SIAMESE ASSET
ASSET OF LIFE

เอกสารชี้แจงแก้ไขและเพิ่มเติม “นโยบายรักษาความปลอดภัยสารสนเทศ บริษัท ไซมิส แอสเสท จำกัด (มหาชน)” รายละเอียดดังนี้

ในท้ายทุกหน้าของเอกสารนโยบายได้เปลี่ยนแปลงจาก “บริษัท ไซมิส แอสเสท จำกัด” เป็น “บริษัท ไซมิส แอสเสท จำกัด (มหาชน)”

หน้า 10 หัวข้อ 5.3.1 เพิ่มหัวข้อย่อยที่ 5

5) กำหนดให้พนักงาน บริษัท ไซมิส แอสเสท จำกัด (มหาชน) และบริษัทย่อย ใช้งานอีเมล์ แอดเดรส (e-mail address) ขององค์กรโดยใช้ชื่อ Domain (siameseasset.co.th)

ผู้ขอแก้ไข	อนุมัติแก้ไข
10 ต.ค. 2562	10 ต.ค. 2562
นายเกียรติศักดิ์ ชำนาญหาญ	นายขจรศิษฐ์ สิ่งสรรเสริญ
IT Manager	Managing Director

SIAMESE ASSET
ASSET OF LIFE

เอกสารชี้แจงแก้ไขและเพิ่มเติม “นโยบายรักษาความปลอดภัยสารสนเทศ บริษัท ไซมิส แอสเสท จำกัด” รายละเอียดดังนี้

หน้า 10 หัวข้อ 5.3.1 เพิ่มหัวข้อย่อยที่ 5

5) กำหนดให้พนักงาน บริษัท ไซมิส แอสเสท จำกัด และบริษัทย่อย ใช้งานอีเมล์ แอดเดรส (e-mail address) ขององค์กรโดยใช้ชื่อ Domain (siameseasset.co.th)

ผู้ขอแก้ไข

30/05/61

นาย เกียรติศักดิ์ ชำนาญหาญ

IT Manager

อนุมัติแก้ไข

30 MAY 2018

นายขจรศิษฐ์ สิ่งสรรเสริญ

Managing Director

SIAMESE ASSET
ASSET OF LIFE

เอกสารชี้แจงแก้ไขและเพิ่มเติม "นโยบายรักษาความปลอดภัยสารสนเทศ บริษัท ไซมิส แอทแสท จำกัด" รายละเอียดดังนี้

หน้า 18 เพิ่มหัวข้อที่ 9.3.2 การปฏิบัติการใช้งานคอมพิวเตอร์พกพา และอุปกรณ์แบบพกพา (Notebook and Mobile Device)

9.3.2 การปฏิบัติการใช้งานคอมพิวเตอร์พกพา และอุปกรณ์แบบพกพา (Notebook and Mobile Device)

เป็นการควบคุมการใช้งานอุปกรณ์พกพาเฉพาะที่เป็นของบริษัท และอุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัท

1) บริษัทมีนโยบายให้ผู้ใช้งานใช้อุปกรณ์พกพาเฉพาะที่เป็นของบริษัทในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท เท่านั้นหากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท ต้องได้ รับการอนุมัติจากหัวหน้าหน่วยงาน และหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศก่อนการใช้งาน

2) บริษัทขอสงวนสิทธิ์ ในการตรวจสอบ ระงับเพิกถอนการใช้งาน และลบข้อมูลทั้งหมด บนอุปกรณ์พกพาทั้งที่เป็นของบริษัทและของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บ ข้อมูลและสารสนเทศของบริษัท หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐานหรือ ข้อมูลสารสนเทศของบริษัท

3) บริษัทไม่อนุญาตให้ผู้ใช้ทำการติดตั้ง และแก้ไขเปลี่ยนแปลงโปรแกรมในอุปกรณ์พกพาเฉพาะที่เป็นของบริษัท โดยการพลการซึ่งการติดตั้งโปรแกรมเพิ่มเติม ผู้ใช้งานต้องทำการกรอกแบบฟอร์ม IT-007 โดยได้รับอนุมัติจากหัวหน้างานและ หัวหน้าแผนกสารสนเทศเท่านั้น แต่หากโปรแกรมที่ต้องการติดตั้งเพิ่มเติมต้องมีรายละเอียดในการสั่งซื้อนั้น จำเป็นต้องได้รับการอนุมัติเพิ่มเติมจากผู้บริหารระดับสูงในการดำเนินการ

4) อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท จะต้องเป็นอุปกรณ์พกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย รวมทั้งต้องกำหนดค่ารหัสผ่านและติดตั้งระบบป้องกันหน้าจออุปกรณ์ เพื่อป้องกันการเข้าถึงอุปกรณ์ในขณะไม่ใช้งานตามนโยบายที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด

5) อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท จะต้องเป็นอุปกรณ์พกพาที่ติดตั้งโปรแกรมป้องกันไวรัส ซึ่งต้องมีการอัพเดทล่าสุดอยู่เสมอ และการใช้สื่อบันทึกข้อมูลต้องมีการตรวจสอบหาไวรัสโดย โปรแกรมป้องกันไวรัสทุกครั้ง

6) ผู้ใช้งานที่นำอุปกรณ์พกพาส่วนตัวและอุปกรณ์พกพาเฉพาะที่เป็นของบริษัทต้องไม่เก็บข้อมูลสำคัญของบริษัท ไว้บนอุปกรณ์พกพาที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัท

ผู้ขอแก้ไข

30 APR 2018

นาย เกียรติศักดิ์ ชำนาญหาญ

IT Manager

อนุมัติแก้ไข

30 APR 2018

สุนันทา สิ่งสรรเสริญ

VP-HR & Admin

SIAMESE ASSET
ASSET OF LIFE

เอกสารชี้แจงแก้ไขและเพิ่มเติม "นโยบายรักษาความปลอดภัยสารสนเทศ บริษัท ไซมิส แอทแสท จำกัด" รายละเอียดดังนี้

หน้า 9 หัวข้อ 5.1.1 เพิ่มข้อความ "และ แบบฟอร์ม Request for COMPU (IT-006-1)"

5.1.1 การควบคุมการเข้าถึง (Access Control)

หน่วยงานด้านเทคโนโลยีสารสนเทศ จัดทำ แบบฟอร์ม IT Request (IT-007) **และ แบบฟอร์ม Request for COMPU (IT-006-1)** ที่สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และนำรายการดังกล่าวมาทบทวนตามความต้องการทางธุรกิจ และความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

หน้า 9 หัวข้อ 5.3 เพิ่มข้อความ "และ แบบฟอร์ม Request for COMPU (IT-006-1)"

5.3 นโยบายบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

จุดประสงค์และขอบเขต

เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต โดยอาศัยแบบฟอร์ม IT Request (IT-007) **และ แบบฟอร์ม Request for COMPU (IT-006-1)** ควบคุมสิทธิในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบเริ่มตั้งแต่การขอจดทะเบียนไปจนถึงการยกเลิกสิทธิในกรณีที่ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้อีกต่อไป รวมไปถึงการควบคุมสิทธิของผู้ใช้ซึ่งมีสิทธิพิเศษที่สามารถแก้ไขสิทธิต่าง ๆ ของระบบได้

หน้า 10 เพิ่มหัวข้อ 5.3.2 การควบคุมผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege)

5.3.2 การควบคุม ผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege)

1) บริษัทฯ กำหนดผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) ต้องได้รับความเห็นชอบจากผู้บริหาร
2) เพื่อป้องกันการใช้งาน ของผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) บริษัทฯ ทำการเก็บของ password ไว้ในตู้เซฟ และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
3) บริษัทฯ กำหนดให้ผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) เมื่อมีการเปลี่ยนแปลง ต้องทำการเปลี่ยนแปลงรหัสผ่านทันทีอย่างเคร่งครัด
4) บริษัทฯ ได้กำหนดทำการเปลี่ยนรหัสผ่าน ผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) ทุก 3 เดือน

ผู้ขอแก้ไข	อนุมัติแก้ไข
28/02/2018.	28/2/61
นาย เกียรติศักดิ์ ชำนาญหาญ	สุนันทา สิ่งสรรเสริญ
IT Manager	VP-HR & Admin

SIAMESE ASSET
ASSET OF LIFE

ประกาศ

เลขที่ : IT - 001 / 2562

เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท ไซมิส แอสเสท จำกัด และบริษัทย่อย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกตามจากภัยต่าง ๆ บริษัทฯ จึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการป้องกันภัยคุกคามจากภายนอกและภายใน

นโยบายความมั่นคงปลอดภัยสารสนเทศ ฉบับนี้ได้ผ่านการทบทวนและให้บังคับใช้กับบริษัท ไซมิส แอสเสท จำกัด และบริษัทย่อย โดยให้มีผลตั้งแต่วันที่ 28 กุมภาพันธ์ 2562 เป็นต้นไป และกำหนดให้มีการทบทวนใหม่อย่างน้อยปีละหนึ่งครั้ง

จึงประกาศมาให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ 28 กุมภาพันธ์ 2562

.....

(นายขจรศิษฐ์ สิ่งสรรเสริญ)

กรรมการผู้จัดการ

บริษัท ไซมิส แอสเสท จำกัด

SIAMESE ASSET
ASSET OF LIFE

ประกาศ

เลขที่ : AD - 002 / 2561

เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท ไซมิส แอสเสท จำกัด และบริษัทย่อย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกตามจากภัยต่าง ๆ บริษัทฯ จึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการป้องกันภัยคุกคามจากภายนอกและภายใน

นโยบายความมั่นคงปลอดภัยสารสนเทศ ฉบับนี้ได้ผ่านการทบทวนและให้บังคับใช้กับบริษัท ไซมิส แอสเสท จำกัด และบริษัทย่อย โดยให้มีผลตั้งแต่วันที่ 28 กุมภาพันธ์ 2561 เป็นต้นไป และกำหนดให้มีการทบทวนใหม่อย่างน้อยปีละหนึ่งครั้ง

จึงประกาศมาให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ 28 กุมภาพันธ์ 2561

(นายชจรศิษฐ์ สิ่งสรรเสริญ)
กรรมการผู้จัดการ
บริษัท ไซมิส แอสเสท จำกัด

SIAMESE ASSET
ASSET OF LIFE

IT-004

นโยบายความมั่นคงปลอดภัยสารสนเทศ

(Information Security Policy)

Rev.5 Date: 10/10/2562

SIAMESE ASSET
ASSET OF LIFE

สารบัญ

SIAMESE ASSET
ASSET OF LIFE

สารบัญ

1. ความมั่นคงปลอดภัยสารสนเทศ (Information Security)

1.1 นโยบายความปลอดภัยสารสนเทศ (Management Directions for Information Security Policy)

จุดประสงค์และขอบเขต

เพื่ออธิบายถึงจุดประสงค์และขอบเขตของนโยบายความปลอดภัยสารสนเทศในภาพรวม แสดงถึงทิศทางของผู้บริหารขององค์กรด้านความปลอดภัยสารสนเทศที่ต้องการให้บุคคลที่เกี่ยวข้องกับข้อมูลขององค์กรยึดถือและนำมาใช้ในการปฏิบัติงาน โดยมีเป้าหมาย คือ การทำให้การปฏิบัติงานของพนักงานที่เกี่ยวข้องกับข้อมูล รวมถึงระบบที่เกี่ยวข้องกับข้อมูลให้มีความปลอดภัยด้านสารสนเทศที่เพียงพอในการรองรับการดำเนินธุรกิจ ณ ปัจจุบัน และในอนาคตขององค์กร

นโยบายความปลอดภัยสารสนเทศ ครอบคลุมถึงการปกป้องข้อมูลขององค์กรเป็นหลัก เนื่องด้วยข้อมูล ถือได้ว่าเป็นทรัพย์สินที่มีความสำคัญเป็นอย่างมากในการดำเนินธุรกิจขององค์กร ซึ่งในกรณีที่ข้อมูลสำคัญขององค์กร ไม่มีความปลอดภัย ไม่สามารถรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลได้นั้น จะส่งผลกระทบต่อองค์กร ไม่ว่าจะเป็นด้านการเงิน ด้านความเชื่อถือ หรือด้านชื่อเสียงขององค์กร ข้อมูลที่กล่าวถึงในนโยบายนี้มิได้จำกัดอยู่แต่ในรูปอิเล็กทรอนิกส์เท่านั้น ข้อมูลอาจอยู่ในรูปอื่น ๆ เช่น เอกสาร สิ่งพิมพ์ ฟิล์ม หรือแม้แต่ในรูปของการสนทนา อย่างไรก็ดี การปกป้องข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ จะกล่าวถึงเป็นส่วนใหญ่ เนื่องจากข้อมูลขององค์กรส่วนใหญ่นั้นจะอยู่ในรูปอิเล็กทรอนิกส์ ซึ่งในอนาคตจะมีแนวโน้มเพิ่มขึ้นตามลำดับ

เนื้อหานโยบาย และการดำเนินการ

1.1.1 การจัดทำนโยบายความปลอดภัยสารสนเทศ (Policies for Information Security)

1) นโยบายความปลอดภัยสารสนเทศฉบับนี้ถูกจัดทำเป็นลายลักษณ์อักษรตามจุดประสงค์และขอบเขตและได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการมีการประกาศใช้และถือปฏิบัติทั่วทั้งองค์กรโดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นขององค์กรตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สินสารสนเทศขององค์กร
2) ผู้บริหารพนักงานตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและทรัพย์สินสารสนเทศขององค์กรมีหน้าที่โดยตรงที่จะต้องสนับสนุนดำเนินการตามข้อบังคับการใช้งานระบบเทคโนโลยีสารสนเทศและกฎเกณฑ์การใช้ทรัพย์สิน(IT-005/2559) และให้ความร่วมมือในการดำเนินการตามนโยบายอย่างเคร่งครัดการฝ่าฝืนนโยบายนี้ถือเป็นความผิดที่ร้ายแรงโดยมีบทลงโทษถึงขั้นสูงสุดตามระเบียบขององค์กร

1.1.2 การทบทวนโบบายความปลอดภัยสารสนเทศ (Review of The Policies for Information Security)

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

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

2. โครงสร้างความปลอดภัยสารสนเทศ (Organization of Information Security)

2.1 นโยบายโครงสร้างภายในองค์กร (Internal Organization Policy)

จุดประสงค์และขอบเขต

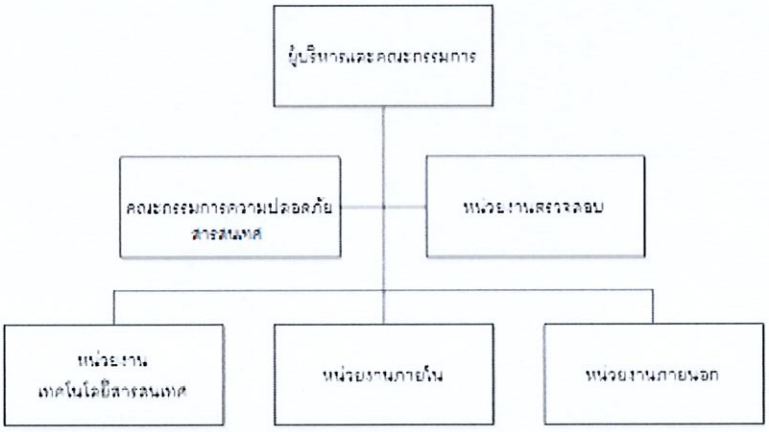
เพื่อให้การจัดการความปลอดภัยสารสนเทศให้เป็นไปอย่างมีระบบและมีความชัดเจน ตั้งแต่ระดับบริหารจนถึงระดับปฏิบัติการ องค์กรจึงได้จัดทำโครงสร้างความปลอดภัยสารสนเทศ รวมถึงการกำหนดบทบาท และหน้าที่ ในการบริหารจัดการความปลอดภัยของสารสนเทศภายในองค์กร

เนื้อหานโยบาย และการดำเนินการ

2.1.1 กำหนดบทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles And Responsibilities)

ผู้บริหารให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ โดยอนุมัติให้มีการจัดตั้งคณะกรรมการด้านความปลอดภัยสารสนเทศ ดังนี้

1) ลักษณะโครงสร้างของคณะกรรมการความปลอดภัยสารสนเทศ แสดงดังภาพด้านล่างนี้



ภาพที่ 1 แสดงโครงสร้างองค์กรของคณะกรรมการความปลอดภัยสารสนเทศ

2) คณะกรรมการความปลอดภัยสารสนเทศ ประกอบจากผู้บริหารของหน่วยงานต่าง ๆ ดังนี้

a) หัวหน้าฝ่ายงานก่อสร้าง
b) หัวหน้าฝ่าย Business develop
c) หัวหน้าฝ่ายการเงิน
d) หัวหน้าฝ่ายบัญชี
e) หัวหน้าฝ่ายบริหารส่วนกลาง
f) หัวหน้าฝ่ายสอบภายใน
g) หัวหน้าฝ่ายงานการตลาด
h) หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
i) หัวหน้าฝ่ายทรัพยากรบุคคล
j) หัวหน้าฝ่ายงานขาย
k) หัวหน้าฝ่ายควบคุมต้นทุน
l) หัวหน้าฝ่ายจัดหา
m) หัวหน้าฝ่ายบริการลูกค้า

3) คณะกรรมการความปลอดภัยสารสนเทศมีหน้าที่ดังนี้

a) ตรวจสอบ และอนุมัติ ปรับปรุงนโยบายความปลอดภัยสารสนเทศ ตามกำหนด หรือตามสถานการณ์

b) วางแผนประชาสัมพันธ์ และอบรมบุคลากรทุกหน่วยเข้าใจถึงความปลอดภัยสารสนเทศ

c) ตรวจสอบ และให้ความเห็นชอบโครงการที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

d) วางแผน ตรวจสอบ และบริหารจัดการความเสี่ยงต่าง ๆ ที่เกิดจากข้อจำกัดของระบบ

e) ตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องด้านความมั่นคงปลอดภัย กรณีฉุกเฉิน

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

คณะกรรมการความปลอดภัย ได้ทำการกำหนดบทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องตามโครงสร้างของคณะกรรมการความปลอดภัยสารสนเทศ ดังนี้

1) หน่วยงานด้านเทคโนโลยีสารสนเทศ จัดตั้งขึ้นเพื่อป้องกันความเสียหายขององค์กรอันเกิดจากภัยคุกคามด้านข้อมูล เช่น การสูญหายของข้อมูล หรือการเจาะระบบสารสนเทศ เป็นต้น และทำให้การดำเนินการในส่วนที่เกี่ยวข้องกับข้อมูลมีความปลอดภัยในระดับที่สอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

2) หน่วยงานตรวจสอบ รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศขององค์กร โดยมอบหมายให้ รองกรรมการฝ่ายบริหาร

3) หน่วยงานภายใน คือ พนักงานทุกคนขององค์กร ที่มีส่วนเกี่ยวข้องกับสารสนเทศไม่ว่าทางใดทางหนึ่ง มีหน้าที่รับผิดชอบดังนี้

a) ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศอย่างเคร่งครัด

b) รักษาความลับของข้อมูล สารสนเทศขององค์กร และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง

c) รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัยเมื่อเกิดเหตุการณ์ดังกล่าวให้กับหน่วยงานด้านเทคโนโลยีสารสนเทศ

d) ใช้งานข้อมูล และทรัพย์สินทางข้อมูลขององค์กรอย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบ หรือได้รับอนุญาตเท่านั้น

4) หน่วยงานภายนอก คือ บุคคลภายนอกที่เข้ามาปฏิบัติงานในองค์กรหรือทำงานให้กับองค์กร ซึ่งมีส่วนเกี่ยวข้องในการใช้ข้อมูลหรือทรัพย์สินสารสนเทศอื่นขององค์กร เช่น ผู้ให้บริการ/ผู้จำหน่าย ระบบคู่สัญญาหรือผู้ที่ได้รับอนุญาตโดยมีหน้าที่ความรับผิดชอบเช่นเดียวกับพนักงานขององค์กร

2.2 นโยบายการจัดขั้นความลับของสารสนเทศ (Information Classification Policy)

จุดประสงค์และขอบเขต

นโยบายได้กำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้น และได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้นโยบายยังได้กำหนดถึงบทบาทของเจ้าของข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้องกับการจัดลำดับชั้นของข้อมูล เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

เนื้อหานโยบาย และการดำเนินการ

2.2.1 ขั้นความลับสารสนเทศ (Classification of Information)

สารสนเทศต้องมีการจัดชั้นความลับ โดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ซึ่งคณะกรรมการได้จัดทำ เอกสารแสดงการจัดการขั้นความลับและการกำหนดระดับการเข้าถึงข้อมูลสารสนเทศ (IT-006/2560) เพื่อให้หน่วยงานต่าง ๆ มาลงทะเบียนเอกสารต่าง ๆ ตามลำดับชั้นที่กำหนดไว้ ดังนี้

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

1) ชั้นที่ 1 ข้อมูลเปิดเผยได้
ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย

2) ชั้นที่ 2 ข้อมูลใช้ภายในองค์กรเท่านั้น
เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้พนักงานทุกคนภายในองค์กรทราบได้ แต่ไม่สามารถเปิดเผยต่อบุคคลภายนอกองค์กรได้ เนื่องจากอาจสร้างความเสียหายให้กับองค์กรได้

3) ชั้นที่ 3 ข้อมูลลับ
เป็นข้อมูลใช้ภายในองค์กรที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบเพื่อให้เพียงพอต่อการปฏิบัติงาน

4) ชั้นที่ 4 ข้อมูลลับมาก
เป็นข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้ใช้บางกลุ่มขององค์กร (ส่วนใหญ่เป็นผู้บริหารเท่านั้น) และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เนื่องจากข้อมูลประเภทนี้ มีความจำเป็นต่อการปฏิบัติงานขององค์กรและจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือ ทำให้เกิดผลเสียหายร้ายแรงต่อองค์กร

5) ชั้นที่ 5 ข้อมูลลับที่สุด
ข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้บริหารระดับสูงขององค์กรเท่านั้น และเป็นการใช้เพื่อการวินิจฉัยและตัดสินใจที่สำคัญขององค์กร ไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เลย เนื่องจากข้อมูลประเภทนี้มีความจำเป็นต่อการปฏิบัติงานขององค์กรจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือทำให้เกิดผลเสียหายร้ายแรงต่อองค์กร การนำข้อมูลในชั้นนี้ไปเปิดเผยต่อบุคคลภายนอกไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

3. ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

3.1 นโยบายก่อนการจ้างงาน (Prior to Employment Policy)

จุดประสงค์และขอบเขต

เพื่อเป็นแนวทางการรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการทรัพยากรบุคคลตั้งแต่การรับเข้าทำงานจนถึงการเลิกจ้าง เพราะกระบวนการด้านทรัพยากรบุคคลจึงมีความจำเป็นในการช่วยทำให้สารสนเทศขององค์กรมีความปลอดภัย

เนื้อหานโยบาย และการดำเนินการ

3.1.1 การคัดเลือก (Screening)

การตรวจสอบภูมิหลังของผู้สมัครงาน ต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมาย และระเบียบข้อบังคับ โดยหน่วยงานทรัพยากรบุคคลต้องตรวจสอบประวัติของบุคคลก่อนที่จะทำการว่าจ้าง เช่น หลักฐานการศึกษา บุคคลอ้างอิง ประวัติการทำงานจากหน่วยงานต้นสังกัดเดิม และเอกสารที่ทางราชการออกให้ เป็นต้น โดยเฉพาะตำแหน่งงานที่เกี่ยวข้องกับข้อมูลสำคัญขององค์กร จะต้องมีการตรวจสอบเป็นพิเศษ

3.1.2 ข้อตกลง และเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

ข้อตกลง และเงื่อนไขในสัญญาจ้างกับพนักงาน มีการระบุถึงหน้าที่ความรับผิดชอบ (Job Description) ที่ชัดเจน และระบุถึงความรับผิดชอบด้านความปลอดภัยสารสนเทศ การฝ่าฝืนหรือละเลยต่อหน้าที่และนโยบายถือว่ามีความผิด ต้องพิจารณาตามบทลงโทษขององค์กร ซึ่งขึ้นอยู่กับความรุนแรงของผลกระทบที่เกิดขึ้นกับองค์กร

3.2 นโยบายระหว่างการจ้างงาน (During Employment Policy)

จุดประสงค์และขอบเขต

เพื่อลดความเสี่ยงของสารสนเทศที่เกิดจากบุคลากร ทั้งที่เกิดจากการละเมิดความปลอดภัยสารสนเทศโดยเจตนาและไม่ได้เจตนา หรือจากการละเลยต่อการปฏิบัติหน้าที่ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

เนื้อหานโยบาย และการดำเนินการ

3.2.1 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

ฝ่ายทรัพยากรบุคคล จัดให้พนักงานทุกคน ต้องเข้ารับฟังการอบรมให้ตระหนักถึงความปลอดภัยสารสนเทศเพิ่ม อย่างน้อยปีละ 1 ครั้ง เพื่อรับทราบถึงนโยบายความปลอดภัยเพิ่มเติมขององค์กรเหตุการณ์ละเมิดความปลอดภัย และกรณีศึกษาใหม่ ๆ ในขณะที่หน่วยงานด้านเทคโนโลยีสารสนเทศ จะต้องได้รับการฝึกอบรมจากหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง

3.2.2 กระบวนการทางวินัย (Disciplinary Process)

กระบวนการทางวินัยต้องกำหนดอย่างเป็นทางการ พนักงานทุกคนต้องลงลายมือชื่อรับทราบ ข้อบังคับการใช้ระบบสารสนเทศและกฎเกณฑ์การใช้ทรัพย์สิน (IT-005/2559) ซึ่งกระบวนการทางวินัยที่กำหนดขึ้นนี้เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร หน่วยงานทรัพยากรบุคคล และหน่วยงานด้านกฎหมายต้องกำหนดบทลงโทษสำหรับพนักงาน ซึ่งละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง

3.3 นโยบายหลังการสิ้นสุด หรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment Policy)

จุดประสงค์และขอบเขต

เพื่อเพิ่มความปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการบุคลากรที่กำลังจะเลิกจ้าง โดยระบุหน้าที่ความรับผิดชอบและบทบาทของผู้เกี่ยวข้องกับกระบวนการ นอกจากนี้ยังเป็นการควบคุมความปลอดภัย ของสารสนเทศให้ดียิ่งขึ้น และเพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

เนื้อหานโยบาย และการดำเนินการ

3.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

หน่วยงานทรัพยากรบุคคลและหน่วยงานต่าง ๆ ร่วมกันกำหนดขั้นตอนการปฏิบัติ ของพนักงานที่ออกจากองค์กร เมื่อสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อมีการเปลี่ยนการจ้างงาน ดังนี้

1) หน่วยงานที่เกี่ยวข้อง มีหน้าที่แจ้งไปยังหน่วยงานทรัพยากรบุคคล ถึงเรื่องการลาออก หรือการปรับเปลี่ยนตำแหน่งของพนักงาน
2) หน่วยงานทรัพยากรบุคคล ปฏิบัติตาม นโยบายการควบคุมการเข้าถึงระบบ (อ้างอิงนโยบาย ข้อที่ 5.2) โดยต้องแจ้งหน่วยงานด้านเทคโนโลยีสารสนเทศทราบทันทีที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานขององค์กรเพื่อทำการถอดถอนสิทธิ การเข้าใช้ระบบงานต่าง ๆ และการเข้า-ออกพื้นที่ขององค์กร
3) หน่วยงานด้านเทคโนโลยีสารสนเทศ ปฏิบัติตาม หัวข้อ การคืนทรัพย์สิน (อ้างอิงนโยบาย ข้อที่ 4.1.4) โดยทำการตรวจสอบทรัพย์สินของพนักงาน และรายงานผลการตรวจสอบกลับมายังหน่วยงานทรัพยากรบุคคล
4) หน่วยงานด้านเทคโนโลยีสารสนเทศ ทำการสำรองข้อมูลที่จำเป็นของพนักงานดังกล่าว เป็นเวลาน้อย 90 วัน และแจ้งให้หน่วยงานที่เกี่ยวข้องทราบถึงวิธีเข้าถึงข้อมูลดังกล่าวได้

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

4. การบริหารจัดการทรัพย์สิน (Asset Management)

4.1 นโยบาย และหน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets Policy)

จุดประสงค์และขอบเขต

ทรัพย์สิน หมายถึง ทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ข้อมูล ซอฟต์แวร์ หรือแม้แต่อุปกรณ์ที่เกี่ยวข้องในการประมวลผล นอกจากนี้องค์กรควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน อย่างไรก็ดี เจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว เพื่อให้มีการระบุทรัพย์สินขององค์กร และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

เนื้อหานโยบาย และการดำเนินการ

4.1.1 การจัดการบัญชีทรัพย์สิน (Inventory of Assets)

ทุกหน่วยงานขององค์กรที่เกี่ยวข้องกับข้อมูล จะต้องดำเนินการจัดทำบัญชีทรัพย์สิน ที่เกี่ยวข้องกับข้อมูลขององค์กร โดยระบุรายละเอียดต่าง ๆ ลง ทะเบียนทรัพย์สิน (Compu-ASrepBFZ) หน่วยงานเทคโนโลยีสารสนเทศ จะทำการตรวจสอบทรัพย์สิน ร่วมกับผู้ถือครองทรัพย์สิน เพื่อปรับปรุงบัญชีทรัพย์สินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of Assets)

ในการจัดทำทะเบียนทรัพย์สิน แต่ละหน่วยงานจะต้องกำหนดเจ้าของทรัพย์สินที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น เจ้าของทรัพย์สิน ต้องสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สินตลอดจนการแจ้งถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินทราบ

4.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable Use of Assets)

กฎเกณฑ์การใช้อย่างเหมาะสมสำหรับการใช้งานสารสนเทศ ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการระบุจัดทาเป็นลายลักษณ์อักษร ผู้ใช้งาน พนักงาน หน่วยงานภายนอกต้องยินยอมทำตามข้อกำหนดในการใช้งานข้อมูลและทรัพย์สินสารสนเทศ

4.1.4 การคืนทรัพย์สิน (Return of Assets)

พนักงาน และลูกจ้างของหน่วยงานภายนอก ทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง โดยทรัพย์สินที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจะต้องมีการตรวจสภาพทรัพย์สินจากฝ่ายเทคโนโลยีสารสนเทศเสียก่อน หากผลการตรวจสอบพบว่ามีความชำรุดเสียหาย หรือมีข้อมูลบางอย่างขาดหายไป ผู้รับผิดชอบจะต้องได้รับผิดชอบตามข้อกำหนดที่ได้ตกลงไว้

4.2 นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล เพื่อป้องกันความเสียหายต่อการดำเนินธุรกิจ อันเนื่องมาจากความเสียหายของสื่อบันทึกข้อมูลต่าง ๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

เนื้อหานโยบาย และการดำเนินการ

4.2.1 การบริหารจัดการสื่อบันทึกข้อมูล (Management of Media)

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์การกำหนดไว้

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

4.2.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ

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

4.2.3 การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

5. การควบคุมการเข้าถึง (Access Control)

5.1 นโยบายความต้องการทางธุรกิจเกี่ยวกับการเข้าถึง (Business Requirements of Access Control Policy)

จุดประสงค์และขอบเขต

เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็น และความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความปลอดภัย

เนื้อหานโยบาย และการดำเนินการ

5.1.1 การควบคุมการเข้าถึง (Access Control)

หน่วยงานด้านเทคโนโลยีสารสนเทศ จัดทำ แบบฟอร์ม IT Request (IT-007) และแบบฟอร์ม Request for COMPU (IT-006-1) ที่สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และนำรายการดังกล่าวมาทบทวนตามความต้องการทางธุรกิจ และความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

5.2 นโยบายการควบคุมการเข้าถึงระบบ (System and Application Access Control Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิเข้าใช้งานในระดับระบบปฏิบัติการ (Operating System) หน่วยงานด้านเทคโนโลยีสารสนเทศ ควรจัดให้มีการกำหนดข้อความเตือนก่อนการเข้าสู่ระบบ การตรวจสอบผู้ใช้ และการบริหารรหัสผ่านสาหรับผู้ใช้งาน รวมถึงการควบคุมเวลาในการเชื่อมต่อสู่ระบบข้อมูล

เนื้อหานโยบาย และการดำเนินการ

5.2.1 การจัดการเข้าถึงสารสนเทศ (Information Access Restriction)

การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ผู้ดูแลระบบ ต้องจัดการให้ระบบแสดงข้อความเตือนถึง "การอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิ์เข้าใช้งาน" ก่อนที่จะทำการเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ขององค์กร และระบบต้องเปิดโอกาสให้ผู้ใช้สามารถยกเลิกการเชื่อมต่อเข้าสู่ระบบในกรณีที่ทราบว่าระบบนั้น ๆ ไม่ได้เกี่ยวข้องกับตนเอง

1) ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้ (User-ID) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้ แต่ละคนได้
2) ผู้ใช้ควรออกจากระบบเครือข่าย (Log-off) ทันที เมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก
3) ผู้ใช้ถูกติดตั้งโปรแกรมถนอมหน้าจอ (Screen Saver) ที่มีรหัสผ่านบนเครื่องคอมพิวเตอร์ โดยโปรแกรมเหล่านี้จะเริ่มทำงานหลังจากไม่มีการใช้งานใด ๆ บนเครื่องคอมพิวเตอร์นั้น ๆ ตามเวลาที่กำหนดไว้
4) หากไม่มีการใช้งานเป็นเวลานาน ผู้ใช้ต้องปิดเครื่องคอมพิวเตอร์ หรือเครื่องปลายทางให้เรียบร้อย

5.3 นโยบายบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

จุดประสงค์และขอบเขต

เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต โดยอาศัยแบบฟอร์ม IT Request (IT-007) และ แบบฟอร์ม Request for COMPU (IT-006-1) ควบคุมสิทธิ์ในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบ เริ่มตั้งแต่การขอจดทะเบียนไปจนถึงการยกเลิกสิทธิในกรณีที่ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้อีกต่อไป รวมไปถึงการควบคุมสิทธิของผู้ใช้ซึ่งมีสิทธิพิเศษที่สามารถแก้ไขสิทธิต่าง ๆ ของระบบได้

เนื้อหานโยบาย และการดำเนินการ

5.3.1 การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and Deregistration)

กระบวนการลงทะเบียน และถอดถอนสิทธิ์ผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการให้สิทธิ์การเข้าถึง

1) พนักงานทุกคนที่มีสิทธิ์เข้าใช้งานระบบข้อมูลต้องมีรหัสผู้ใช้เฉพาะบุคคลในการเข้าสู่ระบบ
2) รหัสผู้ใช้เป็นรหัสเฉพาะบุคคล โดยไม่มีการใช้รหัสผู้ใช้ร่วมกัน (Shared User ID) ในกรณีที่พนักงานลาออก รหัสผู้ใช้รายนั้นต้องไม่ถูกนำกลับมาใช้ใหม่
3) ในการร้องขอเพื่อเข้าใช้งานระบบใด ๆ ผู้บังคับบัญชาในหน่วยงานต้องทำการพิจารณาเพื่อเห็นชอบ
4) หน่วยงานเจ้าของข้อมูล และหน่วยงานด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการร่วมกันในการถอดถอนสิทธิ์ของผู้ใช้ ซึ่งไม่มีความต้องการใช้ระบบอีกต่อไปโดยทันที
5) กำหนดให้พนักงาน บริษัท ไซมิส แอสเสท จำกัด (มหาชน) และบริษัทย่อย ใช้งานอีเมล์ แอดเดรส (e-mail address) ขององค์กรโดยใช้ชื่อ Domain (siameseasset.co.th)

5.3.2 การควบคุม ผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege)

1) บริษัทฯ กำหนดผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) ต้องได้รับความเห็นชอบจากผู้บริหาร
2) เพื่อป้องกันการใช้งาน ของผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) บริษัทฯ ทำการเก็บซอง password ไว้ในตู้เซฟ และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
3) บริษัทฯ กำหนดให้ผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) เมื่อมีการเปลี่ยนแปลง ต้องทำการเปลี่ยนแปลงรหัสผ่านทันทีอย่างเคร่งครัด
4) บริษัทฯ ได้กำหนดทำการเปลี่ยนรหัสผ่าน ผู้ใช้งานระบบที่มีสิทธิพิเศษ (User privilege) ทุก 3 เดือน

5.3.3 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

เจ้าของระบบต้องมีการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง

5.4 นโยบายหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อมุ่งเน้นให้ผู้ใช้งานระบบมีความตระหนักถึงความปลอดภัยในการใช้งานระบบข้อมูล โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่าน และต้องทราบถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานคอมพิวเตอร์

เนื้อหานโยบาย และการดำเนินการ

5.4.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูล การพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังต่อไปนี้

1) รหัสผ่านสำหรับการเข้าสู่ระบบถือเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสผู้ใช้ของตน ให้บุคคลอื่น
2) ผู้ใช้ต้องกำหนดและใช้รหัสผ่านที่มีประกอบด้วย ตัวเลข สัญลักษณ์ และตัวอักษร รวมกันมากกว่า 8 ตัวอักษร
3) ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ ทุก ๆ 90 วัน ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตาม และผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำกับของเดิม หรือไม่ใช้วิธีเปลี่ยนตัวเลขต่อท้ายในรหัสผ่าน
4) ผู้ใช้ต้องตรวจสอบว่าสิทธิ์ที่ตนได้รับในการเข้าใช้ระบบเหมาะสมกับหน้าที่ที่ตนรับผิดชอบหรือไม่ ถ้าพบว่าสิทธิที่ได้รับไม่เหมาะสมต้องแจ้งผู้บังคับบัญชาให้รับทราบเพื่อพิจารณาและปรับเปลี่ยน ให้เหมาะสม

6. การเข้ารหัสข้อมูล (Cryptography)

6.1 นโยบายมาตรการเข้ารหัสข้อมูล (Cryptographic Controls Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม และได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศเพื่อรักษาความปลอดภัยของข้อมูลทั้งในด้านความลับและความถูกต้องของข้อมูล จำเป็นต้องพิจารณาถึงการนำซอฟต์แวร์และเทคนิคต่าง ๆ มาให้ในการเข้ารหัสข้อมูลที่มีความเสี่ยง

เนื้อหานโยบาย และการดำเนินการ

6.1.1 การใช้มาตรการเข้ารหัสข้อมูล (Use of Cryptographic Controls)

นโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศต้องมีการจัดทำและปฏิบัติตาม

1) รหัสผ่านต่าง ๆ ที่เก็บอยู่ในระบบฐานข้อมูล จะถูกเข้ารหัสไว้ เจ้าของรหัส รวมถึงซอฟต์แวร์เจ้าของข้อมูลเท่านั้นที่ทราบรหัสผ่านดังกล่าว
3) เพื่อป้องกันการนำข้อมูลออกสู่ภายนอกจากอุปกรณ์คอมพิวเตอร์ผ่าน USB Port หน่วยงานเทคโนโลยีสารสนเทศทำการLock ไม่ให้พนักงานสามารถใช้งาน USB Port ได้
3) ในการรับส่ง Email ได้ทำการเปิดใช้งานการเข้ารหัส (Encryption) โดยทำการเข้ารหัสในระดับของ Field ข้อมูล

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

7. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

7.1 นโยบายพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Areas Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในองค์กร และกำหนดมาตรการป้องกันที่เหมาะสมตามระดับของความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศขององค์กรขั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับการอนุญาต ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคาม และการรบกวนไม่ว่าโดยตั้งใจหรือจากภัยธรรมชาติ

เนื้อหานโยบาย และการดำเนินการ

7.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

หน่วยงานได้จัดหาที่ต้อง ห้อง Server ที่มีสภาพแวดล้อมภายนอกปลอดภัยจากภัยคุกคามภายนอก คือ อยู่ในสถานที่ ๆ เข้าถึงได้โดยยากจากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้

7.1.2 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing Office, Room and Facilities)

มีการจัดเตรียมอุปกรณ์รักษาความปลอดภัยในการเข้าถึงห้อง Server ดังนี้

1) มีการติดตั้งกล้องวงจรปิด และบันทึกภาพภายในห้องตลอดเวลา โดยสามารถ**ดูข้อมูลย้อนหลังได้ 30 วัน**
2) ห้องระบบคอมพิวเตอร์ต้อง**ติดตั้งระบบประตูอัตโนมัติ** ที่สามารถปิดทันทีโดยอัตโนมัติหลังจากที่เปิดประตูแล้ว และจะต้องมีสัญญาณเตือนเมื่อมีการเปิดประตูทิ้งไว้

7.1.3 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environmental Threats)

การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ

1) ศูนย์คอมพิวเตอร์ ต้องมีระบบป้องกันอัคคีภัย ระบบปรับอากาศและความชื้น ระบบกระแสไฟฟ้า
2) เครื่องปรับอากาศ มี 2 ชุดทำงานสลับกัน โดยตั้งความเย็นอยู่ที่ไม่เกิน 20 องศา และมีความชื้นอยู่ที่ไม่เกิน 45%

7.2 นโยบายเกี่ยวกับการจัดการอุปกรณ์ (Equipment Management Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินการขององค์กร อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายถือว่าเป็นอุปกรณ์ที่สำคัญต่อสารสนเทศและการดำเนินธุรกิจ ดังนั้น อุปกรณ์เหล่านี้ควรมีการป้องกันอันตรายจากสภาพแวดล้อม รวมถึงการจำกัดการนำอุปกรณ์ดังกล่าวไปใช้นอกสถานที่

เนื้อหานโยบาย และการดำเนินการ

7.2.1 การติดตามการทำงานของเครื่องแม่ข่าย (Server Monitor)

มีการจัดทำรายงานสถานการณ์ทำงานของเครื่องแม่ข่ายต่าง ๆ รวมถึงอุปกรณ์รอบข้างที่จำเป็น เป็นประจำทุกวัน โดยผู้ปฏิบัติจะทำการบันทึกสถานการณ์การทำงานต่าง ๆ ใน รายการสถานการณ์ทำงานของคอมพิวเตอร์แม่ข่าย (IT-003) และมีการจัดทำรายงานสรุปสถานการณ์ทำงานของเครื่อง Server ให้กับทางผู้บริหารให้ทราบเป็นประจำทุก 1 เดือน

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

7.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้องได้รับการป้องกันการล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่าง ๆ

1) อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สำคัญต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน (UPS) เพื่อให้ระบบทำงานต่อเนื่องหรือสิ้นสุดการทำงานอย่างเหมาะสมเมื่อระบบไฟฟ้าขัดข้อง

2) ต้องทำการตรวจสอบอุปกรณ์สำรองไฟฟ้าฉุกเฉินตามขั้นตอนของผู้ผลิตอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าวสามารถรองรับการทำงานได้เมื่อเกิดปัญหาไฟฟ้าขัดข้อง

3) ต้องพิจารณาใช้ระบบเครื่องกำเนิดไฟฟ้าสำรอง (Power Generator) กับระบบที่มีความสำคัญในการดำเนินธุรกิจขององค์กรที่มีความจำเป็นต้องทำงานต่อเนื่อง

4) ต้องทำการทดสอบและตรวจสอบความพร้อมของเครื่องกำเนิดไฟฟ้าสำรอง รวมทั้งแหล่งพลังงานสำรองอย่างน้อยทุกเดือน

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

8. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

8.1 นโยบายการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities Policy)

จุดประสงค์และขอบเขต

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย เพื่อทำให้เกิดการปฏิบัติงานด้านระบบประมวลผลที่มีความปลอดภัยและถูกต้อง ควรกำหนดหน้าที่ ความรับผิดชอบ และกระบวนการด้านการจัดการและปฏิบัติงานของระบบประมวลผลที่ชัดเจน ซึ่งหน้าที่ความรับผิดชอบที่กำหนดนี้ ควรพิจารณาถึงการแบ่งแยกหน้าที่ที่เหมาะสม นอกจากกระบวนการทำงานปกติแล้ว ควรมีการกำหนดขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์กระทบความปลอดภัยขึ้นในระบบประมวลผล เพื่อรองรับกับเหตุการณ์ดังกล่าว

เนื้อหานโยบาย และการดำเนินการ

8.1.1 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

การใช้ทรัพยากรของระบบต้องมีการติดต่อ ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ หน่วยงานเทคโนโลยีสารสนเทศ จึงได้จัดทำ แผนแม่แบบเทคโนโลยีสารสนเทศ (IT-010) เพื่อทำให้เกิดความมั่นใจว่าสารสนเทศขององค์กรมีความปลอดภัย และสามารถเข้าถึงและใช้งานได้ตามสิทธิ์โดยง่าย มีการจัดเตรียมซอฟต์แวร์ คอมพิวเตอร์ และอุปกรณ์ต่าง ๆที่คอยสนับสนุนการทางานของหน่วยงานตาม ๆ ตามแผนกลยุทธ์ภาพรวมองค์กร

8.2 นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware Policy)

จุดประสงค์และขอบเขต

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี เพื่อควบคุม และป้องกันซอฟต์แวร์ และข้อมูล จากโปรแกรมที่ไม่ประสงค์ดีและซอฟต์แวร์อันตราย

เนื้อหานโยบาย และการดำเนินการ

8.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against Malware)

มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกัน Virus Version ล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่อง Server โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา
2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้โปรแกรมค้นหา Virus ทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย
3) ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตมีการตรวจหา Virus ก่อนนำไปใช้งาน
4) ห้ามพนักงานดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนา Virus หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ
5) ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้นต้องตรวจสอบ Virus คอมพิวเตอร์ก่อนใช้งานทุกครั้ง

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

8.6 นโยบายการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

เนื้อหานโยบาย และการดำเนินการ

8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิค จุดอ่อนต่อช่องโหว่ขององค์กร มีการเก็บรวบรวม และการการประเมิน และเตรียมมาตรการที่เหมาะสมต้องถูกนำมาใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง โดยช่องโหว่ทั้งหมดจะถูกจัดเก็บไว้ที่เอกสาร ช่องโหว่ทางเทคนิค (IT-014) และช่องโหว่ทั้งหมดจะถูกนำมาทวนสอบกับคณะกรรมการความมั่นคงอย่างน้อยปีละ 1 ครั้ง

8.7 นโยบายตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations Policy)

จุดประสงค์และขอบเขต

เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินระบบให้บริการ

เนื้อหานโยบาย และการดำเนินการ

8.7.1 มาตรการตรวจประเมินระบบ (Information Systems Audit Controls)

ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการต้องมีการวางแผนและตกลงร่วมกันอย่างระมัดระวัง เพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ หน่วยงานเทคโนโลยีสารสนเทศ จะทำการกำหนดแผนการประเมินระบบสำคัญต่าง ๆ ไว้ใน รายการตรวจประเมินระบบ (IT-015) และนำผลการตรวจประเมินเสนอคณะกรรมการบริหารความมั่นคงตามกำหนดระยะเวลา

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

9. ความมั่นคงปลอดภัยสำหรับข้อมูลสารสนเทศ (Communications Security)

9.1 นโยบายบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการป้องกันสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ เพื่อทำให้ระบบเครือข่ายมีความปลอดภัย และสามารถใช้เป็นสื่อในการรับส่งข้อมูลต่าง ๆ ได้อย่างมีประสิทธิภาพ

เนื้อหานโยบาย และการดำเนินการ

9.1.1 มาตรการเครือข่าย (Network Controls)

เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่าง ๆ หัวหน้าหน่วยงานควบคุมระบบเครือข่ายต้องรับผิดชอบในการจัดให้มีการควบคุมการปฏิบัติการด้านเครือข่าย ดังต่อไปนี้

1) กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร (IT-016) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สายที่ใช้ในการสื่อสารของเครือข่ายทั้งหมดอย่างชัดเจน โดยจัดทำและปรับปรุง แผนภาพเครือข่าย (IT-016) ให้ทันสมัยอยู่เสมอ
2) จัดให้มีการควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่จัดไว้
3) มีมาตรการในการควบคุมดูแลสภาพและประเมินประสิทธิภาพการใช้งานของคู่สาย สายสื่อสารและอุปกรณ์ในเครือข่ายสื่อสาร เพื่อให้พร้อมใช้งานตลอดเวลา
4) บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ
5) ประเมินประสิทธิภาพของระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และวางแผนในการปรับปรุงระบบเครือข่ายให้สามารถรองรับปริมาณงานที่จะขยายตัวในอนาคต

9.1.2 ความมั่นคงปลอดภัยสาหรับบริการเครือข่าย (Security of Network Services)

กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าบริการเหล่านี้จะมีการให้บริการโดยองค์กรเองหรือจ้างการให้บริการก็ตาม ผู้ให้บริการทางเครือข่าย ต้องได้รับการตรวจสอบ และวิเคราะห์ในเรื่องระดับการให้บริการ รูปแบบความปลอดภัยของเครือข่าย การจัดการความต้องการขององค์กร

9.2 นโยบายการถ่ายโอนสารสนเทศ (Information Transfer Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กร และถ่ายโอนกับหน่วยงานนอกองค์กร

เนื้อหานโยบาย และการดำเนินการ

9.2.1 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)

สารสนเทศที่เกี่ยวข้องกับการส่งข้อความอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม

9.2.2 การตรวจสอบรายการการใช้งานเครือข่าย (Network Monitoring)

หน่วยงานสารสนเทศมีการตรวจสอบการใช้งานเครือข่าย ของฝ่ายต่าง ๆ และมีการจัดทำ รายงานสรุปการใช้งานเครือข่าย (IT-017) เพื่อนำเสนอต่อคณะกรรมการความมั่นคงตามกำหนดระยะเวลา

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

9.3 นโยบายด้านคอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกล (Mobile Device and Teleworking Policy)

จุดประสงค์และขอบเขต

เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกล เช่น การ Remote เข้ามาทำงานที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) จากทั้งภายใน และภายนอกองค์กร

เนื้อหานโยบาย และการดำเนินการ

9.3.1 การปฏิบัติการจากระยะไกล (Teleworking)

เป็นมาตรการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกล ต้องมีการนำมาใช้เพื่อป้องกันข้อมูลที่มีการเข้าถึง การประมวลผล หรือการจัดเก็บจากสถานที่ดังกล่าว

1) มีการระบุอย่างชัดเจนว่า ใครสามารถที่จะ Remote เข้ามาทำงานได้
2) กรณีที่ต้องให้หน่วยงานภายนอก Remote เข้ามา ต้องมีการบันทึก และมีการเฝ้าดูการทำงานตลอดเวลา และมีการเปลี่ยนแปลง Password ในการเข้าใช้ของหน่วยงานภายนอกทุกครั้ง หรือมีการกำหนด Expired User/Password
3) มีการกำหนด Session Timeout กรณีที่ผู้ Remote เข้ามาปล่อยหน้าจอทิ้งไว้
4) จัดทำบันทึกการเชื่อมต่อระยะไกลใน รายการเชื่อมต่อระยะไกล (IT-018)

9.3.2 การปฏิบัติการใช้งานคอมพิวเตอร์พกพา และอุปกรณ์แบบพกพา (Notebook and Mobile Device)

เป็นการควบคุมการใช้งานอุปกรณ์พกพาเฉพาะที่เป็นของบริษัท และอุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัท

1) บริษัทมีนโยบายให้ผู้ใช้งานใช้อุปกรณ์พกพาเฉพาะที่เป็นของบริษัทในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัทเท่านั้นหากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท ต้องได้ รับการอนุมัติจากหัวหน้าหน่วยงาน และหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศก่อนการใช้งาน
2) บริษัทขอสงวนสิทธิ์ ในการตรวจสอบ ระงับเพิกถอนการใช้งาน และลบข้อมูลทั้งหมด บนอุปกรณ์พกพาทั้งที่เป็นของบริษัทและของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บ ข้อมูลและสารสนเทศของบริษัท หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐานหรือ ข้อมูลสารสนเทศของบริษัท
3) บริษัทไม่อนุญาตให้ผู้ใช้ทำการติดตั้ง และแก้ไขเปลี่ยนแปลงโปรแกรมในอุปกรณ์พกพาเฉพาะที่เป็นของบริษัท โดยการพลการซึ่งการติดตั้งโปรแกรมเพิ่มเติม ผู้ใช้งานต้องทำการกรอกแบบฟอร์ม IT-007 โดยได้รับอนุมัติจากหัวหน้างานและ หัวหน้าแผนกสารสนเทศเท่านั้น แต่หากโปรแกรมที่ต้องการติดตั้งเพิ่มเติมต้องมีรายละเอียดในการสั่งซื้อนั้น จำเป็นต้องได้รับการอนุมัติเพิ่มเติมจากผู้บริหารระดับสูงในการดำเนินการ
4) อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท จะต้องเป็นอุปกรณ์พกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย รวมทั้งต้องกำหนดค่ารหัสผ่านและติดตั้งระบบป้องกันหน้าจออุปกรณ์ เพื่อป้องกันการเข้าถึงอุปกรณ์ในขณะไม่ใช้งานตามนโยบายที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด
5) อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท จะต้องเป็นอุปกรณ์พกพาที่ติดตั้งโปรแกรมป้องกันไวรัส ซึ่งต้องมีการอัพเดทล่าสุดอยู่เสมอ และการใช้สื่อบันทึกข้อมูลต้องมีการตรวจสอบหาไวรัสโดย โปรแกรมป้องกันไวรัสทุกครั้ง
6) ผู้ใช้งานที่นำอุปกรณ์พกพาส่วนตัวและอุปกรณ์พกพาเฉพาะที่เป็นของบริษัทต้องไม่เก็บข้อมูลสำคัญของบริษัท ไว้บนอุปกรณ์พกพาที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลสารสนเทศของบริษัท

10. การจัดหา การพัฒนาและการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

10.1 นโยบายด้านความมั่นคงปลอดภัยของระบบ (Security Requirements of Information Systems Policy)

จุดประสงค์และขอบเขต

การควบคุมการจัดหา การพัฒนา การบำรุงรักษาและแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ การทดสอบจนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง โดยมีอ้างอิงเพื่อประกอบนโยบาย การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบคอมพิวเตอร์ (IT-008)

เนื้อหานโยบาย และการดำเนินการ

10.1.1 การวิเคราะห์ความต้องการ ความปลอดภัยของข้อมูลและข้อกำหนด (Information Security Requirements Analysis and Specification)

ความต้องการในการพัฒนาระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้ว ต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศโดยมีขั้นตอนการดำเนินการดังนี้

1) ผู้ร้องขอพัฒนาระบบ และเจ้าของระบบงาน ต้องกำหนดความต้องการพัฒนาหรือจัดหาระบบงานภายใต้ความปลอดภัยสารสนเทศ ก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจัดทำเป็นเอกสาร Software Develop Form (IT-019) ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงานโดย เอกสาร Software Develop Form (IT-019) ต้องมีความครบถ้วนในเนื้อหาของการพัฒนาหรือจัดหาระบบงาน และบันทึกในเอกสาร รายการบันทึกเอกสาร Software Develop Form (IT-027)
2) ความต้องการที่เกิดขึ้น จะต้องได้รับการอนุมัติจากผู้มีสิทธิ์อนุมัติตามเอกสาร Software Develop Form (IT-019) ก่อนส่งมายัง หน่วยงานเทคโนโลยีสารสนเทศถึงความเป็นไปได้ในการพัฒนาหรือจัดหาระบบงาน เพื่อให้ผู้บริหารระดับสูงพิจารณาอนุมัติ
3) ในการร้องขอพัฒนาระบบทางเจ้าหน้าที่สารสนเทศจะทำการเปิด Ticket Service request ในระบบ Helpdesk system และจะปิด Ticket Service request นั้นก็ต่อเมื่อได้ข้อสรุปของการร้องขอพัฒนาระบบ
4) กรณีการร้องขอพัฒนาระบบได้รับอนุมัติผู้บริหารระดับสูงทางเจ้าหน้าที่สารสนเทศจะทำการเปิด Project ในระบบ Helpdesk System เพื่อควบคุมการดำเนินการร้องขอพัฒนาระบบ และ และบันทึกในเอกสาร รายการบันทึกเอกสาร Software Develop Form (IT-027)

10.2 นโยบายสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes Policy)

จุดประสงค์และขอบเขต

เพื่อให้ความต้องการในการพัฒนาระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้ว อยู่ภายใต้ความมั่นคงปลอดภัยสารสนเทศต้องมีการออกแบบ และดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ (System development Life Cycle : SDLC)

เนื้อหานโยบาย และการดำเนินการ

10.2.1 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบ (System development Life Cycle : SDLC) มีการควบคุมโดยปฏิบัติตามขั้นตอนสำหรับการเปลี่ยนแปลง ระบบที่กำหนดไว้อย่างเป็นทางการ โดยหน่วยงานเทคโนโลยีสารสนเทศจะทำการปรับปรุงในเอกสารควบคุมเวอร์ชั่นโปรแกรม(IT-020)

10.2.2 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

การทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการทำ User Acceptance Test (UAT) สำหรับในการพัฒนาระบบใหม่หรือการปรับปรุงระบบที่มีอยู่แล้วดังนี้

1) กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อให้มั่นใจว่า ข้อมูลที่ได้มีความถูกต้องสมบูรณ์ ทั้งนี้ การตรวจสอบควรครอบคลุมถึงความต้องการพัฒนาระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้ว
2) ผู้ร้องขอ เจ้าของระบบงาน และผู้จัดการฝ่ายสารสนเทศจะต้องเป็นผู้ทดสอบ และตรวจรับระบบตามเอกสาร Software Develop Form (IT-019) และบันทึกในเอกสาร รายการบันทึกเอกสาร Software Develop Form (IT-027)
3) ผู้พัฒนาระบบต้องจัดทำเอกสาร Customization Signoff เพื่อยืนยันการตรวจรับระบบ

10.3 นโยบายสำหรับการทดสอบข้อมูล (Test Data Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

เนื้อหานโยบาย และการดำเนินการ

10.3.1 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกัน เพื่อลดความเสี่ยงของการเข้าถึง หรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

1) การพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) ระบบที่ใช้งานจริง (Production System) และ ระบบเพื่องานทดสอบ (Testing system)
2) การพัฒนาระบบ ต้องไม่มีการติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาโปรแกรมอื่น ๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง (Production System)
3) การพัฒนาระบบ โดยโอนย้าย หรือติดตั้ง โปรแกรมที่พัฒนาเสร็จ ไปยังระบบที่ใช้งานจริง (Production System) ต้องตรวจสอบ Version ของการพัฒนาระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้วให้ตรงกับ Version ที่อ้างถึงในส่วนของการรับรองระบบทดสอบ (Acceptance Testing)
4) การพัฒนาระบบ โดยโอนย้าย หรือติดตั้ง โปรแกรมที่พัฒนาเสร็จ ไปยังระบบที่ใช้งานจริง (Production System) ต้องระบุผู้รับผิดชอบในการติดตั้ง วันที่ติดตั้ง สถานที่ติดตั้ง ชื่อเซิฟเวอร์ที่ติดตั้ง เส้นทางของโปรแกรมที่ติดตั้งรวมถึงชื่อของไฟล์โปรแกรมที่ติดตั้งและ Version ในเอกสาร Software Develop (IT-019) และผู้จัดการฝ่ายสารสนเทศเป็นผู้ตรวจรับ และบันทึกในเอกสาร รายการบันทึกเอกสาร Software Develop Form (IT-027)
5) การพัฒนาระบบในการควบคุม Version หน่วยงานเทคโนโลยีสารสนเทศจะทำการปรับปรุงในเอกสารควบคุมเวอร์ชั่นโปรแกรม(IT-020) รวมถึงการรวบรวมเอกสารการใช้งาน เอกสารประกอบ และติดตามผู้ให้บริการ

10.4 นโยบายสำหรับการสื่อสารการเปลี่ยนแปลง (Communicate of change policy)

จุดประสงค์และขอบเขต

เพื่อสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

เนื้อหานโยบาย และการดำเนินการ

10.4.1 การสื่อสารการเปลี่ยนแปลง (Communicate of change)

กำหนดให้มีการแจ้งผู้ที่เกี่ยวข้องทางอีเมล์ (e-mail) และจัดอบรม(Training) ในการพัฒนาระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้วโดยได้ระบุตัวผู้สื่อสารรวมถึงช่องทางการสื่อสารในเอกสาร Software Develop (IT-019) และบันทึกในเอกสาร รายการบันทึกเอกสาร Software Develop Form (IT-027)

11. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

11.1 นโยบายเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

เนื้อหานโยบาย และการดำเนินการ

11.1.1 ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินขององค์กรโดยผู้ให้บริการภายนอก ต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกและจัดทำเป็นลายลักษณ์อักษร

11.2 นโยบายการจัดการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงให้บริการของผู้ให้บริการภายนอก เพื่อจัดทำ และรักษาระดับความปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่ได้จัดทำไว้

เนื้อหานโยบาย และการดำเนินการ

11.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services)

องค์กรต้องมีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

1) ต้องมีการตรวจสอบการให้บริการจากหน่วยงานภายนอก ผู้ทำหน้าที่ตรวจสอบจำเป็นต้องมีความรู้ ความเข้าใจในเรื่องความปลอดภัยสารสนเทศ ตลอดจนเงื่อนไขและข้อตกลงต่าง ๆ
2) ในกรณีที่มีเหตุการณ์ที่กระทบต่อความปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการ เพื่อรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมายในกรณีที่จำเป็น
3) มีการตรวจประเมินผู้ให้บริการจากภายนอกทุกปี โดยจัดทำใน รายงานการตรวจประเมินผู้ให้บริการภายนอก (PUR-014)

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

12. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1 นโยบายการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และการปรับปรุง (Management of Information Security Incidents and Improvements Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ เพื่อให้มีวิธีการที่สอดคล้อง และได้ผลในการบริหารจัดการเหตุการณ์ ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

เนื้อหานโยบาย และการดำเนินการ

12.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการต้องมีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำระบบ Helpdesk tool system สำหรับการรับแจ้งปัญหา

12.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

ประเด็นปัญหาต่าง ๆ ที่ได้รับแจ้ง และได้ดำเนินการแก้ไขเสร็จแล้วตามกำหนดระยะเวลา จะถูกนำข้อมูลดังกล่าวมาประมวลผลเพื่อสรุปออกมาเป็นรายงาน เพื่อแสดงให้เห็นว่าในช่วงเวลาที่ผ่านมานั้น มีปัญหาเรื่องอะไรมากที่สุด สาเหตุของปัญหาดังกล่าวเกิดจากอะไร และจะมีวิธีการป้องกันไม่ให้ปัญหานั้นเกิดขึ้นมาได้อย่างไร โดยหน่วยงานเทคโนโลยีสารสนเทศ จะทำรายงานสรุปดังกล่าว เพื่อนำเสนอ คณะกรรมการความมั่นคงปลอดภัยสารสนเทศ เป็นประจำทุก 3 เดือน เพื่อร่วมพิจารณาปัญหาและวางแนวทางป้องกันปัญหาที่เกิดขึ้นในอนาคต

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

13. การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

13.1 นโยบายความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันและรับมือกับการหยุดชะงักของการดำเนินธุรกิจ อันเนื่องมาจากภัยคุกคามต่อการทำงานของระบบ ไม่ว่าจะด้วยอุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหาย ต่อองค์กรไม่มากก็น้อย ดังนั้นจึงควรจัดทำแผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ เพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักขององค์กรต่อไปได้

เนื้อหานโยบาย และการดำเนินการ

13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity)

องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสภาพการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดภัยพิบัติ ผู้บริหารหรือหน่วยงานที่เกี่ยวข้องต้องมีการจัดการกระบวนการต่าง ๆ เพื่อพัฒนาและคงไว้ซึ่งความต่อเนื่องทางธุรกิจ การจัดการกระบวนการต่าง ๆ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจดังกล่าว ต้องคำนึงถึงสิ่งต่าง ๆ ดังต่อไปนี้

1) การวิเคราะห์และการประเมินความเสี่ยงที่กระทบต่อการดำเนินธุรกิจขององค์กร
2) การจัดทำเอกสารกลยุทธ์เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ ต้องสอดคล้องกับเป้าหมายทางธุรกิจ ขององค์กร
3) การฝึกอบรมพนักงาน เพื่อให้ตระหนักถึงความมั่นคงปลอดภัย และเข้าใจในแผนฯ พร้อมทั้งสามารถปฏิบัติตามแผนฯ ได้
4) การกำหนดหน้าที่ความรับผิดชอบในการประสานงาน การพัฒนา การตรวจทาน และการปรับปรุงแผน

13.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)

องค์กรต้องกำหนด จัดทำ การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (IT-022) และปรับปรุงกระบวนการ ขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

1) มีการสื่อสารไปยังพนักงานทุกคนทราบถึงแผนการดำเนินการเมื่อเกิดเหตุฉุกเฉิน
2) แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่าง ๆ ต้องมีการทดลอง ซักซ้อม ตามระยะเวลาที่กำหนด
3) เจ้าของแผนงานและแนวทางปฏิบัติซึ่งเจ้าของแผนฯ ต้องรับผิดชอบในการบำรุงรักษา และทดสอบ พัฒนาหลักเกณฑ์ความต้องการและเงื่อนไขสำหรับการนำแผนฯ ไปใช้

13.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review And Evaluate Information Security Continuity)

องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมไว้ (IT-022) ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้อง และได้รับผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น พื้นฐานของการจัดการเพื่อให้เกิดความต่อเนื่องในการดำเนินธุรกิจคือ เข้าใจถึงกระบวนการ และเหตุการณ์ที่สามารถก่อให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจ ดังนั้น หน่วยงานเจ้าของกระบวนการรวมถึงหน่วยงานเจ้าของระบบงานธุรกิจที่สนับสนุนกระบวนการธุรกิจนั้นต้องเข้าร่วมในการดำเนินการ ระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจตลอดจนการประเมินความเสี่ยงเพื่อให้ได้มา ซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วนในการดำเนินการจัดทำแผนบริหารจัดการความต่อเนื่องทางธุรกิจในการดำเนินธุรกิจลำดับต่อไป

13.2 นโยบายการเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies Policy)

จุดประสงค์และขอบเขต

เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

เนื้อหานโยบาย และการดำเนินการ

13.2.1 สภาพพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

14. ความสอดคล้อง (Compliance)

14.1 นโยบายความสอดคล้องด้านกฎหมายและสัญญาจ้าง (Compliance with Legal and Contractual Requirements Policy)

จุดประสงค์และขอบเขต

เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และที่เป็นความต้องการด้านความมั่นคงปลอดภัย

เนื้อหานโยบาย และการดำเนินการ

14.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of Applicable Legislation and Contractual Requirements)

ความต้องการทั้งหมดที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง รวมทั้งวิธีการขององค์กรเพื่อให้สอดคล้องกับความต้องการดังกล่าว ต้องมีการระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัย สำหรับแต่ละระบบและสำหรับหน่วยงาน องค์กรกำหนดให้เอกสารสัญญาต่าง ๆ ที่มีผลเกี่ยวข้องกับกฎหมาย ลิขสิทธิ์ซอฟต์แวร์ และสิทธิ์ในทรัพย์สินทางปัญญา (Intellectual Property Rights) ถูกจัดเก็บไว้ที่ หน่วยงานด้านกฎหมาย โดยจะจัดเก็บอยู่ใน แบบฟอร์มรายการสัญญา (IT-023)

14.2 นโยบายการทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบาย และขั้นตอนปฏิบัติขององค์กร

เนื้อหานโยบาย และการดำเนินการ

14.2.1 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with Security Policies and Standards)

ผู้จัดการฝ่ายต่าง ๆ มีหน้าที่ต้องดำเนินการทบทวนความสอดคล้องของขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบายมาตรฐาน และความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง คณะกรรมการความมั่นคงปลอดภัยกำหนดให้หน่วยงานความปลอดภัยสารสนเทศ นำเสนอระบบโครงสร้างสารสนเทศ ระบบความปลอดภัยหลัก เทคโนโลยีใหม่ ๆ รวมถึงข้อมูลเชิงเทคนิค กับคณะกรรมการความมั่นคงปลอดภัย ปีละ 1 ครั้ง เพื่อใช้เป็นข้อมูลในการพิจารณาความสอดคล้องกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยคณะกรรมการความปลอดภัยสารสนเทศ ได้จัดทำรายการต่าง ๆ ที่จะต้องปฏิบัติไว้ในแบบฟอร์ม การทวนสอบความมั่นคงปลอดภัยสารสนเทศ (IT-024) เพื่อใช้เป็นตัวกลางในการตรวจสอบการทวนสอบขั้นตอนต่าง ๆ ว่าได้ปฏิบัติตามครบถ้วนหรือไม่

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591

เอกสารและแบบฟอร์มประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ

SIAMESE ASSET PUBLIC COMPANY LIMITED 1077/48 Phahon Yothin Road, Sam Sen Nai Subdistrict, Phaya Thai District, Bangkok 10400 Tel. 0-2617-1555 Fax. 0-2617-1591 www.siameseasset.co.th
บริษัท ไซมิส แอสเสท จำกัด (มหาชน) 1077/48 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400 โทรศัพท์ 0-2617-1555 โทรสาร 0-2617-1591