมูลในชั้นนี้ไปเปิดเผยต่อบุคคลภายนอกไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย

2) เจ้าของข้อมูลต้องรับผิดชอบในการกำหนดลำดับชั้นของข้อมูลนั้น โดยคำนึงถึงความต้องการและผลกระทบด้านธุรกิจเป็นหลัก
3) เนื่องจากลำดับชั้นของข้อมูลอาจมีการเปลี่ยนแปลงตามระยะเวลา เจ้าของข้อมูลต้องสอบทานลำดับชั้น ของข้อมูลที่รับผิดชอบอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับสภาพปัจจุบันของข้อมูลนั้น
4) ข้อมูลที่สำคัญต้องมีผู้ดูแลรับผิดชอบข้อมูล โดยผู้ดูแลข้อมูลต้องปกป้องข้อมูลตามแนวทาง การปฏิบัติที่สอดคล้องกับลำดับชั้นของข้อมูล
5) การเปลี่ยนแปลงระดับการป้องกันข้อมูลและลำดับชั้นข้อมูล จำเป็นต้องได้รับความเห็นชอบและอนุมัติจากเจ้าของข้อมูล

3.2.2 การจัดการทรัพย์สินสารสนเทศ

1) การอนุญาตให้เข้าใช้ข้อมูลที่จัดอยู่ในชั้นลับขึ้นไป ต้องกระทำโดยเจ้าของข้อมูลนั้น ในการกำหนดสิทธิ การเข้าใช้ข้อมูล โดยยึดถือตามความจำเป็นทางธุรกิจ
2) พนักงานต้องตระหนักถึงหน้าที่ และความรับผิดชอบในการเปิดเผย และแบ่งปันข้อมูล ทั้งในองค์กรและกับหน่วยงานภายนอก
3) ข้อมูลที่จัดอยู่ในชั้นลับขึ้นไป จะต้องมีการทำเครื่องหมายกำหนดลำดับชั้นตามแนวทางในการปกป้องข้อมูล ข้อมูลที่จัดอยู่ในชั้นต่ำกว่านี้ไม่จำเป็นต้องมีการจัดทำป้ายกำหนดลำดับชั้น

4. นโยบายความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security Policy)

4.1 การสร้างความปลอดภัยก่อนการจ้างงาน (Prior to Employment)

จุดประสงค์และขอบเขต

แนวทางการรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการทรัพยากรบุคคล ตั้งแต่ การรับเข้าทำงานจนถึงการเลิกจ้าง มีส่วนสำคัญที่ช่วยลดความเสี่ยงด้านบุคลากรขององค์กร เนื่องจากสารสนเทศที่หลากหลาย ทำให้การควบคุมความปลอดภัยสารสนเทศโดยระบบอย่างเดียวไม่อาจ เกิดประสิทธิผลเต็มที่ ดังนั้น กระบวนการด้านทรัพยากรบุคคลจึงมีความจำเป็นในการช่วยทำให้สารสนเทศขององค์กรมีความปลอดภัย

เนื้อหานโยบาย

4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความปลอดภัย

1) พนักงานทุกคนมีบทบาทหน้าที่รับผิดชอบในการรักษาความปลอดภัยสารสนเทศ รวมถึงการปฏิบัติตามนโยบายและระเบียบปฏิบัติด้านความปลอดภัยสารสนเทศ
2) กรณีที่พนักงานมีหน้าที่เกี่ยวข้องกับข้อมูลที่มีความสำคัญหรือความลับ ต้องมีการกำหนดหน้าที่และความรับผิดชอบด้านความปลอดภัยสารสนเทศที่มีลักษณะเฉพาะกับหน้าที่งานนั้นในคำอธิบายหน้าที่งาน

4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร

1) หน่วยงานทรัพยากรบุคคลต้องตรวจสอบประวัติของบุคคลก่อนที่จะทำการว่าจ้าง เช่น หลักฐานการศึกษา บุคคลอ้างอิง ประวัติการทำงานจากหน่วยงานต้นสังกัดเดิม และเอกสารที่ทางราชการออกให้ เป็นต้น
2) หน่วยงานทรัพยากรบุคคล ต้องสร้างความตระหนักถึงความรับผิดชอบด้านความปลอดภัยสารสนเทศตั้งแต่การจ้างพนักงาน รวมทั้งระบุความรับผิดชอบดังกล่าวในสัญญาว่าจ้าง
3) บุคคลที่ถูกว่าจ้างเพื่อทำงานในระบบที่สำคัญขององค์กร ในตำแหน่งที่มีความสำคัญ จำเป็นต้อง มีการตรวจสอบเป็นพิเศษ

4.1.3 การกำหนดเงื่อนไขการจ้างงาน

1) เงื่อนไขการจ้างงาน ควรกำหนดถึงหน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศและการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ การฝ่าฝืนหรือละเลยต่อหน้าที่และนโยบาย ความปลอดภัยสารสนเทศขององค์กรถือว่ามีความผิด ต้องพิจารณาตามบทลงโทษขององค์กร ซึ่งขึ้นอยู่กับความรุนแรงของผลกระทบที่เกิดขึ้นกับองค์กร

2) หน่วยงานหรือบุคคลจากหน่วยงานภายนอกซึ่งองค์กรว่าจ้าง จะต้องทำความเข้าใจและรับทราบนโยบายความปลอดภัยสารสนเทศในสาระสำคัญ โดยเฉพาะอย่างยิ่งในเรื่องการไม่เปิดเผยข้อมูล ก่อนการเริ่มปฏิบัติงานจริงในองค์กร
3) พนักงานมีหน้าที่และความรับผิดชอบในการดูแลรักษาความลับของข้อมูล แม้ว่าเมื่อนำข้อมูล ไปทำงานภายนอกอาคารสำนักงาน นำข้อมูลไปทำงานที่บ้าน หรือการเข้าสู่ระบบขององค์กร จากภายนอก (Remote Access)

4.2 การสร้างความปลอดภัยในระหว่างการจ้างงาน (During Employment)

จุดประสงค์และขอบเขต

เพื่อลดความเสี่ยงของสารสนเทศที่เกิดจากบุคลากร ทั้งที่เกิดจากการละเมิดความปลอดภัยสารสนเทศโดยเจตนาและไม่ได้เจตนา หรือจากการละเลยต่อการปฏิบัติหน้าที่ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

เนื้อหานโยบาย

4.2.1 หน้าที่ในการบริหารจัดการทางด้านความปลอดภัย

ผู้ใช้งาน พนักงาน หน่วยงานภายนอกต้องปฏิบัติตามนโยบายและระเบียบปฏิบัติทางด้าน ความปลอดภัยสารสนเทศขององค์กร

4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความปลอดภัยสารสนเทศให้กับพนักงาน

1) หน่วยงานทรัพยากรบุคคล ควรจัดการอบรมพนักงานใหม่ทุกคนขององค์กร โดยเนื้อหาต้องครอบคลุม ถึงนโยบาย ระเบียบปฏิบัติ วิธีการทำงาน และข้อบังคับการทำงานต่างๆ
2) หน่วยงานด้านทรัพยากรบุคคลและหน่วยงานต้นสังกัดของพนักงาน ต้องจัดการอบรมให้ความรู้ ในการทำงานกับพนักงานอย่างสม่ำเสมอ เพื่อเพิ่มเติมความรู้และเพิ่มประสิทธิภาพในการทำงานให้กับพนักงาน
3) พนักงานทุกคน ควรเข้ารับฟังการอบรมให้ตระหนักถึงความปลอดภัยสารสนเทศเพิ่มเติมเป็นระยะๆ เพื่อรับทราบถึงนโยบายความปลอดภัยเพิ่มเติมขององค์กร เหตุการณ์ละเมิดความปลอดภัย และกรณีศึกษาใหม่ๆ และเป็นการเน้นย้ำในนโยบายความปลอดภัยสารสนเทศขององค์กร

4.2.3 กระบวนการทางวินัยเพื่อลงโทษ

หน่วยงานทรัพยากรบุคคล และหน่วยงานด้านกฎหมายต้องกำหนดบทลงโทษสำหรับพนักงาน ซึ่งละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง

4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or Change of Employment)

จุดประสงค์และขอบเขต

เพื่อเพิ่มความปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการบุคลากรที่กำลังจะเลิกจ้าง โดยระบุหน้าที่ความรับผิดชอบและบทบาทของผู้เกี่ยวข้องกับกระบวนการ นอกจากนี้ยังเป็นการควบคุมความปลอดภัย ของสารสนเทศให้ดียิ่งขึ้น

เนื้อหานโยบาย

4.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน

หน่วยงานทรัพยากรบุคคลและหน่วยงานที่เกี่ยวข้อง ต้องร่วมกันกำหนดขั้นตอนการปฏิบัติ ของพนักงานที่ออกจากองค์กรเมื่อสิ้นสุดการจ้างงาน

4.3.2 การคืนทรัพย์สิน

เมื่อมีการโอนย้าย หรือพ้นสภาพการเป็นพนักงาน รวมถึงหน่วยงานภายนอกเมื่อสิ้นสุดการทำงานให้กับองค์กรต้องทำการคืนทรัพย์สินขององค์กรให้ฝ่ายที่ดูแลทรัพย์สินนั้นๆ

4.3.3 การถอดถอนสิทธิในการเข้าถึง

หน่วยงานทรัพยากรบุคคล ต้องแจ้งหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้องทราบทันทีที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานขององค์กรเพื่อทำการถอดถอนสิทธิ การเข้าใช้ระบบงานต่างๆ และการเข้า-ออกพื้นที่ขององค์กร

5. นโยบายความปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security Policy)

5.1 พื้นที่ที่ต้องการรักษาความปลอดภัย (Secure Areas)

จุดประสงค์และขอบเขต

เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในองค์กร และกำหนดมาตรการป้องกันที่เหมะสมตามระดับของความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศขององค์กรขั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับการอนุญาต ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามและการรบกวนไม่ว่าโดยตั้งใจหรือจากภัยธรรมชาติ

เนื้อหานโยบาย

5.1.1 การกำหนดเขตพื้นที่ควบคุม

จัดระดับความสำคัญของพื้นที่ในอาคารสำนักงานขององค์กร และกำหนดให้มีพื้นที่ควบคุมโดยใช้การประเมินความเสี่ยง ซึ่งการจัดทำการประเมินความเสี่ยงในพื้นที่อาคารสำนักงานขององค์กรเพื่อกำหนดหาพื้นที่ควบคุมความปลอดภัย และหามาตรการการควบคุมที่เหมาะสมกับพื้นที่ดังกล่าว

5.1.2 การควบคุมการเข้า-ออก

1) พนักงานทุกคนต้องติดบัตรพนักงานให้เห็นอย่างชัดเจน ตลอดเวลาในขณะที่อยู่ในอาคารสำนักงานขององค์กร
2) ผู้ที่มาติดต่อ ต้องติดต่อเจ้าหน้าที่รักษาความปลอดภัยเพื่อทำการแลกบัตรอนุญาตให้เข้าสถานที่ และต้องติดบัตรให้เห็นอย่างชัดเจน ตลอดเวลาที่อยู่ในอาคารสำนักงานขององค์กร
3) สิทธิในการผ่านเข้า-ออกพื้นที่ของพนักงาน จะต้องทำการยกเลิกทันทีเมื่อพนักงานลาออกหรือสิ้นสุดการเป็นพนักงาน
4) สิทธิในการผ่านเข้า-ออกของพนักงานในพื้นที่ที่มีความสำคัญ ต้องมีการตรวจสอบเป็นรายไตรมาส
5) อาคารที่มีศูนย์คอมพิวเตอร์ ห้องระบบคอมพิวเตอร์หรือระบบสื่อสารต้องมีมาตรการความมั่นคงปลอดภัยที่เข้มงวด เพื่อป้องกันการผ่านเข้า-ออกของผู้ที่ไม่ได้รับอนุญาต
6) พื้นที่ที่มีการติดตั้งอุปกรณ์ควบคุมการเข้า-ออก ห้ามพนักงานทำการหลีกเลี่ยงหรืองดเว้นการทำงานของอุปกรณ์ควบคุมการผ่านเข้า-ออก เช่น การเปิดจากภายในและอนุญาตให้บุคคลจากด้านนอกเข้าโดยมิได้มีการควบคุม ติดตามหรือสอบถาม เป็นต้น

5.1.3 การรักษาความปลอดภัยของศูนย์คอมพิวเตอร์

1) ไม่ควรมีป้ายหรือสัญลักษณ์ที่แสดงถึงที่ตั้งสถานที่ของศูนย์คอมพิวเตอร์

2) ห้องประมวลผลในศูนย์คอมพิวเตอร์เป็นพื้นที่หวงห้าม โปรแกรมเมอร์ และผู้ใช้งานทั่วไปไม่มีสิทธิ ที่จะเข้าไปในพื้นที่ดังกล่าวโดยไม่มีการควบคุม
3) ต้องมีการตรวจสอบประตูฉุกเฉินในสถานที่ สำหรับการประมวลผลที่สำคัญว่ามีการล็อค อย่างเรียบร้อย ตลอดจนมีการใช้งานอย่างถูกต้องและปลอดภัยตามวัตถุประสงค์
4) อุปกรณ์และสื่อที่ใช้สำรองข้อมูล ต้องจัดเก็บไว้ในสถานที่ปลอดภัยห่างจากอุปกรณ์ที่เก็บข้อมูลหลัก ในระยะที่สามารถป้องกันความเสียหายเมื่อมีเหตุเกิดขึ้นกับสถานที่จัดเก็บอุปกรณ์หลัก
5) ห้องระบบคอมพิวเตอร์ต้องติดตั้งระบบประตูอัตโนมัติ ที่สามารถปิดทันทีโดยอัตโนมัติหลังจากที่เปิดประตูแล้ว และจะต้องมีสัญญาณเตือนเมื่อมีการเปิดประตูทิ้งไว้

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม

1) ศูนย์คอมพิวเตอร์ ต้องมีการควบคุมความปลอดภัย ที่อาจเกิดจากไฟไหม้ น้ำท่วม แผ่นดินไหว เป็นต้น
2) ศูนย์คอมพิวเตอร์ ต้องมีระบบป้องกันอัคคีภัย ระบบปรับอากาศและความชื้น ระบบกระแสไฟฟ้า

5.2 ความปลอดภัยของอุปกรณ์ (Equipment Security)

จุดประสงค์และขอบเขต

อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายถือว่าเป็นอุปกรณ์ที่สำคัญต่อสารสนเทศและการดำเนินธุรกิจ ดังนั้น อุปกรณ์เหล่านี้ควรมีการป้องกันอันตรายจากสภาพแวดล้อม รวมถึงการจำกัดการนำอุปกรณ์ดังกล่าวไปใช้นอกสถานที่

เนื้อหานโยบาย

5.2.1 การจัดวางและการป้องกันอุปกรณ์

อุปกรณ์คอมพิวเตอร์ต้องได้รับการจัดวางโดยคำนึงถึงสิ่งต่างๆ ต่อไปนี้

1) อุปกรณ์ต้องมีการจัดวางเพื่อลดการเข้าถึงบริเวณทำงานโดยไม่จำเป็น
2) อุปกรณ์ประมวลผลสารสนเทศที่มีข้อมูลสำคัญต้องมีการจัดวางในมุมที่เหมาะสม เพื่อลดความเสี่ยง ในการมองเห็นข้อมูลโดยบุคคลที่ไม่เกี่ยวข้องและไม่ได้รับอนุญาตระหว่างการใช้งาน
3) การรักษาอุปกรณ์ควรเก็บให้ปลอดภัยเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต
4) ต้องมีการตรวจสอบดูแลสภาพแวดล้อม เช่น อุณหภูมิและความชื้น ซึ่งสามารถทำให้เกิดการทำงาน ที่ผิดพลาดของอุปกรณ์ประมวลผลสารสนเทศ
5) ต้องมีการติดตั้งระบบป้องกันฟ้าผ่าในทุกอาคาร

5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน

1) อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สำคัญต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน (UPS) เพื่อให้ระบบทำงานต่อเนื่องหรือสิ้นสุดการทำงานอย่างเหมาะสมเมื่อระบบไฟฟ้าขัดข้อง
2) ต้องทำการตรวจสอบอุปกรณ์สำรองไฟฟ้าฉุกเฉินตามขั้นตอนของผู้ผลิตอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าวสามารถรองรับการทำงานได้เมื่อเกิดปัญหาไฟฟ้าขัดข้อง
3) ต้องพิจารณาใช้ระบบเครื่องกำเนิดไฟฟ้าสำรอง (Power Generator) กับระบบที่มีความสำคัญในการดำเนินธุรกิจขององค์กรที่มีความจำเป็นต้องทำงานต่อเนื่อง
4) ต้องทำการทดสอบและตรวจสอบความพร้อมของเครื่องกำเนิดไฟฟ้าสำรอง รวมทั้งแหล่งพลังงานสำรองอย่างน้อยทุกเดือน

5.2.3 การบำรุงรักษาอุปกรณ์

1) อุปกรณ์ทั้งหมดต้องมีการตรวจสอบและบำรุงรักษาตามวิธีที่ถูกต้องของผู้ผลิต เพื่อความพร้อมของระบบอยู่เสมอ
2) การบำรุงรักษาอุปกรณ์ที่เกี่ยวข้องกับระบบประมวลผลขององค์กร จะต้องดำเนินการเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
3) การส่งอุปกรณ์ต่างๆ ไปซ่อมแซมภายนอก ต้องมีการควบคุมที่เหมาะสมเพื่อรักษาความลับและความถูกต้องของข้อมูลที่อยู่ในอุปกรณ์เหล่านั้น

5.2.4 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน

1) มาตรฐานที่กล่าวไว้ในนโยบายความปลอดภัยสารสนเทศ มีผลบังคับใช้กับอุปกรณ์และข้อมูลขององค์กรทั้งในและนอกสถานที่
2) พนักงานที่เดินทางไปพร้อมกับเครื่องคอมพิวเตอร์แบบพกพา หรืออุปกรณ์และข้อมูลขององค์กร ต้องดูแลเครื่องคอมพิวเตอร์และข้อมูลภายในอย่างระมัดระวัง

6. นโยบายการบริหารจัดการด้านการสื่อสารและการปฏิบัติการ (Communication and Operation Management Policy)

6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational Procedure and Responsibilities)

จุดประสงค์และขอบเขต

เพื่อทำให้เกิดการปฏิบัติงานด้านระบบประมวลผลที่มีความปลอดภัยและถูกต้อง ควรกำหนดหน้าที่ความรับผิดชอบ และกระบวนการด้านการจัดการและปฏิบัติงานของระบบประมวลผลที่ชัดเจน ซึ่งหน้าที่ความรับผิดชอบที่กำหนดนี้ ควรพิจารณาถึงการแบ่งแยกหน้าที่ที่เหมาะสม นอกจากกระบวนการทำงานปกติแล้ว ควรมีการกำหนดขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์กระทบความปลอดภัยขึ้นในระบบประมวลผล เพื่อรองรับกับเหตุการณ์ดังกล่าว

เนื้อหานโยบาย

6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร

1) หน่วยงานที่ดูแลระบบ ต้องมีการจัดทำเอกสารขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบประมวลผล เช่น ระเบียบในการสำรองข้อมูล กระบวนการในการเปิด-ปิดระบบ กระบวนการซ่อมบำรุง เป็นต้น รวมถึงการจัดทำเอกสารขั้นตอนการปฏิบัติงานในกรณีที่เกิดความล้มเหลวหรือความผิดพลาดของระบบ เช่น ระเบียบปฏิบัติ ที่เกี่ยวข้องกับการกู้ระบบ (Recovery Procedure)
2) หัวหน้าหน่วยงานที่ดูแลระบบถือว่าเป็นเจ้าของเอกสารขั้นตอนการปฏิบัติงานดังกล่าว
3) เจ้าของเอกสารต้องปรับปรุงเอกสารดังกล่าวให้มีความถูกต้องเสมอ
4) เอกสารระเบียบปฏิบัติในการปฏิบัติงานด้านระบบข้อมูล ถือว่าเป็นเอกสารควบคุม การเปลี่ยนแปลงในเอกสารดังกล่าวต้องได้รับอนุญาตจากเจ้าของเอกสาร

6.1.2 การควบคุมการเปลี่ยนแปลงในการปฏิบัติงาน

1) ระบบประมวลผลและระบบเครือข่ายที่ใช้งานจริง จะต้องมีระเบียบปฏิบัติในการควบคุมการเปลี่ยนแปลง ของระบบ (Change Control Procedure)
2) เมื่อมีการดำเนินการเปลี่ยนแปลงในระบบ ผู้ดำเนินการเปลี่ยนแปลงจะต้องบันทึกรายละเอียดที่สำคัญของการเปลี่ยนแปลงดังกล่าว นอกจากนี้ รายละเอียดบันทึกการทำงาน (Audit Log) ในระหว่าง การเปลี่ยนแปลงซึ่งบันทึกโดยระบบ จะต้องมีการจัดเก็บเพื่อตรวจสอบภายหลัง
3) ก่อนดำเนินการเปลี่ยนแปลงในระบบ ต้องมีการทดสอบด้วยวิธีใดวิธีหนึ่งในระบบทดสอบ เพื่อให้แน่ใจว่าการเปลี่ยนแปลงนั้นๆ จะไม่ก่อให้เกิดความเสียหายต่อระบบ

4) หลังจากทำการเปลี่ยนแปลงแล้ว หน่วยงานที่ดูแลระบบต้องทำการทดสอบเพื่อยืนยันว่าระบบสามารถทำงานได้ปกติ
5) การขอเปลี่ยนแปลงในระบบสารสนเทศ ต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานเจ้าของระบบ

6.1.3 การแบ่งแยกระบบที่ใช้ในการพัฒนาออกจากระบบที่ใช้ในการปฏิบัติงาน

1) ในการพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) และระบบที่ใช้งานจริง (Production System)
2) ต้องจัดให้มีระเบียบปฏิบัติที่ชัดเจนในการโอนย้ายโปรแกรมที่พัฒนาเสร็จแล้ว ไปยังระบบที่ใช้งานจริง
3) ต้องไม่มีการติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาโปรแกรมอื่นๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง

6.2 การบริหารจัดการสำหรับการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management)

จุดประสงค์และขอบเขต

เพื่อจัดทำ และรักษาระดับความปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่ได้จัดทำไว้

เนื้อหานโยบาย

6.2.1 การให้บริการของหน่วยงานภายนอก

การให้บริการโดยหน่วยงานภายนอก ต้องระบุข้อตกลงในการจัดการความปลอดภัย รายละเอียดบริการ และรูปแบบของการบริหารจัดการ

6.2.2 การตรวจสอบการให้บริการของหน่วยงานภายนอก

1) ต้องมีการตรวจสอบการให้บริการจากหน่วยงานภายนอก ผู้ทำหน้าที่ตรวจสอบจำเป็นต้องมีความรู้ ความเข้าใจในเรื่องความปลอดภัยสารสนเทศ ตลอดจนเงื่อนไขและข้อตกลงต่าง ๆ
2) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการ เพื่อรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมายในกรณีที่จำเป็น

6.2.3 การบริหารจัดการการเปลี่ยนแปลงการให้บริการ

1) การเปลี่ยนแปลงการให้บริการ อาจพิจารณาเปลี่ยนแปลงอันเนื่องมาจากการปรับปรุงบริการ การแก้ไขหรือปรับปรุงนโยบายและการปฏิบัติ เพื่อแก้ไขเหตุการณ์และปรับปรุงด้านความปลอดภัย
2) การเปลี่ยนแปลงการให้บริการ อาจมีสาเหตุอันเนื่องมาจากการเปลี่ยนแปลงหรือปรับปรุงเครือข่าย การใช้เทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ การพัฒนาเครื่องมือและสภาพแวดล้อม การเปลี่ยนแปลงสถานที่ตั้งของพื้นที่การให้บริการ และการเปลี่ยนแปลงผู้ขาย

6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)

จุดประสงค์และขอบเขต

เพื่อลดความเสี่ยงในการเกิดความล้มเหลวของระบบ และให้มั่นใจได้ว่าระบบจะอยู่ในสถานะ พร้อมใช้งาน ควรมีการทดสอบระบบก่อนนำมาใช้งานจริง

เนื้อหานโยบาย

6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ

1) หน่วยงานผู้ดูแลระบบต้องตรวจทานความสามารถในการรองรับการทำงานของระบบ โดยการติดตามการใช้งานทรัพยากรของระบบอย่างต่อเนื่อง
2) ระบบใหม่ที่จะนำมาใช้งานจริง ต้องได้รับการทดสอบในเรื่องความสามารถในการรองรับการทำงาน ของระบบนั้นๆ ซึ่งควรมีประสิทธิภาพเทียบเท่าหรือเหนือกว่าความต้องการทางเทคนิคและความต้องการทางธุรกิจ

6.3.2 การตรวจรับระบบ

1) เจ้าของระบบงานธุรกิจ มีหน้าที่ในการกำหนดเกณฑ์ของการทดสอบที่มีความชัดเจนเพื่อรับรอง ความถูกต้องของระบบใหม่
2) ต้องมีการลงนามเห็นชอบในการรับรองความถูกต้องของโปรแกรมที่ทดสอบก่อนนำไปใช้งานจริง โดยเจ้าของระบบงานหลัก/หน่วยงานที่ร่วมทำการทดสอบ

6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against Malicious and Mobile Code)

จุดประสงค์และขอบเขต

เพื่อควบคุม และป้องกันซอฟต์แวร์ และข้อมูล จากโปรแกรมที่ไม่ประสงค์ดีและซอฟต์แวร์อันตราย

เนื้อหานโยบาย

6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี

1) ก่อนการนำซอฟต์แวร์ หรือข้อมูลจากภายนอกมาใช้งาน ต้องมีการตรวจสอบซอฟต์แวร์ หรือข้อมูลดังกล่าวให้แน่ใจว่าไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่
2) หน่วยงานผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ปเวอร์
3) หน่วยงานผู้ดูแลระบบ ต้องกำหนดให้โปรแกรมค้นหาไวรัสทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย
4) ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตต้องมีการตรวจหาไวรัสก่อนนำไปใช้งาน
5) ห้ามพนักงานดำเนินการใดๆ ที่เกี่ยวกับการพัฒนาไวรัส หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ
6) ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้นต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

6.5 การสำรองข้อมูล (Back-up)

จุดประสงค์และขอบเขต

เพื่อให้อุปกรณ์ประมวลผลสารสนเทศถูกต้องสมบูรณ์และพร้อมใช้งานเสมอ

เนื้อหานโยบาย

6.5.1 การสำรองข้อมูล

1) ข้อมูลทางธุรกิจที่สำคัญต้องมีการกำหนดระยะเวลาในการเก็บรักษาอย่างชัดเจน
2) จัดทำระเบียบปฏิบัติที่เป็นเอกสารในการสำรองและกู้คืนข้อมูล ในระบบงานที่สำคัญ
3) หน่วยงานผู้ดูแลระบบ ต้องทำการสำรองข้อมูลและเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูล
4) หน่วยงานผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยระบบหลักต้องมีการทดสอบอย่างน้อยปีละหนึ่งครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบ บนระบบทดสอบ
5) คอมพิวเตอร์ส่วนบุคคล ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลไฟล์ที่สำคัญ

6.6 การบริหารจัดการทางด้านความปลอดภัยสำหรับเครือข่าย (Network Security Management)

จุดประสงค์และขอบเขต

เพื่อทำให้ระบบเครือข่ายมีความปลอดภัย และสามารถใช้เป็นสื่อในการรับส่งข้อมูลต่าง ๆ ได้อย่างมีประสิทธิภาพ

เนื้อหานโยบาย

6.6.1 มาตรการเครือข่าย

หัวหน้าหน่วยงานควบคุมระบบเครือข่าย ต้องรับผิดชอบในการจัดให้มีการควบคุมการปฏิบัติการด้านเครือข่าย ดังต่อไปนี้

1) กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร (Network Configuration) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สายที่ใช้ในการสื่อสารของเครือข่ายทั้งหมดอย่างชัดเจน
2) จัดให้มีการควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่จัดไว้
3) มีมาตรการในการควบคุมดูแลสภาพและประเมินประสิทธิภาพการใช้งานของคู่สาย สายสื่อสารและอุปกรณ์ในเครือข่ายสื่อสาร เพื่อให้พร้อมใช้งานตลอดเวลา
4) บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ
5) ประเมินประสิทธิภาพของระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และวางแผนในการปรับปรุงระบบเครือข่ายให้สามารถรองรับปริมาณงานที่จะขยายตัวในอนาคต

6.6.2 ความปลอดภัยสำหรับบริการเครือข่าย

ผู้ให้บริการทางเครือข่าย ต้องได้รับการตรวจสอบ และวิเคราะห์ในเรื่องระดับการให้บริการ รูปแบบความปลอดภัยของเครือข่าย การจัดการความต้องการขององค์กร

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling)

จุดประสงค์และขอบเขต

เพื่อป้องกันความเสียหายต่อการดำเนินธุรกิจ อันเนื่องมาจากความเสียหายของสื่อบันทึกข้อมูลต่างๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม

6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

1) สื่อบันทึกข้อมูลต้องตั้งชื่อตามที่กำหนด และต้องมีทะเบียนควบคุมการใช้งาน
2) การเบิกและจ่ายสื่อบันทึกข้อมูลจะต้องผ่านการอนุมัติจากผู้มีอำนาจของหน่วยงานผู้ใช้
3) สื่อบันทึกข้อมูลต้องมีการตรวจนับอย่างน้อยปีละ 1 ครั้ง

4) การนำอุปกรณ์คอมพิวเตอร์ใดๆ ออกจากองค์กร ต้องได้รับอนุญาตอย่างเป็นทางการจากผู้บริหาร อุปกรณ์คอมพิวเตอร์ซึ่งบันทึกข้อมูลที่สำคัญต้องมีผู้รับผิดชอบและต้องมีการบันทึกการนำออกทุกครั้ง

6.7.2 การกำจัดสื่อบันทึกข้อมูล

1) ข้อมูลลำดับชั้นลับมากขึ้นไป ที่อยู่ในรูปเอกสารที่ต้องการทำลาย ต้องทำลายโดยการเข้าเครื่องย่อยกระดาษ เผาทำลาย หรือด้วยวิธีการอื่นที่จะไม่สามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้
2) การทำลายสื่อบันทึกข้อมูลที่บันทึกข้อมูลลำดับชั้นลับมากขึ้นไป ต้องได้รับการอนุมัติจากผู้มีอำนาจและต้องมีการบันทึกการทำลายทุกครั้ง เพื่อเป็นหลักฐานในการตรวจสอบในภายหน้า

6.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ

1) พนักงานทุกคน ต้องรับผิดชอบในการจัดการและป้องกันข้อมูลที่สำคัญอย่างเหมาะสมกับความสำคัญของข้อมูลตามมาตรฐานแนวทางการปกป้องข้อมูล
2) ต้องทำการควบคุมในการเข้าถึงทางกายภาพสำหรับอุปกรณ์เทปแม่เหล็ก แผ่นดิสก์ และสื่อบันทึกข้อมูลสำคัญต่างๆ โดยอนุญาตให้เฉพาะผู้ที่มีหน้าที่รับผิดชอบเท่านั้นที่มีสิทธิในการเข้าถึง และต้องมีการตรวจทานความเหมาะสมของรายชื่อผู้มีสิทธิเข้าถึงดังกล่าวอย่างสม่ำเสมอ

6.7.4 การสร้างความปลอดภัยสำหรับเอกสารระบบ

1) หน่วยงานผู้ดูแลระบบ ต้องจัดให้มีการปรับปรุงเอกสารระบบให้มีความทันสมัยและมีความพร้อมใช้อยู่เสมอ
2) เอกสารระบบที่สำคัญ จะต้องมีการจัดเก็บอย่างปลอดภัย รวมทั้งมีการควบคุมและป้องกันการเข้าถึงอย่างเหมาะสม ซึ่งผู้มีหน้าที่รับผิดชอบโดยตรงเท่านั้นที่มีสิทธิในการเข้าใช้เอกสารนั้น

7. นโยบายการควบคุมการเข้าถึง (Access Control Policy)

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement For Access Control)

จุดประสงค์และขอบเขต

เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็น และความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความปลอดภัย

เนื้อหานโยบาย

7.1.1 นโยบายการควบคุมการเข้าถึงระบบ

เจ้าของระบบงานธุรกิจ โดยความร่วมมือกับหน่วยงานด้านเทคโนโลยีสารสนเทศ ต้องจัดทำนโยบายและมาตรการควบคุมการเข้าใช้ระบบข้อมูลขององค์กรเป็นเอกสารชัดเจน และนโยบายนี้ ต้องสอดคล้องกับความต้องการทางธุรกิจ

7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

จุดประสงค์และขอบเขต

เพื่อป้องกันการเข้าใช้ระบบโดยไม่ได้รับอนุญาต ต้องมีวิธีการควบคุมสิทธิในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบเริ่มตั้งแต่การขอจดทะเบียนไปจนถึงการยกเลิกสิทธิในกรณีที่ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้อีกต่อไป รวมไปถึงการควบคุมสิทธิของผู้ใช้ซึ่งมีสิทธิพิเศษที่สามารถแก้ไขสิทธิต่างๆ ของระบบได้

เนื้อหานโยบาย

7.2.1 การลงทะเบียนผู้ใช้

1) ผู้ดูแลระบบโดยความเห็นชอบของเจ้าของระบบงานธุรกิจ ต้องจัดทำระเบียบปฏิบัติสำหรับการ ขอจดทะเบียนและการขอยกเลิกสิทธิในการเข้าใช้ระบบข้อมูลทุกระบบ
2) พนักงานทุกคนที่มีสิทธิเข้าใช้งานระบบข้อมูลต้องมีรหัสผู้ใช้เฉพาะบุคคลในการเข้าสู่ระบบ
3) รหัสผู้ใช้เป็นรหัสเฉพาะบุคคล โดยเป็นของผู้ที่ร้องขอเท่านั้น ในกรณีที่พนักงานลาออก รหัสผู้ใช้รายนั้น ต้องไม่ถูกนำกลับมาใช้ใหม่
4) ห้ามใช้งานรหัสผู้ใช้แบบกลุ่มหรือการใช้รหัสผู้ใช้ร่วมกัน (Shared User-ID) ในกรณีที่จำเป็นเจ้าของระบบงานธุรกิจจะต้องจัดทำการประเมินความเสี่ยงและหามาตรการควบคุมชดเชย เพื่อลดความเสี่ยงจากการใช้งานรหัสผู้ใช้ในลักษณะดังกล่าวให้อยู่ในระดับที่ยอมได้

5) ในการร้องขอเพื่อเข้าใช้งานระบบใดๆ ผู้บังคับบัญชาในหน่วยงานต้องทำการพิจารณาเพื่อเห็นชอบ การร้องขอเข้าใช้งานในระบบนั้นๆ ของพนักงานที่อยู่ภายใต้บังคับบัญชา โดยพิจารณาตามหน้าที่ ความรับผิดชอบของบุคคลนั้นๆ
6) ผู้ใช้ระบบขององค์กรทุกคนต้องลงนามรับทราบถึงกฎระเบียบ และเงื่อนไขในการใช้งานระบบขององค์กรและยินยอมปฏิบัติตามระเบียบการใช้งานของระบบนั้นๆ
7) หน่วยงานเจ้าของระบบงานธุรกิจมีหน้าที่สอบทานรหัสผู้ใช้ที่ไม่ได้ถูกใช้งานแล้ว หรือรหัสผู้ใช้ที่มีอยู่ซ้ำซ้อนกันในระบบอย่างสม่ำเสมอ ตลอดจนการดำเนินการยกเลิกรหัสผู้ใช้ดังกล่าว
8) หน่วยงานเจ้าของข้อมูล และหน่วยงานด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการร่วมกันในการถอดถอนสิทธิของผู้ใช้ ซึ่งไม่มีความต้องการใช้ระบบอีกต่อไปโดยทันที

7.2.2 การบริหารจัดการสิทธิในการใช้งานระบบ

1) การกำหนดสิทธิพิเศษใดๆ ให้กับผู้ใช้งานระบบต่างๆ (เช่น ผู้บริหารระบบปฏิบัติการ, ผู้บริหารฐานข้อมูลหรือโปรแกรมประยุกต์ หรือผู้ใช้ที่สามารถลบล้างการควบคุมโปรแกรมประยุกต์ เป็นต้น) ต้องกำหนดขึ้นอย่างเหมาะสมบนพื้นฐานของหน้าที่ความรับผิดชอบและความจำเป็นของงานเท่านั้น
2) ผู้ใช้งานซึ่งมีรหัสผู้ใช้ที่มีสิทธิพิเศษ ต้องมีรหัสผู้ใช้ส่วนตัวสำหรับการปฏิบัติงานปกติด้วย
3) หน่วยงานด้านเทคโนโลยีสารสนเทศ จะเป็นผู้พิจารณาในการอนุญาตให้หรือถอดถอนสิทธิพิเศษ ในระดับระบบปฏิบัติการ และหน่วยงานเจ้าของระบบงานธุรกิจจะเป็นผู้พิจารณาให้หรือถอดถอน สิทธิพิเศษสำหรับผู้ใช้ที่ร้องขอเข้าใช้ระบบนั้นๆ
4) หน่วยงานด้านเทคโนโลยีสารสนเทศ มีหน้าที่ตรวจสอบและเพิกถอนรหัสผู้ใช้ที่มีสิทธิพิเศษในระดับระบบปฏิบัติการ และหน่วยงานเจ้าของระบบงานธุรกิจมีหน้าที่ตรวจสอบและเพิกถอนรหัสผู้ใช้ที่มี สิทธิพิเศษในระดับแอพพลิเคชั่นซึ่งไม่ใช้งานแล้วหรือมีความซ้ำซ้อนกันอยู่ในระบบโดยถือเป็นหน้าที่ ที่ต้องปฏิบัติอย่างสม่ำเสมอ

7.2.3 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

1) หน่วยงานเจ้าของระบบงานธุรกิจ ต้องกำหนดความถี่ในการตรวจทานสิทธิการเข้าใช้งานของผู้ใช้ ในระบบซึ่งตนกำกับดูแล
2) หน่วยงานเจ้าของระบบงานธุรกิจ ต้องเพิกถอนสิทธิในการเข้าใช้งานของผู้ใช้ซึ่งไม่มีหน้าที่เกี่ยวข้อง อีกต่อไปออกจากระบบในทันที เพื่อป้องกันการลักลอบใช้งานโดยไม่ได้รับอนุญาต

7.3 หน้าที่ความรับผิดชอบของผู้ใช้ (User Responsibilities)

จุดประสงค์และขอบเขต

เพื่อมุ่งเน้นให้ผู้ใช้งานระบบมีความตระหนักถึงความปลอดภัยในการใช้งานระบบข้อมูล โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่าน และต้องทราบถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานคอมพิวเตอร์

เนื้อหานโยบาย

7.3.1 การใช้งานรหัสผ่าน

1) รหัสผ่านสำหรับการเข้าสู่ระบบถือเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสผู้ใช้ของตน ให้บุคคลอื่น
2) ผู้ใช้ต้องกำหนดและใช้รหัสผ่านที่มีความปลอดภัยและยากแก่การคาดเดา
3) ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตาม
4) ผู้ใช้ต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับทันทีที่เข้าระบบครั้งแรก เพื่อป้องกันบุคคลอื่นลักลอบใช้งาน
5) ผู้ใช้ต้องไม่เขียนรหัสผ่านบนสิ่งใดๆ เช่น กระดาษทด สมุดฉีก เป็นต้น
6) ผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำกับของเดิม หรือไม่ใช้วิธีเปลี่ยนตัวเลขต่อท้ายในรหัสผ่านเมื่อระบบบังคับ ให้เปลี่ยนรหัสผ่าน
7) ผู้ใช้ต้องตรวจสอบว่า สิทธิที่ตนได้รับในการเข้าใช้ระบบเหมาะสมกับหน้าที่ที่ตนรับผิดชอบหรือไม่ ถ้าพบว่าสิทธิที่ได้รับไม่เหมาะสม ต้องแจ้งผู้บังคับบัญชาให้รับทราบเพื่อพิจารณาและปรับเปลี่ยน ให้เหมาะสม

7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล

1) ผู้ใช้ที่ใช้งานระบบข้อมูลผ่านเครื่องคอมพิวเตอร์ หรือเครื่องปลายทาง (Terminal) หลังจากใช้งานเสร็จ ต้องออกจากระบบและปิดโปรแกรมทุกครั้ง
2) ผู้ใช้ควรออกจากระบบเครือข่าย (Log-off) ทันที เมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก
3) ผู้ใช้ควรติดตั้งโปรแกรมถนอมหน้าจอ (Screen Saver) ที่มีรหัสผ่านบนเครื่องคอมพิวเตอร์โดยโปรแกรมเหล่านี้จะเริ่มทำงานหลังจากไม่มีการใช้งานใดๆ บนเครื่องคอมพิวเตอร์นั้นๆ ตามเวลาที่กำหนดไว้
4) หากไม่มีการใช้งานเป็นเวลานาน ผู้ใช้ควรปิดเครื่องคอมพิวเตอร์หรือเครื่องปลายทางให้เรียบร้อย

7.3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

1) เอกสารและสื่อต่างๆ ที่ใช้สำหรับการทำงาน ควรจัดเก็บไว้ในตู้เก็บเอกสารที่สามารถล็อคได้ หลังจากการใช้งาน

2) พนักงานต้องล็อคหน้าจอ หรือใช้โปรแกรมถนอมหน้าจอพร้อมรหัสผ่านทุกครั้ง เมื่อไม่ได้ปฏิบัติงาน อยู่หน้าเครื่องคอมพิวเตอร์ เพื่อป้องกันมิให้ผู้อื่นลักลอบใช้งานเครื่องคอมพิวเตอร์ในเวลาดังกล่าว
3) ข้อมูลที่มีการเขียนไว้บนกระดานต้องลบทันทีหลักจากที่ไม่ได้ใช้งานแล้ว

7.4 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

จุดประสงค์และขอบเขต

เพื่อป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิเข้าใช้งานในระดับระบบปฏิบัติการ (Operating System) หน่วยงานด้านเทคโนโลยีสารสนเทศ ควรจัดให้มีการกำหนดข้อความเตือนก่อนการเข้าสู่ระบบ การตรวจสอบผู้ใช้และการบริหารรหัสผ่านสำหรับผู้ใช้งาน รวมถึงการควบคุมเวลาในการเชื่อมต่อสู่ระบบข้อมูล

เนื้อหานโยบาย

7.4.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างปลอดภัย

ผู้ดูแลระบบ ต้องจัดการให้ระบบแสดงข้อความเตือนถึง “การอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าใช้งาน” ก่อนที่จะทำการเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ขององค์กร และระบบต้องเปิดโอกาสให้ผู้ใช้สามารถยกเลิกการเชื่อมต่อเข้าสู่ระบบในกรณีที่ทราบว่าระบบนั้นๆ ไม่ได้เกี่ยวข้องกับตนเอง

7.4.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน

1) ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้ (User-ID) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้แต่ละคนได้
2) การอนุญาตให้ใช้รหัสผู้ใช้ร่วมกันหรือใช้รหัสผู้ใช้ “GUEST” ต้องขึ้นอยู่กับเหตุผลความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค ที่สำคัญต้องมีการควบคุมเพิ่มเติมเพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้แต่ละคนได้
3) รหัสผู้ใช้ทุกรหัสต้องมีรหัสผ่านและเจ้าของรหัสผู้ใช้เท่านั้นที่มีสิทธิทราบรหัสผ่าน

7.4.3 การหมดเวลาการใช้งานระบบสารสนเทศ (Session Time-out)

การเชื่อมต่อเข้าสู่ระบบจากเครื่องปลายทาง ถ้าพบว่าไม่มีการใช้งานระบบเป็นระยะเวลาที่กำหนด ระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

8. นโยบายการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance Policy)

8.1 ข้อกำหนดด้านความปลอดภัยระบบสารสนเทศ (System Requirements of Information System)

จุดประสงค์และขอบเขต

เพื่อให้มั่นใจได้ว่าการพัฒนาระบบงาน ได้คำนึงถึงความปลอดภัย และการควบคุมที่เพียงพอ องค์กร ต้องมีการกำหนดให้มีการพิจารณาถึงความต้องการด้านความปลอดภัยของระบบงาน ก่อนที่จะมีการพัฒนาระบบงาน รวมถึงการกำหนดให้มีควบคุมภายในของระบบงาน

เนื้อหานโยบาย

8.1.1 การวิเคราะห์และกำหนดความต้องการด้านความปลอดภัยสารสนเทศ

1) เจ้าของระบบงานธุรกิจ ต้องกำหนดความต้องการด้านความปลอดภัยสารสนเทศ ก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นเอกสาร ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน
2) หน่วยงานที่เกี่ยวข้องกับการพัฒนาระบบงาน ต้องปฏิบัติตามนโยบายและมาตรฐานต่างๆ ขององค์กร ในการพัฒนาระบบงาน

8.2 ข้อกำหนดด้านการประมวลผลในระบบสารสนเทศ (Correct Processing in Application)

จุดประสงค์และขอบเขต

เพื่อให้มั่นใจว่าระบบงานที่ได้รับการพัฒนา ได้คำนึงถึงการป้องกันความผิดพลาด โดยกำหนดให้ มีการควบคุมภายในระบบงาน เช่น การตรวจสอบความถูกต้องของข้อมูล ตั้งแต่ การนำข้อมูลเข้าสู่ระบบ การประมวลผล จนกระทั่งการตรวจสอบผลลัพธ์ที่ได้จากระบบ เป็นต้น

เนื้อหานโยบาย

8.2.1 การตรวจสอบข้อมูลนำเข้า

โปรแกรมระบบงานที่มีการป้อนข้อมูลเข้าสู่ระบบ จะต้องมีการตรวจสอบความถูกต้องของข้อมูลที่ได้รับจากการป้อนข้อมูล ก่อนที่จะนำข้อมูลนั้นไปประมวลผลต่อ

8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล

1) ระบบประมวลผล ต้องออกแบบให้มีความสามารถในการสอบทาน เพื่อตรวจจับกรณีประมวลผลข้อมูล มีความผิดพลาดหรือเสียหาย

2) ระบบประมวลผล ต้องออกแบบให้มีความสามารถแจ้งถึงความผิดพลาดต่าง ๆ จากการประมวลผล เช่น ข้อความแจ้งเมื่อระบบขัดข้อง เป็นต้น

8.2.3 การตรวจสอบข้อมูลผลลัพธ์

1) กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อให้มั่นใจว่า ข้อมูลมีความถูกต้องสมบูรณ์ ทั้งนี้ การตรวจสอบควรครอบคลุมถึง
   1.1) การตรวจสอบถึงความผิดพลาดต่าง ๆ ของรายงาน เช่น จำนวนเงินติดลบ เป็นต้น
   1.2) กำหนดให้มีระเบียบปฏิบัติในการทดสอบข้อมูลผลลัพธ์
2) ในการประมวลผลที่สำคัญ ต้องกำหนดให้มีระเบียบปฏิบัติในกรณีที่ตรวจพบข้อผิดพลาดของข้อมูลผลลัพธ์ รวมถึงกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการข้อมูลผลลัพธ์ไปใช้

8.3 มาตราการในการเข้ารหัสข้อมูล (Cryptographic Controls)

จุดประสงค์และขอบเขต

เพื่อรักษาความปลอดภัยของข้อมูลทั้งในด้านความลับและความถูกต้องของข้อมูล จำเป็นต้องพิจารณาถึงการนำซอฟต์แวร์และเทคนิคต่าง ๆ มาให้ในการเข้ารหัสข้อมูลที่มีความเสี่ยง

เนื้อหานโยบาย

8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล

1) กำหนดให้มีระเบียบปฏิบัติในเรื่องการใช้การเข้ารหัส รวมถึงซอฟต์แวร์และมาตรฐานวิธีการเข้ารหัส ที่อนุญาตให้ใช้งานสำหรับข้อมูลในลำดับชั้นต่าง ๆ
2) ต้องมีการปรับปรุงรายชื่อซอฟต์แวร์และมาตรฐานในด้านการเข้ารหัสให้ทันสมัยอยู่เสมอ
3) ต้องมีการพิจารณาถึงลำดับชั้นของข้อมูลและแนวทางในการจัดการข้อมูลในลำดับชั้นดังกล่าว ประกอบการพิจารณาในการใช้งานการเข้ารหัส

8.4 การสร้างความปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of System Files)

จุดประสงค์และขอบเขต

เพื่อรักษาความถูกต้องของโปรแกรม และความปลอดภัยข้อมูลในระบบงานที่ใช้จริง องค์กรจำเป็นต้องมีการควบคุมและจัดการสำหรับการเข้าถึงข้อมูลและซอฟต์แวร์ต่าง ๆ ที่เกี่ยวเนื่องกับระบบงานที่ใช้จริง เช่น Source Code และข้อมูลที่ใช้ในการทดสอบ ในการรักษาความปลอดภัยนี้ถือเป็นหน้าที่และความรับผิดชอบ ของผู้ใช้งานและเจ้าหน้าที่พัฒนาระบบงานที่มีส่วนเกี่ยวข้องในการใช้ระบบงานข้อมูลนั้น

เนื้อหานโยบาย

8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการหรือระบบที่ใช้งานจริง

1) ก่อนมีการปรับปรุงเวอร์ชั่นใหม่ในระบบใช้งานจริงจะต้องได้รับเอกสารการอนุมัติการใช้โปรแกรม เวอร์ชั่นใหม่ และหลักฐานประกอบอื่น ๆ เช่น รายงานผลการทดสอบเพื่อการรับรองความถูกต้อง จากผู้ใช้งาน เป็นต้น และต้องปรับเปลี่ยน Source Code ในสมุดทะเบียน (Library) ให้สอดคล้องกัน
2) ไม่จัดเก็บ Source Code ของโปรแกรมไว้ในระบบใช้งานจริง
3) ต้องจัดเก็บรายการบันทึกเพื่อการตรวจสอบต่าง ๆ ของการแก้ไข Source Code และโปรแกรม
4) ต้องมีการสำรองและจัดเก็บโปรแกรมเวอร์ชั่นก่อนการแก้ไข เพื่อนำกลับมาใช้เมื่อมีความจำเป็น
5) เจ้าหน้าที่ผู้ดูแลสมุดทะเบียน (Library) ที่ได้รับการอนุญาตจากผู้บริหารแล้วเท่านั้น จะเป็นผู้ดำเนินการปรับปรุงซอฟต์แวร์ที่อยู่ในระบบใช้งานจริงเฉพาะส่วนที่ตนเองรับผิดชอบ

8.4.2 การป้องกันข้อมูลที่ใช้สำหรับทดสอบระบบ

ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงไปใช้เพื่อการทดสอบระบบงานที่พัฒนาใหม่ ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง โดยการควบคุมต่าง ๆ ต้องประกอบด้วย

1) ได้รับอนุญาตก่อนการนำสำเนาข้อมูลจริงไปใช้ในระบบงานทดสอบในแต่ละครั้ง
2) มีการควบคุมในการเข้าถึงข้อมูลที่ใช้ในการทดสอบระบบ
3) มีการดัดแปลงข้อมูลจริงบางส่วนก่อนนำมาใช้ในการทดสอบ
4) ทำการลบข้อมูลทดสอบออกจากระบบทันทีเมื่อเสร็จสิ้นการทดสอบ
5) มีการจัดเก็บบันทึกการทำรายการในระบบ (Audit Log) เพื่อตรวจสอบกิจกรรมการทดสอบ

8.4.3 การควบคุมการเข้าถึง Source Code ของโปรแกรม

1) แต่งตั้งเจ้าหน้าที่ผู้ดูแลสมุดทะเบียน (Library) ที่เก็บ Source Code ของแต่ละระบบในความรับผิดชอบ
2) ต้องมีการจำกัดสิทธิในการเข้าถึง Library ที่เก็บ Source Code ของโปรแกรม ซึ่งรวมถึงสิทธิในการเข้าถึงของเจ้าหน้าที่หน่วยงานด้านเทคโนโลยีสารสนเทศด้วย
3) การอัพเดท Source Code ของโปรแกรมใน Library และการนำ Source Code ของโปรแกรมให้กับผู้พัฒนาระบบ จะต้องดำเนินการโดยเจ้าหน้าที่ผู้ดูแล Library ที่ได้รับมอบหมายในแต่ละระบบ
4) ต้องมีการจัดเก็บบันทึกการทำรายการในระบบ (Audit Log) เพื่อตรวจสอบการเข้าถึง Library ต่างๆ

5) บันทึกรายละเอียดโปรแกรมเวอร์ชั่นเก่าที่จะทำการจัดเก็บอย่างชัดเจน โดยมีรายละเอียดต่างๆ เช่น วัน-เดือน-ปี ที่โปรแกรมเวอร์ชั่นนี้ได้ใช้งานอยู่ในระบบใช้งานจริง ซอฟต์แวร์ต่างๆ ที่ทำงานรวมกัน กับโปรแกรมนี้ เป็นต้น

8.5 การสร้างความปลอดภัยสำหรับกระบวนการพัฒนาระบบและการสนับสนุน (Security in Development and Support Process)

จุดประสงค์และขอบเขต

เพื่อควบคุมความปลอดภัยของระบบงานที่พัฒนาเองหรือจากหน่วยงานภายนอก โดยมีการควบคุม เริ่มตั้งแต่การพัฒนา การทดสอบ การนำไปใช้งานจริง และการปรับปรุงแก้ไขในภายหลัง

เนื้อหานโยบาย

8.5.1 ขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ

1) การปรับปรุงแก้ไขระบบงานหรือโปรแกรมต่าง ๆ ต้องปฏิบัติตามระเบียบว่าด้วยเรื่องการปรับปรุงแก้ไขระบบงานหรือโปรแกรม
2) การปรับปรุงการแก้ไขระบบงานต่าง ๆ ต้องจัดทำเป็นเอกสารและสามารถติดตามสถานะได้ รวมถึงต้องมีเอกสารสนับสนุน เช่น แผนการทดสอบการปรับปรุงแก้ไขโปรแกรมระบบ และผลการทดสอบ เป็นต้น
3) การปรับปรุงแก้ไขระบบงานควรพิจารณาถึง
    3.1) การอนุมัติโดยหน่วยงานเจ้าของระบบงาน
    3.2) การระบุถึงเครื่องคอมพิวเตอร์ ซอฟท์แวร์ ฐานข้อมูล ที่จะต้องเปลี่ยนแปลง
    3.3) การป้องกันผลกระทบที่อาจเกิดขึ้นกับการทำงาน
    3.4) การสำรองข้อมูลก่อนการปรับปรุงหรือบำรุงรักษาระบบ
    3.5) การจัดทำเอกสารประกอบการเปลี่ยนแปลงให้ทันสมัย
    3.6) การควบคุมเวอร์ชั่นที่เปลี่ยนแปลง
    3.7) การจัดเก็บบันทึกเพื่อการตรวจสอบการแก้ไข
4) การปรับปรุงแก้ไขระบบต้องจัดทำเป็นหนังสือขออนุมัติหรือแก้ไขระบบงานหรือโปรแกรม

9. นโยบายการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ (Information Security Incident Management Policy)

9.1 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวกับความปลอดภัย (Management of Information Security Incidents and Improvements)

จุดประสงค์และขอบเขต

เพื่อให้มีวิธีการที่สอดคล้อง และได้ผลในการบริหารจัดการเหตุการณ์ ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

เนื้อหานโยบาย

9.1.1 การจัดการเหตุการณ์ที่มีผลกระทบต่อความปลอดภัยของข้อมูล

การจัดการเหตุการณ์ที่มีผลกระทบต่อความปลอดภัยสารสนเทศควรพิจารณาถึงแนวทาง ดังต่อไปนี้

1) มีการรายงานเหตุการณ์ไปยังหน่วยงานที่รับผิดชอบที่ได้กำหนดไว้ เช่น หน่วยงานความปลอดภัยสารสนเทศ
2) จำแนกลักษณะของเหตุการณ์ เช่น ความเสียหายของอุปกรณ์ ความผิดพลาดของผู้ใช้งานหรือผู้ปฏิบัติงาน การลักลอบเข้าใช้งาน การโจมตีระบบจากภายในหรือภายนอก และประเมินลำดับความสำคัญตามความเร่งด่วน ซึ่งสามารถแบ่งได้ 3 ระดับ ดังนี้
   2.1) การเตือนภัยระดับสูง ได้แก่ เหตุการณ์ที่สามารถส่งผลเสียอย่างรุนแรงต่อองค์กร และต้องได้รับการแก้ไขโดยทันที ซึ่งรวมถึงความเสียหายต่ออุปกรณ์บนเครือข่ายที่เชื่อมต่ออุปกรณ์ดังกล่าว
   2.2) การเตือนภัยระดับปานกลาง ได้แก่ เหตุการณ์ที่จะก่อให้เกิดความเสียหายคุกคามต่อความปลอดภัยขององค์กรในอนาคต แต่ยังไม่แสดงผลเสียหายรุนแรงในขณะนั้น ซึ่งอาจไม่จำเป็น ที่ต้องทำการแก้ไขโดยทันที ทั้งนี้ ขึ้นอยู่กับสถานการณ์ว่ามีความจำเป็นที่ต้องเร่งแก้ไขเพียงใด
   2.3) การเตือนภัยระดับต่ำ ได้แก่ เหตุการณ์ที่ก่อให้เกิดความเสียหายขัดข้องเล็กน้อย ไม่ส่งผลกระทบ คุกคามต่อการทำงานขององค์กร การเตือนภัยประเภทนี้ ถือว่าเป็นการรายงานข้อมูลให้ทราบในเบื้องต้น ซึ่งอาจทำการแก้ไขในภายหลังได้
3) กำหนดขั้นตอนในการจัดการเหตุการณ์ดังกล่าว โดยคำนึงถึงลำดับความสำคัญตามความเร่งด่วน และความรุนแรงของเหตุการณ์ โดยขั้นตอนประกอบด้วย
   3.1) การตรวจสอบหาสาเหตุของปัญหา
   3.2) แผนงานในการลดผลกระทบ
   3.3) ขั้นตอนในการแก้ไข
   3.4) การสื่อสารกับผู้ใช้งานที่เกี่ยวข้อง

3.5) การทำเอกสารบันทึกการดำเนินการในเหตุการณ์ดังกล่าว

4) จัดทำรูปแบบของเหตุการณ์และการวิเคราะห์ถึงต้นเหตุปัญหาเพื่อหามาตรการในการลดการเกิดปัญหาดังกล่าว รวมทั้งปรับปรุงการจัดการเพื่อลดผลกระทบที่มีประสิทธิภาพมากขึ้นในกรณีที่เกิดปัญหาขึ้น ในอนาคต

10. นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy)

10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินธุรกิจ (Information Security Aspects of Business Continuity Management)

จุดประสงค์และขอบเขต

เพื่อป้องกันและรับมือกับการหยุดชะงักของการดำเนินธุรกิจ อันเนื่องมาจากภัยคุกคามต่อการทำงานของระบบไม่ว่าจะด้วยอุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหาย ต่อองค์กรไม่มากก็น้อย ดังนั้นจึงควรจัดทำแผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ เพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักขององค์กรต่อไปได้

เนื้อหานโยบาย

10.1.1 กระบวนการในการสร้างความต่อเนื่องในการดำเนินธุรกิจ

ผู้บริหารหรือหน่วยงานที่เกี่ยวข้องต้องมีการจัดการกระบวนการต่างๆ เพื่อพัฒนาและคงไว้ซึ่งความต่อเนื่องทางธุรกิจ การจัดการกระบวนการต่างๆ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจดังกล่าว ต้องคำนึงถึง สิ่งต่างๆ ดังต่อไปนี้

1) การวิเคราะห์และการประเมินความเสี่ยงที่กระทบต่อการดำเนินธุรกิจขององค์กร
2) การจัดทำเอกสารกลยุทธ์เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ ต้องสอดคล้องกับเป้าหมายทางธุรกิจ ขององค์กร
3) การพัฒนาแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่สอดคล้องกับกลยุทธ์ขององค์กร
4) การฝึกอบรมพนักงาน เพื่อให้ตระหนักถึงความมั่นคงปลอดภัย และเข้าใจในแผนฯ พร้อมทั้งสามารถปฏิบัติตามแผนฯ ได้ ในกรณีเกิดเหตุการณ์ฉุกเฉินต่างๆ
5) การทดสอบ การตรวจทานและปรับปรุงแผนและกระบวนการต่างๆ เพื่อก่อให้เกิดความต่อเนื่องในการดำเนินธุรกิจให้มีความทันสมัยอยู่เสมอ
6) การกำหนดหน้าที่ความรับผิดชอบในการประสานงาน การพัฒนา การตรวจทาน การปรับปรุง และการนำแผนไปปฏิบัติเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจอย่างชัดเจน
7) การประเมินและหาแนวทางที่ใช้ในการลดหรือโอนความเสี่ยงอื่น เช่น การทำประกันให้ครอบคลุมผลเสียหายที่อาจเกิดขึ้น เป็นต้น

10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องในการดำเนินธุรกิจ

พื้นฐานของการจัดการเพื่อให้เกิดความต่อเนื่องในการดำเนินธุรกิจ คือ เข้าใจถึงกระบวนการ และเหตุการณ์ที่สามารถก่อให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจ ดังนั้น หน่วยงานเจ้าของกระบวนการรวมถึงหน่วยงานเจ้าของระบบงานธุรกิจที่สนับสนุนกระบวนการธุรกิจนั้น ต้องเข้าร่วมในการดำเนินการ ระบุเหตุการณ์ที่

อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ตลอดจนการประเมินความเสี่ยง เพื่อให้ได้มา ซึ่งข้อมูลที่มีความถูกต้องและครบถ้วนในการดำเนินการจัดทำแผนบริหารจัดการความต่อเนื่องทางธุรกิจในการดำเนินธุรกิจลำดับต่อไป

10.1.3 การจัดทำและใช้งานแผนความต่อเนื่องในการดำเนินธุรกิจ

1) สร้างโครงร่างสำหรับแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจสำหรับทุกหน่วยงาน และต้องมีรูปแบบของแผนฯ รวมถึงสื่อให้กับเจ้าของแผนฯ ของแต่ละหน่วยงานทราบในการจัดทำ เพื่อความสอดคล้องกันของแต่ละหน่วยงาน
2) แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่างๆ ต้องถูกจัดทำเพื่อให้มั่นใจได้ว่าสามารถทำให้กระบวนการทางธุรกิจ ดำเนินการต่อได้ภายในระยะเวลาที่กำหนดหลังจากที่มีการหยุดชะงักของการให้บริการ หรือหลังประสบภัยต่างๆ
3) ต้องกำหนดเจ้าของแผนงานและแนวทางปฏิบัติซึ่งเจ้าของแผนฯ ต้องรับผิดชอบในการบำรุงรักษา และทดสอบ พัฒนาหลักเกณฑ์ความต้องการและเงื่อนไขสำหรับการนำแผนฯ ไปใช้
4) แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจทุกแผน จะต้องได้รับการอนุมัติจากผู้บริหารขององค์กร ก่อนนำไปปฏิบัติ

10.1.4 การทดสอบ ปรับเปลี่ยนและปรับปรุงแผนเพื่อก่อให้เกิดความต่อเนื่อง

เจ้าของแผนฯ มีหน้าที่ปรับปรุงแผนฯ และต้องจัดให้มีการทดสอบแผนฯ อย่างสม่ำเสมอ เพื่อทำให้มั่นใจได้ว่าเมื่อเกิดเหตุการณ์ที่กระทบต่อกระบวนการทางธุรกิจ องค์กรสามารถใช้แผนฯ และดำเนินการ ตามแผนฯ ได้ในทางปฏิบัติที่สามารถรับมือและลดระดับความเสียหายที่จะเกิดขึ้น รวมทั้งสามารถกู้ระบบสำคัญ กลับคืนมาได้อย่างทันท่วงที โดยทำการทดสอบอย่างน้อยปีละ 2 ครั้งเพื่อเป็นการป้องกันและเตรียมความพร้อมในภาวะฉุกเฉิน