บริษัท เจริญอุตสาหกรรม จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

chin huay	นโยบายเรื่อง : นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	เลขที่	
		วันที่เริ่มใช้	26 กุมภาพันธ์ 2565
	อนุมัติโดย : มติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 2/2565 วันที่ 25 กุมภาพันธ์ 2565	ฉบับที่	REV 1

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้บริษัท เจริญอุตสาหกรรม จำกัด (มหาชน) และบริษัทในเครือ หรือต่อไปนี้เรียกว่า "บริษัท" สามารถใช้สารสนเทศและระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่เหมาะสม หรือถูกคุกคามจากภัยต่างๆ ซึ่งจะช่วยลดความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน และบุคลากร

บริษัทฯ จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยให้มีนโยบาย (Policy) ข้อกำหนด (Standard) และขั้นตอนปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นลายลักษณ์อักษร โดยสอดคล้องตามกฎหมาย มาตรฐานและแนวปฏิบัติสากล ของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

I. วัตถุประสงค์

1. เพื่อกำหนดและประกาศนโยบาย แนวทางปฏิบัติ ข้อกำหนด และขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับบริษัทฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติตามอย่างเหมาะสม
2. เพื่อให้เกิดความเชื่อมั่นในความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ ว่า สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีความพร้อมใช้งาน (Availability)
3. เพื่อเผยแพร่ให้เจ้าหน้าที่และผู้ใช้งานสารสนเทศของบริษัทฯ ได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

II. คำจำกัดความ

คำศัพท์	คำนิยาม
บริษัท	บริษัท เจริญอุตสาหกรรม จำกัด (มหาชน) และ บริษัทในเครือ
คณะกรรมการบริษัท	คณะกรรมการของบริษัท เจริญอุตสาหกรรม จำกัด
ฝ่ายบริหาร	กรรมการผู้จัดการและผู้อำนวยการฝ่ายต่าง ๆ ของบริษัท
นโยบาย ฯ	นโยบายเทคโนโลยีสารสนเทศ
หน่วยงานเทคโนโลยีสารสนเทศ	หน่วยงานตามโครงสร้างของบริษัทที่มีหน้าที่รับผิดชอบงานด้านเทคโนโลยี สารสนเทศ
ผู้ใช้งาน	พนักงานประจำ พนักงานตามสัญญาจ้าง ผู้ให้บริการภายนอก คู่ค้าหรือลูกค้า
ผู้ให้บริการภายนอก	บุคคลจากภายนอกองค์กรซึ่งผู้ประกอบธุรกิจ ว่าจ้างเพื่อใช้บริการที่เกี่ยวข้อง กับระบบสารสนเทศ
ระบบเทคโนโลยีสารสนเทศ	ระบบคอมพิวเตอร์ที่หน่วยงานเทคโนโลยีสารสนเทศให้บริการ
ทรัพย์สินสารสนเทศ	1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ 2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูล อิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ 4) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดการพัฒนา หรือ สิทธิ์ในการใช้จากเจ้าของผลิตภัณฑ์

III. บทบาทหน้าที่และความรับผิดชอบ

1. คณะกรรมการบริษัท

1. กำหนดนโยบายเทคโนโลยีสารสนเทศของบริษัท
2. กำกับดูแลให้ฝ่ายบริหารปฏิบัติตามนโยบายฯ ให้สอดคล้องกับความต้องการของบริษัท
3. พิจารณาสนับสนุนการจัดหาทรัพย์สินต่างๆ เพื่อให้การบริหารจัดการและให้บริการระบบสารสนเทศมีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายตามประกาศฉบับนี้

2. **ฝ่ายบริหาร**
    1. กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบาย ฯ
    2. ติดตามควบคุมและกำกับดูแลให้หน่วยงานที่เกี่ยวข้องดำเนินการตามนโยบายฯที่กำหนด

3. **หน่วยงานเทคโนโลยีสารสนเทศ**
    1. ติดตามดูแลให้ผู้ใช้งานปฏิบัติตามนโยบายฯ หลักเกณฑ์ระเบียบปฏิบัติของบริษัทที่เกี่ยวข้องอย่าง ถูกต้องเหมาะสม และหากมีการปฏิบัติที่ไม่ถูกต้องให้รายงานต่อฝ่ายบริหารทราบ
    2. สื่อสารนโยบายฯ ให้แก่ผู้ใช้งาน ผู้ประกอบการธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามรถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง
    3. จัดสรร โอนย้าย หรือจัดซื้อทรัพย์สินสารสนเทศตามตำแหน่งความรับผิดชอบ
    4. ทำทะเบียนควบคุมทรัพย์สินสารสนเทศ และจัดทำสำเนาเอกสารที่เกี่ยวข้องแยกเก็บเพื่อสะดวกต่อการ ตรวจสอบ เช่น ใบกำกับภาษี สำหรับเครื่องคอมพิวเตอร์ อุปกรณ์ ลิขสิทธิ์ (License)

4. **ฝ่ายบุคคล**
    1. ประกาศ และรับพนักงานตามนโยบาย
    2. แจ้งผู้ดูแลระบบ เพื่อจัดเตรียมทรัพย์สินสารสนเทศให้เหมาะสมและเพียงพอตามนโยบาย
    3. แจ้งให้ผู้ดูแลระบบ กรณีพนักงานมีการลาออก โอนย้ายหน่วยงาน

5. **ฝ่ายจัดซื้อ** จัดซื้อทรัพย์สินสารสนเทศตามความต้องการ
6. **ฝ่ายบัญชี/การเงิน** ทำการขึ้นทะเบียนทรัพย์สินสารสนเทศ

IV. แนวทางปฏิบัติ

1. การจัดทำนโยบาย จัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษรและผู้บริหาร เจ้าหน้าที่ฝ่ายเทคโนโลยีและสารสนเทศ และผู้ใช้งานของแต่ละฝ่ายงานต้องมีส่วนร่วมในการจัดทำนโยบาย และอย่างน้อยต้องได้รับอนุมัติจากคณะกรรมการบริหาร
2. ทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ
3. จัดเก็บนโยบายที่เป็นลายลักษณ์อักษรไว้ที่ระบบ Intranet ของบริษัท หรือ ติดประกาศเพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้อง สามารถเข้าถึงได้โดยง่าย

V. องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีดังนี้

1. นโยบายย่อยการควบคุมการเข้าถึงสารสนเทศ (Access control)

วัตถุประสงค์

เพื่อมีการควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศ เพื่อกำหนดมาตรการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต ป้องกันการบุกรุกทั้งด้านกายภาพ ผ่านระบบเครือข่าย และจากโปรแกรม ที่จะสร้างความเสียหายแก่ข้อมูลหรือทำให้ระบบหยุดชะงัก และสามารถตรวจสอบติดตามการพิสูจน์ตัวบุคคลที่ใช้งานข้อมูลหรือระบบสารสนเทศขององค์การได้อย่างถูกต้อง

โดยมีการแบ่งการควบคุมการเข้าถึง Access Control ออกเป็นดังต่อไปนี้

6.1 ส่วนของการบริหารจัดการการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการบริหารจัดการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศ โดยต้องมีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ทั้งนี้เพื่อให้เกิดความมั่นคงปลอดภัยต่อข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท

ขอบเขต

1. จัดให้มีการอบรมการใช้งานระบบเทคโนโลยีสารสนเทศ ให้กับผู้ใช้งานใหม่ โดยร่วมกับทางฝ่ายทรัพยากรบุคคล ผ่านการอบรมปฐมนิเทศพนักงานพนักงานหรืออบรมพิเศษตามความเหมาะสม
2. การลงทะเบียนผู้ใช้งาน (User Registration)
    1) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน โดยต้องระบุข้อมูลพื้นฐานเป็นอย่างน้อย ดังนี้ ชื่อและนามสกุล
    2) ตำแหน่ง หน่วยงาน ระยะเวลาในการใช้งาน
    3) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
3. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) กำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่ และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร
4. ต้องให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น กรณีมีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การแบ่งปันแฟ้มข้อมูล (Share Files)
5. กรณีผู้ดูแลระบบมีความจำเป็นต้องให้สิทธิ์เพิ่มเป็นกรณีพิเศษ ต้องได้รับการอนุมัติจากผู้บริหาร และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยต้องดำเนินการอย่างน้อย ดังนี้
    1) ควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

2) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6. ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานดังนี้
   1) ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง
   2) ทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน
   3) ตรวจสอบสิทธิ์และติดตามการใช้งานตามสิทธิ์ที่ได้รับของแต่ละระบบ
7. ตัดผู้ใช้งานออกจากทะเบียนโดยปฏิบัติตามขั้นตอนปฏิบัติของการตัดผู้ใช้งาน เมื่อมีการเพิกถอนสิทธิ์ตามกรณีต่อไปนี้
   1) สิ้นสุดหน้าที่ตามงานที่รับผิดชอบ เช่น การโอนย้ายงาน การลาออก
   2) ผู้บังคับบัญชาแจ้งเป็นลายลักษณ์อักษรว่าให้เพิกถอนสิทธิ์

6.2 ส่วนของการใช้งานรหัสผ่าน (User Password Management and Password)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและผู้ดูแลระบบได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการบริหารจัดการและการใช้งานรหัสผ่าน สร้างความมั่นคงปลอดภัยจากบุคคลและซอฟต์แวร์ที่ไม่ประสงค์ดีที่ไม่ได้รับอนุญาตเข้ามาล่วงรู้รหัสผ่าน อันส่งผลกระทบต่อความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของบริษัท

ขอบเขต

1. กำหนดขั้นตอนปฏิบัติ สำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
2. เปลี่ยนรหัสผ่านโดยทันทีภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น
3. ต้องเก็บรหัสผ่านไว้เป็นความลับ และไม่ใช้รหัสผ่านร่วมกับผู้อื่น
4. กำหนดรหัสผ่านที่มีคุณภาพ โดยให้สอดคล้องกับข้อกำหนดเรื่องการตั้งและเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยของบริษัท
5. เปลี่ยนรหัสผ่านทุกครั้ง ในทันทีที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้
6. กรณีมีความจำเป็นต้องยกเว้นตาม password policy ต้องขออนุมัติยกเว้น (exception to policy) ก่อน

6.3 ส่วนของการยืนยันตัวบุคคล (User Identification and Authentication)

วัตถุประสงค์

เพื่อให้สามารถระบุตัวตนในการใช้งานระบบสารสนเทศ โดยผู้ใช้งานต้องมี ชื่อบัญชีผู้ใช้งาน (User account) และ รหัสผ่าน (Password) ที่บริษัทเป็นผู้กำหนดให้เท่านั้น จึงจะสามารถใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทได้

ขอบเขต

1. กำหนดการควบคุมบุคคลที่มีสิทธิ์เข้าสู่ระบบสารสนเทศของบริษัท และสามารถระบุให้บุคคลนั้นกระทำการใดในระบบสารสนเทศใดได้บ้าง รวมถึงการอนุญาตให้ใช้สารสนเทศตามระดับชั้นความลับและจัดเก็บข้อมูลการใช้งานระบบของบุคคลนั้น
2. กำหนดให้ผู้ใช้งานที่เป็นเจ้าของชื่อบัญชีผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น โดยไม่ได้เกิดจากความประมาทเลินเล่อของผู้ใช้งาน
3. กำหนดให้ผู้ใช้งานต้องเก็บรักษารหัสผ่านของบัญชีผู้ใช้งาน ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น
4. กำหนดให้ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

6.4 ส่วนของการเข้าถึงระบบเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของการเชื่อมต่อทางเครือข่าย ควบคุมการเชื่อมต่อทางเครือข่าย และป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท

ขอบเขต

1. การใช้บริการเครือข่าย
    1) มีการกำหนดระบบสารสนเทศที่ต้องควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้ใช้งานได้
    2) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น
    3) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ฯลฯ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวปีละ 1 ครั้ง
2. การแบ่งแยกเครือข่าย (Segregation in Network)
    1) จัดทำแผนผังระบบเครือข่าย (Network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
    2) กำหนดให้มีการจัดแบ่งเครือข่ายภายในองค์กรออกเป็นเครือข่ายภายใน และภายนอก
    3) กำหนดมาตรการความมั่นคงปลอดภัยที่เหมาะสมกับเครือข่ายเหล่านั้น เช่นใช้ Firewall กั้นและป้องกันเครือข่ายย่อยเหล่านั้นจากการถูกบุกรุก หรือเข้าถึงโดยไม่ได้รับอนุญาต
    4) กำหนดให้มีการใช้เกตเวย์เช่น ไฟร์วอลล์เพื่อกั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

กรองหรือจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อยเหล่านั้น และควบคุมการเข้าถึงเครือข่ายภายในโดยไม่ได้รับอนุญาต

3. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)
   1) มีการตรวจสอบการเชื่อมต่อเครือข่าย
   2) จำกัดสิทธิ์ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย
   3) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย
4. การควบคุมการจัดเส้นทางเครือข่าย (Network Routing Control) มีการควบคุมดังนี้
   1) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย
   2) ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ต้องปิด (Port) หรือการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical disconnect) และจุดเชื่อมต่อ (Disable port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง

6.5 ส่วนของการควบคุมการเข้าถึง (Logical Access Control)

วัตถุประสงค์

เพื่อให้การบริหารจัดการบัญชีและสิทธิ์ของผู้ใช้งานมีประสิทธิภาพเป็นไปตามหลักความจำเป็นของการใช้งาน และสอดคล้องกับหลักการแบ่งแยกงาน IT ที่ดี โดยสามารถป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ขอบเขต

1. มีการแบ่งแยกหน้าที่ในการทำงานของผู้มีหน้าที่ดูแลระบบงานประมวลผลหลักตามความเหมาะสม เพื่อไม่ให้ บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ โดยอย่างน้อยต้องครอบคลุมการ
   1) แบ่งแยกบุคคลากรที่มีหน้าที่พัฒนาระบบงาน (Developer) ออกจากผู้ดูแลระบบ (System Administrator) และผู้ดูแลระบบฐานข้อมูล(Database Administrator)
   2) แบ่งแยก System Administrator ออกจาก Computer Operator
   3) แบ่งแยกบุคคลากรที่มีหน้าที่พัฒนาระบบงาน (Developer) ออกจาก คนที่ได้สิทธิ์ในการโอนย้ายระบบขึ้นสู่ Production (Migration)
2. มีกระบวนการควบคุมดูแลการเบิกใช้บัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด (Highest Privilege User) อย่างเหมาะสม โดยครอบคลุม
   1) มีการจัดเก็บรหัสผ่านของบัญชีผู้ใช้ที่มีสิทธิ์สูงสุดโดยหน่วยงานที่มีความเป็นอิสระจากหน่วยงานของผู้ขอเบิกใช้
   2) มีการจำกัดผู้ใช้งานที่มีสิทธิ์ในการเบิกใช้และช่วงเวลาในการเบิกใช้บัญชีผู้ใช้ที่มีสิทธิ์สูงสุดไว้สำหรับกรณีที่มีความจำเป็นเท่านั้น
   3) มีขั้นตอนในการอนุมัติการเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด โดยหัวหน้างานของผู้ขอเบิกใช้และหัวหน้างานหน่วยงานผู้จัดเก็บบัญชีผู้ใช้ที่มีสิทธิ์สูงสุด

4) มีการควบคุมโดยอย่างน้อยระบบต้อง สามารถระบุตัวตนของผู้เข้าใช้งานและบันทึกไว้เพื่อการตรวจสอบย้อนหลังได้

6.6 ส่วนของการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อกำหนดขอบเขตและหลักเกณฑ์การใช้งานระบบปฏิบัติการ โดยมีผู้ดูแลระบบ ทำหน้าที่ในการควบคุม ดูแลระบบปฏิบัติการ

นิยาม

"ระบบปฏิบัติการ" (Operating System) หมายถึง ซอฟต์แวร์ระบบ (system software) ที่ทำหน้าที่ควบคุมการทำงานของฮาร์ดแวร์ทั้งหมด รวมทั้งการปฏิบัติงานของโปรแกรมด้วย เพื่อให้โปรแกรมและฮาร์ดแวร์ต่าง ๆ ทำงานประสานกัน

ขอบเขต

1. จัดให้มีระบบปฏิบัติการ (Operating System) ไว้เพื่อรองรับการปฏิบัติงานที่เกี่ยวข้องกับบริษัทเท่านั้น
2. กำหนดให้ผู้ใช้งานแต่ละบุคคลมี ชื่อผู้ใช้ และ รหัสผ่าน ในการใช้งานระบบปฏิบัติการหรือเครื่องคอมพิวเตอร์ตามบทบาทหน้าที่ที่บุคคลนั้นได้รับเท่านั้น
3. เมื่อไม่มีการใช้งาน หรือลงบันทึกออก (Log out) จากระบบปฏิบัติการทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน หลังจากนั้นเมื่อต้องการใช้งานระบบปฏิบัติการอีก ต้องใส่รหัสผ่านอีกครั้งเพื่อเข้าใช้งาน
4. จำกัดระยะเวลาและจำนวนครั้งในการป้อนรหัสผ่านเพื่อเข้าถึงระบบปฏิบัติการ หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนที่กำหนดไว้ ให้ทำการล็อคสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีก จนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อคให้
5. ควบคุมการใช้งาน ชื่อผู้ใช้ และ รหัสผ่าน ของระบบปฏิบัติการของตน ไม่นำชื่อผู้ใช้ และ รหัสผ่าน ของตนไปมอบให้บุคคลอื่น
6. ควบคุมการติดตั้งซอฟต์แวร์คอมพิวเตอร์ที่มีลิขสิทธิ์ของบริษัทลงบนระบบปฏิบัติการ โดยผู้ใช้งานต้องขออนุมัติต่อผู้บังคับบัญชาและผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อขอใช้งานเพิ่มเติมได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดลิขสิทธิ์
7. ห้ามมิให้ผู้ใช้งานกระทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไขระบบปฏิบัติการหรือทำสำเนา เพื่อนำไปใช้งานที่อื่นโดยไม่ได้รับอนุญาต เนื่องจากระบบปฏิบัติการที่บริษัท จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นและสำคัญ
8. ต้องจัดทำบัญชีผู้ใช้ บัญชีเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่ระบุถึงระบบปฏิบัติการ ซอฟต์แวร์ที่ติดตั้ง และผู้มีสิทธิ์ใช้งาน พร้อมปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ

6.7 ส่วนของการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงระบบสารสนเทศและโปรแกรมประยุกต์โดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท

ขอบเขต

1. กำหนดให้ผู้ดูแลระบบต้องควบคุม จำกัด หรือให้สิทธิ์การเข้าถึงสารสนเทศ ข้อมูลและฟังก์ชั่นต่าง ๆ ของระบบสารสนเทศและโปรแกรมประยุกต์ ดังนี้
    - ต้องลงทะเบียนการเข้าใช้งานเพื่อทำการระบุตัวตน
    - ห้ามไม่ให้กระทำการโอนย้ายสิทธิ์แก่ผู้อื่น โดยสิทธิ์การเข้าใช้งานให้เป็นสิทธิ์เฉพาะบุคคลเท่านั้น
    - ให้ทำการยกเลิกสิทธิ์การเข้าใช้งานทันทีที่ผู้ได้รับสิทธิ์นั้น ไม่ได้รับสิทธิ์การเข้าใช้งานอีกต่อไป
    - กำหนดให้มีการพิสูจน์ตัวตน (Authentication) ก่อนการเข้าถึงระบบงานทุกครั้ง
2. กำหนดให้ระบบที่ใช้งานเฉพาะที่จำเป็น และตามสิทธิ์การใช้งานเท่านั้น
3. กำหนดให้ผู้ดูแลระบบต้องทำการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงานหนึ่ง โดยให้นำข้อมูลออกได้เฉพาะที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งานเท่านั้น
4. กำหนดให้มีการทบทวนสิทธิ์ในการเข้าถึงอย่างน้อยปีละ 1 ครั้ง

6.8 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

วัตถุประสงค์

เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

ขอบเขต

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูล ที่คำนึงถึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (encryption algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการดำเนินนโยบายและบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (key management)
2. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูล ตลอดช่วงเวลาการใช้งาน (key management whole life cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ

6.9 ส่วนของการควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สาคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

ขอบเขต

1. การควบคุมศูนย์คอมพิวเตอร์
    1) กำหนดสิทธิ์บุคคล ในการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ โดยให้เฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องเท่านั้น หากมีความจำเป็นต้องเข้า ต้องให้ผู้ดูแลระบบเป็นผู้รับผิดชอบนำพาเข้าไป และต้องมีผู้ดูแลระบบอยู่กับบุคคลนั้นตลอดเวลา
    2) กำหนดให้บุคคลภายนอกที่เข้าดำเนินการบำรุงรักษา บริหารจัดการช่องทางติดต่อสื่อสารของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องแจ้งให้ผู้ดูแลระบบรับทราบก่อนทุกครั้ง และเก็บบันทึกการเข้า-ออก ในเอกสาร Onsite visit form
    3) จัดเก็บบันทึกการเข้า-ออกศูนย์คอมพิวเตอร์ โดยบันทึกในแบบฟอร์ม (Onsite visit form) โดยมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาเข้า-ออกหน่วยงาน และรายละเอียดการเข้าใช้ศูนย์
    4) จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม
2. การป้องกันความเสียหาย
    1) ระบบป้องกันไฟไหม้
        - มีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น
        - ศูนย์คอมพิวเตอร์หลัก มีถังเพลิงเพื่อใช้ดับเพลิงในเบื้องต้น และได้รับการตรวจสอบ ดูแลอุปกรณ์ดับเพลิงตามกำหนดเวลาที่ระบุไว้ในคู่มือการใช้งาน
    2) ระบบป้องกันไฟฟ้าขัดข้อง โดยมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ โดยมีเครื่องสำรองไฟที่ศูนย์คอมพิวเตอร์สามารถรองรับการทำงานที่มีความต่อเนื่องได้
    3) ใช้ระบบ DR-Site แทนระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ เพื่อให้การดำเนินงาน มีความต่อเนื่องระบบควบคุมอุณหภูมิและความชื้น

6.10 การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท (mobile device and teleworking)

วัตถุประสงค์

เพื่อให้อุปกรณ์ที่ใช้ปฏิบัติงานมีความปลอดภัยและไม่เป็นช่องทางที่ทำให้ข้อมูลสำคัญ. รั่วไหลหรือมีการเข้าใช้งานโดยไม่ได้รับอนุญาต

ขอบเขต

1. กำหนด Security Baseline สำหรับอุปกรณ์ที่ใช้ปฏิบัติงาน เพื่อป้องกันความเสี่ยงที่อุปกรณ์เหล่านั้นป้องกันการแพร่กระจายของโปรแกรมที่ไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญ ตามระดับความเสี่ยงที่เหมาะสม โดยอย่างน้อยครอบคลุม ดังนี้
    - กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ยี่ห้อ รุ่น
      ระบบปฏิบัติการ
      รหัสประจำเครื่อง (serial number) และหมายเลขอ้างอิงอุปกรณ์เครือข่าย (MAC address) เป็นต้น
    - ควบคุมให้มีการติดตั้งเฉพาะซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (patches) ที่เหมาะสม
    - ติดตั้งโปรแกรมรักษาความปลอดภัย เช่น anti-Virus/ anti-malware เป็นต้น โดยมีการปรับปรุงประสิทธิภาพของการป้องกันโปรแกรม ไม่ประสงค์ดี (malware) ให้เพียงพอและเป็นปัจจุบัน เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ
    - ควบคุมไม่ให้มีการจัดเก็บข้อมูลที่มีระดับชั้นความลับสูงสุดในเครื่องคอมพิวเตอร์ของผู้ใช้งาน แต่หาก มีความจำเป็นต้องจัดเก็บ ต้องมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น มีการเข้ารหัส เป็นต้น
    - จำกัดการเข้าถึง shared drive หรือ shared folder ตามความจำเป็นในการใช้งานเท่านั้น
    - การควบคุมการใช้สื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการอนุญาต ให้ใช้งาน Universal Serial Bus (USB) หรือ external harddisk เป็นต้น
    - การควบคุมการใช้ Email เช่น กำหนดแนวทางการใช้งาน Email เป็นต้น

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงานทั้งอุปกรณ์และอุปกรณ์ส่วนตัว (Bring Your Own Device : BYOD) เช่น personal computer, notebook, tablet, smartphone, removable media เป็นต้น เพื่อให้มีแนวทางที่ใช้ในการควบคุม ความเสี่ยงจากการใช้งานอุปกรณ์ดังกล่าว
    - การควบคุมการใช้ BYOD ในการเข้าถึงระบบเครือข่าย ระบบงานและข้อมูลตามความเหมาะสม
    - มีกระบวนการตรวจสอบ วิเคราะห์ และติดตามความเสี่ยงของอุปกรณ์ที่นำมาใช้งาน.

- กรณีเครื่องคอมพิวเตอร์ (personal computer, notebook) ต้องติดตั้ง anti-virus/ anti-malware หรือโปรแกรมตามที่กำหนด
- ไม่อนุญาตให้อุปกรณ์โทรศัพท์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) นำมาใช้งาน
- ใช้วิธีการพิสูจน์ตัวตนอุปกรณ์ที่เชื่อถือได้ขององค์กร เช่น trusted root certification authorities, digital certificate เป็นต้น

2. ในกรณีที่มีการปฏิบัติงานขององค์กรจากระยะไกล (teleworking site) ต้องกำหนด มาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึง ประมวลผล และจัดเก็บในพื้นที่ปฏิบัติงาน

2. นโยบายย่อยการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

ขอบเขต

1. ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Change Control Procedures) สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น
   1) คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
   2) ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
   3) ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
   4) ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น
2. การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบ (Technical Review of Applications After Operating System Changes) เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ ผู้ดูแลระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย
3. การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages) เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสาร

4. มีการแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop environment) ออกจากส่วนที่ใช้งานจริง (Production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้การแบ่งแยกส่วนโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง

3. นโยบายย่อยการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อกำหนดวิธีการให้มั่นใจว่าบุคลากร และผู้ที่ทำสัญญาจ้างทั้งหมดนั้นเข้าใจบทบาทหน้าที่และความรับผิดชอบของตน รวมถึงการสรรหาคนทำงานที่มีความเหมาะสมกับบทบาทที่ได้รับมอบหมาย และเพื่อลดความเสี่ยงต่อความมั่นคงปลอดภัยด้านสารสนเทศ

ขอบเขต

กรณี ก่อนการจ้างงาน (Prior to Employment)

1. เพื่อคัดสรรบุคลากรที่ตรงกับความต้องการของบริษัท และเพื่อให้บุคลากรเข้าใจในหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของตนเอง
2. การคัดเลือก (Screening) มีการตรวจสอบประวัติของผู้สมัคร เช่น การตรวจสอบประวัติอาชญากรรม (หากมีการร้องขอ ในบางตำแหน่ง)

กรณี ระหว่างการจ้างงาน (During employment)

1. ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้พนักงาน เจ้าหน้าที่หน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบและปฏิบัติตามนโยบาย กฎ ระเบียบและขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทด้วย
2. ต้องจัดอบรมให้ความรู้แก่พนักงาน เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทด้วย
3. พนักงานใหม่ทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารและระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงาน โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย
4. ฝ่ายบริหารทรัพยากรบุคคล และ ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ให้แก่บุคลากรด้วย
5. ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของบริษัท หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

กรณี การยกเลิกการจ้างงาน (Termination of Change of Employment)

1. การยกเลิกการเข้าถึง (Removal of Access rights) หลังจากมีการยกเลิก การจ้างพนักงานแล้ว เจ้าหน้าที่กลุ่มบริหารทรัพยากรบุคคลจะต้องแจ้งให้เจ้าหน้าที่เทคโนโลยีสารสนเทศ ยกเลิกการเข้าถึงข้อมูลต่าง ๆ ของหน่วยงาน
2. การคืนทรัพย์สิน (Return on Assets) พนักงานที่พ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

4. นโยบายย่อยการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อบริษัทในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติ เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (Access risk) ดังนั้น การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมี วัตถุประสงค์เพื่อป้องกันทรัพย์สินสารสนเทศของบริษัทจากการเข้าถึงโดยผู้ให้บริการภายนอก อย่างไม่เหมาะสม

ขอบเขต

1. ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service level agreement) อย่างชัดเจน
2. จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม เพื่อป้องกันการรั่วไหลของข้อมูล(Information Leakage)
3. ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด
4. ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ (กรณีที่มีคู่มือกำกับ)

5. นโยบายย่อยการบริการจัดการสินทรัพย์สารสนเทศ (Information Asset Management)

วัตถุประสงค์

เพื่อควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบสารสนเทศให้ได้รับการป้องกันและปกป้องให้มีความมั่นคงปลอดภัย จากการเข้าถึงและนำไปใช้งานของผู้ไม่มีสิทธิ์ ในระดับที่เหมาะสมตามระดับชั้นความลับ

นิยาม

"สินทรัพย์สารสนเทศ" หมายถึง สินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์และโปรแกรมประยุกต์ (Software and Application Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) ที่เกี่ยวข้องกับงานสารสนเทศ

ขอบเขต

1. ต้องจัดทำบัญชีและเก็บทะเบียนสินทรัพย์สารสนเทศ เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ประเมินความเสี่ยงและบริหารจัดการที่มีต่อสินทรัพย์อย่างเหมาะสม
2. ผู้ใช้งานต้องปฏิบัติตามนโยบาย แนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ ระเบียบข้อบังคับ คู่มือ คำแนะนำ และเอกสารใดๆที่เกี่ยวข้องกับการใช้งานสินทรัพย์ด้านเทคโนโลยีสารสนเทศ อย่างเคร่งครัด
3. กำหนดหน้าที่และความรับผิดชอบที่มีต่อสินทรัพย์ข้อมูลและเอกสาร (เจ้าของข้อมูล) โดยแบ่งได้ดังนี้
    1) จัดให้มีการบริหารจัดการเรื่องสิทธิ์ในการใช้ซอฟต์แวร์ (License Management) อย่างเหมาะสม เพื่อไม่ให้มีเกิดการละเมิดลิขสิทธิ์การใช้ซอฟต์แวร์
    2) บริหารจัดการระดับชั้นความลับของข้อมูลให้เป็นไปตามความต้องการของการปฏิบัติงานให้มีความเหมาะสมและสอดคล้องกับระดับชั้นความลับนั้นๆ
    3) จัดทำแนวทางและขั้นตอนปฏิบัติของการอนุญาตให้ใช้ข้อมูลและสินทรัพย์ ตรวจทาน และรับรองสิทธิ์การเข้าใช้ระบบเทคโนโลยีสารสนเทศ ซอฟต์แวร์และโปรแกรมประยุกต์ ที่เหมาะกับระดับความสำคัญของข้อมูล
4. การจัดการสื่อบันทึกข้อมูล (media handling) เพื่อป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศสำคัญที่ถูกจัดเก็บในสื่อบันทึกข้อมูล
    1) กรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ผู้ประกอบธุรกิจต้องจัดให้มีกระบวนการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลและไม่ให้สามารถกู้คืนข้อมูลได้
    2) ต้องจัดให้มีกระบวนการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับหรือมีความสำคัญ
    3) กรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่
    4) ต้องจัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต
    5) ต้องจัดให้มีกระบวนการดูแลรักษาความปลอดภัยกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ทำการ
5. ต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญ ให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยการวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (capacity planning) ต้องประเมินการใช้ของระบบงาน อุปกรณ์สารสนเทศ บุคลากร และผู้ให้บริการ เพื่อให้สามารถรองรับการใช้งานในอนาคต

6. นโยบายย่อยการรักษาความปลอดภัยระบบสารสนเทศ (Information Security Management System)

6.1 แนวทางปฏิบัติในการป้องกันและรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย

วัตถุประสงค์

เพื่อเป็นแนวทางปฏิบัติให้กับผู้ดูแลระบบ ซึ่งปฏิบัติงานกับระบบคอมพิวเตอร์แม่ข่าย (Server) ได้อย่างถูกต้องและปลอดภัย

ขอบเขต

1. กำหนดเปิดใช้บริการ (Service) เท่าที่จำเป็น
2. ดำเนินการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System software) เช่น ระบบปฏิบัติการ เป็นต้น อย่างสม่ำเสมอ
3. กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน
4. พิจารณาและดำเนินการให้สอดคล้อง Baseline Server Configuration and Hardening Guidelines ตามความเหมาะสม

6.2 การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (protection from malware)

วัตถุประสงค์

เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

ขอบเขต

จัดให้มีการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี รวมทั้งแก้ไขเพื่อให้ระบบกลับมาใช้งานได้ตามปกติ (recovery) โดยขั้นต่ำต้องกำหนดมาตรการ ดังนี้

1. กำหนดนโยบายห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต
2. มีกระบวนการป้องกัน และตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ที่อาจมีโปรแกรมไม่ประสงค์ดี
3. ติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม
4. ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาต ต้องมีการตรวจสอบ
5. จัดให้มีการติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้

ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

6.3 การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)

วัตถุประสงค์

เพื่อให้มีข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย สามารถใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

ขอบเขต

1. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารที่สำคัญด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดที่ครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้และจัดเก็บย้อนหลังเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามกฎหมายที่เกี่ยวข้องกำหนด
2. มีการใช้ระบบในการควบคุมค่าเวลาของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่ายสื่อสารให้ตรงกับ เครื่องแม่ข่าย Network Time Protocol : NTP (clock synchronization) เพื่อให้ค่าเวลาในการบันทึก เหตุการณ์มีความถูกต้องในลักษณะ real-time ซึ่งเครื่องแม่ข่าย NTP ต้องรับสัญญาณนาฬิกาจากแหล่ง ที่มีความน่าเชื่อถือ
3. ข้อมูลการบันทึกเหตุการณ์ของอุปกรณ์สำคัญควรจัดเก็บไว้ที่เครื่องแม่ข่ายที่แยกเฉพาะ อย่างน้อยครอบคลุม access log และ activity log โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย
4. มีการสอบทานบันทึกการเข้าถึง (access Log) และบันทึกการดำเนินงาน (activity log) ของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่มีสิทธิ์สูงอย่างสม่ำเสมอ เช่น system administrator หรือ system operator เป็นต้น เพื่อให้มั่นใจได้ว่าผู้ปฏิบัติงานเข้าถึงและปฏิบัติงานตามขอบเขตหน้าที่ที่ได้รับมอบหมาย

6.4 (system configuration management)

วัตถุประสงค์

เพื่อให้มีกระบวนการควบคุมการเปลี่ยนแปลงการตั้งค่าระบบที่มีความรัดกุมปลอดภัยและเป็นไปตามมาตรฐาน

ขอบเขต

1. จัดทำเอกสาร minimum baseline standard เพื่อใช้เป็นมาตรฐานการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร โดยมีการทบทวนปรับปรุงเอกสารให้เป็นปัจจุบันอย่างสม่ำเสมอ
2. การเปลี่ยนแปลงการตั้งค่าบนระบบที่ให้บริการจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง

ที่กำหนด เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

3. มีการจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน (system configuration version control) โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ
4. มีการสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงด้านเทคโนโลยี
5. อย่างสม่ำเสมอ เพื่อให้สอดคล้องตามมาตรฐาน
6. กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสาร minimum baseline standard ควรผ่านกระบวนการขออนุมัติยกเว้น (exception to policy) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

6.5 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

วัตถุประสงค์

เพื่อให้สามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบ รวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

ขอบเขต

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มี การติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง
2. กำหนดกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของ เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือ รับมือได้อย่างเหมาะสม
3. มีกระบวนการหรือเครื่องมือในการรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ มีการวิเคราะห์และจัดการข้อมูล ภัยคุกคามที่อาจเกิดขึ้นอย่างต่อเนื่อง ครอบคลุม ลักษณะการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ ภัยคุกคาม รวมถึงวิธีการรับมือกับภัยคุกคามนั้น เพื่อนำมาใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์
4. ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญ ควรจัดให้มีการรายงานผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง รวมทั้งจัดให้มีกระบวนการป้องกัน

6.6 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management)

วัตถุประสงค์

เพื่อให้ได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของระบบ และสามารถ ดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์

1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ การบริหารจัดการช่องโหว่ (Vulnerability Management)

2. มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment) ควรกำหนด ขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบบงานสำคัญควรจัดทำอย่างน้อยปีละ 1 ครั้ง
3. มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย

7. นโยบายย่อยการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

ขอบเขต

1. ต้องจัดให้มีขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถและประสบการณ์ โดยต้องมีการกำหนดขั้นตอนและกระบวนการการกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

2. ต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์โดยให้ดำเนินการดังนี้

    1) จัดทำแบบฟอร์มที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ จะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้
    โดยเนื้อหาต้องประกอบด้วย วันเวลา เหตุการณ์ การดำเนินการแก้ไข ผลการแก้ไข ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา

    2) รายงานคณะผู้บริหาร เมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย
    ตัวอย่างเช่น

        - พบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (ineffective security control)
        - เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ
        - การบุกรุกด้านกายภาพ
        - การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (non-compliances with policies)

- การเข้าถึงโดยไม่ได้รับอนุญาต (access violations)

ฯลฯ

8. นโยบายย่อยด้านการการสำรองข้อมูล (Backup)

วัตถุประสงค์

เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ ในเวลาที่ต้องการ

ขอบเขต

1. การสำรอง
    1) ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง
    2) ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้
        - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
        - ประเภทสื่อบันทึก ()
        - จำนวนที่ต้องสำรอง (copy)
        - ขั้นตอนและวิธีการสำรองโดยละเอียด
        - สถานที่และวิธีการเก็บรักษาสื่อบันทึก
    3) ควรมีการบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเพื่อตรวจสอบความถูกต้องครบถ้วน

2. การทดสอบ
    1) ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้
    2) ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบการนำข้อมูลสำรองมาใช้งาน
3. การเก็บรักษา
    1) ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย
    2) ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน recycle bin

9. นโยบายย่อยด้านการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ (Business Continuity Management)

วัตถุประสงค์

กำหนดแนวทางการป้องกันและเตรียมความพร้อมในการจัดการเมื่ออยู่ในภาวะวิกฤติ โดยต้องดำเนินการให้บริษัท ดำเนินภารกิจได้อย่างต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

ขอบเขต

1. ต้องจัดลำดับความสำคัญของกระบวนการสร้างความต่อเนื่องทางธุรกิจ ระบุเหตุการณ์ที่ทำให้กระบวนการทางธุรกิจหยุดชะงัก ความเป็นไปได้และผลกระทบที่จะเกิดขึ้นและแผนบริหารความต่อเนื่องทางธุรกิจจะจัดทำขึ้นสำหรับระบบงานที่มีความสำคัญ
2. แผนบริหารความต่อเนื่องทางธุรกิจทั้งหมดจะได้รับการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเมื่อเกิดเหตุฉุกเฉิน แผนที่นำมาทดสอบสามารถใช้งานได้จริง
3. ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจเพื่อให้แผนทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
4. จัดทำระบบสำรองข้อมูลของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ

อนุมัติโดย

ลงชื่อ.....ประธานกรรมการบริษัท

(ศ.นพ.อุดมศิลป์ ศรีแสงนาม)