



สมาคมสโมสรนักลงทุน

INVESTOR CLUB ASSOCIATION

1 อาคาร ทีพี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โทร. 0 2666 9449

1 TP & T Tower, 12th FL., Vibhavadi Rangsit Rd., Chatuchak, Chatuchak, Bangkok 10900 Tel. 0 2666 9449

IC-PUA 6/2568

ประกาศสมาคมสโมสรนักลงทุน

เลขที่ IC-PUA 6/2568

เรื่อง สอบราคาโครงการพัฒนาและปรับปรุง IC Website

สมาคมสโมสรนักลงทุน ซึ่งต่อไปนี้จะเรียกว่า "สมาคม" มีความประสงค์จะสอบราคาโครงการพัฒนาและปรับปรุง IC Website โดยมีข้อแนะนำและข้อกำหนด ดังต่อไปนี้

1. เอกสารแนบท้ายเอกสารสอบราคา

- 1.1 ขอบเขตงาน (Terms of Reference: TOR) โครงการพัฒนาและปรับปรุง IC Website
- 1.2 แบบใบเสนอราคา
- 1.3 แบบสัญญา
- 1.4 แบบหนังสือค้ำประกัน
 - (1) หลักประกันสัญญา
- 1.5 แบบบัญชีเอกสาร
 - (1) บัญชีเอกสารส่วนที่ 1
 - (2) บัญชีเอกสารส่วนที่ 2
- 1.6 ระเบียบปฏิบัติงานขั้นตอนการพัฒนาระบบ (System Development Procedure) รหัสเอกสาร : IT-2PR-05
- 1.7 ระเบียบปฏิบัติงานนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัสเอกสาร:IT-1PC-01
- 1.8 แบบฟอร์มเอกสารการตรวจสอบการตั้งค่าตามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Secure Configuration Baseline_V.1.0) รหัสเอกสาร: IT-2FM-10

2. คุณสมบัติผู้เสนอราคา

2.1 ผู้เสนอราคาต้องมีอาชีพที่เกี่ยวข้องกับการรับจ้างบริการออกแบบ ปรับปรุงและพัฒนาเว็บไซต์ ด้วยเทคโนโลยีที่ใช้สำหรับพัฒนาเว็บไซต์ที่ทันสมัย โดยให้มีระบบการบริหารจัดการข้อมูลเว็บไซต์ได้ด้วยตนเอง โดยมีผลงานและประสบการณ์ที่เกี่ยวข้องกับการดำเนินงานในลักษณะเดียวกันหรือใกล้เคียงให้กับหน่วยงานราชการหรือหน่วยงานเอกชนอย่างน้อย 2 ผลงาน โดยมีผลงานที่ดำเนินการมาไม่เกิน 2 ปี และมูลค่าของผลงานต่อ 1 เว็บไซต์ ไม่น้อยกว่า 200,000 บาท โดยแนบสำเนาสัญญาหรือหนังสือรับรองผลงานจ้างจากผู้ว่าจ้างมาพร้อมการเสนอราคา

2.2 ผู้เสนอราคาต้องมีทุนจดทะเบียนไม่น้อยกว่า 1 ล้านบาท โดยมีหลักฐานการจดทะเบียน ซึ่งกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ออกให้หรือรับรองไม่เกิน 6 เดือน

2.3 ผู้เสนอราคาต้องไม่เป็นผู้ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานของราชการ และทางส่วนราชการได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคล หรือบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ

2.4 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นนั้น

2.5 ผู้เสนอราคาจะต้องปฏิบัติตามวิธีปฏิบัติงาน ตามขั้นตอนการพัฒนาระบบ (System Development Procedure) รหัสเอกสาร : IT-2PR-05

2.6 ผู้เสนอราคาจะต้องปฏิบัติตามระเบียบปฏิบัติงาน ตามนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัสเอกสาร:IT-1PC-01

2.7 ผู้เสนอราคาจะต้องปฏิบัติตามระเบียบปฏิบัติงาน ตามเอกสารการตรวจสอบการตั้งค่าตามนโยบาย และแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Secure Configuration Baseline_V.1.0) รหัสเอกสาร: IT-2FM-10

3. หลักฐานการเสนอราคา

ผู้เสนอราคาจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมกับซองใบเสนอราคา โดยแยกไว้ในซองของใบเสนอราคาเป็น 3 ส่วน คือ

3.1 ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้ (ข้อมูลบริษัททั่วไป)

(1) ผู้เสนอราคาต้องเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญ หรือ ห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วน ผู้จัดการ ผู้มีอำนาจควบคุม พร้อมรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัด หรือ บริษัท (มหาชน) จำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุมและบัญชีผู้ถือหุ้นรายใหญ่ พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้เสนอราคาเป็นผู้เสนอการาร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (1)

(3) หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมาย ในกรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน

(4) บัญชีเอกสารส่วนที่ 1 (ข้อมูลบริษัททั่วไป)

3.2 ส่วนที่ 2 ข้อเสนอแนะด้านเทคนิค

- (1) ตารางเปรียบเทียบระหว่างข้อกำหนดของสมาคมกับข้อเสนอของบริษัท พร้อมเอกสารประกอบรายละเอียดข้อเสนอบริษัท

ลำดับที่	รายละเอียดที่กำหนด	รายละเอียดที่เสนอ	หน้าที่อ้างอิง

- (2) ประวัติและผลการทำงาน และประสบการณ์ของทีมงาน
- (3) แนวคิดการออกแบบเว็บไซต์สมาคม และแสดง Demo
- (4) ด้านข้อเสนอโครงการ แผนการดำเนินงาน (Work Plan)
- (5) รายละเอียดหรือข้อมูลพื้นที่บริการรับฝากเว็บไซต์
- (6) แนวทางในการแก้ไขปัญหา กรณีมีปัญหาเกี่ยวกับอุปกรณ์ระบบและบริการ
- (7) แผนการบำรุงรักษาและค่าใช้จ่ายในการบำรุงรักษาในระยะเวลา 1 ปี

3.3 ส่วนที่ 3 ข้อเสนอแนะด้านราคา

- (1) ใบเสนอราคาตามแบบเอกสารแนบ 1.2 (ปิดผนึก)

4. การเสนอราคา

4.1 ผู้เสนอราคาต้องยื่นเสนอราคาตามแบบที่กำหนดไว้ในเอกสารสอบราคานี้ โดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น และจะต้องกรอกข้อความให้ถูกต้องครบถ้วน ลงลายมือชื่อของผู้เสนอราคาให้ชัดเจน จำนวนเงินที่เสนอต้องระบุตรงกันทั้งตัวเลขและตัวอักษร โดยไม่มีการขูดลบหรือแก้ไข หากมีการขูดลบ ตก เต็ม แก้ไขเปลี่ยนแปลง จะต้องลงลายมือชื่อผู้เสนอราคาพร้อมประทับตรา (ถ้ามี) กำกับไว้ทุกแห่ง

4.2 ผู้เสนอราคาจะต้องเสนอราคาเป็นเงินบาท และเสนอราคาต่อหน่วย และหรือต่อรายการตามเงื่อนไขที่ระบุไว้ให้ถูกต้อง ทั้งนี้ ราคารวมที่เสนอจะต้องตรงกันทั้งตัวเลขและตัวหนังสือ ถ้าตัวเลขและตัวหนังสือไม่ตรงกันให้ถือตัวหนังสือเป็นสำคัญ โดยคิดราคารวมทั้งสิ้นซึ่งไม่รวมค่าภาษีมูลค่าเพิ่ม แต่รวมภาษีอากรอื่น ค่าขนส่ง ค่าจดทะเบียน และค่าใช้จ่ายอื่น ๆ ทั้งปวง จนกระทั่งส่งมอบงานทุกอย่างให้ ณ สมาคมสโมสรนักร้อง เลขที่ 1 อาคาร ที พี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 ราคาที่เสนอ จะต้องเสนอกำหนดยื่นราคาไม่น้อยกว่า 60 วัน นับแต่วันยื่นซองเสนอราคาโดยภายในกำหนดยื่นราคาผู้เสนอราคาต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และจะถอนการเสนอราคามีได้

4.3 ก่อนยื่นซองข้อเสนอ ผู้เสนอราคาควรตรวจดู ข้อกำหนด รายละเอียด และขอบเขตงาน ฯลฯ ให้ถี่ถ้วนและเข้าใจเอกสารสอบราคาทั้งหมดเสียก่อนที่จะตกลงยื่นซองสอบราคาตามเงื่อนไขในเอกสารสอบราคา

4.4 ผู้เสนอราคาจะต้องยื่นซองใบเสนอราคาที่ปิดผนึกของเรียบร้อย จ่าหน้าซองถึง ประธานคณะกรรมการจัดซื้อจัดจ้าง โดยระบุไว้ที่หน้าซองว่า “ใบเสนอราคาตามเอกสารสอบราคา เลขที่ IC-PUA 6/2568” ยื่นต่อพนักงานภายในวันและเวลาที่กำหนด เมื่อพ้นกำหนดเวลายื่นซองสอบราคาแล้วจะไม่รับซองสอบราคาโดยเด็ดขาด

5. หลักเกณฑ์การพิจารณาคัดเลือกจัดซื้อจัดจ้าง

5.1 คณะกรรมการจะพิจารณาเปิดซองคุณสมบัติบริษัทหรือผู้ยื่นเสนอราคา เมื่อถูกต้องตามข้อกำหนดครบถ้วนแล้ว ซึ่งสมาคมจะเชิญผู้เสนอราคาให้มาเสนอผลงานกับคณะกรรมการ รายละเอียดไม่เกิน 45 นาที รวมการตอบข้อซักถามของคณะกรรมการ โดยวัน เวลา และสถานที่ สมาคมจะแจ้งให้ทราบต่อไป

5.2 สมาคมจะพิจารณาคัดเลือกโดยใช้หลักเกณฑ์วิธีพิจารณาประสิทธิภาพต่อราคาเท่านั้น

5.3 ผู้เสนอราคาต้องระบุรายละเอียดต่างๆ เพื่อประกอบการพิจารณาดังนี้

5.3.1 คุณสมบัติของผู้เสนอราคา ประวัติและผลการดำเนินงาน ประสบการณ์ของทีมงาน

5.3.2 ผู้เสนอราคานำเสนอแนวคิดการออกแบบเว็บไซต์สมาคม และแสดง Demo ตัวอย่างแนวคิดการออกแบบ แสดงผลงานเว็บไซต์ที่เคยจัดทำ โดยมีหน้าแสดงผลบนเว็บไซต์ และ Back-end ที่แสดงให้เห็นการบริหารจัดการข้อมูลและการอัปเดตข้อมูล นำเสนอแผนการดำเนินงาน แนวทางในการใช้เทคโนโลยีหรือซอฟต์แวร์ที่เหมาะสมตามขอบเขตงาน นำเสนอขอบเขตการรับประกัน แผนการบำรุงรักษาและค่าใช้จ่ายในการบำรุงรักษาในระยะเวลา 1 ปี

5.3.3 รายละเอียดหรือข้อมูลพื้นที่บริการรับฝากเว็บไซต์ (Web Hosting)

5.4 ผู้เสนอราคาที่ผ่านมาเกณฑ์การพิจารณา จะต้องมียะเนนข้อเสนอด้านเทคนิคตั้งแต่ 80 คะแนน ขึ้นไป

5.5 เมื่อผ่านเกณฑ์พิจารณาใน ข้อ 5.4 แล้ว สมาคมจึงจะเปิดซองราคา โดยจะพิจารณาคัดเลือกเฉพาะรายที่เสนอราคาภายในวงเงินที่กำหนด และการตัดสินจะใช้วิธีประสิทธิภาพต่อราคา ซึ่งการตัดสินของคณะกรรมการถือเป็นที่สุด

เกณฑ์การพิจารณาให้คะแนน 100 คะแนน	คะแนน
1. ผลงานที่ผ่านมา / ความน่าเชื่อถือและประสบการณ์	10
2. แนวคิดในการออกแบบเว็บไซต์ที่สื่อถึงสมาคม / ความสวยงามในการออกแบบ / การจัดทำกราฟิกต่างๆ / User Friendly / มีความสะดวก / ง่ายต่อการใช้งาน	20
3. ระบบ Administration panel ที่ง่ายต่อการอัปเดตข้อมูล / ไม่ซับซ้อน	20
4. เทคโนโลยีและซอฟต์แวร์ที่นำมาใช้มีประสิทธิภาพ / มีความทันสมัย	20
5. แนวทางในการแก้ไขปัญหา กรณีมีปัญหากับอุปกรณ์ระบบงานและบริการ	20
6. แผนการบำรุงรักษาและค่าใช้จ่ายในการบำรุงรักษาในระยะเวลา 1 ปี	10
รวมคะแนน	100

6. การทำสัญญา

ผู้ชนะการสอบราคาจะต้องทำสัญญาตามแบบสัญญาดังระบุใน ข้อ 1.3 กับสมาคม ภายใน 5 วัน นับถัดจากวันที่ได้รับแจ้งจากสมาคม และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละสิบของ มูลค่าทั้งสิ้นตามสัญญาที่ประกาศสอบราคาได้ให้สมาคมยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่ง อย่างใดดังต่อไปนี้

(1) เงินโอนเข้าบัญชีสมาคม

(2) หนังสือค้ำประกันของธนาคารภายในประเทศตามแบบหนังสือค้ำประกัน ดังระบุใน ข้อ 1.4 (1) หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ยภายใน 15 วัน นับถัดจากวันที่ผู้ชนะการสอบราคา พ้นจากข้อผูกพันตาม สัญญาแล้ว

8. กำหนดยื่นซองสอบราคา

วันที่ 11 – 29 เมษายน 2568 ระหว่างเวลา 09.00-16.00 น. ณ แผนกจัดซื้อ สมาคมสโมสรนักงทุน เลขที่ 1 อาคาร ที พี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

9. กำหนดวันผู้ยื่นซองเสนอราคาชี้แจงรายละเอียดเพิ่มเติม (Present)

ระหว่างวันที่ 13-15 พฤษภาคม 2568 ณ สมาคมสโมสรนักงทุน เลขที่ 1 อาคาร ที พี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

ทั้งนี้สมาคมจะแจ้งกำหนดเวลาที่ชัดเจนแต่ละรายให้ทราบต่อไป

ผู้สนใจติดต่อขอทราบรายละเอียดได้ที่ แผนกจัดซื้อ โทรศัพท์ 02 666 9449 ต่อ 8006 หรือ 086 612 1183 (คุณเดียนรุ่ง) หรือ e-Mail : duenrunka@ic.or.th ในระหว่างวันทำการ (วันจันทร์-วันศุกร์ เวลา 09.00-16.00 น.) ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ 10 เมษายน 2568



(นางสาวรองนก มานะกิจจกมล)

ผู้จัดการสมาคมสโมสรนักงทุน

ขอบเขตของงาน (Terms of Reference: TOR)

โครงการพัฒนาและปรับปรุง IC Website

1. ความเป็นมา

ปัจจุบันสมาคมให้บริการเว็บไซต์จำนวน 3 เว็บไซต์ ได้แก่

1. เว็บไซต์สมาคม (<https://ic.or.th>) เป็นช่องทางหลักในการเข้าสู่บริการต่างๆ ของสมาคม อาทิ ระบบงาน eMT และ RMTS ระบบลงทะเบียนผู้ใช้บริการและสมาชิก ระบบการสมัครฝึกอบรม การเข้าชมคลังความรู้ เป็นต้น นอกจากนี้ยังเป็นช่องทางสำคัญในการสื่อสารข้อมูลข่าวสารผ่านไปยังสมาชิกและผู้ใช้บริการโดยตรง รวมทั้งเป็นสื่อในการสร้างภาพลักษณ์องค์กรไปสู่สาธารณชนในวงกว้าง

2. เว็บไซต์คลังความรู้ Knowledge Management (KM) (<https://km.ic.or.th>) เป็นศูนย์กลางคลังความรู้ด้านการส่งเสริมการลงทุน จากสำนักงานคณะกรรมการส่งเสริมการลงทุน และด้านงานบริการระบบงานต่างๆ ของสมาคม โดยให้บริการทั้งรูปแบบเอกสารอิเล็กทรอนิกส์ และคลิปวิดีโอ ซึ่งมุ่งเน้นความรู้เกี่ยวกับงานสิทธิและประโยชน์ด้านเครื่องจักรและวัตถุดิบแก่ผู้ใช้บริการ เพื่อการปฏิบัติงานที่ถูกต้องตามเงื่อนไขและนโยบายที่กำหนด ลดปัญหาความผิดพลาดที่จะเกิดขึ้นในอนาคต ตลอดจนให้แนวปฏิบัติในการแก้ไขปัญหาแบบเจาะลึกให้แก่ผู้ใช้บริการ จากการปฏิบัติงานที่ผิดพลาดเพื่อนำไปสู่แนวทางที่ถูกต้อง

3. เว็บไซต์สมัครหลักสูตรฝึกอบรมสัมมนาออนไลน์ (<https://icis.ic.or.th/>) เป็นช่องทางสำหรับสมาชิกและผู้ใช้บริการได้ลงทะเบียนสมัครเข้าร่วมกิจกรรมฝึกอบรมและสัมมนาในหลักสูตรต่างๆ ที่สมาคมจัดขึ้น โดยเชื่อมโยงกับระบบลงทะเบียนสมาชิก ในการเช็คสถานะสมาชิกเพื่อรับส่วนลดหรือสิทธิพิเศษต่างๆ ตลอดจนส่งข้อมูลเชื่อมโยงกับระบบบัญชีการเงิน ในการออกใบแจ้งค่าบริการ การชำระเงิน และการออกใบกำกับภาษี ให้แก่ผู้สมัครเข้ารับการฝึกอบรม เป็นต้น

นอกจากนี้ สมาคมยังมีบริการเว็บบอร์ด FAQ 108 ตอบคำถามงานส่งเสริมการลงทุน (<https://www.faq108.co.th/board/>) ให้บริการข้อมูลความรู้ด้านสิทธิประโยชน์สำหรับผู้ได้รับส่งเสริมการลงทุน โดยการให้บริการ 3 เว็บไซต์ของสมาคม และเว็บบอร์ดที่ผ่านมา มีสถิติของผู้เข้าเยี่ยมชมเว็บไซต์เพิ่มมากขึ้นทุกๆ ปี ตลอดจนในปัจจุบันมีเทคโนโลยีที่เกี่ยวข้องกับการบริหารจัดการเว็บไซต์ ที่สามารถดำเนินการพัฒนาให้เว็บไซต์มีประสิทธิภาพ ครอบคลุมถึงการเป็นเครื่องมือในการจัดการทางด้านงานสื่อสาร ทั้งภายในและภายนอกองค์กรที่มีประสิทธิภาพ รวดเร็ว คล่องตัว อีกทั้งยังสามารถเชื่อมต่อเข้ากับเครือข่ายสังคม (Social Media) ประเภทต่างๆ ทำให้สามารถเผยแพร่กระจายข่าวสารได้อย่างรวดเร็ว เข้าถึงกลุ่มเป้าหมายผู้ใช้บริการของสมาคมได้อย่างทั่วถึง

ดังนั้น การปรับปรุงเว็บไซต์ของสมาคมเพื่อให้การแสดงผลมีประสิทธิภาพดีขึ้น และพัฒนาให้มีความทันสมัย สวยงาม สะดวกในการใช้งานและค้นหาข้อมูล มีมาตรฐานในระดับสากล จะสามารถสร้างภาพลักษณ์ที่ดีให้กับสมาคม และเป็นเครื่องมือในการสนับสนุนงานบริการให้กับผู้ใช้บริการอย่างรอบด้าน และคำนึงถึงความปลอดภัยในการ

สื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตเป็นสำคัญ ด้วยระบบ Secure Sockets Layer Certificate (SSL Certificate)

2. วัตถุประสงค์

2.1 เพื่อพัฒนาและออกแบบเว็บไซต์และเว็บบอร์ดของสมาคม ซึ่งเป็นช่องทางหลักในการสื่อสารและประชาสัมพันธ์ข้อมูลข่าวสารแก่ผู้ให้บริการ ให้มีรูปแบบมีความน่าเชื่อถือ ทันสมัย และเป็นมิตรต่อผู้ให้บริการ (User Friendly)

2.2 เพื่อพัฒนาให้เว็บไซต์มีความปลอดภัย และรองรับการเข้าใช้งานผ่านอุปกรณ์คอมพิวเตอร์ และอุปกรณ์เคลื่อนที่ที่รองรับการแสดงผลเว็บไซต์

2.3 ลดความซ้ำซ้อนในการบริหารจัดการเว็บไซต์ของสมาคม ให้รวมอยู่ภายใต้เว็บไซต์เดียว

2.4 เพื่อรองรับการให้บริการเว็บไซต์คลังความรู้ ให้สามารถแสดงผล VDO ที่มีประสิทธิภาพและรวดเร็วยิ่งขึ้น ตลอดจนมีระบบ Login เพื่อกำหนดสิทธิการเข้าถึงเว็บไซต์ สร้างความแตกต่างในสิทธิประโยชน์ของสมาชิก

2.5 เพื่อเป็นช่องทางในการสื่อสารการรับสมัครหลักสูตรฝึกอบรมสัมมนาของสมาคม

2.6 เพื่อรองรับการเชื่อมต่อเว็บไซต์ของสมาคมด้วย Application Programming Interface (API) ไปยังระบบอื่นๆ ของสมาคมอย่างมีประสิทธิภาพ

3. คุณสมบัติผู้เสนอราคา

3.1 ผู้เสนอราคาต้องมีอาชีพที่เกี่ยวข้องกับการรับจ้างบริการออกแบบ ปรับปรุงและพัฒนาเว็บไซต์ ด้วยเทคโนโลยีที่ใช้สำหรับพัฒนาเว็บไซต์ที่ทันสมัย โดยให้มีระบบการบริหารจัดการข้อมูลเว็บไซต์ได้ด้วยตนเอง โดยมีผลงานและประสบการณ์ที่เกี่ยวข้องกับการดำเนินงานในลักษณะเดียวกันหรือใกล้เคียงให้กับหน่วยงานราชการหรือหน่วยงานเอกชนอย่างน้อย 2 ผลงาน โดยมีผลงานที่ดำเนินการมาไม่เกิน 2 ปี และมูลค่าของผลงานต่อ 1 เว็บไซต์ ไม่น้อยกว่า 200,000 บาท โดยแนบสำเนาสัญญาหรือหนังสือรับรองผลงานจ้างจากผู้ว่าจ้างมาประกอบการเสนอราคา

3.2 ผู้เสนอราคาต้องมีทุนจดทะเบียนไม่น้อยกว่า 1 ล้านบาท โดยมีหลักฐานการจดทะเบียน ซึ่งกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ออกให้หรือรับรองไม่เกิน 6 เดือน

3.3 ผู้เสนอราคาต้องไม่เป็นผู้ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานของราชการ และทางส่วนราชการได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้พ้นบุคคล หรือบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ

3.4 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นนั้น

3.5 ผู้เสนอราคาจะต้องปฏิบัติตามวิธีปฏิบัติงาน ตามขั้นตอนการพัฒนาระบบ (System Development Procedure) รหัสเอกสาร : IT-2PR-05 รายละเอียดตามเอกสารแนบ 1

3.6 ผู้เสนอราคาจะต้องปฏิบัติตามระเบียบปฏิบัติงาน ตามนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัสเอกสาร:IT-1PC-01 รายละเอียดตามเอกสารแนบ 2

3.7 ผู้เสนอราคาจะต้องปฏิบัติตามระเบียบปฏิบัติงาน ตามเอกสารการตรวจสอบการตั้งค่าตามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Secure Configuration Baseline_V.1.0) รหัสเอกสาร: IT-2FM-10 รายละเอียดตามเอกสารแนบ 3

4. ขอบเขตการดำเนินงาน

พัฒนาและปรับปรุงเว็บไซต์หลัก โดยดำเนินการควรวรรณ 3 เว็บไซต์ ได้แก่ 1. เว็บไซต์สมาคม 2. เว็บไซต์คลังความรู้ 3. เว็บไซต์รับสมัครหลักสูตรฝึกอบรมสัมมนาออนไลน์ และเว็บไซต์ให้รวมอยู่ในเว็บไซต์เดียว ภายใต้โดเมน IC.OR.TH โดยต้อง Migrate Content จากเว็บไซต์เดิม มีรายละเอียดแต่ละรายการ ดังนี้

4.1 คุณสมบัติด้านเทคนิค

4.1.1 ด้านออกแบบ

4.1.1.1 ออกแบบหน้าเว็บไซต์ให้มีรูปแบบมีความน่าเชื่อถือ ทันสมัย และเป็นมิตรต่อผู้ใช้บริการ (User Friendly) สอดคล้องกับผู้ใช้เว็บไซต์ที่เป็นนักธุรกิจ และผู้ประกอบการ

4.1.2 ด้านการออกแบบโครงสร้าง และบริหารจัดการเนื้อหาเว็บไซต์

4.1.2.1 ออกแบบ ปรับปรุง และจัดวางโครงสร้างเนื้อหาเว็บไซต์ให้ง่ายต่อการเข้าถึงและสืบค้นข้อมูล

4.1.2.2 ออกแบบโครงสร้างในการแสดงผลของเว็บไซต์ในรูปแบบ หมวดหมู่หลัก (Section), หมวดหมู่ย่อย (Category), เนื้อหา (Content)

4.1.2.3 จัดทำระบบจัดการเนื้อหาบนเว็บไซต์ (Web CMS) ให้มีส่วนของเมนูผู้ควบคุมระบบ (Administration panel) ทำให้ผู้ใช้งานสามารถบริหารจัดการเนื้อหาได้รวดเร็ว เน้นการจัดการระบบผ่านเว็บ (Web interface) ที่สามารถเพิ่มเติม ตัดแปลง แก้ไข แล้วประยุกต์นำมาใช้งานให้เหมาะสมตามแต่รูปแบบและประเภทของเว็บไซต์

4.1.2.4 ผู้รับจ้างจะต้องทำการถ่ายโอนข้อมูลจาก 3 เว็บไซต์เดิมมายังเว็บไซต์ใหม่ ทั้งหน้าเว็บไซต์หลัก และเว็บไซต์ย่อย โดยจะต้องอยู่ในระบบโครงสร้างเว็บไซต์เดียวกัน

4.1.2.5 ติดตั้งระบบติดต่อสอบถามพร้อมระบบกรองข้อมูล (Contact us with Captcha)

4.1.2.6 ระบบจัดการ Intro page หรือ Pop Up ในวันสำคัญตามเทศกาล ประกาศสำคัญ ข่าวสารและกิจกรรมของสมาคม โดยผู้รับจ้างจะต้องดำเนินการออกแบบ Intro page หรือ Pop Up ตามเทศกาล และสำหรับวันสำคัญของพระมหากษัตริย์ และพระบรมวงศานุวงศ์ ผู้รับจ้างจะต้องเป็นผู้ประสานงานในการดำเนินการขอพระราชทานอนุญาตในการขอใช้ภาพพระบรมฉายาลักษณ์ พระฉายาลักษณ์ และตราสัญลักษณ์ของพระมหากษัตริย์ และพระบรมวงศานุวงศ์ให้เรียบร้อยก่อนดำเนินการเผยแพร่ (เฉพาะกรณีที่สำนักงานปลัดสำนักนายกรัฐมนตรีมีประกาศ

ให้จัดทำแบบคำขออนุญาตใช้พระบรมฉายาลักษณ์และตราสัญลักษณ์ เช่น งานเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว เนื่องในโอกาสมหามงคลเฉลิมพระชนมพรรษา 6 รอบ 28 กรกฎาคม 2567)

4.1.2.7 มีระบบค้นหาข้อมูลภายในเว็บไซต์ ให้สามารถค้นหาข้อมูลจากคีย์เวิร์ดได้

4.1.2.8 มีระบบสนทนาออนไลน์ (Live Chat)

4.1.2.8.1 สามารถสนทนากับผู้เข้าชมเว็บไซต์ผ่านแพลตฟอร์มที่กำหนดได้

4.1.2.8.2 สามารถส่งข้อความตอบกลับอัตโนมัติได้

4.1.2.8.3 สามารถแสดงประวัติการสนทนาได้

4.1.2.9 มีระบบจัดการการเชื่อมโยงลิงก์ไปยังหน่วยงานที่เกี่ยวข้อง (Web Link)

4.1.2.10 มีระบบเว็บบอร์ด

4.1.2.10.1 สามารถสร้างห้องสนทนาได้ไม่จำกัด

4.1.2.10.2 กำหนดผู้เข้าใช้ในแต่ละห้องได้

4.1.2.10.3 สามารถแนบไฟล์รูปได้ รองรับไฟล์ jpg, gif, png ได้เป็นอย่างดี

4.1.3 ด้านการแสดงผลวิดีโอ

4.1.3.1 ต้องมีระบบการแสดงผลวิดีโอ (VDO) ให้แสดงผลวิดีโอได้ภายใน 1-3 วินาที โดยใช้เทคโนโลยีที่ทันสมัยและเหมาะสม

4.1.4 ด้านการบริหารจัดการอัปเดตข้อมูลบนเว็บไซต์

4.1.4.1 ต้องให้พนักงานสมาคมสามารถดูแลการอัปเดตข้อมูลในเว็บไซต์ได้ด้วยตนเอง รวมทั้งไม่เกิดปัญหาต่อการจัดจ้างผู้พัฒนาเว็บไซต์ในอนาคต

4.1.4.2 ต้องมีการอัปเดตระบบ Administrator หรือระบบ Back-end ให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ และง่ายต่อการใช้งานในการบริหารจัดการเนื้อหาข้อมูล

4.1.4.3 การเชื่อมต่อกับระบบภายนอก โดยให้สามารถเชื่อมต่อกับสื่อสังคมออนไลน์ เช่น เฟซบุ๊ก, เอกซ์, อินสตาแกรม และระบบแชต (Chat) เช่น ไลน์, แมสเซนเจอร์, WeChat, Chat Widget ได้

4.1.5 ด้านระบบความปลอดภัยในการใช้งานเว็บไซต์

4.1.5.1 ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสมาคม รวมถึงให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงการรักษาความลับข้อมูลของสมาคม

4.1.5.2 ต้องมีระบบความปลอดภัย SSL Certificate ดำเนินการติดตั้งโดยใช้ SSL ของสมาคม

4.1.5.3 ต้องมีระบบเก็บข้อมูลสถิติ Cookies Consent

4.1.6 ด้านการแสดงผล Responsive

4.1.6.1 ต้องรองรับการแสดงผลหลายอุปกรณ์ (Responsive Web Design) ได้แก่ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เคลื่อนที่ที่รองรับการแสดงผลเว็บไซต์

4.1.6.2 ระบบเว็บไซต์ 1 ภาษา ได้แก่ ภาษาไทย

4.1.7 ด้านการเชื่อมต่อกับระบบอื่น

4.1.7.1 เชื่อมต่อ API กับระบบฐานข้อมูลสมาชิกของสมาคม (IC-UM) เพื่อตรวจสอบสถานะสมาชิก และวันหมดอายุสมาชิก และเพื่อกำหนดสิทธิการเข้าถึงบริการเว็บไซต์สำหรับสมาชิกของสมาคม

4.1.7.2 เชื่อมต่อ API กับ Server Active Directory เพื่อกำหนดสิทธิการเข้าถึงของพนักงานสมาคม

4.2 คุณสมบัติเฉพาะฟังก์ชันคลังความรู้ KM

4.2.1 ด้านการเชื่อมต่อกับระบบอื่น

4.2.1.1 เชื่อมต่อ API กับระบบฐานข้อมูลสมาชิกของสมาคม (IC-UM) เพื่อกำหนดสิทธิการเข้าถึงแบบ “Public” สำหรับผู้ใช้บริการทั่วไป และ “Private” สำหรับสมาชิก

4.2.1.2 เชื่อมต่อ API กับ Server Active Directory เพื่อกำหนดสิทธิการเข้าถึงของพนักงานสมาคม

4.3 คุณสมบัติเฉพาะฟังก์ชันการสมัครหลักสูตรฝึกอบรมออนไลน์

4.3.1 ด้านการจัดการงานฝึกอบรมสัมมนา

4.3.1.1 มีระบบบริหารจัดการเนื้อหาหลักสูตรฝึกอบรมหรือสัมมนา

- สามารถเพิ่ม ลด และแก้ไขหลักสูตรได้
- สามารถจัดการเนื้อหารายละเอียดแต่ละหลักสูตร (Content) ได้
- สามารถจัดการหมวดหมู่หลักสูตรสัมมนาได้
- สามารถตั้งวัน-เวลาในการแสดงหลักสูตรได้
- สามารถตั้งวัน-เวลาในการแสดงอัตราค่าสัมมนาได้หลายอัตรา และสามารถกำหนดอัตราค่าสัมมนาได้หลายอัตรา
- สามารถกำหนดจำนวนผู้สมัครสูงสุดในแต่ละหลักสูตรได้
- สามารถเพิ่มผู้ลงทะเบียน สมัครเข้าอบรมได้มากกว่า 1 คน / 1 TAX ID
- สามารถกำหนดสิทธิ์ผู้ลงทะเบียนเฉพาะโควต้าสมาชิกได้มากกว่า 1 คน / 1 TAX ID
- มีระบบปฏิทิน แสดงกิจกรรมหรือโครงการที่จัด
- มีระบบจัดการหน้า Dashboard

- สามารถเพิ่มช่องข้อมูลในหลักสูตรที่ต้องการได้ ประกอบด้วย เลขที่ผู้ทำบัญชี เลขที่ผู้สอบบัญชี เลขบัตรประชาชน และอัปโหลดสำเนาบัตรประชาชนในรูปแบบ jpeg, pdf, doc, docx ขนาดไม่เกิน 5MB ได้ และเพิ่มผู้ลงทะเบียนได้มากกว่า 1 คน / 1 TAX ID
- สามารถเพิ่มที่อยู่และสาขาสำหรับออกใบเสร็จรับเงินแต่ละบริษัทได้
- สามารถเพิ่มช่องข้อมูลให้ผู้สมัครลงทะเบียน ยินยอม รับทราบนโยบายข้อมูลส่วนบุคคลก่อนยืนยันลงทะเบียนได้
- สามารถรองรับเว็บเบราว์เซอร์ Internet explorer, Chrome, Microsoft Edge, Firefox, safari browser เป็นต้น
- สามารถกำหนดสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานและดูแลระบบได้

4.3.1.2 มีระบบการจัดการงานฝึกอบรมสัมมนา

- ต้องมีระบบรองรับการจัดกลุ่มหลักสูตรฝึกอบรมเฉพาะสิทธิสมาชิกและจำกัดจำนวนผู้เข้าร่วมสัมมนา
- มีระบบรองรับการจัดการ เพิ่ม/แก้ไข/ลบ ข้อมูลผู้ลงทะเบียนเข้าร่วมสัมมนาได้ ยกเว้นชำระค่าสัมมนาแล้วไม่อนุญาตให้ลบทุกกรณี แต่อนุญาตให้แก้ไขได้
- มีระบบรองรับการจัดการ (ลบ) ข้อมูลผู้ลงทะเบียนเข้าร่วมสัมมนาและเชื่อมโยง
- ต้องมี Template สำเร็จรูป ให้สามารถตั้งค่าแก้ไขปรับแต่ง Email Template เองได้
- ต้องมีระบบตอบกลับอีเมลอัตโนมัติ ยืนยันผู้สมัครฝึกอบรม พร้อมส่ง QR Code สำหรับสแกนใช้งาน
- ต้องมีระบบสแกน QR Code ยืนยันผู้สมัครในวันจัดงาน
- ต้องมีระบบฝากข้อความถึงพนักงานและสามารถตอบกลับข้อความได้
- ต้องมีระบบแสดงสถานที่จัดงานเชื่อมโยง Google Map
- พิมพ์รายงานรายชื่อผู้สมัครฝึกอบรมรายหลักสูตร ใบเซ็นชื่อ ป้ายชื่อ ประกาศนียบัตร และหนังสือรับรองการเข้าร่วมฝึกอบรม หนังสือรับรองผู้ทำบัญชี หนังสือรับรองผู้สอบบัญชี (Certificate) ได้ และนำเข้าลายเซ็นดิจิทัลทรอนิกส์ได้

4.3.2 การเชื่อมต่อกับระบบอื่น

4.3.2.1 เชื่อมต่อ API กับระบบฐานข้อมูลสมาชิกของสมาคม (IC-UM) เพื่อตรวจสอบสถานะสมาชิก วันหมดอายุสมาชิก และสิทธิส่วนลดอัตโนมัติ

4.3.2.1.1 มีระบบการตรวจสอบสมาชิก และผู้ใช้บริการ

- สามารถเชื่อมโยงข้อมูลสมาชิกและผู้ใช้บริการ กับฐานข้อมูลของสมาคมได้

- ระบบแสดงชื่อบริษัท ที่อยู่สำหรับออกใบเสร็จรับเงินของผู้สมัคร
ฝึกอบรมเมื่อกรอกเลข Tax ID
- ระบบสืบค้นข้อมูลทะเบียนสมาชิก มีหน้าจอสำหรับสมาชิก ให้
สอบถามข้อมูลส่วนตัวได้

4.3.2.2 เชื่อมต่อ API กับระบบบัญชีการเงิน (TR Cloud) ในการออกใบแจ้งชำระค่าบริการ (Bill Payment) การอัปโหลดหลักฐานการชำระเงิน และการส่งค่าสถานะยืนยันการชำระเงินกลับมายังระบบสมัครหลักสูตรฝึกอบรมออนไลน์

4.3.2.2.1 มีระบบแจ้งการชำระเงิน ใบแจ้งชำระค่าบริการ (Bill Payment) และ
อัปโหลด หลักฐานการชำระเงิน

- สามารถเชื่อมโยงข้อมูลออกใบแจ้งชำระค่าบริการ (Bill Payment)
กับระบบบัญชีของสมาคมได้
- สามารถเชื่อมโยงข้อมูลใบแจ้งชำระค่าบริการ (Bill Payment)
กับระบบบัญชีของสมาคมได้
- สามารถแสดงยอดเงินค่าลงทะเบียน พร้อมทั้งสามารถแก้ไขเพิ่ม หรือ
ลดยอดเงินได้
- แสดงที่อยู่การออกใบแจ้งชำระค่าบริการ (Bill Payment) ตามระบบ
บัญชี หรือตามข้อมูลผู้สมัครลงทะเบียน
- ใบแจ้งชำระค่าบริการ (Bill Payment) แสดงรหัสอ้างอิงหลักสูตร
และรหัสการชำระเงินได้ และแสดงรายละเอียดตามระบบบัญชีของ
สมาคม
- สามารถส่งใบแจ้งชำระค่าบริการ (Bill Payment) ให้ผู้ลงทะเบียน
แบบ Auto และแบบ Manual
- มีหน้าจอสำหรับให้ผู้ลงทะเบียนอัปโหลดหลักฐานการชำระเงินได้
- ระบบแสดงสถานะการชำระเงิน แสดงเลขที่และวันที่ใบเสร็จรับเงิน
ได้
- Export ข้อมูลการชำระเงินรายหลักสูตรสัมมนาเป็น pdf. และไฟล์
Excel ได้

4.3.2.3 เชื่อมต่อ API กับ Server Active Directory เพื่อกำหนดสิทธิการเข้าถึงของพนักงาน
สมาคม

4.4 ด้านการรายงานผลและข้อมูลทางสถิติ

- 4.4.1 ต้องมีระบบนับจำนวนผู้เข้าชมเว็บไซต์ ให้สามารถเก็บประวัติการเข้าชมเว็บไซต์ โดย Google Analytics ได้ และจัดทำรายงานและเก็บประวัติการรายงานผลและสถิติต่างๆ
- 4.4.2 นำส่งรายงานสถิติการใช้งาน (Google Analytic) โดยแยกรายงาน ได้แก่ เว็บไซต์หลัก ฟังก์ชัน คลังความรู้ ฟังก์ชันสมัครอบรมสัมมนาออนไลน์ และเว็บบอร์ด แบบรายเดือน
 - 4.4.2.1 รายงานสถิติการใช้งานแบบรายเดือน โดยมีรายงานจำนวนผู้เข้าใช้งานเว็บไซต์ และรายงาน 10 อันดับหน้าเว็บไซต์ที่เข้าชมมากที่สุด
 - 4.4.2.2 รายงานสถิติการใช้งานแบบรายเดือน โดยมีรายงานการเข้าชมวิดีโอ 10 อันดับแรก ที่เข้าชมมากที่สุด
 - 4.4.2.3 มีระบบจัดเก็บข้อมูลลงทะเบียนผู้เข้าร่วมฝึกอบรมรายหลักสูตร และ Export ข้อมูล เป็นไฟล์ Excel ได้
 - 4.4.2.4 มีระบบรายงานผล และข้อมูลทางสถิติ ในการเรียกดูรายงานรายหลักสูตร หรือ ตามเงื่อนไขที่กำหนด และต้อง Export ข้อมูล เป็นไฟล์ pdf. และ Excel ได้
 - 4.4.2.5 รายงานสถิติการใช้งานแบบรายเดือน โดยมีรายงาน 10 อันดับหลักสูตรที่เข้าชม มากที่สุด
- 4.4.3 นำส่ง Report Capacity พื้นที่การให้บริการ Web Hosting แบบรายเดือน
- 4.4.4 นำส่งรายงานผลภัยคุกคาม (Incident Report) แบบรายเดือน

4.5 การจัดทำคู่มือและสอนการใช้งานเว็บไซต์เบื้องต้น

- 4.5.1 คู่มือการใช้งานเว็บไซต์ (User Manual) ที่อธิบายการใช้งานระบบทุกๆ ด้านโดยละเอียด สำหรับ ผู้ดูแลและบริหารเว็บไซต์
- 4.5.2 คู่มือการดูแลและบำรุงรักษาเว็บไซต์ที่มีรายละเอียดการติดตั้งระบบ การใช้งานระบบ และการสำรองข้อมูลระบบ อย่างครบถ้วน
- 4.5.3 อบรมการใช้งานเว็บไซต์ให้กับผู้ดูแลระบบ ผู้ดูแลและผู้บริหารเว็บไซต์ จำนวนไม่น้อยกว่า 3 ครั้ง

4.6 ขอบเขตงานบริการรับฝากพื้นที่เว็บไซต์ (Web Hosting)

- 4.6.1 จัดสรรพื้นที่จัดเก็บเว็บไซต์ (Web Hosting) ที่เป็นพื้นที่ Private Hosting โดยมีขนาดพื้นที่ จัดเก็บเว็บไซต์ไม่ต่ำกว่า 200 GB และ Bandwidth ไม่จำกัด และต้องจัดเก็บข้อมูลเว็บไซต์ ตามข้อ 4 เป็นระยะเวลา ไม่น้อยกว่า 1 ปี
- 4.6.2 ผู้เสนอราคาต้องเสนอศูนย์ข้อมูล Web Hosting ตั้งอยู่ในประเทศไทย โดยได้รับการรับรอง มาตรฐาน ISO 27001 (มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ) และมาตรฐาน CSA-Star (มาตรฐานด้าน ความมั่นคงปลอดภัยของระบบการประมวลผลแบบคลาวด์) เป็นอย่างน้อย

5. ข้อกำหนดและเงื่อนไขการรับประกัน

5.1 ด้านลิขสิทธิ์แอปพลิเคชัน

5.1.1 ลิขสิทธิ์และกรรมสิทธิ์ใดๆ บนเว็บไซต์นี้ รวมถึงคู่มือถือเป็นลิขสิทธิ์และกรรมสิทธิ์ของสมาคมทันที หลังการส่งมอบงาน

5.1.2 ในกรณีที่มีผู้กล่าวอ้างหรือใช้สิทธิ์เรียกร้องใดๆ ว่ามีการละเมิดลิขสิทธิ์ และเรียกร้องความเสียหายจากบุคคลใด หน่วยงานใด หรือเจ้าของลิขสิทธิ์ ผู้รับจ้างต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว และผู้รับจ้างต้องรับผิดชอบต่อความเสียหาย และค่าใช้จ่ายทั้งหมดที่อาจเกิดขึ้นแก่สมาคม สโมสรนักลงทุนทุกกรณี

5.2 ด้านการรับประกันความชำรุดบกพร่องของการปรับปรุงและพัฒนาเว็บไซต์ และบริการดูแลและอัปเดตข้อมูลเว็บไซต์

5.2.1 ผู้รับจ้างจะต้องรับประกันการใช้งานเว็บไซต์ที่พัฒนาขึ้นเป็นเวลาไม่น้อยกว่า 1 ปี นับแต่วันที่สมาคมสโมสรนักลงทุนได้รับมอบงานงวดที่ 5 โดยผู้รับจ้างต้องบริหารจัดการซ่อมแซมหรือแก้ไขระบบงานให้ใช้งานได้ดังเดิม โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น โดยมีขอบเขตการรับประกัน หรือซ่อมแซมหรือแก้ไขระบบงาน ดังนี้

ระดับความสำคัญ	ปัญหา	ระยะเวลาในการแก้ไขปัญหา
ระดับสูงสุด	เว็บไซต์ไม่สามารถใช้งานได้ เช่น เว็บไซต์ถูกโจมตีจากผู้ไม่หวังดี ฐานข้อมูลหายทั้งหมด มีปัญหาด้านการเชื่อมต่อกับเซิร์ฟเวอร์ เป็นต้น	- ภายในเวลา 4 ชั่วโมง ในการนำข้อมูลสำรองขึ้นออนไลน์ หลังได้รับแจ้งปัญหาจากสมาคม - ภายในเวลา 4-8 ชั่วโมง ในการตรวจสอบความเรียบร้อย หลังจากนำข้อมูลสำรองขึ้นออนไลน์เรียบร้อยแล้ว
ระดับสูง	เว็บไซต์ไม่สามารถใช้งานได้ตามปกติ เช่น ไม่สามารถแสดงผลวิดีโอได้ ไม่สามารถอัปโหลดไฟล์ได้ ไม่สามารถใช้งานฟังก์ชันดาวน์โหลดแบบฟอร์มหรือประกาศได้ ไม่สามารถเข้าหน้าต่างๆ ในเว็บไซต์ได้	- ภายในเวลา 3-5 ชั่วโมง ในการดำเนินการตรวจสอบ และหาแนวทางในการแก้ไขปัญหา หลังได้รับแจ้งปัญหาจากสมาคม - ภายในเวลา 4-12 ชั่วโมง ในการกู้คืนระบบ หลังจากตรวจพบสาเหตุของปัญหา
ระดับกลาง	เว็บไซต์สามารถใช้งานได้ แต่แสดงผลไม่สมบูรณ์ เช่น ไม่สามารถแสดงรูปภาพบางส่วนได้ เว็บไซต์ไม่สามารถคลิกลิงก์ได้ ไม่สามารถแสดงผลข้อมูลได้ในบางส่วน	- ภายในเวลา 8-24 ชั่วโมง ในการดำเนินการตรวจสอบและแก้ไขปัญหา หลังได้รับแจ้งปัญหาจากสมาคม
ระดับต่ำ	เว็บไซต์สามารถใช้งานได้ แสดงผลได้ถูกต้อง แต่มีบางส่วนที่ไม่ส่งผลกระทบต่อผู้ใช้ งานเว็บไซต์ที่มีการแสดงผลไม่สมบูรณ์ เช่น ขนาดและรูปแบบตัวอักษรผิดเพี้ยน	- ภายในเวลา 24-48 ชั่วโมง ในการดำเนินการตรวจสอบและแก้ไขปัญหา หลังได้รับแจ้งปัญหาจากสมาคม

	เว็บไซต์ผิดเพี้ยน เป็นต้น	
--	---------------------------	--

5.2.2 ผู้รับจ้างจะต้องดูแลให้เว็บไซต์คงสภาพการใช้งานได้เป็นปกติ และอัปเดตระบบบริหารจัดการเว็บไซต์ให้เป็นปัจจุบัน เป็นเวลาไม่น้อยกว่า 1 ปี (ในช่วงระยะเวลารับประกัน) โดยขอบเขตงานดูแลและอัปเดตข้อมูลเว็บไซต์สมาคม มีดังนี้

- 5.2.2.1 ดูแลตรวจเช็คความพร้อมใช้งานของเว็บไซต์
- 5.2.2.2 ดูแลระบบโปรแกรมให้พร้อมใช้งาน
- 5.2.2.3 ตรวจสอบดูแลการเชื่อมต่อกับเซิร์ฟเวอร์ แจ้งเตือน และแก้ไข
- 5.2.2.4 ตรวจสอบและป้องกันการโจมตีของไวรัส มัลแวร์ แฮ็กเกอร์
- 5.2.2.5 แก้ไขโปรแกรมเบื้องต้น ซึ่งไม่กระทบหรือแก้ไขโครงสร้างของโปรแกรมเดิมที่มีอยู่
- 5.2.2.6 สำรองข้อมูลภายในเว็บไซต์แบบรายวัน และ แบบรายสัปดาห์ทุกวันจันทร์ โดยจัดเก็บใน Web Hosting ที่นำเสนอ และทำการ File Transfer Protocol (FTP) ที่สำรองข้อมูลมายังใน Server ของสมาคม
- 5.2.2.7 ออกแบบ แก้ไข ปรับเปลี่ยนงานด้านกราฟิกภายในเว็บไซต์
- 5.2.2.8 ระบบจัดการ Intro page หรือ Pop Up ในวันสำคัญตามเทศกาล ประกาศสำคัญ ข่าวสารและกิจกรรมของสมาคม โดยผู้รับจ้างจะต้องดำเนินการออกแบบ Intro page หรือ Pop Up ตามเทศกาล และสำหรับวันสำคัญของพระมหากษัตริย์ และพระบรมวงศานุวงศ์ ผู้รับจ้างจะต้องเป็นผู้ประสานงานในการดำเนินการขอพระราชทานอนุญาตในการขอใช้ภาพพระบรมฉายาลักษณ์ พระฉายาลักษณ์ และตราสัญลักษณ์ของพระมหากษัตริย์ และพระบรมวงศานุวงศ์ให้เรียบร้อยก่อนดำเนินการเผยแพร่ (เฉพาะกรณีที่สำนักงานปลัดสำนักนายกรัฐมนตรีมีประกาศให้จัดทำแบบคำขออนุญาตใช้พระบรมฉายาลักษณ์และตราสัญลักษณ์ เช่น งานเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว เนื่องในโอกาสสมโภชฉลองพระชนมพรรษา 6 รอบ 28 กรกฎาคม 2567)
- 5.2.2.9 รายงานสถิติการใช้งาน (Google Analytic) โดยแยกรายงาน ได้แก่ เว็บไซต์หลัก ฟังก์ชัน คลังความรู้ ฟังก์ชันสมัครอบรมสัมมนาออนไลน์ และเว็บบอร์ด แบบรายเดือน
- 5.2.2.10 นำส่ง Report Capacity พื้นที่การให้บริการ Web Hosting แบบรายเดือน
- 5.2.2.11 นำส่งรายงานผลภัยคุกคาม (Incident Report) แบบรายเดือน
- 5.2.2.12 เก็บข้อมูลสถิติ Cookies Consent และรายงานข้อมูลสถิติเมื่อได้รับการร้องขอจากผู้ว่าจ้าง
- 5.2.2.13 ให้คำปรึกษาและเข้าร่วมประชุมกับทางสมาคมสโมสรนักลงทุน เมื่อมีการร้องขอจากผู้ว่าจ้าง
- 5.2.2.14 ตรวจสอบและอัปเดตระบบ Administrator หรือระบบ Back-end ให้เป็นเวอร์ชันล่าสุด

6. ความต้องการด้านความปลอดภัย

6.1 ต้องจัดหาและใช้ License ที่ถูกกฎหมาย

6.2 ต้องมีการทดสอบความปลอดภัยของแอปพลิเคชัน (Application Security Testing) โดยการตรวจสอบโค้ดและการทดสอบการเจาะระบบเพื่อระบุและแก้ไขช่องโหว่ก่อนการขึ้นใช้งานระบบ (โดย Third party ที่สมาคมจัดจ้าง)

7. ระยะเวลาดำเนินงาน

7.1 ระยะเวลาดำเนินการพัฒนาและปรับปรุง IC Website ให้แล้วเสร็จ ภายใน 180 วัน นับถัดจากวันที่ลงนามในสัญญา

7.2 ระยะเวลาการให้บริการรับฝากพื้นที่เว็บไซต์ ตามรายละเอียดข้อ 4.6 ภายใน 1 ปี นับจากวันที่คณะกรรมการตรวจรับงานเรียบร้อยแล้ว ผู้รับจ้างจะต้องดำเนินการโอนย้ายข้อมูลทั้งหมดของเว็บไซต์สมาคมจากพื้นที่เดิม นำมาจัดเก็บไว้บนพื้นที่ของผู้รับจ้างที่เตรียมไว้ให้เรียบร้อยแล้ว หลังจากส่งมอบเว็บไซต์ที่พัฒนาแล้วเสร็จ โดยเว็บไซต์จะต้องอยู่ในรูปแบบที่ได้รับการยืนยันใช้งานล่าสุด และมีความพร้อมใช้งานทุกประการ

8. กำหนดการส่งมอบและเงื่อนไขการชำระเงิน

ผู้รับจ้างต้องส่งมอบงานทั้งหมด (ตามข้อ 4) ให้เสร็จสิ้นสมบูรณ์ ตามความต้องการของสมาคม โดยมีรายละเอียดดังนี้

8.1 กำหนดการส่งมอบและสิ่งที่ส่งมอบ

- 1) งวดที่ 1 ส่งมอบภายใน 10 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีรายละเอียดดังนี้
 - แผนการดำเนินงานการพัฒนาและปรับปรุงเว็บไซต์ (Project Plan)
 - แผนผังโครงสร้างเว็บไซต์
- 2) งวดที่ 2 ส่งมอบภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีรายละเอียด ดังนี้
 - ตัวอย่างการออกแบบหน้าเพจเว็บไซต์และโครงสร้างเว็บไซต์
- 3) งวดที่ 3 ส่งมอบภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีรายละเอียด ดังนี้
 - ต้นแบบเว็บไซต์ / Mock Up เว็บไซต์
 - ระบบบริหารจัดการเว็บไซต์ (Back-end) ตามรายละเอียดการปรับปรุงและพัฒนาเว็บไซต์และการจัดทำโครงสร้างเว็บไซต์ (ข้อ 4.1.4.1 และ 4.1.4.2)
- 4) งวดที่ 4 ส่งมอบภายใน 160 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีรายละเอียด ดังนี้
 - ส่งมอบเว็บไซต์ได้รับการพัฒนาแล้วเสร็จ
- 5) งวดที่ 5 ส่งมอบภายใน 180 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีรายละเอียด ดังนี้
 - โอนย้ายข้อมูลเว็บไซต์สมาคมที่พร้อมใช้งานจากพื้นที่เดิม จัดเก็บไว้บนพื้นที่รับฝากเว็บไซต์ (Web Hosting) ของผู้รับจ้าง (ข้อ 4.6 และ 7.2)
 - ต้องทำการแก้ไขและส่งผลการแก้ไขที่ผ่านทั้งหมดของการตรวจสอบความปลอดภัยของเว็บไซต์ที่พัฒนา ตามข้อ 6.2
 - ส่งรายงานผลการทดสอบ UAT Test Script / UAT Result Report

- Training Result
- Deploy Result
- System Design (ฉบับ Update)
 - a. Data Flow
 - b. Data Dictionary
- ER Diagram
- Requirement Specification Document
- API Specification Document
- อบรมการใช้งานเว็บไซต์ให้กับผู้ดูแลระบบ ผู้ดูแลและผู้บริหารเว็บไซต์ จำนวนไม่น้อยกว่า 3 ครั้ง พร้อมคู่มือการใช้งาน Back-end เว็บไซต์ ในรูปแบบเอกสาร (Hard Copy) ตามจำนวนผู้เข้าร่วมอบรม และสำเนาในรูปแบบไฟล์ (Soft Copy) ส่งมอบทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม
- คู่มือการใช้งานเว็บไซต์ (User Manual) ที่อธิบายการใช้งานระบบทุกๆ ด้านโดยละเอียด ในรูปแบบเอกสาร (Hard Copy) จำนวน 2 ฉบับ พร้อมสำเนาในรูปแบบไฟล์ (Soft Copy) ส่งมอบทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม
- คู่มือการดูแลและบำรุงรักษาเว็บไซต์ที่มีรายละเอียดการติดตั้งระบบ การใช้งานระบบ และการสำรองข้อมูลระบบอย่างครบถ้วน รูปแบบเอกสาร (Hard Copy) จำนวน 2 ฉบับ พร้อมสำเนาในรูปแบบไฟล์ (Soft Copy) ส่งมอบทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม
- Source Code ของระบบทั้งหมด ที่สามารถนำมาแก้ไขต่อได้โดยบุคลากรของสมาคม พร้อมคู่มือในการนำระบบขึ้นใช้งาน ในรูปแบบไฟล์ (Soft Copy) ส่งมอบทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม

8.2 เงื่อนไขการชำระเงิน

- งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 10 ของมูลค่าสัญญา เมื่อผู้รับจ้างส่งมอบงานงวดที่ 1 และคณะกรรมการตรวจรับดำเนินการตรวจรับงานเรียบร้อยแล้ว
- งวดที่ 2 เป็นจำนวนเงินในอัตราร้อยละ 10 ของมูลค่าสัญญา เมื่อผู้รับจ้างส่งมอบงานงวดที่ 2 และคณะกรรมการตรวจรับดำเนินการตรวจรับงานเรียบร้อยแล้ว
- งวดที่ 3 เป็นจำนวนเงินในอัตราร้อยละ 20 ของมูลค่าสัญญา เมื่อผู้รับจ้างส่งมอบงานงวดที่ 3 และคณะกรรมการตรวจรับดำเนินการตรวจรับงานเรียบร้อยแล้ว
- งวดที่ 4 เป็นจำนวนเงินในอัตราร้อยละ 30 ของมูลค่าสัญญา เมื่อผู้รับจ้างส่งมอบงานงวดที่ 4 และคณะกรรมการตรวจรับดำเนินการตรวจรับงานเรียบร้อยแล้ว
- งวดที่ 5 เป็นจำนวนเงินในอัตราร้อยละ 30 ของมูลค่าสัญญา เมื่อผู้รับจ้างส่งมอบงานงวดที่ 5 และคณะกรรมการตรวจรับดำเนินการตรวจรับงานเรียบร้อยแล้ว

****หมายเหตุ** ในการชำระเงินแต่ละงวด ราคาของมูลค่าสัญญา ไม่รวมค่าบริการรับฝากพื้นที่เว็บไซต์ (Web Hosting)

การคืนเงินหลักประกันสัญญา เมื่อครบกำหนดการรับประกันการใช้งานและบำรุงรักษาเว็บไซต์ ระยะเวลา 1 ปี (ตามการรับประกันผลงาน ข้อ 5.2)

8.3 งานบริการรับฝากพื้นที่เว็บไซต์ (Web Hosting)

ผู้ว่าจ้างตกลงจ่ายค่าบริการรับฝากพื้นที่เว็บไซต์ให้แก่ผู้รับจ้าง โดยชำระค่าบริการทั้งหมดของงานบริการรับฝากพื้นที่เว็บไซต์ พร้อมกับการชำระเงินงวดที่ 5 ในข้อ 8.2

9. ค่าปรับ

9.1 กรณีผู้รับจ้างไม่สามารถดำเนินการส่งมอบงานได้ทันในแต่ละงวดตามกำหนด ผู้รับจ้างจะต้องชำระค่าปรับในอัตราร้อยละ 0.1 ของมูลค่างานตามสัญญาในแต่ละงวด แต่ต้องไม่ต่ำกว่าวันละ 100 บาท จนกว่าจะสามารถดำเนินการได้ตามข้อกำหนด หรือจนกว่าส่งมอบงานได้ถูกต้องครบถ้วนโดยเศษของวันจะถือเป็นหนึ่งวันเต็ม

9.2 กรณีที่ผู้รับจ้างไม่สามารถดำเนินการตามเงื่อนไขที่ระบุไว้ในขอบเขตการรับประกัน ข้อ 5.2 ผู้รับจ้างจะต้องชำระค่าปรับให้ผู้ว่าจ้างเป็นรายชั่วโมงในอัตราร้อยละ 0.1 ของมูลค่าสัญญา แต่ไม่น้อยกว่า 100 บาท/ชั่วโมง จนกว่าเว็บไซต์จะใช้งานได้ปกติ โดยเศษของชั่วโมงคิดเป็น 1 ชั่วโมง

9.3 หากผู้รับจ้างไม่เข้ามาแก้ไขตามเวลาที่ระบุข้างต้น ผู้ว่าจ้างมีสิทธิจ้างบุคคลภายนอกทำการซ่อมแซม แก้ไข โดยผู้รับจ้างต้องเป็นผู้ออกค่าใช้จ่ายให้แทนผู้ว่าจ้างทั้งสิ้น

10. หลักเกณฑ์การพิจารณาคัดเลือกจัดซื้อจัดจ้าง

10.1 คณะกรรมการจะพิจารณาเปิดซองคุณสมบัติบริษัทหรือผู้ยื่นเสนอราคา เมื่อถูกต้องตามข้อกำหนดครบถ้วนแล้ว ซึ่งสมาคมจะเชิญบริษัทให้มาเสนอผลงานกับคณะกรรมการ รายละเอียดไม่เกิน 45 นาที รวมการตอบข้อซักถามของคณะกรรมการ โดยวัน เวลา และสถานที่ สมาคมจะแจ้งให้ทราบต่อไป

10.2 สมาคมจะพิจารณาคัดเลือกโดยใช้หลักเกณฑ์วิธีพิจารณาประสิทธิภาพต่อราคาเท่านั้น

10.3 ผู้เสนอราคาต้องระบุรายละเอียดต่างๆ เพื่อประกอบการพิจารณาดังนี้

10.3.1 คุณสมบัติของผู้เสนอราคา ประวัติและผลการดำเนินงาน ประสบการณ์ของทีมงาน

10.3.2 ผู้เสนอราคานำเสนอแนวคิดการออกแบบเว็บไซต์สมาคม และแสดง Demo ตัวอย่างแนวคิดการออกแบบ แสดงผลงานเว็บไซต์ที่เคยจัดทำ โดยมีหน้าแสดงผลบนเว็บไซต์ และ Back-end ที่แสดงให้เห็นการบริหารจัดการข้อมูลและการอัปเดตข้อมูล นำเสนอแผนการดำเนินงาน แนวทางในการใช้เทคโนโลยีหรือซอฟต์แวร์ที่เหมาะสมตามขอบเขตงาน นำเสนอขอบเขตการรับประกัน แผนการบำรุงรักษาและค่าใช้จ่ายในการบำรุงรักษาในระยะเวลา 1 ปี

10.3.3 รายละเอียดหรือข้อมูลพื้นที่บริการรับฝากเว็บไซต์ (Web Hosting)

10.4 ผู้เสนอราคาที่ผ่านเกณฑ์การพิจารณา จะต้องมีคะแนนข้อเสนอด้านเทคนิคตั้งแต่ 80 คะแนน ขึ้นไป

10.5 เมื่อผ่านเกณฑ์พิจารณาใน ข้อ 10.4 แล้ว สมาคมจึงจะเปิดซองราคา โดยจะพิจารณาคัดเลือกเฉพาะ รายที่เสนอราคาภายในวงเงินที่กำหนด และการตัดสินจะใช้วิธีประสิทธิภาพต่อราคา ซึ่งการตัดสินของคณะกรรมการ ถือเป็นที่สุด

เกณฑ์การพิจารณาให้คะแนน 100 คะแนน	คะแนน
1. ผลงานที่ผ่านมา / ความน่าเชื่อถือและประสบการณ์	10
2. แนวคิดในการออกแบบเว็บไซต์ที่สื่อถึงสมาคม / ความสวยงามในการออกแบบ / การจัดทำกราฟิกต่างๆ / User Friendly / มีความสะดวก / ง่ายต่อการใช้งาน	20
3. ระบบ Administration panel ที่ง่ายต่อการอัปเดตข้อมูล / ไม่ซับซ้อน	20
4. เทคโนโลยีและซอฟต์แวร์ที่นำมาใช้มีประสิทธิภาพ / มีความทันสมัย	20
5. แนวทางในการแก้ไขปัญหา กรณีมีปัญหาเกี่ยวกับอุปกรณ์ระบบงานและบริการ	20
6. แผนการบำรุงรักษาและค่าใช้จ่ายในการบำรุงรักษาในระยะเวลา 1 ปี	10
รวมคะแนน	100

11. หลักประกันการปฏิบัติตามสัญญา

ผู้ที่ได้รับการคัดเลือกหรือคู่สัญญาจะต้องวางหลักประกันสัญญาการปฏิบัติตามสัญญา มูลค่า 10% ของมูลค่า โครงการ (ไม่รวมภาษีมูลค่าเพิ่ม) มามอบไว้ให้แก่สมาคม ณ วันที่ลงนามในสัญญา

12. การรับประกันผลงาน

12.1 ผู้รับจ้างต้องรับประกันผลงานที่ส่งมอบแก่สมาคม เป็นระยะเวลา 1 ปี นับถัดจากวันที่คณะกรรมการ ตรวจรับดำเนินการตรวจรับงานงวดสุดท้ายเรียบร้อยแล้ว

12.2 ผู้รับจ้างต้องรับประกันการใช้งานเว็บไซต์ และบำรุงรักษาเว็บไซต์ (ตามข้อ 5.2) เป็นระยะเวลา 1 ปี นับถัดจากวันที่คณะกรรมการตรวจรับดำเนินการตรวจรับงานงวดสุดท้ายเรียบร้อยแล้ว

13. การรักษาความลับ

ผู้รับจ้างจะเก็บรักษาข้อมูลอันเป็นความลับ ทั้งที่เป็นเอกสารและข้อมูลทางเทคนิคที่ได้รับมาจาก ผู้ว่าจ้าง ผู้รับจ้างจะไม่ใช้ข้อมูลอันเป็นความลับเพื่อการอื่นใดนอกเหนือจากเพื่อการทำงานตามวัตถุประสงค์ของ สัญญานี้ หากมีการเปิดเผยข้อมูลตลอดจนเอกสารอันเป็นความลับของผู้ว่าจ้าง ผู้รับจ้างต้องรับผิดชอบในความเสียหายดังกล่าว



สมาคมสโมสรนักลงทุน
Investor Club Association

ขั้นตอนการพัฒนาระบบ (System Development Procedure)

รหัสเอกสาร:	IT-2PR-05
หมายเลขปรับปรุงเอกสาร:	1.0
วันที่เอกสารมีผลบังคับใช้:	10 มกราคม 2568
เจ้าของเอกสาร:	ฝ่ายเทคโนโลยีสารสนเทศ



สมาคมสโมสรนักลงทุน
Investor Club Association

เรื่อง : ขั้นตอนการพัฒนาาระบบ (System Development Procedure)

รหัส : IT-2PR-05

วันที่ประกาศใช้ : 10 มกราคม 2568

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ-นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
ผู้จัดทำ	รุ่งรัตน์ อุ่นจิตต์	พนักงานพัฒนาระบบ สารสนเทศอาวุโส		09/01/2568
ผู้ทบทวน	สิริวรรณ ฉลากรไชยา	หัวหน้าฝ่าย เทคโนโลยีสารสนเทศ		10 มกราคม 2568
ผู้อนุมัติ	กรองนก มานะกิจจกมล	ผู้จัดการ สมาคมสโมสรนักลงทุน		10 มกราคม 2568

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุง เอกสาร (version):	วันที่ปรับปรุง เอกสาร	ปรับปรุงโดย	คำอธิบายและเหตุผลในการแก้ไข



สารบัญ

เรื่อง	หน้า
1. บทนำ	4
1.1 วัตถุประสงค์ (Objective).....	4
1.2 ขอบเขต (Scope)	4
2. กรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development Lifecycle).....	4
2.1 การวางแผน (Planning)	4
2.2 การเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis).....	5
2.3 การออกแบบระบบสารสนเทศหรือซอฟต์แวร์ (Design).....	5
2.4 การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development).....	6
2.5 การทดสอบระบบสารสนเทศหรือซอฟต์แวร์ (Testing).....	6
2.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment).....	7
2.7 การบำรุงรักษา (Maintenance).....	7
3. ขั้นตอนการพัฒนาระบบสารสนเทศและซอฟต์แวร์.....	7
3.1 การวางแผนโครงการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Project Planning).....	7
3.2 การบริหารจัดการความต้องการในการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Requirement Management)	8
3.3 การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Design and Analysis).....	9
3.4 การพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development).....	11
3.5 การทดสอบระบบสารสนเทศและซอฟต์แวร์ (Testing).....	12
3.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment).....	13
3.7 การปิดโครงการหรือเสร็จสิ้นการพัฒนาโครงการ (Project Closure)	13
4. การจัดจ้างผู้ให้บริการภายนอก เพื่อการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Outsourcing Development)	14
5. เอกสารที่เกี่ยวข้อง (Related Documents)	14



1. บทนำ

1.1 วัตถุประสงค์ (Objective)

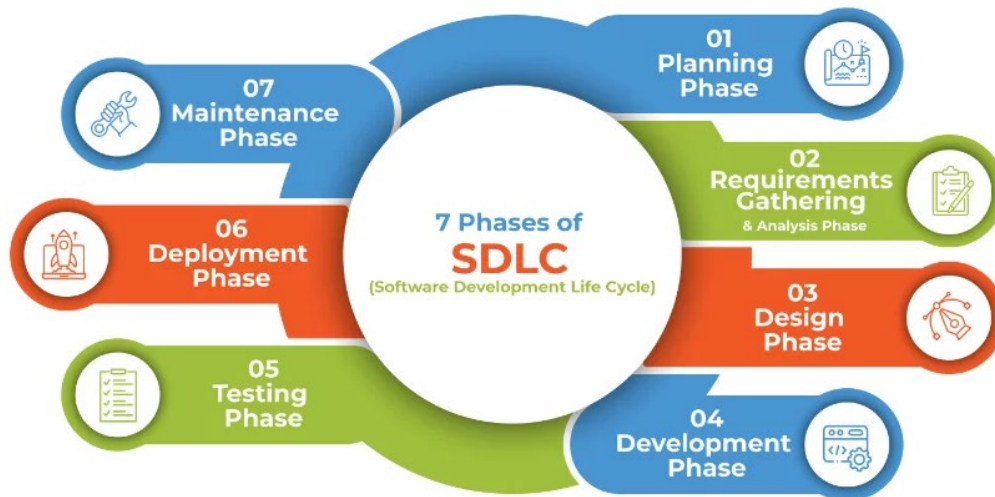
เอกสารฉบับนี้จัดทำขึ้นเพื่ออธิบายกระบวนการดำเนินงานในการจัดหาและการพัฒนาระบบที่นำมาใช้ในสมาคมฯ ให้เป็นไปตามมาตรฐานสากล

1.2 ขอบเขต (Scope)

เอกสารฉบับนี้ จัดทำขึ้นเพื่อใช้ในการกำหนดแนวทางการพัฒนาระบบที่อยู่ภายใต้ขอบเขตการรองรับที่อ้างอิงตามเอกสารขอบเขตระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS and ISMS Scope) (ISO-1PC-02) ที่เป็นการพัฒนาโครงการใหม่

2. กรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development Lifecycle)

เพื่อให้การพัฒนาระบบสารสนเทศและซอฟต์แวร์ เป็นไปในแนวทางที่เป็นมาตรฐานและสามารถบริหารจัดการได้ง่าย จึงกำหนดกรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ให้ครอบคลุมกระบวนการ ดังนี้



ภาพที่ 1 กระบวนการพัฒนาระบบสารสนเทศและซอฟต์แวร์

2.1 การวางแผน (Planning)

เป็นการวางแผนการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ของทั้งโครงการ โดยผู้จัดการโครงการ (Project Manager) จะวางแผนด้านระยะเวลาในการพัฒนา (Time) ขอบเขตงาน (Scope) จำนวนคนที่จะใช้ (Resource) รวมถึงวางแผนว่าใครหรือองค์ใดที่จะมีส่วนเกี่ยวข้องกับการพัฒนาบ้าง เนื่องจากบางครั้งอาจต้องอาศัยปัจจัยอื่น เช่น นโยบาย กฎหมาย หรือระเบียบที่เกี่ยวข้องของสมาคมฯ เข้ามาเป็นปัจจัยการออกแบบระบบสารสนเทศหรือซอฟต์แวร์ด้วย Project Manager จะต้องวางแผนให้ครอบคลุมกิจกรรมในการเก็บ



รวบรวมและวิเคราะห์ความต้องการ (Analysis) การออกแบบ (Design) การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development) และการทดสอบ (Testing) โดยการวางแผนงานที่ละเอียดแม่นยำ จะช่วยลดความเสี่ยงของการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ และสามารถพัฒนาสำเร็จตามเวลา และวัตถุประสงค์ที่กำหนดไว้

2.2 การเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis)

ในขั้นตอนนี้ Project Manager หรือ Product Owner หรือ Business Analyst จะเป็นผู้เก็บรวบรวม Requirement จากลูกค้าหรือผู้มีส่วนเกี่ยวข้อง เพื่อเข้าใจความต้องการจากผู้ใช้งานและการทำงานของระบบ โดยอาจจัดทำอยู่ในรูปแบบ Prototyping เพื่อให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบได้ง่ายขึ้น หลังจากการรวบรวม Requirement เสร็จแล้ว ทีมพัฒนา เช่น ผู้พัฒนาระบบ (Developer) หรือ ผู้ตรวจสอบคุณภาพ (Quality Assurance) สามารถช่วยตรวจสอบ Requirement นั้นได้เพื่อใช้ในการออกแบบและประเมินความเสี่ยงและข้อจำกัดของระบบสารสนเทศหรือซอฟต์แวร์ที่อาจเกิดขึ้น

ตัวอย่างขั้นตอนการเก็บรวบรวมและวิเคราะห์ความต้องการสำหรับการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ สามารถพิจารณาได้ดังต่อไปนี้

- 1) ขั้นตอนการรวบรวมความต้องการ (Requirement Gathering) เป็นขั้นตอนที่ดำเนินการรวบรวมความต้องการที่มีต่อระบบ จากกลุ่มลูกค้าหรือผู้มีส่วนเกี่ยวข้อง โดยการสัมภาษณ์หรือศึกษาปัญหา/ข้อมูลที่มีอยู่ปัจจุบัน
- 2) ขั้นตอนการวิเคราะห์ความต้องการ (Requirement Analysis) เป็นขั้นตอนที่จะวิเคราะห์ข้อมูลความต้องการที่รวบรวมได้ เพื่อออกแบบการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์โดยมีวัตถุประสงค์ ดังนี้
 - จัดกลุ่มความต้องการตามหมวดหมู่ เช่น ฟังก์ชันการทำงาน ประสิทธิภาพ การรักษาความมั่นคงปลอดภัย
 - ประเมินความสำคัญของความต้องการแต่ละข้อ เช่น ความต้องการข้อใดควรมีการดำเนินการทำก่อน
 - กำหนดลำดับความสำคัญของความต้องการ เช่น ระดับผลกระทบของแต่ละความต้องการ

2.3 การออกแบบระบบสารสนเทศหรือซอฟต์แวร์ (Design)

ขั้นตอนนี้หลัก ๆ แล้ว Developer จะนำ Requirement ที่ได้มาออกแบบ เช่น ออกแบบสถาปัตยกรรมที่จะใช้ (Architects) ออกแบบส่วนต่อประสานผู้ใช้งาน (User Interface) ภาษาที่จะใช้ในการพัฒนา ออกแบบฐานข้อมูล ระบบเครือข่ายและความมั่นคงปลอดภัย เป็นต้น ผลลัพธ์ที่ได้จากขั้นตอนนี้จะได้ System Design Specification ซึ่งสามารถให้ผู้มีส่วนเกี่ยวข้องหรือผู้เชี่ยวชาญตรวจสอบและให้คำแนะนำได้



2.4 การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development)

ขั้นตอนนี้ทีม Developer โดยนำ Requirement และ Design ที่ได้จากขั้นตอนที่ 2.2 และ 2.3 มาพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ โดยมีเครื่องมือต่าง ๆ ตามความต้องการของแต่ละระบบ

2.5 การทดสอบระบบสารสนเทศหรือซอฟต์แวร์ (Testing)

เป็นการประกันคุณภาพของระบบสารสนเทศหรือซอฟต์แวร์ โดยการค้นหาข้อผิดพลาด ป้องกันการเกิดข้อผิดพลาด รวมไปถึงตรวจสอบว่าระบบสารสนเทศหรือซอฟต์แวร์ที่พัฒนานั้นเป็นไปตาม Requirement หรือไม่ ในการทดสอบนั้นจะมีการสร้าง Test Case ซึ่งเป็นสถานการณ์และขั้นตอนที่ผู้ใช้งานจะใช้งานระบบ โดยใน Test Case จะมีการระบุ Expected Results คือผลที่คาดหวังจากการทดสอบโดยผลที่คาดหวังนี้จะอ้างอิงตาม Requirement ที่ได้มาจากขั้นตอนการเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis) ในกรณีที่ระบบสารสนเทศหรือซอฟต์แวร์ทำงานถูกต้องเป็นไปตามผลที่คาดหวัง จะทำให้การทดสอบนั้นผ่าน แต่หากไม่เป็นไปตามผลที่คาดหวัง จะทำให้การทดสอบนั้นไม่ผ่าน ต้องให้ Developer ดำเนินการแก้ไข ผู้ทดสอบอาจเลือกวิธีทดสอบแบบ Automated Test ได้ เพื่อให้การทดสอบสามารถทำได้รวดเร็วมากขึ้น

ในขั้นตอนการทดสอบนี้ Project Manager สามารถเพิ่มเติมรายละเอียดของกิจกรรมของการทดสอบได้ตามความเหมาะสม หรือเปลี่ยนแปลงตามแนวทาง (Methodology) ที่ถูกนำมาใช้ในการพัฒนาระบบสารสนเทศ เช่น Agile Development หรือ Waterfall Methodology เป็นต้น

การกำหนดสภาพแวดล้อม (Environment) ในการพัฒนา ทดสอบ และติดตั้งระบบสารสนเทศและซอฟต์แวร์

กำหนดให้สมาคมฯ แบ่งสภาพแวดล้อมเพื่อรองรับการพัฒนา ทดสอบ และติดตั้งระบบสารสนเทศและซอฟต์แวร์ ดังนี้

- 1) Development Environment คือ ระบบสารสนเทศและซอฟต์แวร์ ต้องได้รับการควบคุมการเข้าถึงอย่างเคร่งครัด มีระบบเครือข่ายที่สนับสนุนสภาพแวดล้อม ควรเป็นระบบปิดที่ไม่มีการเชื่อมต่อสภาพแวดล้อมของ Production
- 2) Test Environment คือ ใช้เพื่อการทดสอบระบบสารสนเทศหรือซอฟต์แวร์ หรือการใช้งานอุปกรณ์อื่น ๆ ก่อนการติดตั้งจริง (Deployment) ทั้งนี้ควรเป็นสภาพแวดล้อมที่ใกล้เคียงกับ Production มากที่สุด
- 3) Production Environment คือ สภาพแวดล้อมจริงที่มีการติดตั้งระบบสารสนเทศหรือซอฟต์แวร์ เพื่อใช้งาน

ทั้งนี้การแบ่งแยกสภาพแวดล้อมควรเป็นไปในลักษณะของระบบเครือข่าย (Network) เครื่องคอมพิวเตอร์แม่ข่าย (Server and System) และพื้นที่เชิงกายภาพ (Area/Room) การกำหนดสภาพแวดล้อมในเครื่องคอมพิวเตอร์แม่ข่ายเดียวกัน (เช่น การใช้งาน Virtualized Machine) ต้องมั่นใจว่าการ



ทดสอบที่ล้มเหลวจะไม่ส่งผลกระทบต่อเครื่องคอมพิวเตอร์แม่ข่ายในระดับกายภาพ (Physical Machine Failure) ห้ามมิให้มีการทดสอบใด ๆ เกิดขึ้นบนสภาพแวดล้อม Production หรือเครื่องคอมพิวเตอร์แม่ข่ายของระบบงานใน Production โดยอ้างอิงตามหัวข้อการแบ่งหน้าที่ในการปฏิบัติงานและการจัดทำเอกสารประกอบการปฏิบัติงาน ของการจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and Operations Management) ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)

2.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment)

เป็นขั้นตอนที่นำระบบสารสนเทศหรือซอฟต์แวร์ที่ผ่านการพัฒนาและทดสอบเรียบร้อยแล้วมาติดตั้งในสภาพแวดล้อม Production เพื่อให้สามารถใช้งานได้จริง ขั้นตอนการติดตั้งนี้จะต้องมีการวางแผนอย่างรอบคอบ และมีการเตรียมการเพื่อให้มั่นใจว่าการติดตั้งจะเป็นไปอย่างราบรื่นและไม่ส่งผลกระทบต่อการทำงานขององค์กร อ้างอิงตามหัวข้อนโยบายการบริหารจัดการนำระบบขึ้นใช้งาน (Release & Deployment Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual) และกระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure)

2.7 การบำรุงรักษา (Maintenance)

เป็นขั้นตอนหลังจากที่ระบบสารสนเทศหรือซอฟต์แวร์ถูกติดตั้งใช้งานจริงในสภาพแวดล้อม Production ซึ่งเป็นขั้นตอนในการดูแลและปรับปรุงอย่างต่อเนื่อง เพื่อให้แน่ใจว่าระบบสารสนเทศหรือซอฟต์แวร์สามารถทำงานอย่างถูกต้องโดยไม่มีข้อผิดพลาด และเหมาะสมสอดคล้องกับความต้องการที่เปลี่ยนแปลงของผู้ใช้และองค์กร รวมถึงการป้องกัน Source Code จากภัยคุกคาม นอกจากนี้ การบำรุงรักษา (Maintenance) ยังครอบคลุมถึงการปรับปรุงด้านความมั่นคงปลอดภัย การเพิ่มฟังก์ชันใหม่ และการพัฒนาระบบให้เหมาะสมกับเทคโนโลยีล่าสุดด้วยเช่นกัน โดยขั้นตอนนี้จะต้องดำเนินการอย่างสม่ำเสมอ เพื่อคงคุณภาพกับความน่าเชื่อถือและความมั่นคงปลอดภัยของระบบสารสนเทศและซอฟต์แวร์ในระยะยาว

3. ขั้นตอนการพัฒนากระบวนการสารสนเทศและซอฟต์แวร์

3.1 การวางแผนโครงการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Project Planning)

ก่อนการดำเนินโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ ต้องกำหนดให้มีการจัดทำแผนงานโครงการอย่างละเอียด โดยใช้มาตรฐานของสมาคมฯ หรือของผู้ให้บริการนั้น ๆ ทั้งนี้ ต้องมีเนื้อหาและรายละเอียดอย่างเป็นลายลักษณ์อักษรตามรายการ ดังต่อไปนี้ โดยอ้างอิงแนวทางที่ใช้ในการดำเนินงานโครงการด้านความมั่นคงปลอดภัยสารสนเทศตามหัวข้อ การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ ในเอกสารนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)

- การกำหนดขอบเขต วัตถุประสงค์ และรายละเอียดภาพรวมของโครงการ
- การระบุแนวทาง และกลยุทธ์ที่ใช้ในการพัฒนา



- การระบุผู้รับผิดชอบโครงการ และสมาชิกในโครงการ
- การระบุความเสี่ยงของโครงการ และแนวทางการรับมือ โดยครอบคลุมความเสี่ยงเชิงธุรกิจและเชิงเทคนิค
- การกำหนดกิจกรรม ระยะเวลา และต้นทุนของโครงการ
- ช่องทางและรูปแบบการรายงานความคืบหน้าของโครงการ
- กระบวนการในการควบคุม Configuration Item ในโครงการ เช่น เอกสาร, Package ของซอฟต์แวร์, องค์ประกอบของซอฟต์แวร์ (Software Component) โดยอ้างอิงแนวทางตามหัวข้อการบริหารจัดการ Configuration ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) และอ้างอิงขั้นตอนปฏิบัติการบริหารจัดการองค์ประกอบของบริการด้านเทคโนโลยีสารสนเทศ ในเอกสารกระบวนการจัดองค์ประกอบ (Configuration Management Procedure)
- เอกสารที่จะถูกผลิตขึ้นระหว่างดำเนินการดำเนินโครงการ ทั้งเอกสารส่งมอบและเอกสารที่ใช้อ้างอิงระหว่างดำเนินการดำเนินโครงการ
- เอกสารใด ๆ ที่มีรายละเอียดดังข้างต้น ต้องได้รับการอนุมัติและตรวจสอบโดยพนักงานของสมาคมฯ ตามการแต่งตั้งและบทบาทหน้าที่ความรับผิดชอบ

3.2 การบริหารจัดการความต้องการในการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Requirement Management)

ในการดำเนินโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ ต้องมีเอกสารระบุความต้องการของระบบสารสนเทศหรือซอฟต์แวร์ โดยมีการเก็บข้อมูลจากผู้ใช้งานและผู้ที่เกี่ยวข้อง โดยครอบคลุมรายการ ดังต่อไปนี้

- ความต้องการของระบบสารสนเทศหรือซอฟต์แวร์ (Functional Requirement)
- ความต้องการด้านคุณลักษณะของระบบสารสนเทศหรือซอฟต์แวร์ (Non-functional Requirement) ซึ่งครอบคลุมรายการ ดังต่อไปนี้
 1. ความต้องการด้านความมั่นคงปลอดภัย (Security Requirement) สามารถพิจารณาทั้งระบบหรือจำแนกตามแต่ละ Module ของระบบสารสนเทศหรือซอฟต์แวร์ โดยควรพิจารณาอย่างน้อยดังต่อไปนี้
 - 1) ระดับความมั่นคงปลอดภัยของสารสนเทศ และระบบสารสนเทศ
 - 2) เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยในอดีต
 - 3) ขอบเขตสำหรับการเชื่อมต่อระบบสารสนเทศ
 - 4) ผลกระทบที่อาจเกิดขึ้นกับระบบสารสนเทศอื่น ๆ และภาพรวมของระดับความมั่นคงปลอดภัยสารสนเทศของสมาคมฯ
 - 5) คุณสมบัติด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย



- การควบคุมการเข้าถึง (Access Control) ประกอบด้วย การระบุและพิสูจน์ตัวตน (Identification and Authentication) การกำหนดสิทธิการเข้าถึง (Authorization) และการจัดการหลักฐานการตรวจสอบและการรับผิดชอบต่อการกระทำ (Auditing and Accountability)
- การควบคุมการประมวลผลสารสนเทศในแอปพลิเคชัน (Correct Processing in Applications) ประกอบด้วย การตรวจสอบข้อมูลนำเข้า (Input Data Validation) การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing) การตรวจสอบความถูกต้องของข้อความ (Message Integrity) และการตรวจสอบข้อมูลนำออก (Output Data Validation)
- การป้องกันข้อมูล (Data Protection) ประกอบด้วย การเข้ารหัสข้อมูลที่จัดเก็บ และการเข้ารหัสข้อมูลขณะส่ง
- การสำรองและการกู้คืนระบบ

2. ความต้องการด้านสมรรถนะและประสิทธิภาพ (Performance Requirement) สามารถพิจารณาทั้งระบบหรือจำแนกแต่ละ Module ของระบบสารสนเทศหรือซอฟต์แวร์
3. ความต้องการด้านข้อกำหนด เพื่อสร้างความสอดคล้องกับข้อกำหนด นโยบาย หรือกฎหมาย ที่เกี่ยวข้องกับระบบสารสนเทศหรือซอฟต์แวร์ โดยอ้างอิงกฎหมายและข้อกำหนดที่ต้องปฏิบัติตาม ในเอกสาร รายการกฎหมายและข้อบังคับที่ต้องปฏิบัติตาม (List of Law and Regulatory)

- เอกสารสรุปความต้องการในรายการข้างต้น ต้องดำเนินการเป็นลายลักษณ์อักษรและต้องได้รับการอนุมัติและตรวจสอบโดยพนักงานของสมาคมฯ ตามการแต่งตั้งและบทบาทหน้าที่ความรับผิดชอบ
- เอกสารดังกล่าว ต้องได้รับการตรวจสอบและอนุมัติโดย Project Manager และมีการควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ
- การเปลี่ยนแปลงความต้องการ (Requirement Change Management) หรือคุณลักษณะใด ๆ ของระบบสารสนเทศหรือซอฟต์แวร์ ให้ดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) และชี้แจง Project Manager ตามความเหมาะสม

3.3 การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Design and Analysis)

กำหนดให้มีเอกสารใด ๆ ที่ระบุถึงการออกแบบและวิเคราะห์ระบบสารสนเทศหรือซอฟต์แวร์ ดังต่อไปนี้

- การแสดงถึงการวิเคราะห์ความต้องการของหน่วยงาน และองค์ประกอบ (Module) ของระบบสารสนเทศหรือซอฟต์แวร์ เช่น Business Flowchart
- การวิเคราะห์ถึงความสัมพันธ์ระหว่างผู้ใช้งาน และระบบสารสนเทศหรือซอฟต์แวร์ เช่น Use-case Diagram, Conceptual Diagram



- การวิเคราะห์ถึงข้อมูลเข้า/ออก ระหว่างองค์ประกอบของระบบสารสนเทศหรือซอฟต์แวร์ และการแบ่ง Data Storage เช่น API design, Database design (สามารถพิจารณาได้หลายระดับชั้น)
- การวิเคราะห์ความต้องการเชิงเทคนิค (Technical Requirement) และการรองรับ (Compatibility) ของระบบสารสนเทศหรือซอฟต์แวร์ รวมถึงองค์ประกอบย่อยของระบบสารสนเทศหรือซอฟต์แวร์ เช่น Product Requirement, Software Specification

เอกสารดังกล่าว ต้องได้รับการตรวจสอบและอนุมัติโดย Project Manager และควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ

การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Secure Engineering Principal) ต้องคำนึงถึงหลักวิศวกรรมด้านความมั่นคงปลอดภัยสารสนเทศ โดยมุ่งเน้นการออกแบบเพื่อรองรับการป้องกันคุณสมบัติของข้อมูลสารสนเทศ ได้แก่ ความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) โดยมีแนวทางการพิจารณา ดังนี้

ตารางที่ 1 หลักวิศวกรรมระบบสารสนเทศ

คุณสมบัติ	เกณฑ์พิจารณา	การออกแบบ	
ความลับ (Confidentiality)	เปิดเผยได้ในที่สาธารณะ	การกำหนด ระดับชั้น (Classification)	ข้อมูลทั่วไป
	เปิดเผยได้เพียงบุคคลภายในกลุ่มงานที่เกี่ยวข้อง		ข้อมูลใช้ภายใน
	เปิดเผยได้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับ
	เปิดเผยได้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับมาก
	เปิดเผยได้เฉพาะผู้บริหารระดับสูงหรือบางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับที่สุด
ความถูกต้อง (Integrity)	หากข้อมูลผิดพลาด จะไม่ส่งผลกระทบต่อระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ	ความสำคัญเชิง ข้อมูล (Significance)	ต่ำ
	หากข้อมูลผิดพลาด จะส่งผลในการทำงานผิดพลาดเพียงองค์ประกอบ (Function, Module) หนึ่งในระบบสารสนเทศหรือซอฟต์แวร์เท่านั้น		ปานกลาง
	หากข้อมูลผิดพลาด จะส่งผลในการทำงานผิดพลาดหลายองค์ประกอบ (Function, Module) ในระบบสารสนเทศหรือซอฟต์แวร์เท่านั้น		สูง



คุณสมบัติ	เกณฑ์พิจารณา	การออกแบบ	
	หากข้อมูลผิดพลาด จะส่งผลทำให้ระบบสารสนเทศหรือซอฟต์แวร์ล้มเหลวและหยุดชะงัก		สูงมาก
ความพร้อมใช้ (Availability)	หากขาดข้อมูลดังกล่าว จะไม่ส่งผลกระทบต่อระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ	ความสำคัญเชิงข้อมูล (Significance)	ต่ำ
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) หนึ่งในระบบสารสนเทศหรือซอฟต์แวร์หยุดการทำงาน		ปานกลาง
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) มากกว่าหนึ่งองค์ประกอบในระบบสารสนเทศหรือซอฟต์แวร์หยุดการทำงาน		สูง
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) ระบบสารสนเทศทั้งหมดหรือซอฟต์แวร์หยุดการทำงาน		สูงมาก

3.4 การพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development)

ก่อนการพัฒนาระบบหรือซอฟต์แวร์ ให้มีการดำเนินการกำหนดมาตรฐานในการพัฒนา (Coding Standard) ที่มีเนื้อหาครอบคลุมอย่างน้อยดังนี้ โดยอ้างอิงนโยบายการจัดการ การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual)

- การกำหนดวิธีการตั้งชื่อระหว่างการพัฒนา เช่น การตั้งชื่อตัวแปร, การตั้งชื่อ Package เป็นต้น
- การกำหนดวิธีการสร้างข้อความ Comment
- การกำหนดรูปแบบ (Theme) การแสดงผล (Display) ของระบบสารสนเทศหรือซอฟต์แวร์
- การกำหนดอัลกอริทึม (Algorithm) ที่สามารถนำมาใช้ในการพัฒนา เช่น มาตรฐานการเข้ารหัส, มาตรฐานในการดึงข้อมูลจากฐานข้อมูล
- การกำหนดวิธีการเรียกใช้งานชุดคำสั่งระหว่างองค์ประกอบย่อยของระบบสารสนเทศหรือซอฟต์แวร์ (Function Call)
- การกำหนดชนิดของข้อมูล (Data Type)



- การสร้างชุดคำสั่งต้นแบบและคุณสมบัติการสืบทอด (Inheritance)
- การกำหนดรูปแบบและประเภทของ Log
- กำหนดให้การจัดเก็บ Source Code ของระบบสารสนเทศหรือซอฟต์แวร์ผ่านเครื่องมือควบคุมที่ได้มาตรฐาน โดยมีผู้ที่ได้รับมอบหมายในการบริหารจัดการ

3.5 การทดสอบระบบสารสนเทศและซอฟต์แวร์ (Testing)

กำหนดให้ทุก ๆ ความต้องการ (Requirement) ต้องได้รับการทดสอบ โดยสามารถแบ่งออกได้เป็น 2 ลักษณะ ดังนี้

3.5.1 การทดสอบและตรวจสอบโดยผู้พัฒนา (Verification)

การทดสอบและตรวจสอบโดยผู้พัฒนา มีวัตถุประสงค์เพื่อตรวจสอบความพร้อม ความถูกต้องของระบบสารสนเทศหรือซอฟต์แวร์ เพื่อให้มั่นใจว่าตรงตามความต้องการ โดยประกอบด้วย

- การทดสอบเบื้องต้น (Unit Test)
- การทดสอบการทำงานผสานระหว่างระบบ (System Integration Test)
- การทดสอบความมั่นคงปลอดภัยของระบบ (Security Test) โดยควรครอบคลุมถึง
 - การทดสอบการเข้าถึงข้อมูลและระบบงาน
 - การเข้ารหัสข้อมูล และการปกป้องข้อมูล
 - การตั้งค่าด้านความมั่นคงปลอดภัย เช่น การตั้งค่ารหัสผ่าน การตั้งค่าเวลามาตรฐาน การตั้งค่าการเชื่อมต่อ การจัดเก็บบันทึกเหตุการณ์ (Log) เป็นต้น
 - การทดสอบความมั่นคงปลอดภัยทางเทคนิค ได้แก่ การวิเคราะห์ซอร์สโค้ด (Source Code Analysis) การประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing)

3.5.2 การทดสอบและตรวจสอบโดยผู้ใช้งานในสภาพแวดล้อมจริง (Validation)

เพื่อให้มั่นใจว่าระบบสารสนเทศหรือซอฟต์แวร์ สามารถถูกนำมาใช้ได้จริงในสภาพแวดล้อมจริง และได้รับการยอมรับจากผู้ใช้งาน จำเป็นต้องมีการทดสอบโดยตัวแทนฝ่ายผู้ใช้งาน (User) สามารถแบ่งได้เป็น

- การทดสอบการยอมรับระบบสารสนเทศหรือซอฟต์แวร์ (User Acceptance Test)
 - การทดสอบความพร้อมก่อนการติดตั้งระบบเพื่อใช้งานจริง (Operation Readiness Test)
- กำหนดให้ชุดข้อมูลทดสอบ ต้องเป็นข้อมูลจำลองเท่านั้น ในกรณีมีความจำเป็นต้องใช้ข้อมูลจริงที่มีชั้นความลับหรือเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้มีการดำเนินการขออนุมัติอย่างเป็นทางการเป็นลายลักษณ์อักษร และจะต้องลบข้อมูลทดสอบทั้งหมดออกจากระบบเมื่อเสร็จสิ้นการทดสอบ



กำหนดเอกสารควบคุมการทดสอบระบบสารสนเทศหรือซอฟต์แวร์ ที่ได้รับการตรวจสอบและอนุมัติโดย Project Manager และควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ โดยมีรายละเอียดครอบคลุม ดังนี้

- ชนิดและประเภทของการทดสอบและรายละเอียดเบื้องต้น เช่น วันที่ทดสอบ ผู้ดำเนินการ
- การกำหนดวิธีการและเกณฑ์การทดสอบ เช่น Key Stopper, Testing Methodology
- การกำหนดขั้นตอนการทดสอบและผลลัพธ์ที่คาดหวัง
- การกำหนดเกณฑ์การพิจารณาผลการทดสอบ เช่น ชนิดของผลการทดสอบ (Defect Type)

3.5.3 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of System Test Data)

เพื่อให้มั่นใจว่าข้อมูลที่นำมาทดสอบได้รับการควบคุมและป้องกันอย่างเหมาะสม ผู้พัฒนาและเจ้าของระบบ ควรควบคุมการใช้ข้อมูลสำหรับทดสอบดังนี้

- กำหนดให้มีการควบคุมการเข้าถึงข้อมูลที่ใช้ในการทดสอบเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ควบคุมมิให้นำข้อมูลที่ใช้ในระบบที่ให้บริการจริงไปใช้สำหรับทำการทดสอบระบบ ทั้งนี้ หากมีความจำเป็นต้องใช้ ต้องจัดให้มีการควบคุมอย่างน้อยดังต่อไปนี้
 - ได้รับอนุญาตจากเจ้าของระบบก่อนนำไปใช้ในการทดสอบ
 - ปรับ หรือลบข้อมูลที่มีระดับความลับ “ลับมาก” หรือ “ลับที่สุด”
 - ลบข้อมูลที่ใช้ในการทดสอบภายหลังการทดสอบเสร็จสิ้น
 - มีการบันทึกเหตุการณ์ของการสำเนาข้อมูลจากระบบที่ให้บริการจริงเพื่อใช้ในการทดสอบ

3.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment)

ต้องได้รับความเห็นชอบและอนุมัติผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) ตามหัวข้อนโยบายการบริหารจัดการนำระบบขึ้นใช้งาน (Release & Deployment Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual) และกระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure) อย่างเคร่งครัด

3.7 การปิดโครงการหรือเสร็จสิ้นการพัฒนาโครงการ (Project Closure)

กำหนดพนักงานผู้รับผิดชอบที่ได้รับมอบหมายจากสมาคมฯ ดำเนินการสรุปผลการดำเนินงานทั้งหมด โดยมีเนื้อหาครอบคลุม

- ปัญหาและอุปสรรคที่เกิดขึ้นในโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ การแก้ไขปัญหาหรือองค์ความรู้ใหม่



- ในกรณีที่เป็นการจัดจ้างผู้ให้บริการภายนอก ให้มีการประเมินศักยภาพของผู้ให้บริการภายนอกภายนอกนั้น ๆ
- ข้อมูลอื่น ๆ ตามที่มีร้องขอ

4. การจัดจ้างผู้ให้บริการภายนอก เพื่อการพัฒนากระบวนการสารสนเทศหรือซอฟต์แวร์ (Outsourcing Development)

กำหนดให้ผู้ให้บริการภายนอกใด ๆ ที่ได้รับการจัดจ้างให้พัฒนากระบวนการสารสนเทศหรือซอฟต์แวร์ให้แก่สมาคมฯ ต้องดำเนินการให้สอดคล้องและปฏิบัติตามนโยบายของสมาคมฯ อย่างเคร่งครัด โดยอ้างอิงหัวข้อนโยบายการบริหารจัดการผู้ให้บริการ ตามเอกสารกระบวนการบริหารจัดการผู้ให้บริการ (Supplier Management Procedure) ทั้งนี้ ผู้ให้บริการภายนอกจะต้องเป็นผู้เชี่ยวชาญเฉพาะด้าน และในระหว่างการดำเนินโครงการ บุคลากรที่เกี่ยวข้องและเข้าถึงข้อมูลของสมาคมฯ ต้องมีการลงนามข้อตกลงว่าด้วยการรักษาความลับขององค์กร (Mutual Confidentiality Agreement) ที่มีผลทางกฎหมายแม้สิ้นสุดโครงการ

เพื่อให้การตรวจสอบการพัฒนากระบวนการสารสนเทศหรือซอฟต์แวร์โดยการจ้างผู้ให้บริการภายนอกนั้นเป็นระบบหรือซอฟต์แวร์ที่มีมั่นคงปลอดภัย และมีการพัฒนาที่เป็นไปตามความต้องการขององค์กร ควรกำหนดเกณฑ์ดังต่อไปนี้สำหรับการพิจารณาตรวจสอบระบบสารสนเทศหรือซอฟต์แวร์

- ต้องมีการกำหนดข้อตกลงการให้สิทธิ์ใช้งาน การเป็นเจ้าของ Code และสิทธิ์ในทรัพย์สินทางปัญญาที่เกี่ยวข้องกับเนื้อหาที่จ้างพัฒนา โดยอ้างอิงตามหัวข้อกรรมสิทธิ์ในข้อมูล นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)
- ต้องมีข้อกำหนดหรือสัญญาสำหรับการออกแบบ การเขียนโค้ด และแนวทางการทดสอบที่มีมั่นคงปลอดภัย
- ต้องมีการทดสอบสิ่งส่งมอบก่อนยอมรับ เพื่อประเมินคุณภาพและความถูกต้องของสิ่งที่ส่งมอบ
- ต้องมีหลักฐานแสดงว่ามีการกำหนดระดับความสามารถด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวขั้นต่ำที่สามารถยอมรับได้
- ต้องมีหลักฐานแสดงว่ามีการทดสอบอย่างเพียงพอ เพื่อป้องกันช่องโหว่ที่ทราบ
- ต้องมีหลักฐานแสดงว่าการดำเนินการพัฒนาเป็นไปตาม Requirement ที่ทางสมาคมฯ ได้กำหนดไว้

5. เอกสารที่เกี่ยวข้อง (Related Documents)

- ISO-1PC-02 ขอบเขตระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS and ISMS Scope)
- ISO-1PC-01 นโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual)
- IT-1PC-01 นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)



- IT-2PR-02 กระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure)
- RMEM-2PR-02 กระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure)
- IT-2PR-03 กระบวนการจัดองค์ประกอบ (Configuration Management Procedure)
- PU-2PR-01 กระบวนการบริหารจัดการผู้ให้บริการ (Supplier Management Procedure)
- ISO-2SD-01 รายการกฎหมายและข้อบังคับที่ต้องปฏิบัติตาม (List of Law and Regulatory)



สมาคมสโมสรนักลงทุน
Investor Club Association

นโยบายและการบริหารเทคโนโลยีสารสนเทศ
(IT Policy and Management)

รหัสเอกสาร:	IT-1PC-01
หมายเลขปรับปรุงเอกสาร:	6.0
วันที่เอกสารมีผลบังคับใช้:	3 ธันวาคม 2567
เจ้าของเอกสาร:	ฝ่ายเทคโนโลยีสารสนเทศ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ-นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
ผู้จัดทำ	สมโภช เพ็ญจันทิก	หัวหน้าแผนก บริหารระบบ		29 พฤศจิกายน 2567
ผู้ทบทวน	สิริวรรณ ฉลากรไชยา	หัวหน้าฝ่าย เทคโนโลยีสารสนเทศ		29 พฤศจิกายน 2567
ผู้อนุมัติ	กรองนก มานะกิจจงกล	ผู้จัดการ สมาคมสโมสรนักลงทุน		2 ธันวาคม 2567

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุง เอกสาร (version):	วันที่ปรับปรุง เอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
2.0	4 พ.ค. 64	สิริวรรณ ฉลากรไชยา	แก้ไขเนื้อหาให้มีความชัดเจนยิ่งขึ้น 1. การรักษาความปลอดภัย - แนวทาง 2. การใช้อินเทอร์เน็ต 3. การใช้อุปกรณ์คอมพิวเตอร์ - แนวทาง 4. การใช้คอมพิวเตอร์แบบพกพาและการ เชื่อมต่อระบบเครือข่าย 5.แก้ไข ผู้ให้ข้อมูล เป็น ผู้เปิดเผยข้อมูลให้ ถูกต้องตามคำจำกัดความ
3.0	26 ก.ค. 66	สิริวรรณ ฉลากรไชยา	เพิ่มเติมเนื้อหา 1.การจัดกลุ่มทรัพย์สิน (Asset Grouping) 2.การใช้งานคอมพิวเตอร์แบบพกพาในการ ปฏิบัติงานจากภายนอกและการแก้ไขปัญหา จากระยะทางไกล
4.0	20 พ.ย. 66	สิริวรรณ ฉลากรไชยา	เพิ่มเติมเนื้อหา เอกสารแนบ 2 ข้อ 3 ข้อตกลง ทั่วไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			เพิ่มข้อ 3.5 ผู้รับข้อมูลจะต้องดำเนินการลบข้อมูลที่เป็นข้อมูล Sensitive ภายในระยะเวลา 3 เดือนหลังจากสิ้นสุดระยะเวลาการดำเนินงานของโครงการและรายงานกลับเพื่อให้ทราบว่าดำเนินการแล้วตามมาตรฐาน
5.0	25 เม.ย. 67	สิริวรรณ ฉลากรไชยา	1.นโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy) 1.1 <u>แก้ไขข้อความ</u> ● ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ <u>เป็น</u> ● ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ และต้องมีการกำหนดสิทธิ์ผู้ใช้งานในระดับสูง 1.2 <u>เพิ่มข้อความ</u> ● ในการเข้าใช้งานของผู้ใช้งานในระดับสูง จะต้องมีการร้องขอใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงในแต่ละครั้ง ● พนักงานที่มีความประสงค์ร้องขอเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Account) ต้องจัดทำแบบฟอร์มร้องขอบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Request Form) (IT-2FM-07) ● ผู้ดูแลระบบบันทึกทะเบียนบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privileged Account Inventory) (IT-2FM-09) สำหรับใช้ในการอ้างอิง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			2. สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน 2.1 <u>แก้ไขข้อความ</u> - รายชื่อผู้ใช้งานจะถูกตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานออก <u>เป็น</u> - รายชื่อผู้ใช้งานจะถูกตั้งค่าปิดการใช้งานบัญชีล่วงหน้าและตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานลาออก <u>เพิ่มข้อความ</u> - ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการตรวจสอบวันที่เข้าสู่ระบบล่าสุดของพนักงานที่ลาออก (Check Last Logon Date) ในกรณีที่มีการแจ้งลาออกล่าช้าหรือมีการเลิกจ้างฐานละทิ้งหน้าที่ โดยระบุในส่วนรายละเอียด

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			เพิ่มเติมของแบบฟอร์มการเพิกถอนสิทธิ์ใช้งานบัญชีผู้ใช้ พร้อมบันทึกหลักฐานการตรวจสอบ ฝ่ายเทคโนโลยีสารสนเทศกำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที
6.0	29 พ.ย. 67	สมโภช เผือกจันทิก	- แก้ไขข้อมูล “ศูนย์ข้อมูล” เป็น “ห้องเซิร์ฟเวอร์” - การลงทะเบียนทรัพย์สิน <u>เพิ่มเติม</u> ประเภทของทรัพย์สิน 2 รายการ ได้แก่ Process Asset และ Site Asset - สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน <u>เพิ่มเติม</u> ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของสมาคม ฯ ได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง <u>เพิ่มเติม</u>ข้อความ การแบ่งแยกระบบสารสนเทศ เพื่อลดความผิดพลาดหรือผลกระทบอันเกิดจากการดำเนินการทดสอบ ควรมีการแยกระบบสารสนเทศที่ให้บริการจริง ออกจากระบบสารสนเทศที่ใช้ในการพัฒนา และทดสอบ (เฉพาะระบบที่สามารถดำเนินการได้) <u>เพิ่ม</u> การจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			Operations Management) ในหน้าที่ความรับผิดชอบของผู้ใช้ในหัวข้อ ดังนี้ ● ข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์ หรือส่งออกไปภายนอกองค์กรต้องจัดให้มีการเข้ารหัสข้อมูล ● การจัดทำ การจัดเก็บ การส่งต่อ ลบ ทำลายข้อมูล จะต้องดำเนินการตามขั้นตอนการปฏิบัติการจัดระดับชั้น ความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล ● ต้องควบคุมให้มีมาตรการการปิดบังข้อมูลสารสนเทศเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน 6. แนวทางการเข้าสู่ห้องเซิร์ฟเวอร์ <u>เพิ่มเติม</u> ข้อความ ดังนี้ 6.1 จะต้องกรอกแบบคำขออนุญาตเข้าพื้นที่ห้องเซิร์ฟเวอร์ 6.2 ห้ามนำวัตถุระเบิด เชื้อเพลิง วัสดุติดเพลิงง่าย อาวุธ สารเคมี หรือสิ่งอื่นใดที่อาจก่อให้เกิดความเสียหายทั้งต่อชีวิตและทรัพย์สิน เข้ามาบริเวณห้องเซิร์ฟเวอร์ 7. <u>เพิ่มข้อความ</u> ในหัวข้อการควบคุมการใช้งานระบบเครือข่าย ดังนี้ ● ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของสมาคม ฯ ให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับอาทิพระราชบัญญัติว่าด้วยการกระทำ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับ (ฉบับที่ 2) พ.ศ. 2560 8. <u>เพิ่มข้อความ</u> ในหัวข้อการใช้คอมพิวเตอร์แบบพกพาและการเชื่อมต่อระบบเครือข่าย ดังนี้ ● การทำลายสื่อบันทึกข้อมูล โดยผู้ให้บริการภายนอก จะต้องมีการทำสัญญาข้อตกลงเรื่องการรักษาความลับ 9. <u>เพิ่มข้อความ</u> ในหัวข้อการสำรองข้อมูล ดังนี้ ● สำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลง โดยข้อมูลสำรองนี้จะถูกจัดเก็บไว้ในที่ปลอดภัย ● ทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง 10. เพิ่มหัวข้อการจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ 11. เพิ่มหัวข้อการบริหารจัดการ Configuration 12. เพิ่มหัวข้อการบริหารจัดการคลาวด์

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

สารบัญ

เรื่อง	หน้า
บทนำ	9
ระเบียบว่าด้วยขอบเขตอำนาจหน้าที่และความรับผิดชอบ	10
นโยบายระบบเทคโนโลยีสารสนเทศ	11
คณะกรรมการสารสนเทศสมาคมสโมสรนักลงทุน	13
ฝ่ายเทคโนโลยีสารสนเทศ	14
ความปลอดภัยของอุปกรณ์ และข้อมูล	16
การรักษาความปลอดภัย	25
การเข้าสู่ห้องเซิร์ฟเวอร์	31
กรรมสิทธิ์ในข้อมูล	33
การใช้อินเทอร์เน็ต	34
การใช้จดหมายอิเล็กทรอนิกส์ หรืออีเมล	36
ลิขสิทธิ์โปรแกรม และการสั่งซื้อ หรือการเช่าใช้	40
อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์	42
การแจ้งให้ทราบเรื่องการระงับให้บริการชั่วคราว	44
การใช้อุปกรณ์คอมพิวเตอร์	45
การกู้คืนข้อมูล และระบบคอมพิวเตอร์ที่ได้รับความเสียหาย	49
การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ	51
การบริหารจัดการ Configuration	52
การบริหารจัดการคลาวด์	53
เอกสารแนบ 1	54
เอกสารแนบ 2	55

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

บทนำ

นโยบายเทคโนโลยีสารสนเทศที่จัดทำขึ้นครอบคลุมระบบการปฏิบัติงานคอมพิวเตอร์ ระบบโทรศัพท์ รวมถึงอุปกรณ์ต่าง ๆ ในระบบเครือข่ายคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน เพื่อให้บริการพนักงานและบริษัทภายนอก โดยคำนึงถึงความรับผิดชอบต่อด้านกฎหมาย และได้รับความไว้วางใจจากภาคธุรกิจหลากหลายประเภท

เอกสารฉบับนี้จะกล่าวถึงนโยบายระบบเทคโนโลยีสารสนเทศขององค์กร หน้าที่ความรับผิดชอบของผู้ใช้ระบบคอมพิวเตอร์ และฝ่ายเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อวางแผนนโยบายระบบเทคโนโลยีสารสนเทศให้กับสมาคมสโมสรนักลงทุน และเพื่อให้ฝ่ายต่าง ๆ รวมทั้งหน่วยงานที่เกี่ยวข้องได้ทราบถึงแนวทางการดำเนินงานของพนักงานฝ่ายเทคโนโลยีสารสนเทศและพนักงานสมาคมสโมสรนักลงทุน

ขอบเขตและความรับผิดชอบ

การบริหารการใช้ข้อมูลระบบสารสนเทศภายในองค์กรเป็นความรับผิดชอบหลักของแต่ละฝ่ายในสมาคม ฯ อย่างไรก็ตาม ฝ่ายเทคโนโลยีสารสนเทศยังคงมีอำนาจหน้าที่ควบคุมดูแลระบบสารสนเทศของฝ่ายต่าง ๆ ในองค์กรโดยรวม

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบงานด้านการบริหารจัดการนโยบายในระบบเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน ทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้มีอำนาจหน้าที่ในการตรวจสอบ มอบหมาย และประสานงานในการปฏิบัติงานด้านต่าง ๆ ในระบบเทคโนโลยีสารสนเทศของทั้งองค์กร

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ระเบียบว่าด้วยขอบเขตอำนาจหน้าที่และความรับผิดชอบ

สมาคมสโมสรนักลงทุนมีความต้องการให้อุปกรณ์และการใช้งานในระบบเทคโนโลยีสารสนเทศขององค์กรคงสภาพดี และพร้อมใช้งานในเครื่องขององค์กร เป้าหมายนี้ถือเป็นภารกิจของฝ่ายเทคโนโลยีสารสนเทศ และเพื่อให้การดำเนินงานตามเป้าหมายลุล่วง จึงได้วางระเบียบที่จะสนับสนุนภารกิจดังกล่าวไว้ดังนี้

ฝ่ายเทคโนโลยีสารสนเทศ มีรายละเอียดภารกิจดังนี้

1. ดูแล วางแผน แก้ไข และปรับปรุงระบบคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง เพื่อให้การใช้งานอยู่ในสภาพดีและมีประสิทธิภาพในการทำงานสูงสุด
2. จัดหา แก้ไข จัดเก็บ ประมวลผล เรียกใช้ นำเสนอ และเผยแพร่โปรแกรมหรือข้อมูลอิเล็กทรอนิกส์ให้กับพนักงานทุกระดับในองค์กร
3. สร้างความกลมกลืนในระบบเทคโนโลยีสารสนเทศเพื่อเอื้อประโยชน์ต่อการดำเนินธุรกิจในแต่ละวันขององค์กร

ภารกิจที่กำหนดขึ้นนี้จะต้องสนับสนุน ส่งเสริม และกลมกลืนเป็นหนึ่งเดียวกับแผนงาน ขั้นตอนการปฏิบัติงาน และวัตถุประสงค์ที่กำหนดขึ้นโดยผู้บริหารระดับสูง

เป็นที่ทราบทั่วกันว่า บทบาทของฝ่ายเทคโนโลยีสารสนเทศในองค์กรนั้นแตกต่างจากหน่วยงานอื่น ๆ ตรงที่นอกเหนือจากผลงานโดยตรงที่เกิดขึ้นภายในฝ่ายเอง เช่น การซ่อมแซมและดูแลรักษาอุปกรณ์คอมพิวเตอร์แล้ว ผลงานของฝ่ายเทคโนโลยีสารสนเทศยังประกอบด้วยผลงานอันเกิดจากความร่วมมือกับฝ่ายอื่น ๆ โดยไม่สามารถแยกเป็นผลสำเร็จที่เป็นเฉพาะของตนเองได้ หากแต่ว่าภารกิจของฝ่ายเทคโนโลยีสารสนเทศจะบรรลุไปด้วยความความร่วมมือ และการใช้บริการจากฝ่ายธุรกิจอื่น ๆ ขององค์กร มาตรฐานความสำเร็จของฝ่ายเทคโนโลยีสารสนเทศจึงมาจากทั้งผลการปฏิบัติงานภายในฝ่ายและความสำเร็จในการเพิ่มมูลค่าให้กับธุรกิจขององค์กรด้วยการนำเสนอระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและได้ประสิทธิผล

อีกหนึ่งบทบาทของฝ่ายเทคโนโลยีสารสนเทศเพื่อสนับสนุนเป้าหมายดังกล่าวข้างต้น คือ การมีส่วนร่วมในการให้คำแนะนำสำหรับการจัดทำงบประมาณเพื่อลงทุนในระบบเทคโนโลยีสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศจะทำการประเมินถึงผลกระทบในทางเทคนิค การบริหารจัดการ การให้บริการ และการเงินของเทคโนโลยีสารสนเทศที่จะมีต่อการดำเนินธุรกิจขององค์กรอย่างเหมาะสม ทันท่วงทีสถานการณ์ และด้วยความถูกต้อง

ในหน่วยงานที่ฝ่ายเทคโนโลยีสารสนเทศเข้าไปให้บริการ ฝ่ายเทคโนโลยีสารสนเทศจะมีบทบาทในการจัดเตรียม และดูแลกำกับแผนระยะยาวให้เป็นไปตามวัตถุประสงค์ โดยแผนนี้จะรวบรวมแผนระยะสั้นและเป้าหมายที่ต้องบรรลุ นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศจะต้องจัดเตรียม เก็บรักษา และปรับปรุงมาตรฐาน และขั้นตอนในการปฏิบัติงาน เพื่อสะดวกในการใช้อ้างอิงกรณีที่มีการปรับเปลี่ยนระบบในอนาคต ในขณะเดียวกันก็ไม่ละเลยที่จะให้บริการที่ตอบสนองความต้องการเร่งด่วนที่ร้องขอมา

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

นโยบายระบบเทคโนโลยีสารสนเทศ

หลักการ

ระบบสารสนเทศ ข้อมูล ทรัพย์สินคอมพิวเตอร์ ซึ่งรวมถึงเครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ การสื่อสารด้วยข้อมูลและเสียง (ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์) เครื่องพิมพ์ และอุปกรณ์/ระบบต่อพ่วง ทั้งหมดนี้ถือเป็นทรัพย์สินของสมาคมสโมสรนักลงทุน ผู้ที่ได้รับสิทธิในการใช้ พึงใช้ด้วยความระมัดระวังเพื่อรักษาความถูกต้องของระบบคอมพิวเตอร์ และข้อมูล และเพื่อความปลอดภัยของทรัพย์สิน อนึ่งการใช้ทรัพย์สินเหล่านี้จะต้องใช้เพื่องานที่เกี่ยวข้องกับการดำเนินงานของสมาคม ฯ เท่านั้น

การสื่อสารทุกรูปแบบที่เกิดขึ้นภายในสมาคมสโมสรนักลงทุน หรือส่งออกจากสมาคมสโมสรนักลงทุน ถือเสมือนหนึ่งเป็นตัวแทนและภาพลักษณ์ขององค์กร พนักงาน คณะกรรมการบริหาร และผู้ได้รับสิทธิใช้งาน ดังนั้นจึงควรเป็นไปอย่างเหมาะสม สุภาพ และดำรงไว้ซึ่งความเป็นมืออาชีพ

การรับทราบนโยบาย

พนักงานขององค์กร และบุคคลหรือนิติบุคคลที่ได้รับว่าจ้างโดยสมาคมสโมสรนักลงทุน จะต้องอ่านทำความเข้าใจนโยบายระบบเทคโนโลยีสารสนเทศ และลงนามรับทราบในเอกสาร Acknowledgement Statement ก่อนที่จะเข้าใช้ระบบเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน (ดูตัวอย่างตามเอกสารแนบ 1)

แนวทาง

ทรัพย์สินทางด้านเทคโนโลยีสารสนเทศขององค์กร หมายถึง เครื่องมืออุปกรณ์ระบบคอมพิวเตอร์ โปรแกรมคำสั่ง ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ขนาดเล็ก (LAN) เครือข่ายคอมพิวเตอร์ขนาดกลาง (WAN) โทรศัพท์ และระบบการสื่อสารอื่น ๆ (ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์) การจัดการระบบเทคโนโลยีสารสนเทศต้องดำเนินการตามขั้นตอนการ จัดตั้งงบประมาณ และการสั่งซื้อ หาก ทรัพย์สินทางด้านเทคโนโลยีสารสนเทศใด ที่ไม่ได้มีการจัดตั้งงบประมาณไว้ ให้คณะกรรมการของสมาคมสโมสรนักลงทุน เป็นผู้ทำการอนุมัติตามอำนาจการสั่งจ่าย ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการควบคุมการใช้ทรัพยากรดังกล่าว ให้ใช้ได้อย่างมีประสิทธิภาพและคงไว้ซึ่งความปลอดภัยของข้อมูล

บทสงวนสิทธิ

ฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการติดตาม ตรวจสอบ กลั่นกรอง ปกป้องข้อมูลตามความเหมาะสม เพื่อให้สอดคล้องกับนโยบายขององค์กร การเผยแพร่ข้อมูลขององค์กรโดยพลการ การละเมิดสิทธิเข้าใช้งานระบบ และการใช้ประโยชน์จากทรัพย์สินโดยไม่ได้รับอนุญาตถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมายได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

บทลงโทษทางวินัย

การละเมิดกฎระเบียบที่กำหนดในนโยบายระบบเทคโนโลยีสารสนเทศถือว่าเป็นความผิดทางวินัย ซึ่งผู้กระทำผิดอาจถูกลงโทษโดยการตัดสิทธิต่างๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน

หลักการ

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน มีบทบาทหน้าที่ในการให้คำแนะนำ วางแผน และมีบทบาทในการอนุมัติเรื่องที่เกี่ยวข้องกับการใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศทั้งหมดเพื่อประโยชน์ในการใช้งานสูงสุดของสมาคมสโมสรนักลงทุน

ความรับผิดชอบ

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน มีอำนาจหน้าที่ในการดูแลกิจกรรมของระบบเทคโนโลยีสารสนเทศภายในองค์กร ตามคำสั่งแต่งตั้งของสมาคม ดังนี้

- กำกับ ดูแลการพัฒนาระบบดิจิทัลของสมาคม เพื่อเพิ่มประสิทธิภาพในการดำเนินงานและในการให้บริการแก่ผู้ประกอบการ ให้ระบบมีความมั่นคงและปลอดภัย
- กำกับ ดูแลระบบดิจิทัลของสมาคม ให้สอดคล้องกับนโยบาย และเชื่อมโยงกับระบบดิจิทัลของภาครัฐ ด้านส่งเสริมการลงทุนอย่างมีประสิทธิภาพ
- เสนอแนะการพัฒนาระบบดิจิทัลของสมาคม แก่คณะอนุกรรมการบริหาร และคณะกรรมการสมาคม

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน มีหน้าที่รายงาน และมีสายงานขึ้นตรงต่อคณะกรรมการสมาคมสโมสรนักลงทุน การปรับเปลี่ยนหน้าที่ และสถานะของคณะอนุกรรมการต้องได้รับอนุมัติจากประธานคณะอนุกรรมการพัฒนาระบบสารสนเทศสมาคมสโมสรนักลงทุน จะมีการประชุมตามที่ประธานของคณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน กำหนด

หมายเหตุ: รายชื่อคณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน ตามคำสั่งแต่งตั้งของกรรมการสมาคมสโมสรนักลงทุนในแต่ละสมัย

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ฝ่ายเทคโนโลยีสารสนเทศ

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่สรรหาระบบสารสนเทศ และเทคโนโลยี ตามวัตถุประสงค์ และนโยบาย ของหน่วยงานในสมาคมสโมสรนักลงทุน

คำจำกัดความ

โครงสร้างของ ฝ่ายเทคโนโลยีสารสนเทศแบ่งเป็น 2 กลุ่ม ดังนี้

1. กลุ่มซอฟต์แวร์ระบบงาน และ ธุรกิจ
2. กลุ่มเครือข่ายเน็ตเวิร์คและเทคโนโลยี

ความรับผิดชอบ

ฝ่ายเทคโนโลยีสารสนเทศมีบทบาทในการกำกับดูแลการปฏิบัติงานทั้งหมดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศภายในองค์กร โดยมีหน้าที่ดังนี้

- เป็นผู้ดำเนินการกำหนดนโยบายและกลยุทธ์ในระยะยาว ที่เอื้อประโยชน์ชัดเจนต่อธุรกิจ และดูแลให้ระบบเทคโนโลยีสารสนเทศในอนาคตสามารถรองรับการขยายตัวขององค์กร
- สนับสนุนการทำงานร่วมกันของทุกหน่วยงานที่มีหน้าที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ โดยการสร้างเอกภาพทางด้านแนวความคิดที่เสริมสร้างคุณค่าและแนวทางการทำงาน
- แสวงหาโอกาสและช่องทางในการสนับสนุนการใช้เทคโนโลยี ที่เป็นประโยชน์ต่อองค์กรโดยรวม
- จัดหาผู้เชี่ยวชาญ ผู้ช่วยเหลือ และผู้ประสานงานเพื่อพัฒนา และปรับปรุงเทคโนโลยีสารสนเทศขององค์กร
- สรรหาระบบเทคโนโลยีสารสนเทศที่สามารถใช้ร่วมกันได้อย่างมีประสิทธิภาพ และคุ้มค่าต่อการลงทุน ทั้งนี้หมายถึงการจัดหาระบบอุปกรณ์ และการพัฒนาบุคลากรให้กับหน่วยธุรกิจ
- เป็นผู้ดำเนินการพัฒนานโยบายระบบเทคโนโลยีสารสนเทศ ตลอดจนกำหนดมาตรฐานและขั้นตอนการทำงาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หน้าที่หลัก

โดยทั่วไป ฝ่ายเทคโนโลยีสารสนเทศจะต้องทำหน้าที่เกี่ยวกับ

- ดูแล บริหารจัดการระบบเครื่องคอมพิวเตอร์ อุปกรณ์ฮาร์ดแวร์ และอุปกรณ์เสริมต่างๆ เพื่อให้การใช้งานประจำวันเป็นไปอย่างมีประสิทธิภาพ
- ดูแล บริหารจัดการระบบเครือข่ายเน็ตเวิร์คเช่นระบบ LAN และ WAN
- บริการให้ความช่วยเหลือและแก้ไขปัญหาในการใช้งานระบบคอมพิวเตอร์
- ดูแลรักษาและแก้ไขปัญหาาระบบซอฟต์แวร์ที่ใช้งานประจำวันให้ใช้งานได้อย่างมีประสิทธิภาพ
- แนะนำและจัดการระบบซอฟต์แวร์ใหม่ วางแผนการประยุกต์ใช้งาน เพื่อเพิ่มประสิทธิภาพในการทำงานขององค์กร
- ตรวจสอบและอนุมัติ ข้อกำหนดทางเทคนิคของระบบ (Specification)
- บริการกู้/แก้ไขความเสียหายของข้อมูล (ตามรายละเอียดในหัวข้อความปลอดภัยของอุปกรณ์และข้อมูล)
- ให้คำปรึกษาและบริการเชื่อมต่อระหว่างระบบงานเพื่อสามารถให้ใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพและลดความซ้ำซ้อนของข้อมูล

สายบังคับบัญชา

ฝ่ายเทคโนโลยีสารสนเทศซึ่งบริหารโดยหัวหน้าฝ่ายเทคโนโลยีสารสนเทศจะต้องอยู่ในความรับผิดชอบและรายงานต่อ ผู้จัดการสมาคมสโมสรนักลงทุน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ความปลอดภัยของอุปกรณ์ และข้อมูล

หลักการ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้แนวทางด้านความมั่นคงปลอดภัยของสารสนเทศ โดยพิจารณาองค์ประกอบ 3 ข้อหลัก ได้แก่

องค์ประกอบ	คำอธิบาย
ความลับ (Confidentiality)	การรักษาไว้ซึ่งความลับของสารสนเทศ ไม่ถูกเปิดเผยแก่ระบบ คน และ/หรือหน่วยงานที่ไม่ได้มีส่วนเกี่ยวข้อง
ความสมบูรณ์ (Integrity)	การรักษาไว้ซึ่งความถูกต้องเสถียรภาพของสารสนเทศ ไม่ถูกแก้ไขหรือนำไปใช้อย่างผิดวิธี และสามารถตรวจสอบความถูกต้องของสารสนเทศก่อนการนำไปใช้งานได้
ความพร้อมใช้ (Availability)	การรักษาไว้ซึ่งความพร้อมใช้งานของสารสนเทศ

โดยองค์ประกอบข้างต้น จะถูกนำมาพิจารณาเป็นมูลค่าของทรัพย์สินสารสนเทศในเชิงความมั่นคงปลอดภัย อันรวมไปถึงทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับสารสนเทศ

เป้าหมายสำคัญของการดำเนินกิจกรรมตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือ การลดและหลีกเลี่ยงปัญหาการละเมิดความมั่นคงปลอดภัยสารสนเทศ อันส่งผลต่อภาพลักษณ์และความเชื่อมั่นของผู้ใช้งานระบบ โดยมีการวางเป้าหมายเชิงธุรกิจ คือ ระบบสารสนเทศของสมาคมสโมสรนักลงทุนที่เป็นมืออาชีพในการให้บริการด้วยระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย (Information Security)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

แนวทาง

- 1) แนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดเกณฑ์ในการยอมรับความเสี่ยง

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ยึดแนวทางการพิจารณาความเสี่ยงที่มีผลกระทบต่อทรัพย์สินสารสนเทศทั้งทางตรงและทางอ้อม ผ่านการประเมินมูลค่าความเสียหาย และโอกาสการเกิดขึ้นของภัยคุกคามที่อาศัยช่องโหว่ของทรัพย์สินหรือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ที่ไม่มีประสิทธิภาพ รวมถึงการจัดการการเกิดการเปลี่ยนแปลง (Change) และการร้องขอเหตุผิดปกติ (Incident)

- 2) การลงทะเบียนทรัพย์สิน

ระบบสารสนเทศ หรืออุปกรณ์ที่อยู่ภายในขอบเขตการดำเนินงาน จะต้องได้รับการจำแนกประเภทของทรัพย์สิน ซึ่งจะช่วยให้ผู้ประเมินใช้ในการพิจารณาวิเคราะห์จุดอ่อนหรือช่องโหว่ (Vulnerability) ตลอดจนภัยคุกคาม (Threat) ได้อย่างครอบคลุม โดยแบ่งออกเป็น 5 ประเภทหลัก ได้แก่

ประเภทของทรัพย์สิน	ตัวอย่าง
Hardware Asset	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์สนับสนุนโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวข้อง
Software Asset	ระบบปฏิบัติการ ระบบสารสนเทศ โปรแกรมประยุกต์
Information Asset	ข้อมูลในฐานข้อมูล เอกสาร ข้อมูลการตั้งค่าระบบ ข้อมูล Log คู่มือการปฏิบัติงาน
People Asset	พนักงานและผู้ที่เกี่ยวข้อง
Service Asset	บริการจากหน่วยงานภายนอก หรือหน่วยงานภายใน
Process Asset	กระบวนการ กระบวนการย่อย หรือกิจกรรมที่สำคัญที่หากเสียหาย สูญเสียไปแล้วจะมีผลต่อการปฏิบัติงานตามภารกิจขององค์กร
Site Asset	อาคาร สถานที่ตั้ง พื้นที่การแบ่งเขตโซนภายในสถานที่ เช่น ห้องเซิร์ฟเวอร์ พื้นที่ปฏิบัติงานของเจ้าหน้าที่ เป็นต้น

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

3) การจัดกลุ่มทรัพย์สิน (Asset Grouping)

ในกรณีที่ทรัพย์สินหลายรายการมีความคล้ายคลึงกันหรือเป็นชนิดเดียวกัน เจ้าของทรัพย์สินสามารถจัดกลุ่มทรัพย์สิน โดยการจัดทำรายการทรัพย์สินแยกย่อย เพื่อลดจำนวนรายการทรัพย์สินในการประเมินความเสี่ยง (ประเมินเป็นกลุ่มของทรัพย์สินแทน) และสามารถบริหารจัดการง่ายขึ้น ตัวอย่างกลุ่มของทรัพย์สิน กลุ่มเครื่องคอมพิวเตอร์แม่ข่าย (Server), กลุ่มอุปกรณ์เครือข่าย (Network Device), กลุ่มอุปกรณ์ที่เกี่ยวข้อง (Facility) เป็นต้น โดยรายละเอียดนิยามและรูปแบบข้อมูลที่บันทึกลงในแบบฟอร์มบัญชีทรัพย์สิน (IT-2FM-05) ให้อ้างอิงจาก IT-2PR-03 กระบวนการจัดองค์ประกอบ (Configuration Management Procedure)

4) ประเมินมูลค่าของทรัพย์สิน (Asset Value Evaluation)

ในการประเมินมูลค่าของทรัพย์สินนั้น กำหนดให้ใช้องค์ประกอบด้านความมั่นคงปลอดภัย (Security Components) เป็นเกณฑ์ในการพิจารณา โดยอย่างน้อยประกอบด้วย

- **การรักษาความลับ (Confidentiality):** ทรัพย์สินหรือข้อมูลจะเป็นความลับ อนุญาตให้ผู้ที่มีสิทธิ์เท่านั้นที่จะสามารถเข้าถึงได้
- **การรักษาความถูกต้อง ครบถ้วนสมบูรณ์ (Integrity):** ทรัพย์สินหรือข้อมูลที่จัดเก็บ หรือที่ผ่านการประมวลผลจะต้องมีความถูกต้อง ครบถ้วนสมบูรณ์ ไม่ถูกเปลี่ยนแปลง โดยไม่ได้รับอนุญาต
- **ความพร้อมใช้งาน (Availability):** ทรัพย์สินหรือข้อมูลจะต้องพร้อมใช้งานในเวลาที่ต้องการ

$$\text{Asset Value} = \sum_{i=1}^n (\text{loss value of security components} \times \text{weight})$$

สมาคมสโมสรนักลงทุน กำหนดให้มีการพิจารณาผลกระทบของการสูญเสียคุณลักษณะ C-I-A ในแต่ละด้านมุมของการให้บริการภายใต้ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยอย่างน้อยครอบคลุม ดังนี้

- ความสามารถในการให้บริการ หรือปฏิบัติงานของหน่วยงาน (Operation Perspective)
- ผลกระทบด้านชื่อเสียงองค์กรและภาพลักษณ์ (Reputation)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

มูลค่าทรัพย์สิน (Total Asset Value) จะถูกแบ่งระดับชั้นความสำคัญ โดยการแบ่งช่วงสัดส่วนของค่าเต็มของมูลค่าทรัพย์สิน (100%) กำหนดเกณฑ์พิจารณา ดังนี้

ระดับ	ค่า Total Asset Value (weight = 1)	
High	มากกว่าหรือเท่ากับ 4	4.0-5.0
Medium	มากกว่า 2 และน้อยกว่า 4	2.1-3.9
Low	น้อยกว่าหรือเท่ากับ 2	1.0-2.0

ทรัพย์สินที่มีระดับตั้งแต่ High ขึ้นไปจะเข้าสู่กระบวนการประเมินความเสี่ยง

ตัวอย่างการกำหนดมูลค่าทรัพย์สินของอุปกรณ์ระบบ eMT โดยมุ่งเน้นความสามารถในการให้บริการ (Operation) และภาพลักษณ์ชื่อเสียง (Reputation)

ชื่อทรัพย์สิน	Operation Perspective (50%)			รวม	Reputation Perspective (50%)			รวม
	C (0.33)	I (0.33)	A (0.33)		C (0.33)	I (0.33)	A (0.33)	
ระบบ eMT	1	4	5	3.33	5	5	5	5.00

$$\text{Total Asset Value} = (0.5 * 3.33) + (0.5 * 5.0) = 4.165 \text{ (High)}$$

ทั้งนี้ การเลือกใช้มุมมอง (Perspective) และการกำหนดน้ำหนักของคุณลักษณะของความมั่นคงปลอดภัยสารสนเทศ (Security Component) ให้พิจารณาตามวัตถุประสงค์และเป้าหมายขององค์กร (Mission) เพื่อสร้างความสอดคล้องกับความต้องการทางธุรกิจ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

5) การระบุภัยคุกคามที่เกี่ยวข้อง (Threat Identification)

การระบุภัยคุกคามที่เกี่ยวข้อง โดยพิจารณาจากเหตุการณ์ที่เคยเกิดขึ้น หรือพิจารณาจากช่องโหว่ที่มีในทรัพย์สินสารสนเทศ ทำให้ทางสมาคมสโมสรนักลงทุนทราบว่าภัยคุกคามใดบ้างที่อาจเกิดขึ้นได้กับทรัพย์สินสารสนเทศของสมาคมสโมสรนักลงทุน โดยทั่วไปภัยคุกคามอาจมีที่มาจากแหล่งต่างๆ ต่อไปนี้

ประเภท	ตัวอย่าง
ภัยคุกคามทางธรรมชาติ หรือสถานการณ์ฉุกเฉิน	เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติ หรือสถานการณ์ร้ายแรง ที่ก่อให้เกิดความเสียหายร้ายแรงกับทรัพย์สินสารสนเทศ เช่น น้ำท่วม แผ่นดินไหว พายุ อาคารถล่ม สภาพแวดล้อมเป็นพิษ สถานที่ตั้งอยู่ในพื้นที่มีน้ำรั่ว หรือขาดระบบไฟฟ้า ไฟไหม้ การประชุมชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
ภัยคุกคามจากมนุษย์ หรือผู้ปฏิบัติงาน	เป็นภัยคุกคามที่อาจเกิดจากการโจรกรรมทรัพย์สินของสมาคมสโมสรนักลงทุน การโจมตีระบบเครือข่าย การบุกรุกระบบ การปล่อย Virus หรือ Malware ในระบบ การก่ออาชญากรรมทางคอมพิวเตอร์ ผู้ก่อการร้าย เป็นต้น
ภัยคุกคามด้านการบริหารจัดการหรือกระบวนการภายในหน่วยงาน	เป็นภัยคุกคามที่อาจเกิดจากแผนนโยบายในการบริหารจัดการ ที่อาจส่งผลกระทบต่อการทำงานด้านการสารสนเทศ
ภัยคุกคามด้านไอที/เทคนิค	เป็นภัยคุกคามที่อาจเกิดจากช่องโหว่ของแอปพลิเคชัน หรือช่องโหว่ของเทคโนโลยีที่สมาคมสโมสรนักลงทุนนำมาใช้ เช่น ระบบคอมพิวเตอร์ เครื่องมือ และอุปกรณ์

6) การระบุช่องโหว่หรือจุดอ่อนของทรัพย์สิน (Vulnerability Identification)

การระบุช่องโหว่ที่มีในทรัพย์สิน พิจารณาจาก

- ผลการประเมินความเสี่ยงที่ผ่านมา (Previous risk assessment result)
- ผลการประเมินภายใน (Internal audit report)
- ผลการทดสอบความสอดคล้องทางเทคนิคของระบบ (system compliance testing)

ผลการดำเนินงาน จะทำให้องค์กรทราบช่องโหว่ที่มีในทรัพย์สิน ซึ่งช่องโหว่ดังกล่าวอาจเป็นช่องทางในการบุกรุกหรือละเมิด นำไปสู่เหตุการณ์อันไม่พึงประสงค์ได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

7) การวิเคราะห์และระบุมาตรการควบคุมในปัจจุบันขององค์กร (Control Analysis)

ช่องโหว่ที่พบในทรัพย์สินสารสนเทศ ผู้ประเมินต้องพิจารณามาตรการที่ทางสมาคมสโมสรนักลงทุน ใช้ควบคุมในปัจจุบัน โดยมาตรการจะช่วยลดผลกระทบหรือโอกาสที่จะเกิดภัยคุกคามได้ มาตรการแบ่งออกเป็นสองประเภท ดังต่อไปนี้

- มาตรการในการป้องกัน (Preventive Controls) มาตรการที่ถูกนำมาใช้ เพื่อป้องกันหรือลดโอกาสที่จะเกิดภัยคุกคาม
- มาตรการในการเฝ้าระวัง (Detective Controls) มาตรการที่ถูกนำมาใช้ เพื่อเฝ้าระวังหรือแจ้งเตือนเมื่อเกิดเหตุการณ์ที่เป็นภัยคุกคาม

8) การพิจารณาโอกาสที่จะเกิดภัยคุกคาม (Likelihood Determination)

โอกาสที่จะเกิดเหตุการณ์ภัยคุกคามที่มีผลต่อความมั่นคงปลอดภัยของทรัพย์สิน พิจารณาจากมาตรการที่มีในปัจจุบัน โดยมีรายละเอียด ดังนี้

Likelihood Level	รายละเอียด
5- มีโอกาสเกิดขึ้นสูงมาก (Almost certain)	ภัยคุกคามมีโอกาสดังเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 1 เดือนเนื่องจากขาดมาตรการในการควบคุม
4- มีโอกาสเกิดขึ้นสูง (Likely)	ภัยคุกคามมีโอกาสดังเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 3 เดือน เนื่องจากมาตรการในการควบคุมไม่เพียงพอต่อการป้องกันภัยคุกคาม
3- มีโอกาสเกิดขึ้นปานกลาง (Possible)	ภัยคุกคามมีโอกาสดังเกิดขึ้น หรือเคยเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 6 เดือน เนื่องจากมาตรการในการควบคุมไม่เพียงพอและขาดประสิทธิภาพในการป้องกันภัยคุกคาม
2- มีโอกาสเกิดขึ้นน้อย (Unlikely)	ภัยคุกคามมีโอกาสดังเกิดขึ้นหรือเคยเกิดขึ้นประมาณ 1 ครั้ง ภายใน 1 ปี เนื่องจากมีมาตรการในการควบคุมเพียงพอต่อการป้องกันภัยคุกคาม
1- มีโอกาสเกิดขึ้นน้อยมาก (Rare)	ภัยคุกคามมีโอกาสดังเกิดขึ้น หรือเคยเกิดขึ้นประมาณ 1 ครั้ง ภายใน 5 ปี เนื่องจากมีมาตรการในการควบคุมเพียงพอและมีประสิทธิภาพต่อการป้องกันภัยคุกคาม

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

9) การพิจารณาผลกระทบ (Impact)

พิจารณาระดับของผลกระทบที่มีต่อบริการหรือธุรกิจ หากเกิดภัยคุกคาม โดยมีรายละเอียด ดังนี้

ระดับของผลกระทบ	รายละเอียด
5- รุนแรง (Critical)	มีผลกระทบอย่างรุนแรง ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศและความต่อเนื่องในการให้บริการ (Service Continuity) ส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในระดับสูงที่สุดของทรัพย์สินนั้นๆ (อาจต้องประกาศแผน BCP)
4- มาก (Major)	มีผลกระทบมาก ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ และระดับการให้บริการ (Service Level) อาจส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในระดับสูงของทรัพย์สินนั้นๆ (กระทบกับระบบหลักบางส่วนยังสามารถให้บริการได้)
3-ปานกลาง (Moderate)	มีผลกระทบปานกลาง ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ และระดับการให้บริการ (Service Level) อาจส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในระดับปานกลางของทรัพย์สินนั้นๆ (กระทบกับระบบที่สนับสนุนระบบหลัก)
2- เล็กน้อย (Minor)	มีผลกระทบเล็กน้อย ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ แต่ไม่กระทบต่อระดับการให้บริการ (Service Level) อาจส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในทรัพย์สินนั้นๆ
1-ไม่มีผลกระทบ (Insignificant)	ไม่มีผลกระทบ ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ และระดับการให้บริการ (Service Level)

10) การพิจารณาระดับความเสี่ยง (Risk Determination)

ดำเนินการประเมินความเสี่ยงของทรัพย์สินและกำหนดระดับความเสี่ยงที่สมาคมสโมสรนักลงทุนยอมรับได้ (Acceptable Risk Level) รวมถึงการกำหนดแนวทางในการจัดการความเสี่ยงที่สูงกว่าระดับความเสี่ยงที่ยอมรับได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

11) การพิจารณาระดับความเสี่ยงของทรัพย์สิน

การพิจารณาระดับความเสี่ยงของทรัพย์สินแต่ละรายการ ใช้เกณฑ์การพิจารณาดังตารางต่อไปนี้

Likelihood	ผลกระทบ				
	1- Insignificant	2 - Minor	3- Moderate	4- Major	5- Critical
5- Almost Certain	M	H	H	E	E
4- Likely	M	M	H	H	E
3- Possible	L	M	M	H	E
2- Unlikely	L	M	M	M	H
1- Rare	L	L	L	M	H

คำอธิบาย E: ระดับสูงมาก (Extremely High)

H: ระดับสูง (High)

M: ระดับปานกลาง (Medium)

L: ระดับต่ำ (Low)

12) การพิจารณาระดับความเสี่ยงที่ยอมรับได้

ระดับความเสี่ยงที่สมาคมสโมสรนักลงทุนยอมรับได้นั้น กำหนดให้ต้องเป็นทรัพย์สินที่มีระดับความเสี่ยงน้อยกว่าระดับสูง (H) สำหรับทรัพย์สินที่มีความเสี่ยงตั้งแต่ระดับสูง “H” ขึ้นไป ให้เจ้าของทรัพย์สินร่วมกับเจ้าของความเสี่ยงกำหนดแนวทางในการจัดการทรัพย์สินต่อไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

13) การจัดการความเสี่ยงและมาตรการควบคุมที่นำมาใช้ (Risk Treatment and Control Recommendation)

เมื่อทราบผลการประเมินความเสี่ยงของทรัพย์สิน และพบว่าค่าความเสี่ยงของทรัพย์สินสูงกว่าระดับความเสี่ยงที่สมาคมสโมสรนักลงทุนยอมรับได้ ให้เจ้าของทรัพย์สินดังกล่าว พิจารณาแนวทางในการจัดการความเสี่ยงโดยมี 4 แนวทาง ได้แก่

- การยอมรับความเสี่ยง (Accept Risk)
- การลดความเสี่ยง (Reduce Risk)
- การถ่ายโอนความเสี่ยง (Transfer Risk)
- การหลีกเลี่ยงความเสี่ยง (Avoid Risk)

เมื่อเลือกแนวทางในการจัดการความเสี่ยงได้แล้ว เจ้าของความเสี่ยง จะต้องกำหนดมาตรการควบคุม และแผนการดำเนินงานในการจัดการความเสี่ยง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การรักษาความปลอดภัย

หลักการ

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อแจกแจงระเบียบปฏิบัติสำหรับผู้ใช้อุปกรณ์คอมพิวเตอร์ ข้อห้ามทั่วไปที่จะนำมาประยุกต์ใช้ และอ้างอิงข้อมูลเพิ่มเติมอื่นๆ ที่จะนำมาใช้ในบางสถานการณ์

ขอบเขต

ทรัพยากรที่บริหาร และดูแลโดยฝ่ายเทคโนโลยีสารสนเทศภายใต้นโยบายฉบับนี้ครอบคลุมอุปกรณ์และโปรแกรมคอมพิวเตอร์ เอกสาร และสื่อที่ใช้อ้างอิง ข้อมูลที่เก็บบนอุปกรณ์คอมพิวเตอร์แม่ข่าย ตลอดจนข้อมูลอื่น ๆ ของสมาคมสโมสรนักลงทุนที่เก็บบนสื่ออื่น ๆ เช่น ซีดีรอม เทป รวมถึงอุปกรณ์จัดเก็บประเภทต่าง ๆ ที่อยู่ในการครอบครองของฝ่ายเทคโนโลยีสารสนเทศหรือหน่วยงานใดภายใต้สมาคมสโมสรนักลงทุน

แนวทาง

การเชื่อมต่อทั้งที่เป็นการชั่วคราวและถาวรผ่านระบบเครือข่ายต้องเป็นไปตามที่กำหนดไว้ในนโยบายฉบับนี้ ซึ่งครอบคลุมถึงการเชื่อมต่อถึงในระดับข้อมูลของเครื่องคอมพิวเตอร์แต่ละเครื่องที่ต่อเชื่อมกับเครือข่าย และอุปกรณ์โทรศัพท์ที่ใช้เชื่อมต่อด้วย

อุปกรณ์คอมพิวเตอร์ที่สมาคมสโมสรนักลงทุนไม่ได้เป็นเจ้าของ จะเชื่อมต่อกับระบบเครือข่ายของสมาคมฯ ได้ต่อเมื่อได้รับการอนุมัติโดยผู้จัดการสมาคมฯ โดยฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิ์ในการติดตามเนื้อหาของข้อมูลที่มีการส่งผ่านระบบเครือข่าย และหากมีความจำเป็นในการตรวจสอบเนื้อหาที่ส่งก็สามารถแจ้งให้หัวหน้าฝ่ายที่รับผิดชอบกิจกรรมที่มีความจำเป็นในการเชื่อมต่อ เพื่อรับทราบการติดตามการตรวจสอบ

นโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy)

- การอนุญาตให้มีการเข้าถึงระบบและข้อมูลสารสนเทศใด ๆ ก็ตาม ต้องขึ้นอยู่กับความจำเป็นในการทำงาน
- การเข้าถึงระบบและข้อมูลสารสนเทศต้องมีการยืนยันตัวตนก่อนจึงจะเข้าใช้งานได้ เช่น การยืนยันตัวตนโดยใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นต้น
- ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ และต้องมีการกำหนดสิทธิ์ผู้ใช้งานในระดับสูง
- ในการเข้าใช้งานของผู้ใช้งานในระดับสูงจะต้องมีการร้องขอใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงในแต่ละครั้ง
- ผู้ดูแลระบบสามารถถอดสิทธิ์หรือเปลี่ยนแปลงสิทธิ์ในกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการทำงานของระบบและข้อมูลสารสนเทศได้ตามความเหมาะสม



- ไม่อนุญาตให้มีการใช้งานรหัสผ่านตั้งต้น (Default Password) ที่ติดมากับอุปกรณ์หรือที่มีมากับการตั้งค่าจากโรงงาน
- เจ้าของระบบหรือผู้ดูแลระบบควรมีการทบทวนสิทธิที่ได้มีการอนุญาตให้กับผู้ใช้งานอย่างสม่ำเสมอ
- ควรมีการจัดทำเอกสารแสดงสิทธิที่ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศต่างๆ เพื่อใช้ในการทบทวนและตรวจสอบการเข้าถึง
- พนักงานที่มีความประสงค์ร้องขอเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Account) ต้องจัดทำแบบฟอร์มร้องขอบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Request Form) (IT-2FM-07)
- ผู้ดูแลระบบบันทึกทะเบียนบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privileged Account Inventory) (IT-2FM-09) สำหรับใช้ในการอ้างอิง

สถานะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน

ปัจจุบันนี้ฝ่ายเทคโนโลยีสารสนเทศดำเนินการดูแลการปฏิบัติงานระบบคอมพิวเตอร์ภายในองค์กร โดยทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศจะทำหน้าที่ดูแลจัดการสัญญาการว่าจ้างจากภายนอกกับสมาคม ฯ เพื่อให้สัญญาเป็นไปตามเวลาที่กำหนดอย่างมีประสิทธิภาพและต้นทุนที่เหมาะสม พนักงานที่ได้รับการอนุมัติจะสามารถเข้าใช้ระบบเครือข่ายและทรัพยากรคอมพิวเตอร์ได้ตลอดเวลา

ฝ่ายเทคโนโลยีสารสนเทศได้จัดให้มีหน่วยสนับสนุน และช่วยเหลือการใช้งานคอมพิวเตอร์ให้กับผู้ใช้งานที่ต้องการให้เพิ่มรายชื่อผู้ใช้งาน หรือเข้ารับการอบรม หรือต้องการเอกสารประกอบการใช้งานระบบคอมพิวเตอร์

บัญชีรายชื่อผู้ใช้งานในระบบอยู่ภายใต้ข้อกำหนดต่อไปนี้

- รายชื่อผู้ใช้งานจะถูกตั้งค่าปิดการใช้งานบัญชีล่วงหน้าและตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานลาออก
- ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการตรวจสอบวันที่เข้าสู่ระบบล่าสุดของพนักงานที่ลาออก (Check Last Logon Date) ในกรณีที่มีการแจ้งลาออกล่าช้าหรือมีการเลิกจ้างฐานละทิ้งหน้าที่ โดยระบุในส่วนรายละเอียดเพิ่มเติมของแบบฟอร์มการเพิกถอนสิทธิใช้งานบัญชีผู้ใช้ พร้อมบันทึกหลักฐานการตรวจสอบ
- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการระงับการใช้งาน หรือลบรายชื่อผู้ใช้งาน เมื่อมีความจำเป็น และในกรณีดังกล่าว หัวหน้าฝ่ายเทคโนโลยีสารสนเทศจะทำการอนุมัติล่วงหน้าก่อนที่จะสั่งการให้ระงับหรือการลบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ให้ผู้ใช้งานตรวจสอบ หรือให้เปลี่ยนรหัสการเข้าสู่ระบบใด ๆ ทั้งนี้ขึ้นอยู่กับข้อจำกัดของระบบแต่ละระบบ อนึ่ง กรณีดังกล่าวจะเกิดขึ้นก็ต่อเมื่อได้มีการพิจารณาแล้วว่าอาจจะมีการละเมิดมาตรการความปลอดภัยของระบบคอมพิวเตอร์เท่านั้น
- ฝ่ายเทคโนโลยีสารสนเทศสงวนสิทธิในการระงับสิทธิในการเข้าสู่ระบบใด ๆ เมื่อได้มีการพิจารณาแล้วว่าอาจจะมีการละเมิดมาตรฐานการรักษาความปลอดภัยระบบคอมพิวเตอร์
- ฝ่ายเทคโนโลยีสารสนเทศกำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที
- ฝ่ายเทคโนโลยีสารสนเทศกำหนดการตั้งรหัสผ่าน (Password Management) ต้องมีรูปแบบดังนี้
 - มีความยาวไม่ต่ำกว่า 8 ตัวอักษร
 - ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว
 - ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กอย่างน้อย 1 ตัว
 - ประกอบด้วยตัวเลขอย่างน้อย 1 ตัว
 - ต้องเปลี่ยนรหัสผ่านทุก 90 วัน
 - รหัสผ่านที่เปลี่ยนใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม
- แผนบุคคลมีความรับผิดชอบในการแจ้งฝ่ายเทคโนโลยีสารสนเทศทราบทันทีที่มีการว่าจ้าง การโยกย้ายหรือพ้นสภาพของพนักงานใด ๆ ที่มีรายชื่ออยู่ในทะเบียนผู้ใช้งานระบบคอมพิวเตอร์
- ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของสมาคมฯ ได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง

ข้อห้ามและการใช้งานอย่างเหมาะสม

การกระทำที่ต้องห้าม มีดังนี้

- การปฏิเสธไม่ให้บริการต่อพนักงานผู้ใช้งานของสมาคมสโมสรนักลงทุน
- การแสวงหาประโยชน์จากบัญชีรายชื่อหรือทรัพยากรที่ถูกปล่อยปละละเลย หรือผู้ใช้งานที่ด้อยความรู้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- การพยายามคาดเดา เจาะ หรือหารหัสผ่านในการเข้าสู่ระบบของผู้ใช้งานอื่นๆ
- การใช้อุปกรณ์ หรือโปรแกรม เพื่อลักลอบตัดต่อข้อมูลที่ส่งผ่านระบบเครือข่าย
- การปลอมแปลงจดหมายอิเล็กทรอนิกส์ หรือข่าวสารอิเล็กทรอนิกส์ หรือการจงใจให้เกิดความเข้าใจผิดผ่านการสื่อสารอิเล็กทรอนิกส์

ผู้ใช้งานทุกคนจะต้องใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุนอย่างเหมาะสม ซึ่งรวมถึงข้อดังต่อไปนี้

- จัดการรักษารหัสผ่านในการเข้าสู่ระบบอย่างเหมาะสม เช่น ไม่ให้ยืมใช้ร่วมกัน ไม่เปิดเผยให้เห็น เป็นต้น
- ดูแลให้การเข้าสู่ระบบ และการออกจากระบบเป็นไปอย่างสมบูรณ์ หรือไม่ละทิ้งเครื่องคอมพิวเตอร์ในขณะที่เปิดโปรแกรมค้างไว้
- เคารพในลิขสิทธิ์ของโปรแกรม
- บริหารจัดการข้อมูลที่เป็นความลับอย่างเหมาะสม

บุคคลที่ไม่ใช่พนักงานที่เข้าใช้เครื่องคอมพิวเตอร์โดยลำพัง และไม่มีพนักงานของบริษัทคอยดูแลอยู่ หากถูกพบจะถูกบังคับให้ออกจากระบบทันที โดยที่เครื่องคอมพิวเตอร์ที่ใช้งาน และบัญชีผู้ใช้งานที่เปิดค้างไว้ ให้บุคคลใช้อยู่ขณะตรวจพบจะถูกยึด และระงับไม่ให้ใช้งานต่อไป ในเหตุการณ์ดังกล่าว จะต้องแจ้งให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและผู้บริหารของหน่วยงานที่ครอบคลุมอุปกรณ์คอมพิวเตอร์และข้อมูลนั้นรับทราบ เพื่อดำเนินการต่อไป

นอกจากนี้ ผู้ใช้งานไม่ควรที่จะถือโอกาสอ่านข้อมูลที่เป็นความลับ อันเนื่องมาจากความบังเอิญ หรือจากความผิดพลาดของผู้ละเมิดเข้าสู่ระบบ หรือจากการถือสิทธิในการเข้าสู่ข้อมูลที่เหนือกว่า เป็นต้น เมื่อทราบว่าข้อมูลที่เป็นความลับถูกเปิดเผยก็ไม่ควรที่จะอ่านต่อ และจะต้องรายงานให้ผู้บริหารของฝ่ายเทคโนโลยีสารสนเทศทราบทันที เช่นเดียวกันการเขียนทับข้อมูลที่ไม่ใช่ของตนโดยตั้งใจ และไม่ได้รับอนุญาต ถือเป็นความผิด

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and Operations Management)

การแบ่งหน้าที่ในการปฏิบัติงานและการจัดทำเอกสารประกอบการปฏิบัติงาน

- การกำหนดบทบาทหน้าที่ในการปฏิบัติงาน หน้าที่ในการบริหารจัดการระบบสารสนเทศและระบบเครือข่ายจะต้องแยกออกจากกัน ไม่ควรให้พนักงานคนเดียวกันทำงานที่สำคัญในกระบวนการเดียวกัน เพื่อป้องกันการทุจริตและการสะกดหยุดชะงักของงาน หากพนักงานดังกล่าวไม่สามารถมาปฏิบัติงานได้ ยกเว้นแต่มีข้อจำกัดเรื่องจำนวนของผู้ปฏิบัติงาน
- การบริหารการเปลี่ยนแปลงใด ๆ ในระบบเครือข่าย และระบบสารสนเทศของสมาคมสโมสรนักลงทุน จะต้องปฏิบัติตามขั้นตอนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) ของสมาคมสโมสรนักลงทุน
- การแบ่งแยกระบบสารสนเทศ เพื่อลดความผิดพลาดหรือผลกระทบอันเกิดจากการดำเนินการทดสอบ ควรมีการแยกระบบสารสนเทศที่ให้บริการจริง ออกจากระบบสารสนเทศที่ใช้ในการพัฒนา และทดสอบ (เฉพาะระบบที่สามารถดำเนินการได้)

หน้าที่ความรับผิดชอบของผู้ใช้

- การใช้รหัสผ่านและการกำหนดรหัสผ่านจะต้องปฏิบัติตามแนวทางการจัดการรหัสผ่าน (Password Management)
- การจัดการด้านความปลอดภัยของอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended Equipment) เมื่อไม่ต้องการใช้งานอุปกรณ์หรือเครื่องคอมพิวเตอร์แล้ว ให้ทำการยกเลิกการเชื่อมต่อกับระบบเครือข่าย หรือระบบสารสนเทศ จัดเก็บอุปกรณ์หรือเครื่องคอมพิวเตอร์ไว้ในตู้ที่สามารถปิดล็อกได้ เพื่อป้องกันไม่ให้บุคคลอื่นเข้ามาใช้อุปกรณ์ดังกล่าวโดยไม่ได้รับอนุญาต
- เครื่องคอมพิวเตอร์ทุกเครื่องจะต้องถูกล็อกหน้าจอทุกครั้งเมื่อไม่มีการใช้งาน
- การจัดเก็บเอกสารข้อมูลสำคัญของสมาคมสโมสรนักลงทุน ข้อมูลที่อยู่ในสื่อบันทึกข้อมูลไว้ในสถานที่ที่สามารถปิดล็อกหรือเข้ารหัสข้อมูลดังกล่าวได้ พนักงานจะต้องไม่ทิ้งเอกสารสำคัญไว้บนโต๊ะทำงาน และจัดเก็บโต๊ะทุกครั้งก่อนเลิกงาน
- ข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์หรือส่งออกภายนอกองค์กรต้องจัดให้มีการเข้ารหัสข้อมูลโดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ ทั้งนี้ ต้องพิจารณาเลือกใช้เทคนิคต่าง ๆ ที่มีระดับความมั่นคงปลอดภัยตามมาตรฐานสากล
- การจัดทำการจัดเก็บ การส่งต่อ ลบทำลายข้อมูล จะต้องดำเนินการตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล (Information Classification Labelling and Media Disposal Procedure)



- ต้องควบคุมให้มีมาตรการการปิดบังข้อมูลสารสนเทศเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลทีละเล็กละน้อย และปฏิบัติตามข้อกำหนดทางกฎหมาย กฎหมาย ข้อบังคับ และสัญญา แนวทางและมาตรการความปลอดภัยในการปิดบังข้อมูลเพื่อไม่ให้อาสาสมัครสามารถระบุตัวตนได้ มีดังนี้
 - การปิดบังข้อมูล (Data Masking) เช่น แทนที่เลขบัตรประจำตัวประชาชน 10 หลักแรก ด้วยเครื่องหมาย x แสดงเพียง 4 หลักสุดท้าย (x-xxxx-xxxxx-12-3)
 - การใช้นามแฝง (Pseudonymization) เช่น แทนที่ชื่อลูกค้าด้วยเลขรหัสลูกค้า (ลูกค้า หมายเลข 12345)
 - การทำข้อมูลนิรนาม (Anonymization) เช่น รวมกลุ่มข้อมูลที่มีลักษณะคล้ายคลึงกัน เข้าด้วยกัน (ลูกค้ากลุ่มอายุ 20-30 ปี, เพศชาย, อาชีพพนักงานออฟฟิศ)
 - การเข้ารหัส (Encryption) เช่น การเข้ารหัสการส่งอีเมล
 - การลบหรือเปลี่ยนเป็นค่า null เช่น การลบข้อมูลออกจากระบบ หรือแทนที่ด้วยค่าว่าง (null)
 - การแทนที่ (Substitution) เช่น แทนที่ชื่อจริงด้วยชื่อปลอม หรือแทนที่ที่อยู่จริงด้วยที่อยู่ปลอม
 - การแทนที่ด้วยค่าแฮช (Hashing) เช่น เก็บรหัสผ่านในรูปแบบค่าแฮช เพื่อป้องกันการถูกขโมยและนำไปใช้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การเข้าสู่ห้องเซิร์ฟเวอร์

หลักการ

ห้องเซิร์ฟเวอร์เป็นแหล่งเก็บอุปกรณ์คอมพิวเตอร์ส่วนใหญ่ขององค์กร ระบบความปลอดภัยที่เหมาะสมจึงมีความจำเป็นเพื่อปกป้องสินทรัพย์เหล่านี้ การจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์ เป็นไปเพื่อป้องกันสินทรัพย์คอมพิวเตอร์จากการละเมิดใช้ อุบัติเหตุ หรือเจตนาให้เกิดความเสียหาย หรือการขโมย การอนุมัติเพื่อจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์จะทำเมื่อเห็นว่ามี ความจำเป็น เนื่องจากการกำหนดเงื่อนไขเพื่อบังคับใช้ข้อจำกัดดังกล่าวเฉพาะกลุ่มบุคคล หรือเป็นรายบุคคล เป็นสิ่งที่ทำได้ยากและไม่เหมาะสม ดังนั้นจึงได้กำหนดแนวทางดังต่อไปนี้เพื่อช่วยในการตัดสินใจกรณีที่ต้องจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์

แนวทาง

พนักงานที่ต้องปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์ทุกวัน ซึ่งได้รับสิทธิเข้าสู่ห้องเซิร์ฟเวอร์ ได้แก่

- พนักงานดูแลซอฟต์แวร์
- พนักงานดูแลเครือข่ายเน็ตเวิร์คและเทคโนโลยี
- พนักงานสำนักงานคณะกรรมการส่งเสริมการลงทุนที่ได้รับมอบหมายให้ดูแลฝ่ายเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน

ผู้ได้รับสิทธิอื่นนอกเหนือจากที่กล่าวข้างต้น ยังประกอบไปด้วยบุคคลที่ต้องเข้าไปปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์เป็นประจำ ได้แก่

- พนักงานดูแลโปรแกรมคอมพิวเตอร์ที่มีความรับผิดชอบเกี่ยวข้องกับการทำงานบนเครื่องเซิร์ฟเวอร์ หรืองานนั้นต้องทำบนเครื่องเซิร์ฟเวอร์ ณ ห้องเซิร์ฟเวอร์ การทำงานในห้องเซิร์ฟเวอร์จะถูกจำกัดเฉพาะสถานการณ์ที่จำเป็นเท่านั้น
- พนักงานฝ่ายเทคโนโลยีสารสนเทศอื่น ๆ ซึ่งต้องเข้าไปปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์เป็นประจำ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

โดยหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ (หรือผู้แทน) จะเป็นผู้อนุมัติการเข้าทำงานดังกล่าวข้างต้น ในกรณีที่บุคคลอื่น ๆ ดังกล่าวข้างล่างนี้ มีความจำเป็นต้องเข้าไปทำงานในห้องเซิร์ฟเวอร์ จะต้องกรอกแบบคำขออนุญาตเข้าพื้นที่ห้องเซิร์ฟเวอร์ บุคคลเหล่านั้นจะได้รับอนุญาต โดยมีพนักงานฝ่ายปฏิบัติการคอมพิวเตอร์มีส่วนรับรู้ในการเข้าไปทำงานในจุดนั้น เช่น

- ผู้ขายที่เข้ามาทำงานบำรุงรักษา และช่างระบบคอมพิวเตอร์
- พนักงานฝ่ายงานระบบอื่น ๆ ในองค์กร
- บุคคลอื่น ๆ ที่ได้รับอนุญาต และติดตามโดยพนักงานฝ่ายปฏิบัติการคอมพิวเตอร์

ข้อจำกัดอื่น ๆ ภายในบริเวณห้องเซิร์ฟเวอร์

- ห้ามนำอาหารและเครื่องดื่มเข้ามาบริเวณห้องเซิร์ฟเวอร์
- ห้ามนำอุปกรณ์สื่อสารเข้ามาในบริเวณห้องเซิร์ฟเวอร์ เว้นแต่จะได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- ห้ามนำกล้องถ่ายรูปเข้ามา เว้นแต่จะได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- ห้ามนำวัตถุระเบิด เชื้อเพลิง วัสดุติดเพลิงง่าย อาวุธ สารเคมี หรือสิ่งอื่นใดที่อาจก่อให้เกิดความเสียหายทั้งต่อชีวิตและทรัพย์สิน เข้ามาบริเวณห้องเซิร์ฟเวอร์

การติดตามการเข้า-ออกบริเวณห้องเซิร์ฟเวอร์จะใช้ระบบการบันทึกการเข้า-ออกห้องเซิร์ฟเวอร์

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

กรรมสิทธิ์ในข้อมูล

หลักการ

ระบบเทคโนโลยีสารสนเทศขององค์กร ข้อมูล รวมถึงสินทรัพย์ต่าง ๆ ในระบบคอมพิวเตอร์ ถือเป็นกรรมสิทธิ์ของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน และถือเป็นทรัพย์สินที่มีค่าขององค์กร และข้อมูลทั้งหมดที่เก็บอยู่ในสินทรัพย์เหล่านี้ถือเป็นกรรมสิทธิ์ของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน โดยฝ่ายเทคโนโลยีสารสนเทศมีความรับผิดชอบต่อข้อมูลที่เก็บไว้บนระบบเครือข่าย และระบบข้อมูลกลางอื่น ๆ ที่อยู่ภายใต้การครอบครองและดูแล ในขณะที่ผู้ใช้งานแต่ละคนจะรับผิดชอบข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายคอมพิวเตอร์แต่ละเครื่องที่ตนเองใช้งานอยู่ และอุปกรณ์การจัดเก็บประเภทต่าง ๆ ที่อยู่ในการครอบครอง

แนวทาง

ระบบคอมพิวเตอร์และข้อมูลต่าง ๆ ที่เกี่ยวข้องถือเป็นสินทรัพย์ที่มีมูลค่าขององค์กร และข้อมูลทั้งหมดที่เก็บอยู่ในสินทรัพย์เหล่านี้ถือเป็นสมบัติของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน โดยผู้ใช้งานแต่ละคนจะรับผิดชอบข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายคอมพิวเตอร์แต่ละเครื่องที่ตนเองใช้งานอยู่

ระบบข้อมูลที่สำคัญ และตัวข้อมูลควรจะถูกเก็บรักษาไว้ที่เครื่องแม่ข่ายคอมพิวเตอร์ เพื่อประโยชน์ในการสำรองข้อมูล ข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายเป็นความรับผิดชอบโดยตรงของผู้ใช้งานแต่ละคน ดังนั้นผู้ใช้งานแต่ละคนที่เก็บข้อมูลไว้ที่เครื่องลูกข่ายจะต้องทำสำเนาแฟ้มข้อมูลด้วยตนเอง ข้อมูลใด ๆ ที่ละเมิดต่อกฎหมายไทยและกฎหมายลิขสิทธิ์ แต่ถูกจัดเก็บ รักษา และสามารถเข้าถึงได้ทางเครื่องลูกข่าย จะถือว่าละเมิดต่อนโยบายขององค์กรด้วย

การใช้ข้อมูลและระบบสารสนเทศขององค์กรจะทำได้ก็ต่อเมื่อได้รับอนุมัติโดยผู้จัดการของสมาคมสโมสรนักลงทุนเท่านั้น การมอบสิทธิในการเข้าถึงข้อมูลและระบบสารสนเทศของพนักงานแต่ละคน ควรสอดคล้องกับหน้าที่และงานที่รับผิดชอบ การเปิดเผยข้อมูลควรเป็นไปตามข้อกำหนดในนโยบายว่าด้วยความลับของสมาคมสโมสรนักลงทุน (โปรดดูข้อตกลงว่าด้วยการรักษาความลับขององค์กร หรือ Mutual Confidentiality Agreement ตามเอกสารแนบ 2) การละเมิดนโยบายดังกล่าวนี้จะต้องรายงานให้คณะกรรมการสารสนเทศของสมาคมสโมสรนักลงทุนหรือฝ่ายเทคโนโลยีสารสนเทศทราบทันที ผู้รับเหมาทุกรายที่ต้องเข้าใช้งานระบบสารสนเทศขององค์กรจะต้องเซ็นยอมรับตามข้อตกลงในเอกสารข้อตกลงว่าด้วยการรักษาความลับขององค์กร (Confidential Agreement)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้อินเทอร์เน็ต

หลักการ

สมาคมสโมสรนักลงทุนจะเชื่อมต่ออินเทอร์เน็ตและเปิดให้พนักงานที่ได้รับการอนุมัติใช้งาน โดยหน่วยงานต้นสังกัดจะต้องดำเนินการตามขั้นตอนการแจ้งขอใช้อินเทอร์เน็ตของฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเปิดให้ใช้งานได้ระหว่างเวลาทำการขององค์กรโดยมีวัตถุประสงค์เพื่อประโยชน์ในการปฏิบัติงาน และต้องสอดคล้องโดยตรงกับหน้าที่ และความรับผิดชอบของพนักงาน โดยหัวหน้าฝ่าย/หัวหน้าแผนก ของหน่วยงาน นั้น มีหน้าที่สอดส่องและดูแลให้สอดคล้องกับวัตถุประสงค์ดังกล่าว

แนวทาง

ถึงแม้การใช้อินเทอร์เน็ตส่งผลให้ค่าใช้จ่ายขององค์กรสูงขึ้น แต่ก็ถือว่าเป็นเทคโนโลยีทันสมัยที่มีประโยชน์สำหรับการใช้งาน และถือเป็นหนึ่งในภารกิจขององค์กร เฉพาะพนักงานที่ได้รับอนุมัติเท่านั้นจึงจะเข้าใช้งานอินเทอร์เน็ตได้ ทั้งนี้พนักงานต้องปฏิบัติให้ถูกต้องเหมาะสมตามกฎหมายกำหนด ดังที่มีกำหนดไว้ในหลักการว่าด้วยสิ่งลามกอนาจาร และ นโยบายลิขสิทธิ์โปรแกรมและการสั่งซื้อโปรแกรมคอมพิวเตอร์ เพื่อที่จะป้องกันไม่ให้สมาคมสโมสรนักลงทุนตกเป็นเป้าหมายโจมตีของไวรัสคอมพิวเตอร์ การใช้งานอินเทอร์เน็ตต้องเป็นไปเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับธุรกิจขององค์กร

เพื่อป้องกันไม่ให้ระบบเครือข่ายมีไวรัสคอมพิวเตอร์และโปรแกรมที่ไม่ถูกต้องตามลิขสิทธิ์ จึงห้ามมิให้มีการนำโปรแกรมที่ส่งผ่านมาทางจดหมายอิเล็กทรอนิกส์ หรือโปรแกรมที่ Download จากระบบเครือข่ายภายนอกมาติดตั้ง ในกรณีที่จำเป็นต้องใช้โปรแกรมหมาดังกล่าวจะต้องได้รับการอนุมัติจากหัวหน้าฝ่ายของหน่วยงานนั้น ๆ ก่อน และประสานฝ่ายเทคโนโลยีสารสนเทศเพื่อดำเนินการต่อไป ผู้ละเมิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

การควบคุมการใช้งานระบบเครือข่าย

- ในการขอเข้าใช้งานระบบเครือข่ายนั้นจะต้องได้รับอนุมัติจากหัวหน้าฝ่ายของผู้ที่มีความประสงค์ การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ตต้องเชื่อมต่อผ่านระบบเครือข่ายที่สมาคมสโมสรนักลงทุนจัดไว้เท่านั้น
- ไม่เปิดเผยข้อมูลเวอร์ชันของระบบปฏิบัติการและหมายเลข IP Address ให้บุคคลที่ไม่เกี่ยวข้องทราบ
- การควบคุมการเชื่อมต่อระบบเครือข่าย ควรแบ่งโซนของระบบเครือข่ายตามลักษณะการให้บริการของระบบ ควรกำหนดให้มี Demilitarized Zone (DMZ) คั่นระหว่างการเชื่อมต่อภายนอกกับระบบเครือข่ายของสมาคมสโมสรนักลงทุน แต่ละโซนของระบบเครือข่ายควรแยกออกจากกัน (ถ้าเป็นไปได้)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- การควบคุมการเลือกเส้นทางข้อมูลของเครือข่ายควรใช้ไฟร์วอลล์ (Firewall) เพื่อจำกัดการเข้าถึงผ่านระบบเครือข่าย ควรมีอุปกรณ์ป้องกันการบุกรุกจากภายนอก การจำกัดการเชื่อมต่อผ่านระบบเครือข่ายต้องเป็นไปตามนโยบายด้านการควบคุมการเข้าถึง และข้อกำหนดสำหรับระบบ/แอปพลิเคชัน โดยข้อกำหนดนี้ควรจะมีการปรับปรุงเมื่อจำเป็น
- ระบบเครือข่ายที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอกจะต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ เพื่อตรวจสอบและป้องกันการบุกรุกจากภายนอก จะต้องจำกัดการเชื่อมต่อจากภายนอก โดยกำหนดให้สามารถเข้าถึง Network Zone หรือระบบสารสนเทศที่กำหนดไว้เท่านั้น
- ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของสมาคมฯ ให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ อาทิจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับ (ฉบับที่ 2) พ.ศ. 2560

การเชื่อมต่ออินเทอร์เน็ตจะต้องไม่เป็นไปเพื่อโอนถ่ายข้อมูลดังต่อไปนี้

- ที่ละเมิดต่อกฎหมายไทย หรือกฎหมายลิขสิทธิ์ หรือขัดต่อศีลธรรมหรือขัดต่อเนื้อหาหรือวัตถุประสงค์ของนโยบายฉบับนี้
- ที่มีวัตถุประสงค์ในเชิงพาณิชย์ที่นอกเหนือจากผลประโยชน์ขององค์กร
- ห้ามมิให้ใช้อินเทอร์เน็ตเพื่อเข้าสู่โปรแกรมระบบอื่น ๆ ที่ไม่มีสิทธิเข้าใช้
- การละเมิดเข้าใช้งานอินเทอร์เน็ตไม่ว่ากรณีใด จะต้องรายงานให้ผู้จัดการสมาคม ฯ ทราบ มิฉะนั้นจะถือว่าละเมิดนโยบายขององค์กร
- ห้ามใช้อินเทอร์เน็ตเพื่อเยี่ยมชมเว็บไซต์ (Website) ที่ลามกอนาจาร หรือขัดต่อศีลธรรมอันดีงาม หรือเพื่อโอนถ่ายข้อมูลหรือรูปภาพที่ลามกอนาจาร หรือขัดต่อศีลธรรม ซึ่งผู้กระทำความผิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน และอาจถูกดำเนินคดีอาญา และ/หรือคดีแพ่ง หากการกระทำดังกล่าวถือว่าขัดต่อกฎหมายของประเทศไทย เช่นกัน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้จดหมายอิเล็กทรอนิกส์ หรืออีเมล

หลักการ

ระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail System) ถือเป็นทรัพย์สินขององค์กร บุคคลที่สามารถใช้งานได้จะต้องได้รับอนุมัติ โดยแจ้งขอใช้จดหมายอิเล็กทรอนิกส์ (Electronic Mail) ตามวิธีการที่ฝ่ายบุคคลกำหนด โดยบุคคลที่ได้รับสิทธิดังกล่าวจะต้องใช้จดหมายอิเล็กทรอนิกส์ด้วยวัตถุประสงค์ที่เป็นประโยชน์ต่อสมาคมสโมสรนักลงทุน และเกี่ยวเนื่องกับงานในหน้าที่ของตนเท่านั้น

คำจำกัดความ

“ข้อมูลอิเล็กทรอนิกส์ (Electronic Data)” หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

“จดหมายอิเล็กทรอนิกส์ (Electronic Mail) หรืออีเมล (E-Mail)” หมายถึง การสื่อสารหรือการส่งข้อมูลในรูปของข้อความอิเล็กทรอนิกส์ (Messages) บันทึกหรือเอกสารประกอบ (Attached Files) จากคอมพิวเตอร์ของผู้ส่งไปยังคอมพิวเตอร์ของผู้รับผ่านระบบโทรคมนาคมสื่อสาร หรืออีกนัยหนึ่งจดหมายอิเล็กทรอนิกส์ คือ วิธีการรับส่งข้อความหรือข้อมูลระหว่างคอมพิวเตอร์เครือข่าย (Network) ของสมาคมสโมสรนักลงทุน และให้หมายความรวมถึง การรับและ/หรือส่งข้อความหรือข้อมูลผ่านเครือข่ายอินเทอร์เน็ต (Internet) ด้วย “ผู้ใช้ (User)” หมายถึง พนักงานของสมาคมสโมสรนักลงทุน

แนวทาง

สมาคมสโมสรนักลงทุนจัดให้มีระบบจดหมายอิเล็กทรอนิกส์เพื่อใช้สำหรับติดต่อสื่อสารในเรื่องที่เกี่ยวข้องกับงานขององค์กร หรือของสมาคมสโมสรนักลงทุน เป็นหลัก การใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารส่วนบุคคลจึงควรอยู่บนพื้นฐานของความเหมาะสมและความพอดี

ข้อมูลอิเล็กทรอนิกส์ที่รับส่งผ่านระบบจดหมายอิเล็กทรอนิกส์ ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน หรือระบบอินเทอร์เน็ต ถือเป็นพยานหลักฐานที่สามารถนำมาใช้ในการฟ้องร้องดำเนินคดีกับผู้ก่อการในภายหลังได้ ในกรณีที่มีการใช้ที่ขัดต่อนโยบายหรือก่อให้เกิดความเสียหายต่อสมาคมสโมสรนักลงทุน และ/หรือพนักงาน และ/หรือผู้บริหารของสมาคมสโมสรนักลงทุน แม้ว่าผู้ใช้นั้นจะพ้นสภาพการเป็นพนักงาน หรือสิ้นสุดสัญญาว่าจ้างกับสมาคมสโมสรนักลงทุนแล้วหรือไม่ก็ตาม โดยฝ่ายเทคโนโลยีสารสนเทศจะทำการจัดเก็บข้อมูลดังกล่าวไว้จนกว่าจะสิ้นสุดอายุความในการฟ้องร้องคดี

องค์กรไม่มีนโยบายที่จะเปิดอ่านข้อมูลอิเล็กทรอนิกส์ของผู้ใช้ที่ถูกส่งหรือได้รับผ่านระบบจดหมายอิเล็กทรอนิกส์หรือระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน เว้นแต่

(1) กรณีที่มีเหตุจำเป็น เช่น มีเหตุอันควรสงสัยว่า มีบุคลากรขององค์กรนำข้อมูลความลับขององค์กรออกไปเปิดเผยภายนอกโดยผ่านทางระบบจดหมายอิเล็กทรอนิกส์ หรือมีเหตุอันควรสงสัยว่า บุคลากรของ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

องค์กรใช้จดหมายอิเล็กทรอนิกส์ในทางที่ไม่ถูกต้อง ฯลฯ ซึ่งผู้ที่มีสิทธิตรวจสอบข้อมูลอิเล็กทรอนิกส์ของผู้ใช้แต่ละรายได้จะต้องเป็นผู้บริหารหรือเป็นบุคคลที่ได้รับแต่งตั้งจากคณะกรรมการขององค์กรเท่านั้น หรือ

(2) ในกรณีที่ สมาคมสโมสรนักลงทุนได้รับคำสั่งจากศาลหรือหน่วยงานที่มีอำนาจตามบทบัญญัติแห่งกฎหมายสั่งให้ส่งข้อมูลอิเล็กทรอนิกส์และ/หรือตรวจสอบการสื่อสารในรูปแบบจดหมายอิเล็กทรอนิกส์

เพื่อมิให้เกิดปัญหาในเรื่องของความปลอดภัย การปฏิบัติผิดกฎหมาย และประสิทธิภาพในการทำงาน ผู้ใช้ทุกรายพึงมีความรับผิดชอบดังนี้

- ในฐานะที่เป็นผู้มีส่วนเกี่ยวข้องกับการใช้จดหมายอิเล็กทรอนิกส์ ผู้ใช้แต่ละรายต้องปฏิบัติตามนโยบายที่เกี่ยวข้องกับการใช้จดหมายอิเล็กทรอนิกส์ โดยในการใช้ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน รวมถึงระบบอื่น ๆ ที่สมาคมสโมสรนักลงทุนจัดไว้ให้ นั้น ผู้ใช้ต้องปฏิบัติตามนโยบายที่สมาคมสโมสรนักลงทุนกำหนด
- เนื้อหาของข้อความ เอกสารประกอบ หรือรูปภาพประกอบ และอื่น ๆ ที่ส่งโดยใช้จดหมายอิเล็กทรอนิกส์ควรเป็นไปด้วยความเหมาะสม ไม่ขัดต่อบทบัญญัติของกฎหมาย และสอดคล้องกับนโยบายฉบับนี้ และอยู่ภายใต้ข้อจำกัดเดียวกันกับการติดต่อสื่อสารในรูปแบบอื่น ๆ ที่สมาคมสโมสรนักลงทุนกำหนด
- ข้อมูลอิเล็กทรอนิกส์ที่ผู้ใช้แต่ละรายเก็บสะสมไว้ ต้องใช้เนื้อที่บนเครื่องแม่ข่ายในการเก็บซึ่งฝ่ายเทคโนโลยีสารสนเทศจะกำหนดขนาดของเนื้อที่ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ (Mail Box) ของผู้ใช้แต่ละราย ผู้ใช้ต้องลบข้อมูลอิเล็กทรอนิกส์ที่ไม่จำเป็นและไม่เกี่ยวกับงานขององค์กรออก รวมทั้งข้อมูลอิเล็กทรอนิกส์ที่ไม่ใช้แล้วทิ้งไป แต่หากมีความจำเป็นที่จะต้องใช้เนื้อที่ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์มากกว่านโยบายที่กำหนด ให้หัวหน้าฝ่ายส่งแจ้งความจำเป็นและเหตุผลถึงหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- ปฏิบัติตามนโยบายที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน และระบบคอมพิวเตอร์ที่เกี่ยวข้องที่สมาคมสโมสรนักลงทุนกำหนด
- รักษาความสุภาพ และมารยาทในการสื่อสาร
- ปกป้องความเป็นส่วนตัว และความลับของผู้อื่น
- ช่วยดูแลรับผิดชอบการจำกัดขนาดของข้อมูลอิเล็กทรอนิกส์ที่ใช้งานอยู่
- ใช้เทคโนโลยีสารสนเทศให้มีประสิทธิภาพและก่อให้เกิดประโยชน์แก่งานที่รับผิดชอบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้จดหมายอิเล็กทรอนิกส์ที่ถูกต้อง

การใช้จดหมายอิเล็กทรอนิกส์ที่ถูกต้อง ต้องใช้ให้สอดคล้องกับวัตถุประสงค์ เป้าหมาย และภารกิจขององค์กร ตลอดจนสอดคล้องกับหน้าที่และความรับผิดชอบของผู้ใช้แต่ละราย ตัวอย่างต่อไปนี้แสดงให้เห็นถึงการใช้งานที่ถูกต้อง

- ใช้เพื่อการสื่อสาร รวมถึงการแลกเปลี่ยนข้อมูลสำหรับพัฒนาสายอาชีพ หรือเพื่อศึกษาหาความรู้ หรือทักษะในสายงาน
- ใช้เพื่อการสื่อสารกับหุ้นส่วนทางธุรกิจ เพื่อส่งเอกสาร หรือเพื่อโอนย้ายเอกสารประกอบการทำงาน หรือร่างเอกสารต่าง ๆ
- ใช้เพื่อค้นคว้า หรือรวบรวมข้อมูลเพื่อสนับสนุนคำแนะนำ มาตรฐาน การวิเคราะห์ หรือเพื่อพัฒนาสายอาชีพที่เกี่ยวข้องกับหน้าที่ของผู้ใช้
- ใช้เพื่อการสื่อสาร หรือแลกเปลี่ยนข้อมูลเพื่อสนับสนุนการทำงาน หรือโครงการที่รับผิดชอบร่วมกัน

การใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง และขัดต่อนโยบาย

ตัวอย่างต่อไปนี้แสดงให้เห็นถึงการใช้งานที่ไม่ถูกต้อง

- การใช้ที่เป็นการละเมิดบทบัญญัติแห่งกฎหมาย
- การใช้ที่เป็นการให้ข้อมูลภายในขององค์กร หรือข้อมูลที่เกี่ยวข้องกับความสามารถขององค์กรในด้านต่าง ๆ ซึ่งยังไม่ได้เป็นที่เปิดเผยต่อสาธารณชนแก่บุคคลอื่น โดยไม่ได้รับความเห็นชอบจากผู้บริหาร
- การใช้เพื่อเผยแพร่สิ่งลามกอนาจาร หรือขัดต่อศีลธรรม หรือนโยบายของสมาคมสโมสรนักลงทุน
- การใช้เพื่อส่งข้อความที่ส่อเสียด ยุยง ก่อให้เกิดความแตกแยก หรือความเกลียดชัง หรือก่อให้เกิดความเสื่อมเสีย/เสียหายแก่สมาคมสโมสรนักลงทุน รวมทั้งพนักงาน คณะกรรมการ และคณะกรรมการของสมาคมสโมสรนักลงทุน
- การส่งข้อความ หรือเอกสารแนบที่ไม่มีสาระเกี่ยวข้องกับการดำเนินการ หรือก่อให้เกิดประโยชน์กับสมาคมสโมสรนักลงทุน ที่เกินขอบเขตที่ยอมรับได้ หรือการใช้เพื่อธุรกิจส่วนตัวที่เกินขอบเขตที่ยอมรับได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ผู้ใช้อย่างใดก็ตามที่ใช้งานจดหมายอิเล็กทรอนิกส์ หรือส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์ เครือข่ายของสมาคมสโมสรนักลงทุนด้วยวิธีการอื่น ๆ ที่ขัดต่อนโยบายและหรือข้อตกลงหมายอาจถูกลงโทษ โดยการตัดสิทธิต่าง ๆ อันพึงได้รับ จนถึงขั้นให้พ้นสภาพการเป็นพนักงาน และ/หรือถูกดำเนินคดีทางแพ่งและทางอาญาได้

ผู้ใช้งานจะต้องตระหนักว่า (1) ข้อมูลอิเล็กทรอนิกส์ โดยเฉพาะที่มีเนื้อหาในเชิงลบต่อองค์กรสามารถส่งพิมพ์ หรือทำสำเนาได้โดยง่าย และพึงระมัดระวังว่า การส่งข้อความโดยจดหมายอิเล็กทรอนิกส์ทุกครั้งจะมีชื่อขององค์กรปรากฏอยู่ (2) สมาคมสโมสรนักลงทุนไม่อาจรับประกันได้ว่าจดหมายอิเล็กทรอนิกส์จะมีความเป็นส่วนตัว เนื่องจากบุคคลที่สามอาจจะละเมิดเข้ามาเปิดอ่านข้อมูลอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน เพื่อจุดประสงค์ในการล้วงความลับของสมาคมสโมสรนักลงทุนได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ลิขสิทธิ์โปรแกรม และการสั่งซื้อ หรือการเช่าใช้

หลักการ

นโยบายนี้กำหนดขึ้นเพื่อให้สอดคล้องกับกฎหมายลิขสิทธิ์และเพื่อปกป้องโปรแกรมที่เป็นสินทรัพย์ขององค์กร ถึงแม้ว่านโยบายนี้จะมีมาตรการช่วยในการบังคับใช้ แต่ความสำเร็จในท้ายที่สุดขึ้นอยู่กับความเข้าใจและความร่วมมือของพนักงานทุกคน ฝ่ายเทคโนโลยีสารสนเทศได้รับมอบหมายให้รับผิดชอบให้บังคับใช้นโยบายนี้อย่างต่อเนื่อง

ลิขสิทธิ์ของโปรแกรม

นโยบายของสมาคมสโมสรนักลงทุนในที่นี้คือ การเคารพในลิขสิทธิ์โปรแกรม และปฏิบัติตามสิทธิ์ที่ได้รับในการใช้โปรแกรมตามที่ระบุไว้ในเอกสารลิขสิทธิ์ ผู้ละเมิดต่อนโยบายนี้ถือว่ามีความผิดและอาจถูกลงโทษทางวินัย พนักงานจะต้องไม่ทำสำเนาของโปรแกรมหรือเอกสารที่เกี่ยวข้อง เพื่อนำมาใช้ภายในสำนักงานหรือที่อื่น ๆ โดยพลการ ยกเว้นเสียแต่จะได้รับการยินยอมโดยเจ้าของลิขสิทธิ์เป็นลายลักษณ์อักษร การทำสำเนาโปรแกรมโดยการละเมิดอาจส่งผลให้พนักงานและสมาคมสโมสรนักลงทุนถูกลงโทษทางอาญาและทางแพ่งตามที่กฎหมายระบุ พนักงานจะต้องไม่นำโปรแกรมไปให้บุคคลหรือนิติบุคคลที่สาม หมายรวมถึงผู้ขาย ผู้รับเหมา และลูกค้า พนักงานสามารถใช้โปรแกรมที่ติดตั้งบนระบบเครือข่ายหรือบนเครื่องคอมพิวเตอร์ตามที่ระบุไว้ในสัญญาลิขสิทธิ์เท่านั้น

การซื้อโปรแกรม

โปรแกรมที่ซื้อมาเป็นสินทรัพย์ที่มีมูลค่าสูง และต้องบันทึกไว้เป็นสินทรัพย์ขององค์กร เพื่อติดตามตรวจสอบ ดังนั้นการซื้อโปรแกรมจึงควรปฏิบัติให้สอดคล้องกับกระบวนการอนุมัติสั่งซื้อขององค์กร เพื่อให้การบันทึกสินทรัพย์เป็นไปอย่างถูกต้องตามที่ได้ระบุไว้ในนโยบายการสั่งซื้อทรัพยากรทางเทคโนโลยีสารสนเทศ โปรแกรมทั้งหมดต้องได้รับการอนุมัติใช้โดยฝ่ายเทคโนโลยีสารสนเทศ จำนวนผู้มีสิทธิในการสั่งซื้อได้ถูกจำกัดไว้ เพื่อให้มั่นใจว่าโปรแกรมที่สั่งซื้อทั้งหมดได้รับการบันทึกอย่างถูกต้อง ฝ่ายเทคโนโลยีสารสนเทศจะระงับการสั่งซื้อโปรแกรมใด ๆ ที่จะส่งผลเสียหายต่อระบบเครือข่าย หรือไม่เหมาะสมกับการใช้งานของหน่วยธุรกิจ หน่วยธุรกิจจะต้องปรึกษารื้อกับฝ่ายเทคโนโลยีสารสนเทศก่อนที่จะทำการสั่งซื้อ เนื่องจากฝ่ายเทคโนโลยีสารสนเทศจะสามารถแจ้งได้ว่าการติดตั้งโปรแกรมดังกล่าวไว้แล้วหรือไม่

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การจดทะเบียนโปรแกรม

ภายหลังจากที่ได้รับโปรแกรม ฝ่ายเทคโนโลยีสารสนเทศจะติดต่อกับผู้ขายเพื่อยืนยันการจดทะเบียนอย่างถูกต้อง โปรแกรมที่สั่งซื้อจะได้รับการจดทะเบียนในนามขององค์กร และจะไม่มี การจดทะเบียนในนามส่วนบุคคลโดยเด็ดขาด ภายหลังจากการจดทะเบียนแล้วเสร็จ โปรแกรมจะได้รับการติดตั้งโดยฝ่ายเทคโนโลยีสารสนเทศหรือบุคคล/นิติบุคคลที่ได้รับการมอบหมายอย่างเป็นทางการจากหน่วยงานฝ่ายเทคโนโลยีสารสนเทศเท่านั้น โดยที่ฝ่ายเทคโนโลยีสารสนเทศจะรับผิดชอบเก็บต้นฉบับของสัญญาลิขสิทธิ์และการสั่งซื้อ และแผนกจัดซื้อรับผิดชอบเก็บสำเนา จนกว่าฝ่ายเทคโนโลยีสารสนเทศและแผนกจัดซื้อเห็นสมควรว่าโปรแกรมดังกล่าวไม่สมควรจะนำมาใช้งานอีก โดยให้ปฏิบัติตามขั้นตอนและระเบียบการตัดจำหน่ายทรัพย์สิน

โปรแกรม

สินทรัพย์คอมพิวเตอร์ขององค์กรจะต้องได้มาอย่างถูกกฎหมาย และปราศจากไวรัสคอมพิวเตอร์ เฉพาะโปรแกรมที่สั่งซื้อและได้รับอนุมัติอย่างถูกต้องเท่านั้นที่สามารถนำมาใช้กับระบบคอมพิวเตอร์ขององค์กร หากปราศจากความเห็นชอบจากฝ่ายเทคโนโลยีสารสนเทศ พนักงานไม่สามารถจะนำโปรแกรมอื่นใดมาใช้กับระบบคอมพิวเตอร์ขององค์กรได้ เป็นที่ตระหนักว่า มีโปรแกรมที่มักจะถูกส่งมาพร้อมกับจดหมายอิเล็กทรอนิกส์ หรือ Download จากเครือข่ายภายนอก หรือ แผ่น CD ถูกนำมาติดตั้งลงเครื่องคอมพิวเตอร์ หากทางฝ่ายเทคโนโลยีสารสนเทศตรวจพบโปรแกรมที่ไม่ถูกต้องเหล่านั้นจะถูกตรวจจับและลบทิ้งอัตโนมัติในระหว่างการตรวจสอบภายใน ผู้ละเมิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

การตรวจสอบภายใน

ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องเป็นระยะ ๆ เพื่อดูแลให้สอดคล้องตามนโยบายที่กำหนด ฝ่ายเทคโนโลยีสารสนเทศสามารถตรวจจบบัญชีรายการ และลบโปรแกรมที่ได้มาอย่างไม่ต้องบนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายขององค์กร นอกจากนี้ฝ่ายเทคโนโลยีสารสนเทศอาจจะตรวจสอบเครื่องคอมพิวเตอร์ที่ไม่เชื่อมต่อกับระบบเครือข่ายขององค์กร และทำการลบโปรแกรมที่ไม่จดทะเบียนทันที โดยพนักงานจะต้องให้ความร่วมมือกับฝ่ายเทคโนโลยีสารสนเทศในระหว่างที่มีการตรวจสอบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์

หลักการ

การใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องมีวัตถุประสงค์เพื่อประโยชน์ต่อองค์กร และเกี่ยวข้องกับงานในหน้าที่ของพนักงานเท่านั้น

แนวทาง

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ถือเป็นทรัพย์สินขององค์กร มีใช้ทรัพย์สินส่วนตัว การใช้อุปกรณ์และระบบดังกล่าวต้องมีวัตถุประสงค์ที่เป็นประโยชน์โดยตรงต่อองค์กร

ข้อห้ามในการใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ มีต่อไปนี้

- เป็นการละเมิดต่อกฎหมายไทย
- ให้ข้อมูลของสมาคมสโมสรนักลงทุนโดยที่ไม่ได้รับความเห็นชอบจากผู้จัดการสมาคม ฯ
- เผยแพร่ข้อมูล หรือเอกสารที่ขัดแย้ง และละเมิดนโยบายของสมาคมสโมสรนักลงทุน
- ดำเนินธุรกิจส่วนตัว เกินความเหมาะสมผลในช่วงเวลาทำงาน

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องไม่มีวัตถุประสงค์ในเชิงพาณิชย์ นอกเหนือไปจากที่ได้รับมอบหมาย หรือต้องเป็นไปเพียงเพื่อประโยชน์ของสมาคมสโมสรนักลงทุนเท่านั้น อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์อาจนำมาใช้เพื่อช่วยกิจกรรมต่าง ๆ ขององค์กรมีส่วนร่วม หรืองานกุศลต่าง ๆ ที่องค์กรเป็นผู้สนับสนุน เฉพาะบุคคลที่ได้รับอนุมัติจากสมาคมสโมสรนักลงทุนเท่านั้น จึงจะสามารถใช้งานอุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์

การเข้าใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต จะต้องแจ้งให้ผู้จัดการสมาคม ฯ ทราบในทันที ค่าใช้จ่ายที่อาจเกิดขึ้นจะต้องแจ้งต่อผู้จัดการสมาคม ฯ หรือฝ่ายเทคโนโลยีสารสนเทศ และต้องดำเนินการสอบสวนโดยเร่งด่วน กรณีที่ไม่มีการแจ้งเรื่องเข้าใช้อุปกรณ์ดังกล่าวโดยไม่ได้รับมอบหมาย ถือเป็นการละเมิดนโยบายขององค์กรและต้องมีโทษทางวินัย

เนื้อหาที่ใช้ในการสื่อสารด้วยเสียงต้องดำรงไว้ซึ่งความเป็นมืออาชีพ และมีความเหมาะสม ห้ามมิให้ใช้เนื้อหาที่ไม่มีสาระสำคัญ ไม่สุภาพ สบประมาท แบ่งแยกเชื้อชาติ ล่วงเกินทางเพศ โจมตี ทำลายชื่อเสียง บังคับ ชูเชิญ ช่มชู้ โดยเด็ดขาด

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ข้อความที่สนทนาผ่านอุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ถือเป็นทรัพย์สินขององค์กร มิใช่ทรัพย์สินส่วนบุคคล สมาคมสโมสรนักลงทุนจึงขอสงวนสิทธิในการติดตามตรวจสอบเนื้อหาของการสนทนา รวมทั้งแฟ้มเสียงที่ถูกบันทึกไว้

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องเป็นไปอย่างเหมาะสม หากค่าใช้จ่ายที่เกิดขึ้นมากเกินความสมเหตุสมผลอาจทำให้บุคคลนั้น ๆ สูญสิทธิในการใช้งาน หรือบุคคลนั้นอาจต้องรับผิดชอบค่าใช้จ่ายทั้งหมดหรือส่วนหนึ่ง หรืออาจถือว่ามีความผิดทางวินัยขั้นรุนแรง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การแจ้งให้ทราบเรื่องการระงับให้บริการชั่วคราว

หลักการ

นโยบายนี้ครอบคลุมขั้นตอนที่ฝ่ายเทคโนโลยีสารสนเทศจะแจ้งให้ผู้เกี่ยวข้องรับทราบถึงแผนงานที่อาจจะส่งผล หรือมีผลกระทบต่อให้บริการต่าง ๆ บนระบบเครือข่าย และทำให้การบริการดังกล่าวต้องถูกระงับชั่วคราว ตัวอย่างเช่น การปรับปรุงประสิทธิภาพของเครื่องเซิร์ฟเวอร์ การบำรุงรักษาเครื่องเซิร์ฟเวอร์ หรือแผนบำรุงรักษาอื่นๆ ที่จะส่งผลกระทบต่อระบบไฟฟ้า หรือระบบสื่อสาร ที่หล่อเลี้ยงการทำงานของอุปกรณ์คอมพิวเตอร์ในห้องเซิร์ฟเวอร์

สำหรับการระงับใช้บริการที่มีสาเหตุอื่น ๆ อันได้แก่ ไฟฟ้า คณงานก่อสร้างตัดสายไฟฟ้า หรืออุบัติเหตุ และอุบัติเหตุที่อยู่เหนือการควบคุมของทางฝ่ายเทคโนโลยีสารสนเทศ จะแจ้งให้ผู้เกี่ยวข้องทราบทันทีที่เกิด

แนวทาง

สื่อหลักที่ใช้เพื่อแจ้งให้ทราบ คือ จดหมายอิเล็กทรอนิกส์หรืออีเมลหรือการโทรแจ้งถึงพนักงานทุกคน โดยฝ่ายเทคโนโลยีสารสนเทศจะแจ้งให้ทราบล่วงหน้าอย่างน้อย 48 ชั่วโมง กรณีที่เกิดจากการวางแผนงานล่วงหน้า ตามด้วยการแจ้งให้ทราบในกรณีที่ใช้เวลาเกินกว่ากำหนดการที่วางไว้เป็นระยะ ๆ ตามนโยบายแล้ว การดำเนินแผนงานที่มีผลกระทบดังกล่าวจะหลีกเลี่ยงไปทำนอกเวลางาน อย่างไรก็ตาม ในบางกรณีก็ไม่สามารถหลีกเลี่ยงได้

ในกรณีที่เกิดอุบัติเหตุหรืออุบัติเหตุที่ทำให้การบริการต้องหยุดชะงัก พนักงานของฝ่ายเทคโนโลยีสารสนเทศจะได้จัดให้มีหน่วยช่วยเหลือ และให้ข้อมูลโดยย่อเกี่ยวกับขอบเขตของปัญหา ระยะเวลา สาเหตุ และผลกระทบที่อาจเกิดขึ้นให้ผู้ใช้งานที่ได้รับผลกระทบได้รับทราบ นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศจะชี้แจงให้ทราบถึงปัญหาต่อเนื่องที่จะเกิดขึ้นอันเป็นผลจากหรือเกี่ยวข้องกับการหยุดชะงักของระบบ ข้อสงสัยใด ๆ ที่เกิดขึ้นอันเนื่องมาจากแผนงาน หรือจากเหตุสุดวิสัย สามารถสอบถามได้จากพนักงานประจำหน่วยช่วยเหลือผู้ใช้คอมพิวเตอร์ การติดต่อที่นอกเหนือหน่วยนี้ ทางฝ่ายเทคโนโลยีสารสนเทศจะได้แจ้งให้ทราบเป็นกรณี ๆ ไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้อุปกรณ์คอมพิวเตอร์

หลักการ

พนักงานทุกคนในสมาคมสโมสรนักลงทุนที่ใช้ระบบปฏิบัติงานและอุปกรณ์ในระบบการสื่อสารที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ของสมาคมสโมสรนักลงทุน มีหน้าที่รับผิดชอบในการใช้ระบบดังกล่าวอย่างผู้มีจรรยาบรรณ มีความเป็นมืออาชีพ โดยเป็นไปอย่างถูกต้องตามกฎหมาย ทั้งนี้ผู้ใช้ระบบทุกท่านต้องปฏิบัติตามแนวนโยบายซึ่งได้วางไว้เพื่อการใช้อุปกรณ์ในระบบต่าง ๆ ดังกล่าว

แนวทาง

พนักงานทุกคนในองค์กรควรยึดถือแนวทางปฏิบัติดังต่อไปนี้

- ต้องยึดถือในความเป็นอันหนึ่งอันเดียวกันของระบบต่างๆ ขององค์กร
- ต้องไม่แทรกแซงสิทธิส่วนบุคคลของผู้ใช้คนอื่นใด
- ต้องตระหนักว่า พนักงานต้องจำกัดการเข้าใช้ข้อมูลอันเป็นข้อมูลลับเฉพาะ ซึ่งอยู่นอกเหนืออำนาจหน้าที่ของตน
- ต้องปฏิบัติตามกฎระเบียบข้อบังคับต่าง ๆ ซึ่งควบคุมการใช้งานระบบและอุปกรณ์คอมพิวเตอร์
- ไม่ได้รับอนุญาตให้เข้าสู่ระบบหรือข้อมูลของผู้ใช้รายอื่น
- ไม่ได้รับอนุญาตให้ใช้ข้อมูลต่างๆ ของสมาคม ฯ โดยจุดประสงค์เพื่อการทำวิจัย การอบรม และการจัดทำเอกสารที่ไม่เกี่ยวข้องกับงานของสมาคม ฯ
- จะทำความคุ้นเคยและปฏิบัติตามแนวทางการใช้งานระบบต่าง ๆ รวมถึงระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานอยู่ได้อย่างถูกต้องเหมาะสม

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การควบคุมการเข้าใช้งานระบบปฏิบัติการ

- กระบวนการในการเข้าใช้งานระบบอย่างปลอดภัย จะต้องมีการตรวจสอบสิทธิ์ในการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และจะต้องมีการจัดเก็บ Log ของผู้ใช้งานในระบบ
- การตรวจสอบยืนยันผู้ใช้ระบบปฏิบัติการ จะต้องมีการระบุและตรวจสอบยืนยันตัวบุคคลของผู้ใช้ ผู้ใช้งานแต่ละคนต้องมี User Account ที่ไม่ซ้ำกัน และไม่สามารถใช้ร่วมกันหรือโอนให้กันได้ ทั้งนี้ User Account จะต้องไม่แสดงให้รู้ถึงระดับของการเข้าถึงระบบของผู้ใช้งาน ในกรณีที่จำเป็นต้องใช้ User Account ร่วมกันภายในกลุ่ม เนื่องจากข้อกำหนดบางประการจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร และการนำไปใช้ต้องอยู่ในความควบคุมอย่างเคร่งครัด
- การบริหารจัดการรหัสผ่าน ระบบปฏิบัติการจะต้องมีกลไกเพื่อให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากสามารถเข้าใช้งานครั้งแรกได้ รหัสผ่านที่ได้รับการกำหนดจากเจ้าของผลิตภัณฑ์จะต้องได้รับการเปลี่ยนทันทีเมื่อติดตั้งระบบแล้ว การบริหารจัดการรหัสผ่านในระบบปฏิบัติการจะต้องสอดคล้องกับแนวทางการจัดการรหัสผ่าน (Password Management) ของสมาคมสโมสรนักลงทุน
- การจัดการระยะเวลาในการใช้งาน เครื่องคอมพิวเตอร์ทุกเครื่องต้องมีการตั้งค่าล็อกหน้าจออัตโนมัติที่ระยะเวลา 15 นาที

การควบคุมการเข้าใช้งานแอปพลิเคชันและข้อมูล

- การจำกัดการเข้าใช้งานข้อมูล การควบคุมการเข้าถึงแอปพลิเคชันต้องเป็นไปตามข้อกำหนดและสอดคล้องกับนโยบายด้านการควบคุมการเข้าถึงของสมาคมสโมสรนักลงทุน กำหนดสิทธิ์ในการเข้าถึงข้อมูลตามความรับผิดชอบในการทำงาน
- การแยกระบบข้อมูลที่มีความสำคัญ ระบบที่มีความสำคัญควรจะแยกออกจากการเข้าถึงของบุคคลทั่วไป การให้บริการของแอปพลิเคชันที่มีความสำคัญควรใช้เซิร์ฟเวอร์ที่แยกต่างหาก ในกรณีที่อาจต้องใช้ทรัพยากรร่วมกัน เจ้าของแอปพลิเคชันทั้งสองฝ่ายต้องประเมินความสำคัญของข้อมูลก่อนจะตกลงกันเรื่องใช้ทรัพยากรร่วมกัน

การใช้คอมพิวเตอร์แบบพกพาและการเชื่อมต่อระบบเครือข่าย

- การป้องกันทางกายภาพ (Physical) อุปกรณ์ของสมาคมสโมสรนักลงทุนใด ๆ ที่ต้องนำไปใช้นอกสถานที่ในกิจกรรมของสมาคมสโมสรนักลงทุน จะต้องได้รับการอนุมัติจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ โดยอุปกรณ์ดังกล่าวจะต้องมีการควบคุมด้านความมั่นคงปลอดภัยในระดับเดียวกับอุปกรณ์ที่ใช้ในสำนักงาน เมื่อต้องเดินทางควรเก็บเครื่องคอมพิวเตอร์ในกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์ เพื่อป้องกันการกระแทกกระเทือนในระหว่างการเดินทาง ไม่ควรวางอุปกรณ์ทิ้งไว้ในที่สาธารณะโดยที่ไม่มีคนดูแล (Unattended) ต้องมีการจัดเก็บสื่อที่ใช้ในการเก็บข้อมูลไว้อย่างปลอดภัย เมื่อไม่มีการใช้งาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- การป้องกันการเข้าถึงระบบ (Logical) อุปกรณ์ควรได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต สำหรับเครื่องคอมพิวเตอร์แบบพกพาต้องควบคุมกำหนดการเข้าถึงด้วย User and Password ข้อมูลสารสนเทศของสมาคมสโมสรนักลงทุนที่อยู่ในเครื่องคอมพิวเตอร์แบบพกพาจะต้องทำการสำรองข้อมูลไว้อย่างสม่ำเสมอ พนักงานที่ทำงานจากที่บ้านหรือทำงานนอกสถานที่จัดเก็บเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้งานไว้ในที่ปลอดภัย และจะต้องปฏิบัติตามข้อกำหนดในการทำลายสื่อบันทึกข้อมูลที่หมดอายุการใช้งานหรือชำรุดตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล อย่างเคร่งครัด ทั้งนี้สื่อบันทึกข้อมูลที่สามารถทำลายได้จะต้องได้รับอนุมัติการทำลายจากผู้มีอำนาจก่อนทุกครั้ง หากทำลายสื่อบันทึกข้อมูล โดยผู้ให้บริการภายนอก จะต้องมีการทำสัญญาข้อตกลงเรื่องการรักษาความลับ
- การเชื่อมต่อกับระบบเครือข่ายให้มีความปลอดภัย (Secure Connection) กำหนดให้การเชื่อมต่อระหว่างระบบเครือข่ายของสมาคมสโมสรนักลงทุน และเครื่องคอมพิวเตอร์แบบพกพาต้องเชื่อมต่อผ่านระบบ Virtual Private Network หรือโปรแกรมที่ได้รับอนุญาตเท่านั้น เครื่องคอมพิวเตอร์แบบพกพาจะต้องอัปเดต Antivirus ให้เป็นปัจจุบันที่สุด ก่อนที่จะเชื่อมต่อเข้ากับระบบเครือข่าย ควรดำเนินการอัปเดต Patch ที่เครื่องคอมพิวเตอร์แบบพกพาก่อนที่จะเชื่อมต่อกับระบบเครือข่าย
- ควรอัปเดต Antivirus และ Virus Signature ให้เป็นปัจจุบันอยู่เสมอ

การใช้งานคอมพิวเตอร์แบบพกพาในการปฏิบัติงานจากภายนอกและการแก้ไขปัญหาจากระยะทางไกล

- การปฏิบัติงานจากภายนอกอนุญาตให้บุคลากรของสมาคม ที่จำเป็นต้องปฏิบัติงานจากภายนอกสมาคม ให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy) และวิธีปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศตามแบบฟอร์ม HR-2FM-01 การลงทะเบียนและเพิกถอนสิทธิผู้ใช้ (User Registration-De Registration Form) เพื่อให้มีการตรวจพิสูจน์ตัวตนและควบคุมการทำงานจากระยะไกล โดยการแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินเทอร์เน็ตภายในที่ใช้งานในสมาคม และใช้งานเครือข่ายส่วนตัวเสมือน (Virtual Private Network)
- การแก้ไขปัญหาจากระยะไกลอนุญาตให้บุคลากรของสมาคม สามารถทำการเปิดโปรแกรมรีโมทเพื่อให้พนักงานสารสนเทศเข้าตรวจสอบ เมื่อดำเนินการแล้วเสร็จให้ทำการปิดทันที

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

พนักงานอาจถูกเพิกถอนสิทธิ์การเข้าใช้ระบบปฏิบัติงานคอมพิวเตอร์และอุปกรณ์การสื่อสารต่าง ๆ ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ของสมาคมสโมสรนักลงทุน เนื่องด้วยเหตุผลต่าง ๆ ได้แก่ การคุกคามระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ การดัดแปลงหรือเปิดเผยข้อมูลลับ เช่น ไฟล์ข้อมูลหรือเนื้อหาที่ปรากฏในจดหมาย โดยไม่ได้รับความยินยอมจากผู้ใช้นอกจากนี้ยังหมายถึง การดัดแปลงหรือการทำลายข้อมูลขององค์กร หรือการใช้ระบบเครือข่ายของสมาคมสโมสรนักลงทุนในลักษณะที่ขัดแย้งกับแนวทางที่ได้วางไว้

ฝ่ายเทคโนโลยีสารสนเทศสามารถเพิกถอนหรือยกเลิกการเข้าใช้ระบบได้ตลอดเวลา ทั้งนี้เป็นไปเพื่อรักษาความปลอดภัยของข้อมูลและเพื่อปกป้องสิทธิประโยชน์ของสมาคมสโมสรนักลงทุน พนักงานสามารถขออุทธรณ์การเพิกถอนสิทธิ์เข้าใช้ระบบโดยยื่นต่อผู้จัดการสมาคม ฯ ในกรณีที่มีการใช้ระบบคอมพิวเตอร์ในทางที่ก่อให้เกิดความเสียหาย ผู้ก่อเหตุต้องรับผิดชอบและอาจถูกดำเนินการทางวินัย ซึ่งผู้กระทำผิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การกู้คืนข้อมูล และระบบคอมพิวเตอร์ที่ได้รับความเสียหาย

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการจัดหาแผนกู้คืนข้อมูลที่ได้รับ ความเสียหายที่มีประสิทธิภาพและต้นทุนเหมาะสม แผนนี้มีวัตถุประสงค์เพื่อให้อุปกรณ์และระบบคอมพิวเตอร์ที่สนับสนุนกิจกรรมสำคัญๆ ในการดำเนินธุรกิจขององค์กรสามารถกู้คืนมาได้ตามที่ต้องการ งานที่เกี่ยวข้องกับแผนกู้คืนจะต้องสอดคล้องกับแนวทางที่กำหนดไว้ และความต่อเนื่องของธุรกิจของสมาคมสโมสรนักลงทุน

ขอบเขต

แผนงานนี้จะครอบคลุมการกู้คืนการประมวลผลข้อมูลสำคัญ ๆ ที่เกิดขึ้นในเครื่องแม่ข่ายของฝ่ายเทคโนโลยีสารสนเทศและเครื่องแม่ข่ายที่ห้องเซิร์ฟเวอร์กลาง กรณีเกิดความเสียหายขึ้น และส่งผลกระทบต่อโครงสร้างระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน

แนวทาง

กลยุทธ์ที่ใช้ในแผนกู้คืนข้อมูลที่ได้รับ ความเสียหาย มีดังต่อไปนี้

- ดูแลให้มีอุปกรณ์หรือระบบคอมพิวเตอร์สำรองการทำงาน กรณีที่อุปกรณ์หรือระบบหลักหยุดทำงานกะทันหัน
- มีการสำรองข้อมูลอย่างสม่ำเสมอ
- จัดทำทะเบียนรายการอุปกรณ์ โปรแกรม และข้อตกลงในการบำรุงรักษา รวมถึงนิติบุคคลที่เข้ามาดูแล
- จัดระบบรักษาความปลอดภัย เพื่อปกป้องทรัพย์สินบนระบบเครือข่ายให้พ้นจากการถูกลักขโมย การสับเปลี่ยน และป้องกันมิให้ความลับขององค์กรรั่วไหล

การสำรองข้อมูล

ระบบทุกระบบและข้อมูลของผู้ใช้งานในเครื่องแม่ข่ายจะได้รับการสำรองไว้เป็นประจำทุกวัน และสำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลง โดยข้อมูลสำรองนี้จะถูกจัดเก็บไว้ในที่ที่ปลอดภัย และทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง สำหรับหน่วยงานที่ต้องการการสำรองข้อมูลที่แตกต่างเพิ่มเติมจากที่กล่าวข้างต้นตามข้อบังคับของกฎหมาย ฝ่ายเทคโนโลยีสารสนเทศจะได้ปรึกษาร่วมกับแต่ละหน่วยงานเพื่อวางแผนสำรองข้อมูลให้เป็นกรณีพิเศษต่อไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การกู้คืนข้อมูลบนเครื่องแม่ข่ายคอมพิวเตอร์

ในกรณีเหตุสุดวิสัยที่ทำให้อุปกรณ์และโปรแกรมคอมพิวเตอร์ของแม่ข่ายเสียหายจนไม่สามารถใช้งานได้ ฝ่ายเทคโนโลยีสารสนเทศจะนำข้อมูลสำรองชุดล่าสุดกลับมาติดตั้งให้ใช้งานบนเครื่องแม่ข่ายที่กู้ขึ้นมาใหม่

การกู้คืนข้อมูลบนเครื่องลูกข่ายคอมพิวเตอร์

การสำรองข้อมูลบนเครื่องลูกข่ายเป็นความรับผิดชอบของผู้ใช้งาน ในกรณีที่มีความเสียหายของแฟ้มข้อมูลบนเครื่องลูกข่าย ฝ่ายเทคโนโลยีสารสนเทศจะไม่ถือว่าเป็นความรับผิดชอบที่จะกู้ข้อมูลคืน แต่จะติดตั้งโปรแกรมระบบเพื่อใช้งานต่อไป

การตอบสนองกรณีฉุกเฉิน

แผนงานในรายละเอียดเพื่อกู้คืนข้อมูลที่เสียหายสามารถแจกแจงได้ เมื่อเหตุการณ์ดังกล่าวเกิดขึ้น ทั้งนี้ขึ้นอยู่กับลักษณะของความเสียหาย เวลาที่เกิดความเสียหาย และระยะเวลาโดยประมาณที่เกิดการหยุดชะงักของระบบ

ความรับผิดชอบ

- หน่วยงานบริการระบบเครือข่ายคอมพิวเตอร์ และหน่วยงานบริการระบบคอมพิวเตอร์ ของฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการพัฒนา ปรับปรุง และทบทวนกิจกรรมที่เกี่ยวข้องกับการกู้คืนข้อมูล และระบบคอมพิวเตอร์ที่ได้รับความเสียหาย
- หน่วยงานบริการโปรแกรมระบบ รับผิดชอบในการพัฒนา ปรับปรุง และทบทวนขั้นตอนในการกู้คืนที่เกี่ยวข้องกับโปรแกรมระบบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศหรือเจ้าของโครงการรับผิดชอบในการระบุรายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศตั้งแต่เริ่มต้น จนถึงสิ้นสุดโครงการ เพื่อให้การดำเนินงานโครงการมีความมั่นคงปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้น

แนวทาง

แนวทางที่ใช้ในการดำเนินงานโครงการด้านความมั่นคงปลอดภัยสารสนเทศ มีดังต่อไปนี้

- ต้องระบุรายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศ
- ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัย ตั้งแต่ระยะเริ่มต้น ตลอดจนจบโครงการอย่างสม่ำเสมอ ทั้งที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก เช่น ความปลอดภัยของด้านการสื่อสารภายในและภายนอกได้รับการพิจารณาและปฏิบัติของโครงการ รวมถึงดำเนินการจัดการความเสี่ยง
- ต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย เช่น ข้อกำหนดด้านความปลอดภัยของแอปพลิเคชัน ข้อกำหนดสำหรับการปฏิบัติตามสิทธิ์ในทรัพย์สินทางปัญญา ในช่วงเริ่มต้นของโครงการ
- ต้องมีการทบทวนและติดตามแผนการจัดการความเสี่ยงที่เกี่ยวข้องกับโครงการ รวมถึงมีการวัดผลการจัดการความเสี่ยงดังกล่าว

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การบริหารจัดการ Configuration

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการบริหารจัดการ Configuration เพื่อเป็นการตั้งค่าด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งในฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่าย อย่างถูกต้องตามการตั้งค่าที่กำหนด และไม่ได้ถูกเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

แนวทาง

แนวทางการบริหารจัดการ Configuration มีดังต่อไปนี้

- ต้องจัดให้มีมาตรฐานในการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Configuration Baseline) สำหรับเครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ โดยจัดทำเป็นเอกสาร นำไปปฏิบัติ ฝั่ดติดตามและทบทวนอย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบให้มั่นใจว่ามีการกำหนดค่าการรักษาความมั่นคงปลอดภัยที่จำเป็น
- ต้องกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ เพื่อสามารถตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ การเปลี่ยนแปลงแก้ไข Baseline ของอุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน ต้องผ่านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเพียงพอ และได้รับการอนุมัติก่อนดำเนินการ
- ต้องมีการจัดเก็บการเปลี่ยนแปลงของการกำหนดค่าระบบของทุกอุปกรณ์และระบบงาน โดยมีการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การบริหารจัดการคลาวด์

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการบริหารจัดการคลาวด์ เพื่อให้มีกระบวนการที่ชัดเจนสำหรับการเลือกใช้บริการคลาวด์ การจัดการการใช้งาน การควบคุมการเข้าถึง และการยกเลิกการใช้งานให้สอดคล้องกับข้อกำหนดความมั่นคงปลอดภัยของข้อมูลของสมาคมฯ

แนวทาง

แนวทางการบริหารจัดการคลาวด์ มีดังต่อไปนี้

- ต้องมีการคัดเลือกประเภท รูปแบบการติดตั้งคลาวด์ โดยจะต้องคำนึงถึงปริมาณข้อมูล ความเร็วของการรับส่งข้อมูลระหว่างระบบ และความเชี่ยวชาญของผู้รับผิดชอบ
- ต้องกำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการใช้และการบริหารจัดการการใช้บริการคลาวด์
- ต้องมีกำหนดสิทธิการเข้าถึงระบบคลาวด์ และควรกำหนดให้เข้าถึงได้น้อยที่สุดตามหน้าที่ที่จำเป็นเท่านั้น
- ต้องมีการติดตามเหตุการณ์การละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดกับระบบคลาวด์ และแจ้งเหตุเมื่อเกิดความผิดปกติ รวมถึงตอบสนองต่อเหตุการณ์ที่ไม่ปกติ
- ต้องมีการติดตาม ตรวจสอบ และประเมินผลระหว่างการใช้บริการคลาวด์ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- กรณีมีการยกเลิกหรือย้ายระบบคลาวด์ต้องจัดทำแผน รวมถึงประเมินความเป็นไปได้ของแผนการยกเลิกหรือย้ายการใช้บริการ และต้องดำเนินการให้มั่นใจว่าข้อมูลได้ทำการสำรองก่อนการยกเลิก และข้อมูลทุกส่วนของระบบที่เกี่ยวข้องทั้งหมดที่อยู่บนคลาวด์ ถูกทำลายโดยไม่สามารถกู้คืนกลับมาได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

เอกสารแนบ 1

ACKNOWLEDGEMENT STATEMENT

(ตัวอย่าง)

ข้าพเจ้าได้อ่านเอกสารและทำความเข้าใจนโยบายเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน และยืนยันที่จะปฏิบัติตามเงื่อนไขและ/หรือกฎเกณฑ์ที่มีระบุในเอกสารดังกล่าว ข้าพเจ้าเข้าใจเช่นกันว่า การเซ็นรับรองในเอกสารนี้ไม่ถือว่าการทำสัญญาหรือถูกทำให้เข้าใจว่าเป็นการทำสัญญาในอนาคต แต่เป็นการรับรองว่าข้าพเจ้าได้อ่านและเข้าใจนโยบายและกฎเกณฑ์ต่าง ๆ ที่ได้ระบุในเอกสารดังกล่าวแล้ว

ชื่อ : _____

ลายเซ็น : _____

วันที่ : _____

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

เอกสารแนบ 2

MUTUAL CONFIDENTIALITY AGREEMENT

(ตัวอย่าง)

ระหว่าง

สมาคมสโมสรนักลงทุน

1 อาคารทีพีแอนด์ที ชั้น 12 ถนนวิภาวดี-รังสิต

แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

และ

เพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับของทั้งสองหน่วยงานในระหว่างการหารือในประเด็นทางธุรกิจหรือระบบเทคโนโลยีสารสนเทศระหว่างกัน ทั้งสองฝ่ายมีข้อตกลงดังต่อไปนี้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

1. คำจำกัดความ

- 1.1 “ข้อมูลข่าวสารที่เป็นความลับ” หมายถึงข้อมูลทั้งทางวาจาหรือเอกสารหรือข้อมูลอิเล็กทรอนิกส์ที่มาจากผู้เปิดเผย ทั้งนี้รวมถึงเอกสารและ/หรือ ข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องเช่น โปรแกรมซอฟต์แวร์ ข้อมูลไฟล์อิเล็กทรอนิกส์ต่างๆ คู่มือผู้ใช้งานและคู่มืออื่นๆ
- 1.2 “ผู้เปิดเผย” หมายถึง องค์กรในสัญญาที่ เป็นผู้ให้ข้อมูล
- 1.3 “ผู้รับ” หมายถึง องค์กรให้สัญญาที่ เป็นผู้รับข้อมูล
- 1.4 “โครงการ” หมายถึง _____

2. หน้าที่ของผู้รับ

- 2.1 ผู้รับจะใช้ข้อมูลข่าวสารที่เป็นความลับเพื่อวัตถุประสงค์เฉพาะโครงการนั้นเท่านั้น และจะไม่ใช้เพื่อวัตถุประสงค์อื่น ๆ ยกเว้นจะได้รับคามยินยอมเป็นลายลักษณ์อักษร
- 2.2 ผู้รับตกลงจะไม่เปิดเผยข้อมูลข่าวสารที่เป็นความลับที่ได้รับจากผู้เปิดเผยในรูปแบบใด ๆ ก็ตาม ทั้งนี้ข้อมูลดังกล่าวจะต้องไม่อยู่ภายใต้ข้อ 2.3
- 2.3 ข้อตกลงนี้ไม่ผูกมัดเกี่ยวกับข้อมูลข่าวสารที่เป็นความลับกรณี (ก) ข้อมูลดังกล่าวได้รับรู้โดยสาธารณะอันเนื่องมาจากทางอื่นที่นอกเหนือจากผู้รับ หรือ (ข) ข้อมูลดังกล่าวเป็นข้อมูลที่ได้รับได้ข้อมูลมาจากทางอื่นก่อนที่จะได้รับจากผู้เปิดเผย หรือ (ค) ข้อมูลดังกล่าวเป็นข้อมูลที่ได้รับได้จากองค์กรอื่นซึ่งไม่เป็นการละเมิดข้อตกลงเกี่ยวกับข้อมูลที่เป็นความลับจากผู้เปิดเผย หรือ (ง) ข้อมูลดังกล่าวได้มาหรือคิดค้นมา โดยอยู่นอกเหนือจากข้อมูลที่อยู่ในข้อตกลงนี้ หรือ (จ) ข้อมูลดังกล่าวจำเป็นต้องเปิดเผยโดยข้อบังคับทางกฎหมาย
- 2.4 ข้อมูลข่าวสารที่เป็นความลับที่ได้รับมาเป็นทรัพย์สินของผู้เปิดเผยข้อมูล ในกรณีที่ผู้เปิดเผยข้อมูลต้องการข้อมูลดังกล่าวกลับคืนโดยแจ้งมาเป็นลายลักษณ์อักษร ผู้รับจะต้องส่งข้อมูลดังกล่าวคืน หรือทำลายข้อมูลดังกล่าว ซึ่งรวมทั้งสำเนาต่าง ๆ ตามที่ผู้เปิดเผยข้อมูลร้องขอมา
- 2.5 ทั้งสองฝ่ายยอมรับว่าข้อตกลงนี้ไม่มีผลต่อการโอนย้ายทรัพย์สินทางปัญญาระหว่างฝ่ายใดฝ่ายหนึ่ง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

3. ข้อตกลงทั่วไป

- 3.1 ข้อตกลงนี้ไม่ก่อให้เกิดความสัมพันธ์ทางธุรกิจอื่นใด นอกเหนือจากการเข้าใจร่วมกันในเรื่องการรักษาความลับของข้อมูล
- 3.2 ผู้รับข้อมูลยอมรับว่าความเสียหายทางการเงินอาจไม่เพียงพอต่อการละเมิดข้อตกลงดังกล่าวและตกลงว่า ผู้เปิดเผยข้อมูลสามารถเสนอทางเลือกหรือแนวทางจ่ายค่าเสียหายในกรณีที่มีการละเมิดข้อตกลงดังกล่าวขึ้น
- 3.3 ผู้รับข้อมูลยอมรับว่าข้อมูลที่ได้รับจากผู้เปิดเผยข้อมูลไม่ได้เป็นการรับประกันหรือแสดงให้เห็นว่าข้อมูลดังกล่าวมีความถูกต้องหรือครบถ้วนสมบูรณ์ของข้อมูลที่เป็นความลับดังกล่าว
- 3.4 ผู้รับข้อมูลจะไม่นำส่งข้อมูลดังกล่าวออกนอกประเทศไทยไม่ว่าจะเป็นทางตรงหรือทางอ้อม ยกเว้นจะได้รับการยินยอมเป็นลายลักษณ์อักษรจากผู้เปิดเผยข้อมูล
- 3.5 ผู้รับข้อมูลจะต้องดำเนินการลบข้อมูลที่เป็นข้อมูล Sensitive ภายในระยะเวลา 3 เดือนหลังจากสิ้นสุดระยะเวลาการดำเนินงานของโครงการและรายงานกลับ เพื่อให้ทราบว่าการดำเนินการแล้วตามมาตรฐาน
- 3.6 การเพิ่มเติมหรือแก้ไขข้อตกลงนี้จะต้องจัดทำเป็นลายลักษณ์อักษรพร้อมทั้งเซ็นรับรองโดยทั้งสองฝ่าย
- 3.7 ข้อตกลงนี้ถูกจัดทำขึ้นภายใต้กฎหมายข้อบังคับในประเทศไทย
- 3.8 ทั้งสองฝ่ายยอมรับว่า การเซ็นยินยอมในข้อตกลงนี้และดำเนินการส่งข้อตกลงทางโทรสารเพื่อให้อีกฝ่ายหนึ่งได้รับรู้นั้นเป็นการกระทำที่ยอมรับได้และถือว่ามีผลผูกพันได้ทันที

รับรองโดย _____

รับรองโดย สมาคมสโมสรนักลงทุน

ลงนาม: _____

ลงนาม: _____

ชื่อ: _____

ชื่อ: _____

ตำแหน่ง: _____

ตำแหน่ง: _____

วันที่: _____

วันที่: _____

การตรวจสอบการตั้งค่าตามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Secure Configuration Baseline)

หมายเลขเอกสาร : IT-2FM-10 หมายเลขการปรับปรุงเอกสาร : 1.0 ระดับชั้น : ใช้ภายใน วันที่บังคับใช้ : 10 ม.ค. 68 วันที่ทบทวนข้อมูล : xx/xx/xx

* หมายถึง ข้อกำหนดดังกล่าวเป็นข้อเสนอแนะที่นโยบายกำหนด

เอกสารแนบ 3

/ หมายถึง บังคับให้มีการตั้งค่าตามข้อกำหนด | O หมายถึง ไม่บังคับการตั้งค่า

No.	รายละเอียดนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ	IT Policy	Server	Network Device/ Network Security Device	Client	Application
1	* กำหนดให้รหัสผ่านมีความยาวไม่ต่ำกว่า 8 ตัวอักษร ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว ตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กอย่างน้อย 1 ตัว และตัวเลขอย่างน้อย 1 ตัว	การรักษาความปลอดภัย	/	/	/	/
2	* กำหนดให้เปลี่ยนรหัสผ่านทุก 90 วัน	การรักษาความปลอดภัย	/	/	/	/
3	รหัสผ่านที่เปลี่ยนใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม 10 ครั้งล่าสุด		O	O	O	
4	ล็อกสิทธิ์การเข้าถึงของผู้ใช้ 30 นาที เมื่อมีการป้อนรหัสผ่านผิดเกิน 5 ครั้ง		O	O	O	
5	* กำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที	การรักษาความปลอดภัย	/	/		/
6	* ติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัส	การใช้อุปกรณ์คอมพิวเตอร์	/		/	
7	ตรวจสอบการอัปเดตระบบปฏิบัติการ และแพตช์		O	O	O	
8	ตั้งสัญญาณนาฬิกาของระบบเทคโนโลยีสารสนเทศให้ตรงตามมาตรฐานสากล		O	O	O	
9	ปิดการใช้งาน Protocol ที่ไม่มีการเข้ารหัส เช่น "Telnet" และ "HTTP" เว้นแต่จำเป็นสำหรับการดำเนินงาน		O	O		/
10	ต้องจัดให้มีการบันทึกกิจกรรมของผู้ใช้งานระบบสารสนเทศ อุปกรณ์เครือข่าย และเหตุการณ์ความปลอดภัยต่าง ๆ (Logs)		O	O	O	O
11	* เครื่องคอมพิวเตอร์ต้องถูกล็อกหน้าจอเมื่อไม่มีการใช้งานเป็นเวลา 15 นาที	การรักษาความปลอดภัย			/	
12	ตรวจสอบซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ติดตั้ง ในเครื่องคอมพิวเตอร์ที่ใช้งานของ IC				O	

"ผู้ดำเนินการตรวจสอบ"

ลงชื่อ

ตำแหน่ง (.....)

วันที่ :

"ผู้อนุมัติการตรวจสอบ"

ลงชื่อ

ตำแหน่ง (.....)

วันที่ :

***Reference from CIS Controls V8.1

แบบใบเสนอราคา

เรียน คณะกรรมการจัดซื้อจัดจ้าง

1. ข้าพเจ้า(บริษัท/ห้างหุ้นส่วนจำกัด).....
เลขที่.....
โทรศัพท์.....โดย.....ผู้ลงนามข้างท้ายนี้ ได้พิจารณา
เงื่อนไขต่าง ๆ ในประกาศสมาคมสโมสรนักลงทุน เลขที่ IC-PUA...../..... โดยตลอดและยอมรับข้อกำหนด
และเงื่อนไขนั้นแล้ว รวมทั้งรับรองว่าข้าพเจ้าเป็นผู้มีคุณสมบัติครบถ้วนตามที่กำหนด

2. ข้าพเจ้าขอเสนอราคาของรายการสินค้าหรือบริการ ตามข้อกำหนดเงื่อนไขแบบรูปรายการละเอียดแห่ง
เอกสารสอบราคา ดังนี้

ลำดับที่	รายการ	จำนวน	ราคา/หน่วย	ราคารวม
1.	โครงการพัฒนาและปรับปรุง IC Website			
	ค่าพัฒนาและปรับปรุงเว็บไซต์	1 งาน		
2.	ค่าบริการรับฝากพื้นที่เว็บไซต์ (Web Hosting)	1 ปี		
รวมเป็นเงิน				
บวก : ภาษีมูลค่าเพิ่ม 7%				
รวมเป็นเงินทั้งสิ้น				

รวมเป็นเงินทั้งสิ้น..... (.....)
ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงไว้ด้วย

3. คำเสนอนี้จะยืนอยู่เป็นระยะเวลา 60 วัน นับแต่วันเปิดซองสอบราคา และสมาคมสโมสรนักลงทุนอาจ
รับคำเสนอนี้ ณ เวลาใดก็ได้ก่อนที่จะครบกำหนดระยะเวลาดังกล่าว หรือระยะเวลาที่ยืดออกไปตามเหตุผลอัน
สมควรที่สมาคมสโมสรนักลงทุนร้องขอ

4. กำหนดเวลาส่งมอบ ข้าพเจ้ารับรองที่จะเริ่มทำงานตามสัญญาทันที และจะส่งมอบงานตามเอกสารสอบ
ราคาโดยครบถ้วนถูกต้อง

5. ในกรณีที่ข้าพเจ้าได้รับการพิจารณาให้เป็นผู้ชนะการสอบราคา ข้าพเจ้าจะรับรองที่จะ
5.1 ทำสัญญาตามแบบสัญญาจ้างแนบท้ายเอกสารสอบราคากับ สมาคมสโมสรนักลงทุน ภายใน
5 วัน นับถัดจากวันที่ได้รับหนังสือแจ้งให้ไปทำสัญญา

5.2 มอบหลักประกันปฏิบัติตามสัญญาตามที่ระบุไว้ใน ข้อ 6 ของเอกสารสอบราคาให้แก่สมาคมสโมสรนักงทนก่อนหรือในขณะที่ได้ลงนามในสัญญาเป็นจำนวนร้อยละ 10 ของราคาตามสัญญาที่ได้ระบุไว้ในใบเสนอราคานี้ เพื่อเป็นหลักประกันการปฏิบัติตามสัญญาโดยถูกต้องและครบถ้วน

หากข้าพเจ้าไม่ปฏิบัติให้ครบถ้วนตามที่ระบุไว้ข้างต้นนี้ ข้าพเจ้ายินดีชดใช้ค่าเสียหายใดที่อาจมีแก่สมาคมสโมสรนักงทน และสมาคมสโมสรนักงทนมีสิทธิจะให้ผู้เสนอราคารายอื่นเป็นผู้เสนอราคาได้ หรือสมาคมสโมสรนักงทน อาจเรียกสอบราคาใหม่ก็ได้

6. ข้าพเจ้ายอมรับว่าสมาคมสโมสรนักงทนไม่มีความผูกพันที่จะรับคำเสนอนี้ หรือใบเสนอราคาใด ๆ รวมทั้งไม่ต้องรับผิดชอบในค่าใช้จ่ายใด ๆ อันอาจเกิดขึ้นในการที่ข้าพเจ้าได้เข้าเสนอราคา

7. บรรดาหลักฐานประกอบพิจารณา เช่น ตัวอย่าง (Sample) แคตตาล็อก แบบรูปรายละเอียด คุณลักษณะเฉพาะ (Specifications) ซึ่งข้าพเจ้าได้ส่งให้แก่สมาคมสโมสรนักงทนพร้อมใบเสนอราคา ข้าพเจ้ายินยอมมอบให้สมาคมสโมสรนักงทนไว้เป็นเอกสารและทรัพย์สินของสมาคมสโมสรนักงทน

สำหรับตัวอย่างที่เหลือหรือไม่ใช้แล้วซึ่งสมาคมสโมสรนักงทนคืนให้ ข้าพเจ้าจะไม่เรียกร้องค่าเสียหายใด ๆ ที่เกิดขึ้นกับตัวอย่างนั้น

ข้าพเจ้าได้ตรวจทานตัวเลขและตรวจประกวดเอกสารสอบราคา ที่ได้ยื่นพร้อมใบเสนอราคานี้โดยละเอียดแล้ว และเข้าใจดีว่าสมาคมสโมสรนักงทนไม่ต้องรับผิดชอบใด ๆ ในความผิดพลาดหรือตกหล่น

8. ใบเสนอราคานี้ได้ยื่นเสนอโดยบริสุทธิ์ยุติธรรม และปราศจากกลั่นแกล้งหรือการสมรู้ร่วมคิดกันโดยไม่ชอบด้วยกฎหมายกับบุคคลใดบุคคลหนึ่ง หรือหลายบุคคล หรือกับห้างหุ้นส่วนบริษัทใด ๆ ที่ได้ยื่นเสนอราคาในคราวเดียวกัน

เสนอมา ณ วันที่.....เดือน.....พ.ศ.

ลงชื่อ.....

(.....)

ตำแหน่ง.....

ประทับตรา (ถ้ามี)

ยกร่างสัญญาจ้างโครงการพัฒนาและปรับปรุง IC Website

สัญญาฉบับนี้ทำขึ้น ณ สมาคมสโมสรนักงทุน เลขที่ 1 อาคาร ที พี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900 ลงวันที่ ระหว่าง สมาคมสโมสรนักงทุน สำนักงานใหญ่ตั้งอยู่เลขที่ 1 อาคาร ที พี แอนด์ ที ชั้น 12 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โดย นางสาวกรรณก มาณะกิจจกุล ตำแหน่ง ผู้จัดการสมาคมสโมสรนักงทุน ผู้รับมอบอำนาจลงนามผูกพันนิติบุคคล ซึ่งต่อไปในสัญญานี้จะเรียกว่า “ผู้ว่าจ้าง” ฝ่ายหนึ่ง กับ สำนักงานใหญ่ตั้งอยู่เลขที่ โดย ตำแหน่ง.....ผู้มอำนาจลงนามผูกพันนิติบุคคล ตามหนังสือรับรองของสำนักงานทะเบียนหุ้นส่วนบริษัทกลาง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ เลขที่ ลงวันที่ ทำสัญญานี้ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้รับจ้าง” อีกฝ่ายหนึ่ง คู่สัญญาทั้งสองฝ่ายตกลงทำสัญญาโดยมีเงื่อนไข และรายละเอียดดังต่อไปนี้

ข้อ 1. ข้อตกลงว่าจ้าง

ผู้ว่าจ้างตกลงจ้างและผู้รับจ้างตกลงรับจ้างพัฒนาและปรับปรุง IC Website และบริการรับฝากพื้นที่เว็บไซต์ (Web Hosting) โดยมีรายละเอียดตามเอกสารแนบท้ายสัญญาตามเอกสารแนบ 1 ซึ่งต่อไปในสัญญานี้เรียกว่า “เว็บไซต์”

การทำงานจ้างดังกล่าวตามวรรคหนึ่งของผู้รับจ้างจะต้องดำเนินการตามข้อกำหนดและเงื่อนไขแห่งสัญญานี้ รวมทั้งเอกสารแนบท้ายสัญญาทุกประการ

ผู้รับจ้างตกลงที่จะจัดหาแรงงานที่มีความรู้ความสามารถและใช้วัสดุเครื่องมือเครื่องใช้ตลอดจนอุปกรณ์ต่าง ๆ ชนิดดีเพื่อใช้งานในการจ้างตามสัญญานี้

ข้อ 2. การรับรองคุณภาพ

ผู้รับจ้างให้คำรับรองต่อผู้ว่าจ้างว่าเว็บไซต์หรือระบบงานหรือโปรแกรมประยุกต์ (Application Program) ตามโครงการพัฒนาและปรับปรุง IC Website ที่ได้ออกแบบพัฒนาและติดตั้งให้แก่ผู้ว่าจ้างตามสัญญานี้ มีความถูกต้องชอบด้วยกฎหมายและเป็นไปตามรายละเอียดที่กำหนดไว้ในเอกสารแนบ 1 แนบท้ายสัญญาทุกประการ

ข้อ 3. เอกสารอันเป็นส่วนหนึ่งของสัญญา

เอกสารแนบท้ายดังต่อไปนี้ให้เป็นส่วนหนึ่งของสัญญานี้

เอกสารแนบ 1 ขอบเขตของงาน (Term of Reference: TOR) โครงการพัฒนาและปรับปรุง IC Website

เอกสารแนบ 2 ใบเสนอราคาและข้อเสนอโครงการของผู้รับจ้าง

เอกสารแนบ 3 หลักประกันสัญญา

ความใดในเอกสารแนบท้ายสัญญาที่ขัดแย้งกับข้อความในสัญญานี้ ให้ใช้ข้อความในสัญญานี้บังคับ และในกรณีที่เอกสารแนบท้ายสัญญาขัดแย้งกันเอง ผู้รับจ้างจะต้องปฏิบัติตามคำวินิจฉัยของผู้ว่าจ้าง คำวินิจฉัยของผู้ว่าจ้างให้ถือเป็นที่สุด และผู้รับจ้างไม่มีสิทธิหรือเรียกร้องค่าจ้าง ค่าเสียหายหรือค่าใช้จ่ายใด ๆ เพิ่มเติมจากผู้ว่าจ้างทั้งสิ้น

ข้อ 4. ระยะเวลาดำเนินการ

ระยะเวลาการดำเนินงานพัฒนา ติดตั้ง ทดสอบ และส่งมอบเว็บไซต์ พร้อมทั้งจัดอบรมให้แล้วเสร็จภายใน 180 วัน นับถัดจากวันลงนามสัญญา

ข้อ 5. การส่งมอบ

ผู้รับจ้างจะต้องดำเนินการและส่งมอบงานตามรายละเอียดขอบเขตของงาน (Term of Reference: TOR) โครงการพัฒนาและปรับปรุง IC Website ดังนี้

งวดที่ 1 : ส่งมอบภายใน 10 วัน นับถัดจากวันที่ลงนามในสัญญา (ภายในวันที่.....)

เอกสารที่ส่งมอบ ประกอบด้วย

1. แผนการดำเนินงานการพัฒนาและปรับปรุงเว็บไซต์ (Project Plan)
2. แผนผังโครงสร้างเว็บไซต์

งวดที่ 2 : ส่งมอบภายใน 30 วัน นับถัดจากวันที่ส่งมอบงาน (ภายในวันที่.....)

เอกสารที่ส่งมอบ ประกอบด้วย

1. ตัวอย่างการออกแบบหน้าเพจเว็บไซต์และโครงสร้างเว็บไซต์

งวดที่ 3 : ส่งมอบภายใน 60 วัน นับถัดจากวันที่ส่งมอบงาน (ภายในวันที่.....)

เอกสารที่ส่งมอบ ประกอบด้วย

1. ต้นแบบเว็บไซต์ / Mock Up เว็บไซต์
2. ระบบบริหารจัดการเว็บไซต์ (Back-end) ตามรายละเอียดการปรับปรุงและพัฒนาเว็บไซต์และการจัดทำโครงสร้างเว็บไซต์ (อ้างอิง TOR ข้อ 4.1.4.1 และ ข้อ 4.1.4.2)

งวดที่ 4 : ส่งมอบภายใน 160 วัน นับถัดจากวันที่ส่งมอบงาน (ภายในวันที่.....)

เอกสารที่ส่งมอบ ประกอบด้วย

1. ส่งมอบเว็บไซต์ได้รับการพัฒนาแล้วเสร็จ

งวดที่ 5 : ส่งมอบภายใน 180 วัน นับถัดจากวันที่ส่งมอบงาน (ภายในวันที่.....)

เอกสารที่ส่งมอบ ประกอบด้วย

1. โอนย้ายข้อมูลเว็บไซต์สมาคมที่พร้อมใช้งานจากพื้นที่เดิม จัดเก็บไว้บนพื้นที่รับผลเว็บไซต์ (Web Hosting) ของผู้รับจ้าง (อ้างถึง TOR ข้อ 4.6 และ ข้อ 7.2)
2. ต้องทำการแก้ไขและส่งผลการแก้ไขที่ผ่านทั้งหมดของการตรวจสอบความปลอดภัยของเว็บไซต์ที่พัฒนา ตาม TOR ข้อ 6.2
3. ส่งรายงานผลการทดสอบ UAT Test Script / UAT Result Report
4. Training Result
5. Deploy Result
6. System Design (ฉบับ Update)
 - 6.1 Data Flow
 - 6.2 Data Dictionary
7. ER Diagram
8. Requirement Specification Document
9. API Specification Document
10. อบรมการใช้งานเว็บไซต์ให้กับผู้ดูแลระบบ ผู้ดูแลและผู้บริหารเว็บไซต์ จำนวนไม่น้อยกว่า 3 ครั้ง พร้อมคู่มือการใช้งาน Back-end เว็บไซต์ ในรูปแบบเอกสาร (Hard Copy) ตามจำนวนผู้เข้าร่วมอบรม และสำเนาในรูปแบบไฟล์ (Soft Copy) ส่งมอบทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม
11. คู่มือการใช้งานเว็บไซต์ (User Manual) ที่อธิบายการใช้งานระบบทุกๆ ด้านโดยละเอียด ในรูปแบบเอกสาร (Hard Copy) จำนวน 2 ฉบับ พร้อมสำเนาในรูปแบบไฟล์ (Soft Copy) ส่งมอบทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม
12. คู่มือการดูแลและบำรุงรักษาเว็บไซต์ที่มีรายละเอียดการติดตั้งระบบ การใช้งานระบบ และการสำรองข้อมูลระบบอย่างครบถ้วน รูปแบบเอกสาร (Hard Copy) จำนวน 2 ฉบับ พร้อมสำเนาในรูปแบบไฟล์ (Soft Copy) ส่งมอบทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม

13. Source Code ของระบบทั้งหมด ที่สามารถนำมาแก้ไขต่อได้โดยบุคลากรของ
สมาคม พร้อมคู่มือในการนำระบบขึ้นใช้งาน ในรูปแบบไฟล์ (Soft Copy) ส่งมอบ
ทางอีเมล, Google Drive หรือช่องทางอิเล็กทรอนิกส์อื่นที่เหมาะสม

ข้อ 6. ค่าจ้างและการจ่ายเงิน

ผู้ว่าจ้างตกลงจ่ายและผู้รับจ้างตกลงรับเงินค่าจ้างเป็นเงินจำนวน บาท (.....) และ
ภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท (.....)
ซึ่งได้รวมภาษีอากรอื่นๆ และค่าใช้จ่ายที่ส่งมอบแล้ว โดยผู้ว่าจ้างจะชำระเงินภายใน 30 วัน หลังจากคณะกรรมการ
ตรวจรับงานพิจารณาตรวจรับมอบงานแต่ละงวดเรียบร้อยแล้ว แบ่งชำระเป็นค่าพัฒนาเว็บไซต์และค่าบริการรับ
ฝากพื้นที่เว็บไซต์ และแบ่งชำระเป็นงวด ดังนี้

ค่าพัฒนาเว็บไซต์ เป็นเงินจำนวน บาท (.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน
..... บาท (.....) รวมเป็นเงินทั้งสิ้น บาท (.....)

ค่าบริการรับฝากพื้นที่เว็บไซต์ เป็นเงินจำนวน บาท (.....) และภาษีมูลค่าเพิ่มเป็น
เงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท (.....)

แบ่งชำระเป็นงวด ดังนี้

งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 10 ของมูลค่าสัญญา (ค่าพัฒนาเว็บไซต์) เป็นเงิน บาท
(.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท
(.....) เมื่อส่งงานตามรายละเอียดตามข้อ 5 งวดที่ 1

งวดที่ 2 เป็นจำนวนเงินในอัตราร้อยละ 10 ของมูลค่าสัญญา (ค่าพัฒนาเว็บไซต์) เป็นเงิน บาท
(.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท
(.....) เมื่อส่งงานตามรายละเอียดตามข้อ 5 งวดที่ 2

งวดที่ 3 เป็นจำนวนเงินในอัตราร้อยละ 20 ของมูลค่าสัญญา (ค่าพัฒนาเว็บไซต์) เป็นเงิน บาท
(.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท
(.....) เมื่อส่งงานตามรายละเอียดตามข้อ 5 งวดที่ 3

งวดที่ 4 เป็นจำนวนเงินในอัตราร้อยละ 30 ของมูลค่าสัญญา (ค่าพัฒนาเว็บไซต์) เป็นเงิน บาท
(.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท
(.....) เมื่อส่งงานตามรายละเอียดตามข้อ 5 งวดที่ 4

งวดที่ 5 เป็นจำนวนเงินในอัตราร้อยละ 30 ของมูลค่าสัญญา (ค่าพัฒนาเว็บไซต์) เป็นเงิน บาท
(.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท
(.....) และค่าบริการรับฝากพื้นที่เว็บไซต์ร้อยละร้อยละ 100 ของมูลค่าสัญญา เป็นเงิน บาท

(.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) รวมเป็นเงินทั้งสิ้น บาท (.....)

รวมเป็นเงินทั้งสิ้น บาท (.....) และภาษีมูลค่าเพิ่มเป็นเงินจำนวน บาท (.....) เมื่อส่งงานตามรายละเอียดตามข้อ 5 งวดที่ 5

การจ่ายเงินตามเงื่อนไขแห่งสัญญา ผู้ว่าจ้างจะโอนเงินเข้าบัญชีเงินฝากธนาคารของผู้รับจ้างธนาคาร..... สาขา..... ประเภทบัญชี..... เลขที่บัญชี..... ชื่อบัญชีบริษัท..... ทั้งนี้ผู้รับจ้างตกลงเป็นผู้รับภาระเงินค่าธรรมเนียมหรือค่าบริการอื่นใด เกี่ยวกับการโอนที่ธนาคารเรียกเก็บและยินยอมให้มีการหักเงินดังกล่าวจากจำนวนเงินโอนในงวดนั้น ๆ และผู้รับจ้างจะต้องจัดส่งใบเสร็จรับเงินของผู้รับจ้าง ให้กับผู้ว่าจ้างทุกครั้งที่มีการชำระเงินเรียบร้อยแล้ว

ข้อ 7. หลักประกันสัญญา

ในขณะทำสัญญาผู้รับจ้างได้นำหลักประกันเป็นเงินโอนเข้าบัญชีผู้ว่าจ้าง/หนังสือค้ำประกันธนาคาร..... เลขที่เป็นจำนวนเงินบาท (.....) ซึ่งเท่ากับร้อยละ 10 มูลค่างานตามสัญญา ข้อ 6. (ก่อนภาษีมูลค่าเพิ่ม) มามอบให้แก่ผู้ว่าจ้างเพื่อเป็นหลักประกันการปฏิบัติงานตามสัญญานี้

หลักประกันที่ผู้รับจ้างนำมามอบให้ตามวรรคหนึ่ง จะต้องมียุครอบคลุมความรับผิดชอบทั้งปวงของผู้รับจ้างตลอดอายุสัญญา ถ้าหลักประกันที่ผู้รับจ้างนำมามอบให้ดังกล่าวลดลงหรือเสื่อมค่าลงหรือมียุครอบคลุมถึงความรับผิดชอบของผู้รับจ้างตลอดอายุสัญญา ไม่ว่าด้วยเหตุใดๆ ก็ตาม รวมถึงกรณีผู้รับจ้างส่งมอบงานล่าช้าเป็นเหตุให้ระยะเวลาแล้วเสร็จหรือวันครบกำหนดความรับผิดชอบในความชำรุดบกพร่องตามสัญญาเปลี่ยนแปลงไป ไม่ว่าจะเกิดขึ้นคราวใดผู้รับจ้างต้องหาหลักประกันใหม่หรือหลักประกันเพิ่มเติมให้มีจำนวนครบถ้วนตามวรรคหนึ่งนำมามอบให้แก่ผู้ว่าจ้างภายใน 15 วัน (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง

หลักประกันที่ผู้รับจ้างนำมามอบไว้ตามวรรคหนึ่ง ผู้ว่าจ้างจะคืนให้แก่ผู้รับจ้างโดยไม่มีดอกเบี้ยเมื่อผู้รับจ้างพ้นข้อผูกพันและความรับผิดชอบทั้งปวงตามสัญญานี้แล้ว

ข้อ 8. ค่าปรับ

8.1 กรณีผู้รับจ้าง ไม่สามารถส่งมอบงานให้เสร็จภายในระยะเวลาที่กำหนดตามสัญญาแต่ละงวด โดยสาเหตุล่าช้ามาจากผู้รับจ้าง ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นรายวันในอัตราร้อยละ 0.1 ของค่าจ้างตามสัญญาในแต่ละงวดต่อวัน (ก่อนภาษีมูลค่าเพิ่ม) คิดเป็นเงิน..... บาทต่อวัน (.....) แต่ต้องไม่ต่ำกว่า 100 บาทต่อวัน จนกว่าผู้รับจ้างจะสามารถดำเนินการได้ตามข้อกำหนด หรือจนกว่าส่งมอบงานได้ถูกต้องครบถ้วน โดยเศษของวันจะถือเป็นหนึ่งวันเต็ม หรือจนกว่าผู้ว่าจ้างบอกเลิกสัญญา

8.2 กรณีผู้รับจ้างไม่สามารถให้บริการตามขอบเขตการดำเนินงานและลักษณะการให้บริการตาม TOR ข้อ 5 ได้ภายในระยะเวลาที่กำหนด ผู้รับจ้างยินยอมให้ผู้ว่าจ้างปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.1 ต่อชั่วโมงของมูลค่าตามสัญญา (ก่อนภาษีมูลค่าเพิ่ม) คิดเป็นเงินบาทต่อชั่วโมง (.....) แต่ไม่น้อยกว่า 100 บาทต่อชั่วโมง จนกว่าเว็บไซต์จะใช้งานได้ปกติ

ทั้งนี้ 1 วันมี 24 ชั่วโมง/เศษของชั่วโมงให้คิดเป็น 1 ชั่วโมง หรือจนกว่าผู้ว่าจ้างบอกเลิกสัญญา

8.3 กรณีผู้รับจ้างไม่เข้ามาแก้ไข ตามเวลาที่ระบุข้างต้น ผู้ว่าจ้างมีสิทธิจ้างบุคคลภายนอกทำการซ่อมแซมแก้ไข โดยผู้รับจ้างจะต้องเป็นผู้ออกค่าใช้จ่ายให้แทนผู้ว่าจ้างทั้งสิ้น รวมทั้งค่าเสียหายที่เกิดขึ้น

ข้อ 9. การฝึกอบรมและจัดทำคู่มือ

ผู้รับจ้างจะต้องจัดอบรมการใช้งานเว็บไซต์และจัดทำคู่มือการใช้งานฉบับภาษาไทยให้แล้วเสร็จภายในระยะเวลาที่กำหนด โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติม จัดอบรมใช้งานจำนวนไม่น้อยกว่า 3 ครั้ง รูปแบบ Onsite หรือ Online ดังนี้

9.1 คู่มือการใช้งานเว็บไซต์ (User Manual) ที่อธิบายการใช้งานระบบทุกๆ ด้านโดยละเอียด สำหรับผู้ดูแลและบริหารเว็บไซต์

9.2 คู่มือการดูแลและบำรุงรักษาเว็บไซต์ที่มีรายละเอียดการติดตั้งระบบ การใช้งานระบบ และการสำรองข้อมูลระบบ อย่างครบถ้วน

9.3 อบรมการใช้งานเว็บไซต์ให้กับผู้ดูแลระบบ ผู้ดูแลและบริหารเว็บไซต์ จำนวนไม่น้อยกว่า 3 ครั้ง

ข้อ 10. การรับประกันผลงานและการบำรุงรักษา

10.1 ผู้รับจ้างต้องรับประกันเว็บไซต์ที่พัฒนาเป็นเวลา 12 เดือนนับจากวันที่ผู้ว่าจ้างรับมอบงานการรับประกันผลงานภายหลังการส่งมอบ โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติม

10.2 ผู้รับจ้างจะให้คำแนะนำและปรึกษาในกรณีที่มีปัญหา และหากมีปัญหาอันเนื่องมาจากเว็บไซต์เอง ผู้รับจ้างจะทำการแก้ไขให้ตลอดอายุสัญญา

10.3 ตลอดช่วงระยะเวลาการรับประกันและบำรุงรักษา หากเว็บไซต์ชำรุด เสียหาย บกพร่อง ส่งผลให้เว็บไซต์ไม่สามารถทำงานได้ ผู้รับจ้างจะทำการ Remote Access Service เข้าไปดำเนินการแก้ไขในเวลาไม่เกินรายละเอียดตามสัญญาข้อ 3 เอกสารแนบ 1 ข้อ 5.2 นับตั้งแต่เวลาที่ได้รับแจ้งจากผู้ว่าจ้าง

กรณีสิ้นสุดการรับประกันผลงาน

1. กรณีผู้ว่าจ้างมีความประสงค์ที่จะจ้างบริการบำรุงรักษาระบบต่อเนื่องกับผู้รับจ้าง ผู้รับจ้างคิดค่าจ้างบริการต่อเนื่อง โดยมีรายละเอียดตามสัญญาข้อ 3 เอกสารแนบ 1 ข้อ 5.2
2. กรณีผู้ว่าจ้างมีความประสงค์ทำสัญญาจ้างบริการกับผู้รับจ้างรายใหม่ ผู้รับจ้างต้อง ยินยอมให้ ผู้ว่าจ้างใช้งานอย่างต่อเนื่อง จนกว่าผู้ว่าจ้างจะดำเนินการจัดหาผู้รับจ้างรายใหม่ได้ โดยคิดค่าจ้างบริการต่อเนื่องในอัตราเดียวกับรายละเอียดตามสัญญาข้อ 3 เอกสารแนบ 1 ข้อ 5.2 และอำนวยความสะดวกในการย้ายระบบและข้อมูลแก่ผู้รับจ้างรายใหม่ โดยไม่คิดค่าใช้จ่าย

ข้อ 11. การจ้างช่วง

ผู้รับจ้างจะต้องไม่เอางานทั้งหมด หรือแต่บางส่วนแห่งสัญญานี้ไปจ้างช่วงอีกทอดหนึ่งเว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากผู้ว่าจ้างแล้ว การที่ผู้ว่าจ้างได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนี้ ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดชอบหรือพันธหน้าที่ตามสัญญานี้ และผู้รับจ้างจะยังคงต้องรับผิดชอบในความผิดและความความประมาทเลินเล่อของผู้รับจ้างช่วงหรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ

กรณีผู้รับจ้างไปจ้างช่วงงานแต่บางส่วนโดยฝ่าฝืนความในวรรคหนึ่ง ผู้รับจ้างต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นจำนวนเงินในอัตราร้อยละ 10 (สิบ) ของวงเงินของงานที่จ้างช่วงตามสัญญา ทั้งนี้ไม่ตัดสิทธิผู้ว่าจ้างในการบอกเลิกสัญญา

ข้อ 12. ลิขสิทธิ์และการโอนกรรมสิทธิ์

ผู้รับจ้างรับรองว่าเว็บไซต์ที่ผู้รับจ้างนำมาใช้ติดตั้งในเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือนำมาแก้ไขดัดแปลงเพื่อใช้งานภายใต้สัญญานี้ ผู้รับจ้างเป็นเจ้าของกรรมสิทธิ์หรือได้รับอนุญาตจากเจ้าของลิขสิทธิ์โปรแกรมคอมพิวเตอร์ดังกล่าวแล้วกรรมสิทธิ์ในเว็บไซต์หรือโปรแกรมประยุกต์ (Application Program) และอุปกรณ์ต่าง ๆ (ถ้ามี) ที่ติดตั้งตามสัญญานี้ และข้อมูลทั้งปวงที่ได้จากการดำเนินการตามสัญญาไม่ว่าจะอยู่ในกระบวนการใดขั้นตอนใด หรือรูปแบบใด ตามสัญญาจะโอนไปยังผู้ว่าจ้าง เมื่อผู้ว่าจ้างได้ตรวจรับมอบงานตามสัญญาข้อ 5. แล้ว

ลิขสิทธิ์การออกแบบเว็บไซต์หรือโปรแกรมประยุกต์ (Application Program) ที่ผู้รับจ้างจัดทำขึ้นตามรายละเอียดและเงื่อนไขแห่งสัญญานี้ให้ตกเป็นของผู้ว่าจ้างนับตั้งแต่วันที่ผู้ว่าจ้างตรวจรับมอบงานตามสัญญาแล้ว ซึ่งผู้ว่าจ้างสามารถนำไปจดทะเบียนขึ้นของผู้ว่าจ้างต่อกรมทรัพย์สินทางปัญญาได้ตามกฎหมาย

ข้อ 13. ความรับผิดชอบของผู้รับจ้าง

13.1 ในกรณีที่บุคคลภายนอกกล่าวอ้าง หรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์หรือสิทธิบัตรเกี่ยวกับซอฟต์แวร์ระบบ (System Software) หรือซอฟต์แวร์สนับสนุนที่เสนอ ผู้รับจ้างต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้าง หรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็วและไม่กระทบต่อผู้ว่าจ้าง โดยผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหาย และค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้นทั้งสิ้น

13.2 ผู้รับจ้างจะต้องรับผิดชอบค่าใช้จ่ายต่อผู้ว่าจ้าง ในกรณีที่เจ้าหน้าที่ หรือลูกจ้างของผู้รับจ้าง จงใจหรือประมาทเลินเล่อ หรือไม่มีความรู้ความชำนาญพอ กระทำหรืองดเว้นการกระทำใดๆ ในการติดตั้งและส่งมอบอุปกรณ์ให้ผู้ว่าจ้าง เป็นเหตุให้ระบบคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่เชื่อมต่อในระบบของผู้ว่าจ้างเสียหาย หรือไม่อยู่ในสภาพใช้การได้ดีโดยไม่อาจแก้ไขได้ ผู้รับจ้างจะต้องจัดหาระบบคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่มีคุณภาพและความสามารถในการใช้งานไม่ต่ำกว่าของเดิมทดแทน หรือชดเชยราคากระบบคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่เกิดความเสียหายให้แก่ผู้ว่าจ้างภายในเวลาที่ผู้ว่าจ้างกำหนด

13.3 บรรดาแบบแปลน แผนผัง และเอกสารอื่นใดทำนองนี้ รวมทั้งรายงานหรือเอกสารใด ๆ พร้อมทั้งสิทธิในการเข้าใช้งาน “เว็บไซต์” ที่ผู้รับจ้างได้ทำขึ้นเนื่องจากการปฏิบัติงานตามสัญญาให้ตกเป็นกรรมสิทธิ์และลิขสิทธิ์ของ ผู้ว่าจ้างและจะต้องถือเป็นสิ่งปกปิด ผู้รับจ้างจะต้องไม่ให้สิ่งดังกล่าวแก่ผู้ใดก่อนได้รับความเห็นชอบเป็นหนังสือจากผู้ว่าจ้าง และเมื่องานเสร็จแล้ว ผู้รับจ้างจะต้องส่งมอบงานให้ผู้ว่าจ้างทั้งหมด อย่่างไรก็ตามผู้รับจ้างจะเก็บสำเนาและเอกสารอื่นดังกล่าวไว้เพื่อเป็นประวัติการทำงานของผู้รับจ้างเองได้

13.4 ผู้รับจ้างจะต้องใช้ความชำนาญ ความระมัดระวัง และความขยันหมั่นเพียรในการปฏิบัติงานตามสัญญา และจะต้องปฏิบัติหน้าที่ในความรับผิดชอบให้เป็นไปตามมาตรฐานวิชาชีพ ซึ่งเป็นที่ยอมรับกันโดยทั่วไปด้วยความซื่อสัตย์สุจริต ในการปฏิบัติหน้าที่ใดที่ต้องใช้ดุลยพินิจ ผู้รับจ้างจะต้องปฏิบัติหน้าที่นั้นด้วยความยุติธรรมทั้งต่อผู้ว่าจ้างและบุคคลที่สาม

13.5 ถ้าผู้รับจ้างไม่ปฏิบัติตามสัญญา ข้อหนึ่งข้อใดด้วยเหตุใด ๆ ก็ตาม จนเป็นเหตุให้เกิดความเสียหายแก่ผู้ว่าจ้างแล้ว ผู้รับจ้างต้องชดเชยค่าเสียหาย ให้แก่ผู้ว่าจ้างโดยสิ้นเชิง ภายในกำหนด 30 วัน นับตั้งแต่วันที่ได้รับความแจ้งจากผู้ว่าจ้าง

ข้อ 14. การกำหนดค่าเสียหาย

ค่าเสียหายซึ่งเกิดขึ้นจากผู้รับจ้างตามสัญญานี้ ผู้ว่าจ้างมีสิทธิที่จะหักเอาจากจำนวนเงินค่าจ้างที่ค้างจ่าย หรือบังคับเอาจากหลักประกันสัญญาก็ได้โดยไม่ต้องบอกสงวนสิทธิหากมีเงินค่าจ้างตามสัญญาที่หักไว้จ่ายเป็นค่าเสียหายแล้วยังเหลืออยู่อีกเท่าใดผู้ว่าจ้างจะคืนให้แก่ผู้รับจ้าง โดยไม่มีดอกเบี้ย

ข้อ 15. การขยายเวลาปฏิบัติงานตามสัญญา

ในกรณีที่มีเหตุสุดวิสัย หรือเหตุใด ๆ อันเนื่องมาจากความผิดหรือบกพร่องของผู้ว่าจ้างหรือเหตุการณ์อันหนึ่งอันใดที่ผู้รับจ้างไม่ต้องรับผิดชอบตามกฎหมาย ทำให้ผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จตามเงื่อนไขและกำหนดเวลาแห่งสัญญานี้ได้ ผู้รับจ้างจะต้องแจ้งเหตุหรือพฤติกรรมดังกล่าวพร้อมหลักฐานเป็นหนังสือให้ผู้ว่าจ้างทราบ เพื่อขอขยายเวลาทำงานออกไปภายใน 30 วัน นับแต่วันที่เหตุอันเกิดขึ้น

ถ้าผู้รับจ้างไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้รับจ้างได้ละสิทธิเรียกร้องในการขอขยายเวลาทำงานออกไปโดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น เว้นแต่กรณีเหตุเกิดจากความผิดหรือความบกพร่องของผู้ว่าจ้างซึ่งมีหลักฐานชัดเจน หรือผู้ว่าจ้างทราบดีอยู่แล้วตั้งแต่ต้น

การขยายกำหนดเวลาทำงานตามวรรคหนึ่ง ให้อยู่ในดุลยพินิจของผู้ว่าจ้างที่จะพิจารณาตามที่เห็นสมควร

ข้อ 16. การบอกเลิกสัญญา

ในระหว่างอายุสัญญา หากผู้ว่าจ้างเห็นว่าผู้รับจ้างไม่อาจปฏิบัติตามสัญญาได้ หรือผู้รับจ้างผิดสัญญาข้อใดข้อหนึ่งผู้ว่าจ้างมีสิทธิบอกเลิกสัญญาได้ ในกรณีเช่นนี้ ผู้รับจ้างยินยอมให้ผู้ว่าจ้างดำเนินการนอกเหนือจากการเรียกค่าปรับตามสัญญาข้อ 6 จนถึงวันบอกเลิกสัญญาดังต่อไปนี้

16.1 รับผิดชอบหรือเรียกร้องจากธนาคารผู้ออกหนังสือค้ำประกัน ตามสัญญาข้อ 7 ทั้งหมด หรือแต่บางส่วนแล้วแต่ผู้ว่าจ้างจะเห็นสมควร

16.2 เรียกค่าเสียหายอันพึงมีจากผู้รับจ้าง

ถ้าการไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่ง เป็นเหตุให้เกิดความเสียหายแก่ผู้ว่าจ้างเกินกว่าจำนวนหลักประกันตามสัญญาข้อ 7 ผู้รับจ้างยอมรับผิด และยินยอมชดเชยค่าเสียหายส่วนที่เกินจำนวนความรับผิดชอบของหลักประกันให้แก่ผู้ว่าจ้างจนครบถ้วนภายใน 30 วัน นับถัดจากวันที่ได้รับแจ้งจากผู้ว่าจ้าง

ทั้งนี้ ผู้ว่าจ้างสามารถยกเลิกสัญญาได้ โดยแจ้งผู้รับจ้างทราบล่วงหน้าเป็นเวลาอย่างน้อย 30 วัน

ข้อ 17. การรักษาความลับข้อมูลหรือเอกสาร

คู่สัญญาทั้งสองฝ่ายจะต้องรักษาเอกสารหรือข้อมูลที่ได้รับอีกฝ่ายหนึ่ง ไม่ว่าจะเป็นข้อมูลทางเทคนิคหรือข้อมูลใดๆ ที่บรรจุหรือเกี่ยวกับระบบงานหรือโปรแกรม ซึ่งคู่สัญญาผู้ให้ข้อมูลนั้นประสงค์ให้เป็นความลับและได้แจ้งให้คู่สัญญาอีกฝ่ายหนึ่งทราบเป็นหนังสือแล้ว ไว้เป็นความลับและจะไม่เปิดเผยเอกสารข้อมูลดังกล่าวไม่ว่าด้วยวิธีใดในลักษณะที่จะก่อให้เกิดความเสียหายแก่คู่สัญญาซึ่งเป็นเจ้าของข้อมูลนั้นๆ ให้บุคคลอื่นใดทราบ ทั้งนี้ เว้นแต่กรณีที่จำเป็นต้องเปิดเผยตามบทบัญญัติแห่งกฎหมายระเบียบของทางราชการหรือตามคำสั่งศาล

ข้อ 18. กรณีพิพาทและอนุญาโตตุลาการ

18.1 ในกรณีที่มีข้อโต้แย้งเกิดขึ้นระหว่างคู่สัญญาเกี่ยวกับข้อกำหนดแห่งสัญญานี้หรือเกี่ยวกับการปฏิบัติตามสัญญานี้ และคู่สัญญาไม่สามารถตกลงกันได้ให้เสนอข้อโต้แย้งหรือข้อพิพาทนั้นต่ออนุญาโตตุลาการเพื่อพิจารณาชี้ขาด

18.2 เว้นแต่คู่สัญญาทั้งสองฝ่ายจะเห็นพ้องกันให้อนุญาโตตุลาการคนเดียวเป็นผู้ชี้ขาด การระงับข้อพิพาทให้กระทำโดยอนุญาโตตุลาการ 2 คน โดยคู่สัญญาฝ่ายหนึ่งจะทำหนังสือแสดงเจตนาจะให้มิ้อนุญาโตตุลาการระงับข้อพิพาทและระบุชื่ออนุญาโตตุลาการคนที่ตนแต่งตั้งส่งไปยังคู่สัญญาอีกฝ่ายหนึ่งจากนั้นภายในระยะเวลา 30 วันนับถัดจากวันที่ได้แจ้งดังกล่าว คู่สัญญาฝ่ายที่ได้รับแจ้งจะต้องแต่งตั้งอนุญาโตตุลาการคนที่สอง ถ้าอนุญาโตตุลาการทั้งสองคนดังกล่าวไม่สามารถประนีประนอมระงับข้อพิพาทนั้นได้ให้อนุญาโตตุลาการทั้งสองคนร่วมกันแต่งตั้งอนุญาโตตุลาการ ผู้ชี้ขาดภายในกำหนดเวลา 30 วันนับจากวันที่ไม่สามารถตกลงกันได้ ผู้ชี้ขาดดังกล่าวจะพิจารณาระงับข้อพิพาทต่อไป กระบวนการพิจารณาของอนุญาโตตุลาการให้ถือตามข้อบังคับอนุญาโตตุลาการของสถาบันอนุญาโตตุลาการ กระทรวงยุติธรรม โดยอนุโลม หรือตามข้อบังคับอื่นที่คู่สัญญาทั้งสองฝ่ายเห็นชอบ และให้กระทำในกรุงเทพมหานคร โดยใช้ภาษาไทยหรือภาษาอังกฤษเป็นภาษาในการดำเนินกระบวนการพิจารณา

18.3 ในกรณีที่คู่สัญญาฝ่ายใดฝ่ายหนึ่งไม่แต่งตั้งอนุญาโตตุลาการฝ่ายตนหรือในกรณีที่อนุญาโตตุลาการทั้งสองคนไม่สามารถตกลงกันแต่งตั้งอนุญาโตตุลาการผู้ชี้ขาดได้ คู่สัญญาแต่ละฝ่ายต่างมีสิทธิร้องขอต่อศาลแพ่งเพื่อแต่งตั้งอนุญาโตตุลาการ หรืออนุญาโตตุลาการผู้ชี้ขาดได้แล้วแต่กรณี

18.4 คำชี้ขาดของอนุญาโตตุลาการหรือของอนุญาโตตุลาการผู้ชี้ขาดแล้วแต่กรณีให้ถือเป็นเด็ดขาดและถึงที่สุดผูกพันคู่สัญญา

18.5 คู่สัญญาแต่ละฝ่ายเป็นผู้รับภาระค่าธรรมเนียมอนุญาโตตุลาการฝ่ายตนและออกค่าใช้จ่ายอื่น ในการดำเนินกระบวนการพิจารณาฝ่ายละครั้ง ในกรณีที่มีการแต่งตั้งอนุญาโตตุลาการคนเดียวหรือมีการแต่งตั้งอนุญาโตตุลาการ ผู้ชี้ขาดให้อนุญาโตตุลาการหรืออนุญาโตตุลาการผู้ชี้ขาดเป็นผู้กำหนดภาระค่าธรรมเนียมอนุญาโตตุลาการคนเดียว หรือภาระค่าธรรมเนียมอนุญาโตตุลาการผู้ชี้ขาดคนเดียว แล้วแต่กรณี

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียด
ตลอดแล้วจึงได้ลงลายมือชื่อ พร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยานและคู่สัญญาต่างยึดถือไว้ฝ่าย
ละหนึ่งฉบับ

สมาคมสโมสรนักลงทุน

บริษัท

ลงชื่อ.....ผู้ว่าจ้าง
(นางสาวกรองกนก มานะกิจจงกล)

ลงชื่อ.....ผู้รับจ้าง
(.....)

ลงชื่อ.....พยาน
(นางสาวสุกัญญา แสงเดือน)

ลงชื่อ.....พยาน
(.....)

**แบบหนังสือค้ำประกัน
(หลักประกันสัญญา)**

เลขที่.....

วันที่.....

ข้าพเจ้า.....(ชื่อธนาคาร)สำนักงานตั้งอยู่เลขที่.....ถนน.....ตำบล/แขวง.....
อำเภอ/เขต.....จังหวัด.....โดย.....ผู้มีอำนาจลงนาม
ผูกพันธนาคาร ขอทำหนังสือค้ำประกันฉบับนี้ให้ไว้ต่อสมาคมสโมสรนักลงทุน ซึ่งต่อไปนี้เรียกว่า “ผู้ว่าจ้าง/ผู้ให้บริการ/ผู้ซื้อ” ดังมี
ข้อความต่อไปนี้

1. ตามที่..... (ชื่อบริษัท)ซึ่งต่อไปนี้เรียกว่า “ผู้รับจ้าง/ผู้ให้บริการ/ผู้ขาย”
ได้ทำสัญญา.....ตามสัญญาลงวันที่.....ซึ่งผู้รับจ้าง/ผู้ให้บริการ/ผู้ขายต้องวางหลักประกันการ
ปฏิบัติตามสัญญาต่อผู้ว่าจ้าง/ผู้ให้บริการ/ผู้ซื้อ เป็นจำนวนเงิน.....บาท (.....)

ข้าพเจ้ายอมผูกพันตนโดยไม่มีเงื่อนไขที่จะค้ำประกันชนิดเพิกถอนไม่ได้เช่นเดียวกับลูกหนี้ชั้นต้น ในการชำระเงินให้ตาม
สิทธิเรียกร้องของผู้ว่าจ้าง/ผู้ให้บริการ/ผู้ซื้อ จำนวนไม่เกิน.....บาท (.....) ในกรณีที่ผู้รับจ้าง/ผู้ให้บริการ/
ผู้ขายก่อให้เกิดความเสียหายใด ๆ หรือต้องชำระค่าปรับ หรือค่าใช้จ่ายใด ๆ หรือผู้รับจ้าง/ผู้ให้บริการ/ขายมิได้ปฏิบัติตาม
ภาระหน้าที่ใด ๆ ที่กำหนดในสัญญาดังกล่าวข้างต้นทั้งนี้ โดยข้าพเจ้าจะไม่อ้างสิทธิใด ๆ เพื่อโต้แย้ง และผู้ว่าจ้าง/ผู้ให้บริการ/ผู้ซื้อ
ไม่จำเป็นต้องเรียกร้องให้ผู้รับจ้าง/ผู้ให้บริการ/ผู้ขายชำระหนี้ก่อน

2. หากผู้ว่าจ้าง/ผู้ให้บริการ/ผู้ซื้อ ได้ขยายระยะเวลาให้แก่ผู้รับจ้าง/ผู้ให้บริการ/ผู้ขายหรือยินยอมให้ผู้รับจ้าง/ผู้ให้บริการ/
ผู้ขายปฏิบัติผิดแผกไปจากเงื่อนไขใด ๆ ในสัญญา ให้ถือว่าข้าพเจ้ายินยอมในกรณีนั้น ๆ ด้วย

3. หนังสือค้ำประกันนี้มีผลใช้บังคับตั้งแต่วันทำสัญญาซื้อขาย/สัญญาว่าจ้างดังกล่าวจนถึงภาระหน้าที่ทั้งหลายของ
ผู้รับจ้าง/ผู้ให้บริการ/ผู้ขายจะได้ปฏิบัติให้สำเร็จลุล่วงไป และข้าพเจ้าจะไม่เพิกถอนการค้ำประกันไม่ว่ากรณีใด ๆ トラバเท่าที่
ผู้รับจ้าง/ผู้ให้บริการ/ผู้ขายยังต้องรับผิดชอบต่อ ผู้ว่าจ้าง/ผู้ให้บริการ/ผู้ซื้อตามสัญญาซื้อขาย/สัญญาว่าจ้างอยู่

ข้าพเจ้าได้ลงนามและประทับตราไว้ต่อหน้าพยานเป็นสำคัญ

(ลงชื่อ).....ผู้ค้ำประกัน

(.....)

ตำแหน่ง.....

(ลงชื่อ)..... พยาน

(.....)

(ลงชื่อ)..... พยาน

(.....)

บัญชีเอกสารส่วนที่ 1

☐ 1. ผู้เสนอราคาเป็นนิติบุคคล☐ (ก) ห้างหุ้นส่วนสามัญ หรือ ห้างหุ้นส่วนจำกัด

สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล จำนวน.....แผ่น

บัญชีรายชื่อหุ้นส่วนผู้จัดการและผู้มีอำนาจควบคุม (ถ้ามี) จำนวน.....แผ่น

☐ (ข) บริษัทจำกัด หรือ บริษัท (มหาชน) จำกัด

สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล จำนวน.....แผ่น

หนังสือบริคณห์สนธิ จำนวน.....แผ่น

บัญชีรายชื่อกรรมการผู้จัดการ และผู้มีอำนาจควบคุม (ถ้ามี) จำนวน.....แผ่น

บัญชีผู้ถือหุ้นรายใหญ่ จำนวน.....แผ่น

☐ 2. ผู้เสนอราคาเป็นผู้เสนอราคาร่วมกันในฐานะเป็นผู้ร่วมค้า

สำเนาสัญญาของการเข้าร่วมค้า จำนวน.....แผ่น

☐ (ก) ในกรณีผู้ร่วมค้าเป็นนิติบุคคล

- ห้างหุ้นส่วนสามัญ หรือ ห้างหุ้นส่วนจำกัด

สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล จำนวน.....แผ่น

บัญชีรายชื่อหุ้นส่วนผู้จัดการและผู้มีอำนาจควบคุม (ถ้ามี) จำนวน.....แผ่น

- บริษัทจำกัด หรือ บริษัท (มหาชน) จำกัด

สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล จำนวน.....แผ่น

หนังสือบริคณห์สนธิ จำนวน.....แผ่น

บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) จำนวน.....แผ่น

บัญชีผู้ถือหุ้นรายใหญ่ จำนวน.....แผ่น

☐ (ข) อื่น ๆ (ถ้ามี)☐☐☐☐☐

ข้าพเจ้าขอรับรองว่า เอกสารหลักฐานที่ข้าพเจ้ายื่นพร้อมซองใบเสนอราคาในการสอบราคาหรือ
ประกวดราคาถูกต้องและเป็นความจริงทุกประการ

ลงชื่อ.....ผู้เสนอราคา

(.....)

บัญชีเอกสารส่วนที่ 2

- ☐ 1. ข้อเสนอด้านเทคนิค จำนวน.....แผ่น
- ☐ 2. หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน จำนวนแผ่น
- ☐ 3. หลักประกันซอง จำนวน.....แผ่น
- ☐ 4. อื่น ๆ (ถ้ามี)
- ☐
- ☐
- ☐
- ☐
- ☐

ข้าพเจ้าขอรับรองว่า เอกสารหลักฐานที่ข้าพเจ้ายื่นพร้อมซองใบเสนอราคาในการประกวดราคาหรือสอบราคาถูกต้องและเป็นความจริงทุกประการ

ลงชื่อ.....ผู้เสนอราคา
(.....)



สมาคมสโมสรนักลงทุน
Investor Club Association

ขั้นตอนการพัฒนาระบบ (System Development Procedure)

รหัสเอกสาร:	IT-2PR-05
หมายเลขปรับปรุงเอกสาร:	1.0
วันที่เอกสารมีผลบังคับใช้:	10 มกราคม 2568
เจ้าของเอกสาร:	ฝ่ายเทคโนโลยีสารสนเทศ



ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ-นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
ผู้จัดทำ	รุ่งรัตน์ อุ่นจิตต์	พนักงานพัฒนาระบบ สารสนเทศอาวุโส		09/01/2568
ผู้ทบทวน	สิริวรรณ ฉลากรไชยา	หัวหน้าฝ่าย เทคโนโลยีสารสนเทศ		10 มกราคม 2568
ผู้อนุมัติ	กรองนก มานะกิจจกมล	ผู้จัดการ สมาคมสโมสรนักลงทุน		10 มกราคม 2568

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุง เอกสาร (version):	วันที่ปรับปรุง เอกสาร	ปรับปรุงโดย	คำอธิบายและเหตุผลในการแก้ไข



สารบัญ

เรื่อง	หน้า
1. บทนำ	4
1.1 วัตถุประสงค์ (Objective).....	4
1.2 ขอบเขต (Scope)	4
2. กรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development Lifecycle).....	4
2.1 การวางแผน (Planning)	4
2.2 การเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis).....	5
2.3 การออกแบบระบบสารสนเทศหรือซอฟต์แวร์ (Design).....	5
2.4 การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development).....	6
2.5 การทดสอบระบบสารสนเทศหรือซอฟต์แวร์ (Testing).....	6
2.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment).....	7
2.7 การบำรุงรักษา (Maintenance).....	7
3. ขั้นตอนการพัฒนาระบบสารสนเทศและซอฟต์แวร์.....	7
3.1 การวางแผนโครงการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Project Planning).....	7
3.2 การบริหารจัดการความต้องการในการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Requirement Management)	8
3.3 การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Design and Analysis).....	9
3.4 การพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development).....	11
3.5 การทดสอบระบบสารสนเทศและซอฟต์แวร์ (Testing).....	12
3.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment).....	13
3.7 การปิดโครงการหรือเสร็จสิ้นการพัฒนาโครงการ (Project Closure)	13
4. การจัดจ้างผู้ให้บริการภายนอก เพื่อการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Outsourcing Development)	14
5. เอกสารที่เกี่ยวข้อง (Related Documents)	14



1. บทนำ

1.1 วัตถุประสงค์ (Objective)

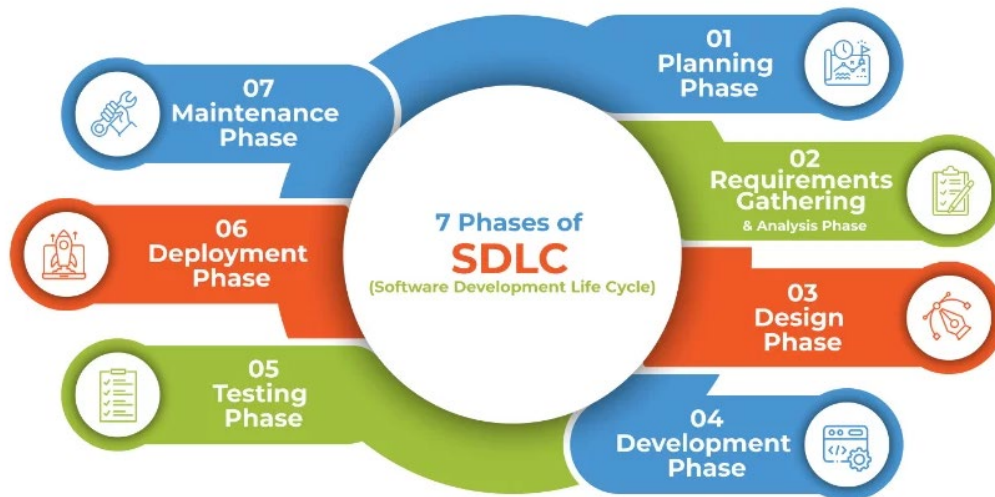
เอกสารฉบับนี้จัดทำขึ้นเพื่ออธิบายกระบวนการดำเนินงานในการจัดหาและการพัฒนาระบบที่นำมาใช้ในสมาคมฯ ให้เป็นไปตามมาตรฐานสากล

1.2 ขอบเขต (Scope)

เอกสารฉบับนี้ จัดทำขึ้นเพื่อใช้ในการกำหนดแนวทางการพัฒนาระบบที่อยู่ภายใต้ขอบเขตการขอรับรองที่อ้างอิงตามเอกสารขอบเขตรบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS and ISMS Scope) (ISO-1PC-02) ที่เป็นการพัฒนาโครงการใหม่

2. กรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development Lifecycle)

เพื่อให้การพัฒนาระบบสารสนเทศและซอฟต์แวร์ เป็นไปในแนวทางที่เป็นมาตรฐานและสามารถบริหารจัดการโดยง่าย จึงกำหนดกรอบการพัฒนาระบบสารสนเทศและซอฟต์แวร์ให้ครอบคลุมกระบวนการ ดังนี้



ภาพที่ 1 กระบวนการพัฒนาระบบสารสนเทศและซอฟต์แวร์

2.1 การวางแผน (Planning)

เป็นการวางแผนการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ของทั้งโครงการ โดยผู้จัดการโครงการ (Project Manager) จะวางแผนด้านระยะเวลาในการพัฒนา (Time) ขอบเขตงาน (Scope) จำนวนคนที่จะใช้ (Resource) รวมถึงวางแผนว่าใครหรือองค์ใดที่จะมีส่วนเกี่ยวข้องกับการพัฒนาบ้าง เนื่องจากบางครั้งอาจต้องอาศัยปัจจัยอื่น เช่น นโยบาย กฎหมาย หรือระเบียบที่เกี่ยวข้องของสมาคมฯ เข้ามาเป็นปัจจัยการออกแบบระบบสารสนเทศหรือซอฟต์แวร์ด้วย Project Manager จะต้องวางแผนให้ครอบคลุมกิจกรรมในการเก็บ



รวบรวมและวิเคราะห์ความต้องการ (Analysis) การออกแบบ (Design) การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development) และการทดสอบ (Testing) โดยการวางแผนงานที่ละเอียดแม่นยำ จะช่วยลดความเสี่ยงของการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ และสามารถพัฒนาสำเร็จตามเวลา และวัตถุประสงค์ที่กำหนดไว้

2.2 การเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis)

ในขั้นตอนนี้ Project Manager หรือ Product Owner หรือ Business Analyst จะเป็นผู้เก็บรวบรวม Requirement จากลูกค้าหรือผู้มีส่วนเกี่ยวข้อง เพื่อเข้าใจความต้องการจากผู้ใช้งานและการทำงานของระบบ โดยอาจจัดทำอยู่ในรูปแบบ Prototyping เพื่อให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบได้ง่ายขึ้น หลังจากการรวบรวม Requirement เสร็จแล้ว ทีมพัฒนา เช่น ผู้พัฒนาระบบ (Developer) หรือ ผู้ตรวจสอบคุณภาพ (Quality Assurance) สามารถช่วยตรวจสอบ Requirement นั้นได้เพื่อใช้ในการออกแบบและประเมินความเสี่ยงและข้อจำกัดของระบบสารสนเทศหรือซอฟต์แวร์ที่อาจเกิดขึ้น

ตัวอย่างขั้นตอนการเก็บรวบรวมและวิเคราะห์ความต้องการสำหรับการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ สามารถพิจารณาได้ดังต่อไปนี้

- 1) ขั้นตอนการรวบรวมความต้องการ (Requirement Gathering) เป็นขั้นตอนที่ดำเนินการรวบรวมความต้องการที่มีต่อระบบ จากกลุ่มลูกค้าหรือผู้มีส่วนเกี่ยวข้อง โดยการสัมภาษณ์หรือศึกษาปัญหา/ข้อมูลที่มีอยู่ปัจจุบัน
- 2) ขั้นตอนการวิเคราะห์ความต้องการ (Requirement Analysis) เป็นขั้นตอนที่จะวิเคราะห์ข้อมูลความต้องการที่รวบรวมได้ เพื่อออกแบบการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์โดยมีวัตถุประสงค์ ดังนี้
 - จัดกลุ่มความต้องการตามหมวดหมู่ เช่น ฟังก์ชันการทำงาน ประสิทธิภาพ การรักษาความมั่นคงปลอดภัย
 - ประเมินความสำคัญของความต้องการแต่ละข้อ เช่น ความต้องการข้อใดควรมีการดำเนินการทำก่อน
 - กำหนดลำดับความสำคัญของความต้องการ เช่น ระดับผลกระทบของแต่ละความต้องการ

2.3 การออกแบบระบบสารสนเทศหรือซอฟต์แวร์ (Design)

ขั้นตอนนี้หลัก ๆ แล้ว Developer จะนำ Requirement ที่ได้มาออกแบบ เช่น ออกแบบสถาปัตยกรรมที่จะใช้ (Architects) ออกแบบส่วนต่อประสานผู้ใช้งาน (User Interface) ภาษาที่จะใช้ในการพัฒนา ออกแบบฐานข้อมูล ระบบเครือข่ายและความมั่นคงปลอดภัย เป็นต้น ผลลัพธ์ที่ได้จากขั้นตอนนี้จะได้ System Design Specification ซึ่งสามารถให้ผู้มีส่วนเกี่ยวข้องหรือผู้เชี่ยวชาญตรวจสอบและให้คำแนะนำได้



2.4 การพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ (Development)

ขั้นตอนนี้ทีม Developer โดยนำ Requirement และ Design ที่ได้จากขั้นตอนที่ 2.2 และ 2.3 มาพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ โดยมีเครื่องมือต่าง ๆ ตามความต้องการของแต่ละระบบ

2.5 การทดสอบระบบสารสนเทศหรือซอฟต์แวร์ (Testing)

เป็นการประกันคุณภาพของระบบสารสนเทศหรือซอฟต์แวร์ โดยการค้นหาข้อผิดพลาด ป้องกันการเกิดข้อผิดพลาด รวมไปถึงตรวจสอบว่าระบบสารสนเทศหรือซอฟต์แวร์ที่พัฒนานั้นเป็นไปตาม Requirement หรือไม่ ในการทดสอบนั้นจะมีการสร้าง Test Case ซึ่งเป็นสถานการณ์และขั้นตอนที่ผู้ใช้งานจะใช้งานระบบ โดยใน Test Case จะมีการระบุ Expected Results คือผลที่คาดหวังจากการทดสอบโดยผลที่คาดหวังนี้จะอ้างอิงตาม Requirement ที่ได้มาจากขั้นตอนการเก็บรวบรวมและวิเคราะห์ความต้องการ (Requirement Gathering and Analysis) ในกรณีที่ระบบสารสนเทศหรือซอฟต์แวร์ทำงานถูกต้องเป็นไปตามผลที่คาดหวัง จะทำให้การทดสอบนั้นผ่าน แต่หากไม่เป็นไปตามผลที่คาดหวัง จะทำให้การทดสอบนั้นไม่ผ่าน ต้องให้ Developer ดำเนินการแก้ไข ผู้ทดสอบอาจเลือกวิธีทดสอบแบบ Automated Test ได้ เพื่อให้การทดสอบสามารถทำได้รวดเร็วมากขึ้น

ในขั้นตอนการทดสอบนี้ Project Manager สามารถเพิ่มเติมรายละเอียดของกิจกรรมของการทดสอบได้ตามความเหมาะสม หรือเปลี่ยนแปลงตามแนวทาง (Methodology) ที่ถูกนำมาใช้ในการพัฒนาระบบสารสนเทศ เช่น Agile Development หรือ Waterfall Methodology เป็นต้น

การกำหนดสภาพแวดล้อม (Environment) ในการพัฒนา ทดสอบ และติดตั้งระบบสารสนเทศและซอฟต์แวร์

กำหนดให้สมาคมฯ แบ่งสภาพแวดล้อมเพื่อรองรับการพัฒนา ทดสอบ และติดตั้งระบบสารสนเทศและซอฟต์แวร์ ดังนี้

- 1) Development Environment คือ ระบบสารสนเทศและซอฟต์แวร์ ต้องได้รับการควบคุมการเข้าถึงอย่างเคร่งครัด มีระบบเครือข่ายที่สนับสนุนสภาพแวดล้อม ควรเป็นระบบปิดที่ไม่มีการเชื่อมต่อสภาพแวดล้อมของ Production
- 2) Test Environment คือ ใช้เพื่อการทดสอบระบบสารสนเทศหรือซอฟต์แวร์ หรือการใช้งานอุปกรณ์อื่น ๆ ก่อนการติดตั้งจริง (Deployment) ทั้งนี้ควรเป็นสภาพแวดล้อมที่ใกล้เคียงกับ Production มากที่สุด
- 3) Production Environment คือ สภาพแวดล้อมจริงที่มีการติดตั้งระบบสารสนเทศหรือซอฟต์แวร์ เพื่อใช้งาน

ทั้งนี้การแบ่งแยกสภาพแวดล้อมควรเป็นไปในลักษณะของระบบเครือข่าย (Network) เครื่องคอมพิวเตอร์แม่ข่าย (Server and System) และพื้นที่เชิงกายภาพ (Area/Room) การกำหนดสภาพแวดล้อมในเครื่องคอมพิวเตอร์แม่ข่ายเดียวกัน (เช่น การใช้งาน Virtualized Machine) ต้องมั่นใจว่าการ



ทดสอบที่ล้มเหลวจะไม่ส่งผลกระทบต่อเครื่องคอมพิวเตอร์แม่ข่ายในระดับกายภาพ (Physical Machine Failure) ห้ามมิให้มีการทดสอบใด ๆ เกิดขึ้นบนสภาพแวดล้อม Production หรือเครื่องคอมพิวเตอร์แม่ข่ายของระบบงานใน Production โดยอ้างอิงตามหัวข้อการแบ่งหน้าที่ในการปฏิบัติงานและการจัดทำเอกสารประกอบการปฏิบัติงาน ของการจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and Operations Management) ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)

2.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment)

เป็นขั้นตอนที่นำระบบสารสนเทศหรือซอฟต์แวร์ที่ผ่านการพัฒนาและทดสอบเรียบร้อยแล้วมาติดตั้งในสภาพแวดล้อม Production เพื่อให้สามารถใช้งานได้จริง ขั้นตอนการติดตั้งนี้จะต้องมีการวางแผนอย่างรอบคอบ และมีการเตรียมการเพื่อให้มั่นใจว่าการติดตั้งจะเป็นไปอย่างราบรื่นและไม่ส่งผลกระทบต่อการทำงานขององค์กร อ้างอิงตามหัวข้อนโยบายการบริหารจัดการนำระบบขึ้นใช้งาน (Release & Deployment Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual) และกระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure)

2.7 การบำรุงรักษา (Maintenance)

เป็นขั้นตอนหลังจากที่ระบบสารสนเทศหรือซอฟต์แวร์ถูกติดตั้งใช้งานจริงในสภาพแวดล้อม Production ซึ่งเป็นขั้นตอนในการดูแลและปรับปรุงอย่างต่อเนื่อง เพื่อให้แน่ใจว่าระบบสารสนเทศหรือซอฟต์แวร์สามารถทำงานอย่างถูกต้องโดยไม่มีข้อผิดพลาด และเหมาะสมสอดคล้องกับความต้องการที่เปลี่ยนแปลงของผู้ใช้และองค์กร รวมถึงการป้องกัน Source Code จากภัยคุกคาม นอกจากนี้ การบำรุงรักษา (Maintenance) ยังครอบคลุมถึงการปรับปรุงด้านความมั่นคงปลอดภัย การเพิ่มฟังก์ชันใหม่ และการพัฒนาระบบให้เหมาะสมกับเทคโนโลยีล่าสุดด้วยเช่นกัน โดยขั้นตอนนี้จะต้องดำเนินการอย่างสม่ำเสมอ เพื่อคงคุณภาพกับความน่าเชื่อถือและความมั่นคงปลอดภัยของระบบสารสนเทศและซอฟต์แวร์ในระยะยาว

3. ขั้นตอนการพัฒนากระบวนการสารสนเทศและซอฟต์แวร์

3.1 การวางแผนโครงการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Project Planning)

ก่อนการดำเนินโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ ต้องกำหนดให้มีการจัดทำแผนงานโครงการอย่างละเอียด โดยใช้มาตรฐานของสมาคมฯ หรือของผู้ให้บริการนั้น ๆ ทั้งนี้ ต้องมีเนื้อหาและรายละเอียดอย่างเป็นลายลักษณ์อักษรตามรายการ ดังต่อไปนี้ โดยอ้างอิงแนวทางที่ใช้ในการดำเนินงานโครงการด้านความมั่นคงปลอดภัยสารสนเทศตามหัวข้อ การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ ในเอกสารนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)

- การกำหนดขอบเขต วัตถุประสงค์ และรายละเอียดภาพรวมของโครงการ
- การระบุแนวทาง และกลยุทธ์ที่ใช้ในการพัฒนา



- การระบุผู้รับผิดชอบโครงการ และสมาชิกในโครงการ
- การระบุความเสี่ยงของโครงการ และแนวทางการรับมือ โดยครอบคลุมความเสี่ยงเชิงธุรกิจและเชิงเทคนิค
- การกำหนดกิจกรรม ระยะเวลา และต้นทุนของโครงการ
- ช่องทางและรูปแบบการรายงานความคืบหน้าของโครงการ
- กระบวนการในการควบคุม Configuration Item ในโครงการ เช่น เอกสาร, Package ของซอฟต์แวร์, องค์ประกอบของซอฟต์แวร์ (Software Component) โดยอ้างอิงแนวทางตามหัวข้อการบริหารจัดการ Configuration ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) และอ้างอิงขั้นตอนปฏิบัติการบริหารจัดการองค์ประกอบของบริการด้านเทคโนโลยีสารสนเทศ ในเอกสารกระบวนการจัดองค์ประกอบ (Configuration Management Procedure)
- เอกสารที่จะถูกผลิตขึ้นระหว่างการดำเนินโครงการ ทั้งเอกสารส่งมอบและเอกสารที่ใช้อ้างอิงระหว่างการดำเนินโครงการ
- เอกสารใด ๆ ที่มีรายละเอียดค้างต้น ต้องได้รับการอนุมัติและตรวจสอบโดยพนักงานของสมาคมฯ ตามการแต่งตั้งและบทบาทหน้าที่ความรับผิดชอบ

3.2 การบริหารจัดการความต้องการในการพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Requirement Management)

ในการดำเนินโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ ต้องมีเอกสารระบุความต้องการของระบบสารสนเทศหรือซอฟต์แวร์ โดยมีการเก็บข้อมูลจากผู้ใช้งานและผู้ที่เกี่ยวข้อง โดยครอบคลุมรายการ ดังต่อไปนี้

- ความต้องการของระบบสารสนเทศหรือซอฟต์แวร์ (Functional Requirement)
- ความต้องการด้านคุณลักษณะของระบบสารสนเทศหรือซอฟต์แวร์ (Non-functional Requirement) ซึ่งครอบคลุมรายการ ดังต่อไปนี้
 1. ความต้องการด้านความมั่นคงปลอดภัย (Security Requirement) สามารถพิจารณาทั้งระบบหรือจำแนกตามแต่ละ Module ของระบบสารสนเทศหรือซอฟต์แวร์ โดยควรพิจารณาอย่างน้อยดังต่อไปนี้
 - 1) ระดับความมั่นคงปลอดภัยของสารสนเทศ และระบบสารสนเทศ
 - 2) เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยในอดีต
 - 3) ขอบเขตสำหรับการเชื่อมต่อระบบสารสนเทศ
 - 4) ผลกระทบที่อาจเกิดขึ้นกับระบบสารสนเทศอื่น ๆ และภาพรวมของระดับความมั่นคงปลอดภัยสารสนเทศของสมาคมฯ
 - 5) คุณสมบัติด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย



- การควบคุมการเข้าถึง (Access Control) ประกอบด้วย การระบุและพิสูจน์ตัวตน (Identification and Authentication) การกำหนดสิทธิการเข้าถึง (Authorization) และการจัดการหลักฐานการตรวจสอบและการรับผิดชอบต่อการกระทำ (Auditing and Accountability)
- การควบคุมการประมวลผลสารสนเทศในแอปพลิเคชัน (Correct Processing in Applications) ประกอบด้วย การตรวจสอบข้อมูลนำเข้า (Input Data Validation) การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing) การตรวจสอบความถูกต้องของข้อความ (Message Integrity) และการตรวจสอบข้อมูลนำออก (Output Data Validation)
- การป้องกันข้อมูล (Data Protection) ประกอบด้วย การเข้ารหัสข้อมูลที่จัดเก็บ และการเข้ารหัสข้อมูลขณะส่ง
- การสำรองและการกู้คืนระบบ

2. ความต้องการด้านสมรรถนะและประสิทธิภาพ (Performance Requirement) สามารถพิจารณาทั้งระบบหรือจำแนกแต่ละ Module ของระบบสารสนเทศหรือซอฟต์แวร์
3. ความต้องการด้านข้อกำหนด เพื่อสร้างความสอดคล้องกับข้อกำหนด นโยบาย หรือกฎหมาย ที่เกี่ยวข้องกับระบบสารสนเทศหรือซอฟต์แวร์ โดยอ้างอิงกฎหมายและข้อกำหนดที่ต้องปฏิบัติตาม ในเอกสาร รายการกฎหมายและข้อบังคับที่ต้องปฏิบัติตาม (List of Law and Regulatory)

- เอกสารสรุปความต้องการในรายการข้างต้น ต้องดำเนินการเป็นลายลักษณ์อักษรและต้องได้รับการอนุมัติและตรวจสอบโดยพนักงานของสมาคมฯ ตามการแต่งตั้งและบทบาทหน้าที่ความรับผิดชอบ
- เอกสารดังกล่าว ต้องได้รับการตรวจสอบและอนุมัติโดย Project Manager และมีการควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ
- การเปลี่ยนแปลงความต้องการ (Requirement Change Management) หรือคุณลักษณะใด ๆ ของระบบสารสนเทศหรือซอฟต์แวร์ ให้ดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) และชี้แจง Project Manager ตามความเหมาะสม

3.3 การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Design and Analysis)

กำหนดให้มีเอกสารใด ๆ ที่ระบุถึงการออกแบบและวิเคราะห์ระบบสารสนเทศหรือซอฟต์แวร์ ดังต่อไปนี้

- การแสดงถึงการวิเคราะห์ความต้องการของหน่วยงาน และองค์ประกอบ (Module) ของระบบสารสนเทศหรือซอฟต์แวร์ เช่น Business Flowchart
- การวิเคราะห์ถึงความสัมพันธ์ระหว่างผู้ใช้งาน และระบบสารสนเทศหรือซอฟต์แวร์ เช่น Use-case Diagram, Conceptual Diagram



- การวิเคราะห์ถึงข้อมูลเข้า/ออก ระหว่างองค์ประกอบของระบบสารสนเทศหรือซอฟต์แวร์ และการแบ่ง Data Storage เช่น API design, Database design (สามารถพิจารณาได้หลายระดับชั้น)
- การวิเคราะห์ความต้องการเชิงเทคนิค (Technical Requirement) และการรองรับ (Compatibility) ของระบบสารสนเทศหรือซอฟต์แวร์ รวมถึงองค์ประกอบย่อยของระบบสารสนเทศหรือซอฟต์แวร์ เช่น Product Requirement, Software Specification

เอกสารดังกล่าว ต้องได้รับการตรวจสอบและอนุมัติโดย Project Manager และควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ

การออกแบบและวิเคราะห์ระบบสารสนเทศและซอฟต์แวร์ (Secure Engineering Principal) ต้องคำนึงถึงหลักวิศวกรรมด้านความมั่นคงปลอดภัยสารสนเทศ โดยมุ่งเน้นการออกแบบเพื่อรองรับการป้องกันคุณสมบัติของข้อมูลสารสนเทศ ได้แก่ ความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) โดยมีแนวทางการพิจารณา ดังนี้

ตารางที่ 1 หลักวิศวกรรมระบบสารสนเทศ

คุณสมบัติ	เกณฑ์พิจารณา	การออกแบบ	
ความลับ (Confidentiality)	เปิดเผยได้ในที่สาธารณะ	การกำหนด ระดับชั้น (Classification)	ข้อมูลทั่วไป
	เปิดเผยได้เพียงบุคคลภายในกลุ่มงานที่เกี่ยวข้อง		ข้อมูลใช้ภายใน
	เปิดเผยได้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับ
	เปิดเผยได้บางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับมาก
	เปิดเผยได้เฉพาะผู้บริหารระดับสูงหรือบางกลุ่มบุคคลที่ได้รับอนุญาตเท่านั้น		ข้อมูลลับที่สุด
ความถูกต้อง (Integrity)	หากข้อมูลผิดพลาด จะไม่ส่งผลกระทบต่อระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ	ความสำคัญเชิง ข้อมูล (Significance)	ต่ำ
	หากข้อมูลผิดพลาด จะส่งผลในการทำงานผิดพลาดเพียงองค์ประกอบ (Function, Module) หนึ่งในระบบสารสนเทศหรือซอฟต์แวร์เท่านั้น		ปานกลาง
	หากข้อมูลผิดพลาด จะส่งผลในการทำงานผิดพลาดหลายองค์ประกอบ (Function, Module) ในระบบสารสนเทศหรือซอฟต์แวร์เท่านั้น		สูง



คุณสมบัติ	เกณฑ์พิจารณา	การออกแบบ	
	หากข้อมูลผิดพลาด จะส่งผลทำให้ระบบสารสนเทศหรือซอฟต์แวร์ล้มเหลวและหยุดชะงัก		สูงมาก
ความพร้อมใช้ (Availability)	หากขาดข้อมูลดังกล่าว จะไม่ส่งผลกระทบต่อระบบสารสนเทศหรือซอฟต์แวร์ใด ๆ	ความสำคัญเชิงข้อมูล (Significance)	ต่ำ
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) หนึ่งในระบบสารสนเทศหรือซอฟต์แวร์หยุดการทำงาน		ปานกลาง
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) มากกว่าหนึ่งองค์ประกอบในระบบสารสนเทศหรือซอฟต์แวร์หยุดการทำงาน		สูง
	หากขาดข้อมูลดังกล่าว จะส่งผลให้องค์ประกอบ (Function, Module) ระบบสารสนเทศทั้งหมดหรือซอฟต์แวร์หยุดการทำงาน		สูงมาก

3.4 การพัฒนาระบบสารสนเทศและซอฟต์แวร์ (Development)

ก่อนการพัฒนาระบบหรือซอฟต์แวร์ ให้มีการดำเนินการกำหนดมาตรฐานในการพัฒนา (Coding Standard) ที่มีเนื้อหาครอบคลุมอย่างน้อยดังนี้ โดยอ้างอิงนโยบายการจัดการ การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual)

- การกำหนดวิธีการตั้งชื่อระหว่างการพัฒนา เช่น การตั้งชื่อตัวแปร, การตั้งชื่อ Package เป็นต้น
- การกำหนดวิธีการสร้างข้อความ Comment
- การกำหนดรูปแบบ (Theme) การแสดงผล (Display) ของระบบสารสนเทศหรือซอฟต์แวร์
- การกำหนดอัลกอริทึม (Algorithm) ที่สามารถนำมาใช้ในการพัฒนา เช่น มาตรฐานการเข้ารหัส, มาตรฐานในการดึงข้อมูลจากฐานข้อมูล
- การกำหนดวิธีการเรียกใช้งานชุดคำสั่งระหว่างองค์ประกอบย่อยของระบบสารสนเทศหรือซอฟต์แวร์ (Function Call)
- การกำหนดชนิดของข้อมูล (Data Type)



- การสร้างชุดคำสั่งต้นแบบและคุณสมบัติการสืบทอด (Inheritance)
- การกำหนดรูปแบบและประเภทของ Log
- กำหนดให้การจัดเก็บ Source Code ของระบบสารสนเทศหรือซอฟต์แวร์ผ่านเครื่องมือควบคุมที่ได้มาตรฐาน โดยมีผู้ที่ได้รับมอบหมายในการบริหารจัดการ

3.5 การทดสอบระบบสารสนเทศและซอฟต์แวร์ (Testing)

กำหนดให้ทุก ๆ ความต้องการ (Requirement) ต้องได้รับการทดสอบ โดยสามารถแบ่งออกได้เป็น 2 ลักษณะ ดังนี้

3.5.1 การทดสอบและตรวจสอบโดยผู้พัฒนา (Verification)

การทดสอบและตรวจสอบโดยผู้พัฒนา มีวัตถุประสงค์เพื่อตรวจสอบความพร้อม ความถูกต้องของระบบสารสนเทศหรือซอฟต์แวร์ เพื่อให้มั่นใจว่าตรงตามความต้องการ โดยประกอบด้วย

- การทดสอบเบื้องต้น (Unit Test)
- การทดสอบการทำงานผสานระหว่างระบบ (System Integration Test)
- การทดสอบความมั่นคงปลอดภัยของระบบ (Security Test) โดยควรครอบคลุมถึง
 - การทดสอบการเข้าถึงข้อมูลและระบบงาน
 - การเข้ารหัสข้อมูล และการปกป้องข้อมูล
 - การตั้งค่าด้านความมั่นคงปลอดภัย เช่น การตั้งค่ารหัสผ่าน การตั้งค่าเวลามาตรฐาน การตั้งค่าการเชื่อมต่อ การจัดเก็บบันทึกเหตุการณ์ (Log) เป็นต้น
 - การทดสอบความมั่นคงปลอดภัยทางเทคนิค ได้แก่ การวิเคราะห์ซอร์สโค้ด (Source Code Analysis) การประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing)

3.5.2 การทดสอบและตรวจสอบโดยผู้ใช้งานในสภาพแวดล้อมจริง (Validation)

เพื่อให้มั่นใจว่าระบบสารสนเทศหรือซอฟต์แวร์ สามารถถูกนำมาใช้ได้จริงในสภาพแวดล้อมจริง และได้รับการยอมรับจากผู้ใช้งาน จำเป็นต้องมีการทดสอบโดยตัวแทนฝ่ายผู้ใช้งาน (User) สามารถแบ่งได้เป็น

- การทดสอบการยอมรับระบบสารสนเทศหรือซอฟต์แวร์ (User Acceptance Test)
 - การทดสอบความพร้อมก่อนการติดตั้งระบบเพื่อใช้งานจริง (Operation Readiness Test)
- กำหนดให้ชุดข้อมูลทดสอบ ต้องเป็นข้อมูลจำลองเท่านั้น ในกรณีมีความจำเป็นต้องใช้ข้อมูลจริงที่มีชั้นความลับหรือเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้มีการดำเนินการขออนุมัติอย่างเป็นทางการเป็นลายลักษณ์อักษร และจะต้องลบข้อมูลทดสอบทั้งหมดออกจากระบบเมื่อเสร็จสิ้นการทดสอบ



กำหนดเอกสารควบคุมการทดสอบระบบสารสนเทศหรือซอฟต์แวร์ ที่ได้รับการตรวจสอบและอนุมัติโดย Project Manager และควบคุมตามกระบวนการควบคุมเอกสารของโครงการนั้น ๆ และสามารถส่งให้แก่สมาคมฯ เมื่อมีการร้องขอ โดยมีรายละเอียดครอบคลุม ดังนี้

- ชนิดและประเภทของการทดสอบและรายละเอียดเบื้องต้น เช่น วันที่ทดสอบ ผู้ดำเนินการ
- การกำหนดวิธีการและเกณฑ์การทดสอบ เช่น Key Stopper, Testing Methodology
- การกำหนดขั้นตอนการทดสอบและผลลัพธ์ที่คาดหวัง
- การกำหนดเกณฑ์การพิจารณาผลการทดสอบ เช่น ชนิดของผลการทดสอบ (Defect Type)

3.5.3 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of System Test Data)

เพื่อให้มั่นใจว่าข้อมูลที่นำมาทดสอบได้รับการควบคุมและป้องกันอย่างเหมาะสม ผู้พัฒนาและเจ้าของระบบ ควรควบคุมการใช้ข้อมูลสำหรับทดสอบดังนี้

- กำหนดให้มีการควบคุมการเข้าถึงข้อมูลที่ใช้ในการทดสอบเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ควบคุมมิให้นำข้อมูลที่ใช้ในระบบที่ให้บริการจริงไปใช้สำหรับทำการทดสอบระบบ ทั้งนี้ หากมีความจำเป็นต้องใช้ ต้องจัดให้มีการควบคุมอย่างน้อยดังต่อไปนี้
 - ได้รับอนุญาตจากเจ้าของระบบก่อนนำไปใช้ในการทดสอบ
 - ปรับ หรือลบข้อมูลที่มีระดับความลับ “ลับมาก” หรือ “ลับที่สุด”
 - ลบข้อมูลที่ใช้ในการทดสอบภายหลังการทดสอบเสร็จสิ้น
 - มีการบันทึกเหตุการณ์ของการสำเนาข้อมูลจากระบบที่ให้บริการจริงเพื่อใช้ในการทดสอบ

3.6 การติดตั้งระบบสารสนเทศและซอฟต์แวร์ (Deployment)

ต้องได้รับความเห็นชอบและอนุมัติผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) ตามหัวข้อนโยบายการบริหารจัดการนำระบบขึ้นใช้งาน (Release & Deployment Policy) ในนโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual) และกระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure) อย่างเคร่งครัด

3.7 การปิดโครงการหรือเสร็จสิ้นการพัฒนาโครงการ (Project Closure)

กำหนดพนักงานผู้รับผิดชอบที่ได้รับมอบหมายจากสมาคมฯ ดำเนินการสรุปผลการดำเนินงานทั้งหมด โดยมีเนื้อหาครอบคลุม

- ปัญหาและอุปสรรคที่เกิดขึ้นในโครงการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ การแก้ไขปัญหาหรือองค์ความรู้ใหม่



- ในกรณีที่เป็นการจัดจ้างผู้ให้บริการภายนอก ให้มีการประเมินศักยภาพของผู้ให้บริการภายนอกภายนอกนั้น ๆ
- ข้อมูลอื่น ๆ ตามที่มีร้องขอ

4. การจัดจ้างผู้ให้บริการภายนอก เพื่อการพัฒนากระบวนการสารสนเทศหรือซอฟต์แวร์ (Outsourcing Development)

กำหนดให้ผู้ให้บริการภายนอกใด ๆ ที่ได้รับการจัดจ้างให้พัฒนากระบวนการสารสนเทศหรือซอฟต์แวร์ให้แก่สมาคมฯ ต้องดำเนินการให้สอดคล้องและปฏิบัติตามนโยบายของสมาคมฯ อย่างเคร่งครัด โดยอ้างอิงหัวข้อนโยบายการบริหารจัดการผู้ให้บริการ ตามเอกสารกระบวนการบริหารจัดการผู้ให้บริการ (Supplier Management Procedure) ทั้งนี้ ผู้ให้บริการภายนอกจะต้องเป็นผู้เชี่ยวชาญเฉพาะด้าน และในระหว่างการดำเนินโครงการ บุคลากรที่เกี่ยวข้องและเข้าถึงข้อมูลของสมาคมฯ ต้องมีการลงนามข้อตกลงว่าด้วยการรักษาความลับขององค์กร (Mutual Confidentiality Agreement) ที่มีผลทางกฎหมายแม้สิ้นสุดโครงการ

เพื่อให้การตรวจสอบการพัฒนากระบวนการสารสนเทศหรือซอฟต์แวร์โดยการจ้างผู้ให้บริการภายนอกนั้นเป็นระบบหรือซอฟต์แวร์ที่มีมั่นคงปลอดภัย และมีการพัฒนาที่เป็นไปตามความต้องการขององค์กร ควรกำหนดเกณฑ์ดังต่อไปนี้สำหรับการพิจารณาตรวจสอบระบบสารสนเทศหรือซอฟต์แวร์

- ต้องมีการกำหนดข้อตกลงการให้สิทธิ์ใช้งาน การเป็นเจ้าของ Code และสิทธิ์ในทรัพย์สินทางปัญญาที่เกี่ยวข้องกับเนื้อหาที่จ้างพัฒนา โดยอ้างอิงตามหัวข้อกรรมสิทธิ์ในข้อมูล ในนโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)
- ต้องมีข้อกำหนดหรือสัญญาสำหรับการออกแบบ การเขียนโค้ด และแนวทางการทดสอบที่มีมั่นคงปลอดภัย
- ต้องมีการทดสอบสิ่งส่งมอบก่อนยอมรับ เพื่อประเมินคุณภาพและความถูกต้องของสิ่งที่ส่งมอบ
- ต้องมีหลักฐานแสดงว่ามีการกำหนดระดับความสามารถด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวขั้นต่ำที่สามารถยอมรับได้
- ต้องมีหลักฐานแสดงว่ามีการทดสอบอย่างเพียงพอ เพื่อป้องกันช่องโหว่ที่ทราบ
- ต้องมีหลักฐานแสดงว่าการดำเนินการพัฒนาเป็นไปตาม Requirement ที่ทางสมาคมฯ ได้กำหนดไว้

5. เอกสารที่เกี่ยวข้อง (Related Documents)

- ISO-1PC-02 ขอบเขตระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS and ISMS Scope)
- ISO-1PC-01 นโยบายและคู่มือระบบบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ และระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ITSMS & ISMS Policy and Manual)
- IT-1PC-01 นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)



- IT-2PR-02 กระบวนการจัดการการสร้างและการติดตั้งระบบสารสนเทศ (Release and Deployment Management Procedure)
- RMEM-2PR-02 กระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure)
- IT-2PR-03 กระบวนการจัดองค์ประกอบ (Configuration Management Procedure)
- PU-2PR-01 กระบวนการบริหารจัดการผู้ให้บริการ (Supplier Management Procedure)
- ISO-2SD-01 รายการกฎหมายและข้อบังคับที่ต้องปฏิบัติตาม (List of Law and Regulatory)



สมาคมสโมสรนักลงทุน
Investor Club Association

นโยบายและการบริหารเทคโนโลยีสารสนเทศ
(IT Policy and Management)

รหัสเอกสาร:	IT-1PC-01
หมายเลขปรับปรุงเอกสาร:	6.0
วันที่เอกสารมีผลบังคับใช้:	3 ธันวาคม 2567
เจ้าของเอกสาร:	ฝ่ายเทคโนโลยีสารสนเทศ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ-นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
ผู้จัดทำ	สมโภช เพ็ญจันทิก	หัวหน้าแผนก บริหารระบบ		29 พฤศจิกายน 2567
ผู้ทบทวน	สิริวรรณ ฉลากรไชยา	หัวหน้าฝ่าย เทคโนโลยีสารสนเทศ		29 พฤศจิกายน 2567
ผู้อนุมัติ	กรองนก มานะกิจจงกล	ผู้จัดการ สมาคมสโมสรนักลงทุน		2 ธันวาคม 2567

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุง เอกสาร (version):	วันที่ปรับปรุง เอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
2.0	4 พ.ค. 64	สิริวรรณ ฉลากรไชยา	แก้ไขเนื้อหาให้มีความชัดเจนยิ่งขึ้น 1. การรักษาความปลอดภัย - แนวทาง 2. การใช้อินเทอร์เน็ต 3. การใช้อุปกรณ์คอมพิวเตอร์ - แนวทาง 4. การใช้คอมพิวเตอร์แบบพกพาและการ เชื่อมต่อระบบเครือข่าย 5.แก้ไข ผู้ให้ข้อมูล เป็น ผู้เปิดเผยข้อมูลให้ ถูกต้องตามคำจำกัดความ
3.0	26 ก.ค. 66	สิริวรรณ ฉลากรไชยา	เพิ่มเติมเนื้อหา 1.การจัดกลุ่มทรัพย์สิน (Asset Grouping) 2.การใช้งานคอมพิวเตอร์แบบพกพาในการ ปฏิบัติงานจากภายนอกและการแก้ไขปัญหา จากระยะทางไกล
4.0	20 พ.ย. 66	สิริวรรณ ฉลากรไชยา	เพิ่มเติมเนื้อหา เอกสารแนบ 2 ข้อ 3 ข้อตกลง ทั่วไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			เพิ่มข้อ 3.5 ผู้รับข้อมูลจะต้องดำเนินการลบข้อมูลที่เป็นข้อมูล Sensitive ภายในระยะเวลา 3 เดือนหลังจากสิ้นสุดระยะเวลาการดำเนินงานของโครงการและรายงานกลับเพื่อให้ทราบว่าดำเนินการแล้วตามมาตรฐาน
5.0	25 เม.ย. 67	สิริวรรณ ฉลากรไชยา	1.นโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy) 1.1 <u>แก้ไขข้อความ</u> ● ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ <u>เป็น</u> ● ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ และต้องมีการกำหนดสิทธิ์ผู้ใช้งานในระดับสูง 1.2 <u>เพิ่มข้อความ</u> ● ในการเข้าใช้งานของผู้ใช้งานในระดับสูง จะต้องมีการร้องขอใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงในแต่ละครั้ง ● พนักงานที่มีความประสงค์ร้องขอเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Account) ต้องจัดทำแบบฟอร์มร้องขอบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Request Form) (IT-2FM-07) ● ผู้ดูแลระบบบันทึกทะเบียนบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privileged Account Inventory) (IT-2FM-09) สำหรับใช้ในการอ้างอิง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			2. สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน 2.1 <u>แก้ไขข้อความ</u> - รายชื่อผู้ใช้งานจะถูกตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานออก <u>เป็น</u> - รายชื่อผู้ใช้งานจะถูกตั้งค่าปิดการใช้งานบัญชีล่วงหน้าและตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานลาออก <u>เพิ่มข้อความ</u> - ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการตรวจสอบวันที่เข้าสู่ระบบล่าสุดของพนักงานที่ลาออก (Check Last Logon Date) ในกรณีที่มีการแจ้งลาออกล่าช้าหรือมีการเลิกจ้างฐานละทิ้งหน้าที่ โดยระบุในส่วนรายละเอียด

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			เพิ่มเติมของแบบฟอร์มการเพิกถอนสิทธิ์ใช้งานบัญชีผู้ใช้ พร้อมบันทึกหลักฐานการตรวจสอบ ฝ่ายเทคโนโลยีสารสนเทศกำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที
6.0	29 พ.ย. 67	สมโภช เผือกจันทิก	- แก้ไขข้อมูล “ศูนย์ข้อมูล” เป็น “ห้องเซิร์ฟเวอร์” - การลงทะเบียนทรัพย์สิน <u>เพิ่มเติม</u> ประเภทของทรัพย์สิน 2 รายการ ได้แก่ Process Asset และ Site Asset - สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน <u>เพิ่มเติม</u> ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของสมาคม ฯ ได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง <u>เพิ่มเติม</u>ข้อความ การแบ่งแยกระบบสารสนเทศ เพื่อลดความผิดพลาดหรือผลกระทบอันเกิดจากการดำเนินการทดสอบ ควรมีการแยกระบบสารสนเทศที่ให้บริการจริง ออกจากระบบสารสนเทศที่ใช้ในการพัฒนา และทดสอบ (เฉพาะระบบที่สามารถดำเนินการได้) <u>เพิ่ม</u> การจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			Operations Management) ในหน้าที่ความรับผิดชอบของผู้ใช้ในหัวข้อ ดังนี้ ● ข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์ หรือส่งออกไปภายนอกองค์กรต้องจัดให้มีการเข้ารหัสข้อมูล ● การจัดทำ การจัดเก็บ การส่งต่อ ลบ ทำลายข้อมูล จะต้องดำเนินการตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล ● ต้องควบคุมให้มีมาตรการการปิดบังข้อมูลสารสนเทศเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน 6. แนวทางการเข้าสู่ห้องเซิร์ฟเวอร์ <u>เพิ่มเติม</u> ข้อความ ดังนี้ 6.1 จะต้องกรอกแบบคำขออนุญาตเข้าพื้นที่ห้องเซิร์ฟเวอร์ 6.2 ห้ามนำวัตถุระเบิด เชื้อเพลิง วัสดุติดเพลิงง่าย อาวุธ สารเคมี หรือสิ่งอื่นใดที่อาจก่อให้เกิดความเสียหายทั้งต่อชีวิตและทรัพย์สิน เข้ามาบริเวณห้องเซิร์ฟเวอร์ 7. <u>เพิ่มข้อความ</u> ในหัวข้อการควบคุมการใช้งานระบบเครือข่าย ดังนี้ ● ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของสมาคม ฯ ให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับอาทิพระราชบัญญัติว่าด้วยการกระทำ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หมายเลขปรับปรุงเอกสาร (version):	วันที่ปรับปรุงเอกสาร	ปรับปรุงโดย (ชื่อ-สกุล)	คำอธิบายและเหตุผลในการแก้ไข
			ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับ (ฉบับที่ 2) พ.ศ. 2560 8. <u>เพิ่มข้อความ</u> ในหัวข้อการใช้คอมพิวเตอร์แบบพกพาและการเชื่อมต่อระบบเครือข่าย ดังนี้ ● การทำลายสื่อบันทึกข้อมูล โดยผู้ให้บริการภายนอก จะต้องมีการทำสัญญาข้อตกลงเรื่องการรักษาความลับ 9. <u>เพิ่มข้อความ</u> ในหัวข้อการสำรองข้อมูล ดังนี้ ● สำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลง โดยข้อมูลสำรองนี้จะถูกจัดเก็บไว้ในที่ปลอดภัย ● ทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง 10. เพิ่มหัวข้อการจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ 11. เพิ่มหัวข้อการบริหารจัดการ Configuration 12. เพิ่มหัวข้อการบริหารจัดการคลาวด์

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

สารบัญ

เรื่อง	หน้า
บทนำ	9
ระเบียบว่าด้วยขอบเขตอำนาจหน้าที่และความรับผิดชอบ	10
นโยบายระบบเทคโนโลยีสารสนเทศ	11
คณะกรรมการสารสนเทศสมาคมสโมสรนักลงทุน	13
ฝ่ายเทคโนโลยีสารสนเทศ	14
ความปลอดภัยของอุปกรณ์ และข้อมูล	16
การรักษาความปลอดภัย	25
การเข้าสู่ห้องเซิร์ฟเวอร์	31
กรรมสิทธิ์ในข้อมูล	33
การใช้อินเทอร์เน็ต	34
การใช้จดหมายอิเล็กทรอนิกส์ หรืออีเมล	36
ลิขสิทธิ์โปรแกรม และการสั่งซื้อ หรือการเช่าใช้	40
อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์	42
การแจ้งให้ทราบเรื่องการระงับให้บริการชั่วคราว	44
การใช้อุปกรณ์คอมพิวเตอร์	45
การกู้คืนข้อมูล และระบบคอมพิวเตอร์ที่ได้รับความเสียหาย	49
การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ	51
การบริหารจัดการ Configuration	52
การบริหารจัดการคลาวด์	53
เอกสารแนบ 1	54
เอกสารแนบ 2	55

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

บทนำ

นโยบายเทคโนโลยีสารสนเทศที่จัดทำขึ้นครอบคลุมระบบการปฏิบัติงานคอมพิวเตอร์ ระบบโทรศัพท์ รวมถึงอุปกรณ์ต่าง ๆ ในระบบเครือข่ายคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน เพื่อให้บริการพนักงานและบริษัทภายนอก โดยคำนึงถึงความรับผิดชอบต่อด้านกฎหมาย และได้รับความไว้วางใจจากภาคธุรกิจหลากหลายประเภท

เอกสารฉบับนี้จะกล่าวถึงนโยบายระบบเทคโนโลยีสารสนเทศขององค์กร หน้าที่ความรับผิดชอบของผู้ใช้ระบบคอมพิวเตอร์ และฝ่ายเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อวางแผนนโยบายระบบเทคโนโลยีสารสนเทศให้กับสมาคมสโมสรนักลงทุน และเพื่อให้ฝ่ายต่าง ๆ รวมทั้งหน่วยงานที่เกี่ยวข้องได้ทราบถึงแนวทางการดำเนินงานของพนักงานฝ่ายเทคโนโลยีสารสนเทศและพนักงานสมาคมสโมสรนักลงทุน

ขอบเขตและความรับผิดชอบ

การบริหารการใช้ข้อมูลระบบสารสนเทศภายในองค์กรเป็นความรับผิดชอบหลักของแต่ละฝ่ายในสมาคม ฯ อย่างไรก็ตาม ฝ่ายเทคโนโลยีสารสนเทศยังคงมีอำนาจหน้าที่ควบคุมดูแลระบบสารสนเทศของฝ่ายต่าง ๆ ในองค์กรโดยรวม

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบงานด้านการบริหารจัดการนโยบายในระบบเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน ทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้มีอำนาจหน้าที่ในการตรวจสอบ มอบหมาย และประสานงานในการปฏิบัติงานด้านต่าง ๆ ในระบบเทคโนโลยีสารสนเทศของทั้งองค์กร

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ระเบียบว่าด้วยขอบเขตอำนาจหน้าที่และความรับผิดชอบ

สมาคมสโมสรนักลงทุนมีความต้องการให้อุปกรณ์และการใช้งานในระบบเทคโนโลยีสารสนเทศขององค์กรคงสภาพดี และพร้อมใช้งานในเครื่องขององค์กร เป้าหมายนี้ถือเป็นภารกิจของฝ่ายเทคโนโลยีสารสนเทศ และเพื่อให้การดำเนินงานตามเป้าหมายลุล่วง จึงได้วางระเบียบที่จะสนับสนุนภารกิจดังกล่าวไว้ดังนี้

ฝ่ายเทคโนโลยีสารสนเทศ มีรายละเอียดภารกิจดังนี้

1. ดูแล วางแผน แก้ไข และปรับปรุงระบบคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง เพื่อให้การใช้งานอยู่ในสภาพดีและมีประสิทธิภาพในการทำงานสูงสุด
2. จัดหา แก้ไข จัดเก็บ ประมวลผล เรียกใช้ นำเสนอ และเผยแพร่โปรแกรมหรือข้อมูลอิเล็กทรอนิกส์ให้กับพนักงานทุกระดับในองค์กร
3. สร้างความกลมกลืนในระบบเทคโนโลยีสารสนเทศเพื่อเอื้อประโยชน์ต่อการดำเนินธุรกิจในแต่ละวันขององค์กร

ภารกิจที่กำหนดขึ้นนี้จะต้องสนับสนุน ส่งเสริม และกลมกลืนเป็นหนึ่งเดียวกับแผนงาน ขั้นตอนการปฏิบัติงาน และวัตถุประสงค์ที่กำหนดขึ้นโดยผู้บริหารระดับสูง

เป็นที่ทราบทั่วกันว่า บทบาทของฝ่ายเทคโนโลยีสารสนเทศในองค์กรนั้นแตกต่างจากหน่วยงานอื่น ๆ ตรงที่นอกเหนือจากผลงานโดยตรงที่เกิดขึ้นภายในฝ่ายเอง เช่น การซ่อมแซมและดูแลรักษาอุปกรณ์คอมพิวเตอร์แล้ว ผลงานของฝ่ายเทคโนโลยีสารสนเทศยังประกอบด้วยผลงานอันเกิดจากความร่วมมือกับฝ่ายอื่น ๆ โดยไม่สามารถแยกเป็นผลสำเร็จที่เป็นเฉพาะของตนเองได้ หากแต่ว่าภารกิจของฝ่ายเทคโนโลยีสารสนเทศจะบรรลุไปด้วยความความร่วมมือ และการใช้บริการจากฝ่ายธุรกิจอื่น ๆ ขององค์กร มาตรฐานความสำเร็จของฝ่ายเทคโนโลยีสารสนเทศจึงมาจากทั้งผลการปฏิบัติงานภายในฝ่ายและความสำเร็จในการเพิ่มมูลค่าให้กับธุรกิจขององค์กรด้วยการนำเสนอระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและได้ประสิทธิผล

อีกหนึ่งบทบาทของฝ่ายเทคโนโลยีสารสนเทศเพื่อสนับสนุนเป้าหมายดังกล่าวข้างต้น คือ การมีส่วนร่วมในการให้คำแนะนำสำหรับการจัดทำงบประมาณเพื่อลงทุนในระบบเทคโนโลยีสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศจะทำการประเมินถึงผลกระทบในทางเทคนิค การบริหารจัดการ การให้บริการ และการเงินของเทคโนโลยีสารสนเทศที่จะมีต่อการดำเนินธุรกิจขององค์กรอย่างเหมาะสม ทันท่วงทีสถานการณ์ และด้วยความถูกต้อง

ในหน่วยงานที่ฝ่ายเทคโนโลยีสารสนเทศเข้าไปให้บริการ ฝ่ายเทคโนโลยีสารสนเทศจะมีบทบาทในการจัดเตรียม และดูแลกำกับแผนระยะยาวให้เป็นไปตามวัตถุประสงค์ โดยแผนนี้จะรวบรวมแผนระยะสั้นและเป้าหมายที่ต้องบรรลุ นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศจะต้องจัดเตรียม เก็บรักษา และปรับปรุงมาตรฐาน และขั้นตอนในการปฏิบัติงาน เพื่อสะดวกในการใช้อ้างอิงกรณีที่มีการปรับเปลี่ยนระบบในอนาคต ในขณะเดียวกันก็ไม่ละเลยที่จะให้บริการที่ตอบสนองความต้องการเร่งด่วนที่ร้องขอมา

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

นโยบายระบบเทคโนโลยีสารสนเทศ

หลักการ

ระบบสารสนเทศ ข้อมูล ทรัพย์สินคอมพิวเตอร์ ซึ่งรวมถึงเครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ การสื่อสารด้วยข้อมูลและเสียง (ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์) เครื่องพิมพ์ และอุปกรณ์/ระบบต่อพ่วง ทั้งหมดนี้ถือเป็นทรัพย์สินของสมาคมสโมสรนักลงทุน ผู้ที่ได้รับสิทธิในการใช้ พึงใช้ด้วยความระมัดระวังเพื่อรักษาความถูกต้องของระบบคอมพิวเตอร์ และข้อมูล และเพื่อความปลอดภัยของทรัพย์สิน อนึ่งการใช้ทรัพย์สินเหล่านี้จะต้องใช้เพื่องานที่เกี่ยวข้องกับการดำเนินงานของสมาคม ฯ เท่านั้น

การสื่อสารทุกรูปแบบที่เกิดขึ้นภายในสมาคมสโมสรนักลงทุน หรือส่งออกจากสมาคมสโมสรนักลงทุน ถือเสมือนหนึ่งเป็นตัวแทนและภาพลักษณ์ขององค์กร พนักงาน คณะกรรมการบริหาร และผู้ได้รับสิทธิใช้งาน ดังนั้นจึงควรเป็นไปอย่างเหมาะสม สุภาพ และดำรงไว้ซึ่งความเป็นมืออาชีพ

การรับทราบนโยบาย

พนักงานขององค์กร และบุคคลหรือนิติบุคคลที่ได้รับว่าจ้างโดยสมาคมสโมสรนักลงทุน จะต้องอ่านทำความเข้าใจนโยบายระบบเทคโนโลยีสารสนเทศ และลงนามรับทราบในเอกสาร Acknowledgement Statement ก่อนที่จะเข้าใช้ระบบเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน (ดูตัวอย่างตามเอกสารแนบ 1)

แนวทาง

ทรัพย์สินทางด้านเทคโนโลยีสารสนเทศขององค์กร หมายถึง เครื่องมืออุปกรณ์ระบบคอมพิวเตอร์ โปรแกรมคำสั่ง ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ขนาดเล็ก (LAN) เครือข่ายคอมพิวเตอร์ขนาดกลาง (WAN) โทรศัพท์ และระบบการสื่อสารอื่น ๆ (ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์) การจัดการระบบเทคโนโลยีสารสนเทศต้องดำเนินการตามขั้นตอนการ จัดตั้งงบประมาณ และการสั่งซื้อ หาก ทรัพย์สินทางด้านเทคโนโลยีสารสนเทศใด ที่ไม่ได้มีการจัดตั้งงบประมาณไว้ ให้คณะกรรมการของสมาคมสโมสรนักลงทุน เป็นผู้ทำการอนุมัติตามอำนาจการสั่งจ่าย ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการควบคุมการใช้ทรัพยากรดังกล่าว ให้ใช้ได้อย่างมีประสิทธิภาพและคงไว้ซึ่งความปลอดภัยของข้อมูล

บทสงวนสิทธิ

ฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการติดตาม ตรวจสอบ กลั่นกรอง ปกป้องข้อมูลตามความเหมาะสม เพื่อให้สอดคล้องกับนโยบายขององค์กร การเผยแพร่ข้อมูลขององค์กรโดยพลการ การละเมิดสิทธิเข้าใช้งานระบบ และการใช้ประโยชน์จากทรัพย์สินโดยไม่ได้รับอนุญาตถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมายได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

บทลงโทษทางวินัย

การละเมิดกฎระเบียบที่กำหนดในนโยบายระบบเทคโนโลยีสารสนเทศถือว่าเป็นความผิดทางวินัย ซึ่งผู้กระทำผิดอาจถูกลงโทษโดยการตัดสิทธิต่างๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน

หลักการ

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน มีบทบาทหน้าที่ในการให้คำแนะนำ วางแผน และมีบทบาทในการอนุมัติเรื่องที่เกี่ยวข้องกับการใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศทั้งหมดเพื่อประโยชน์ในการใช้งานสูงสุดของสมาคมสโมสรนักลงทุน

ความรับผิดชอบ

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน มีอำนาจหน้าที่ในการดูแลกิจกรรมของระบบเทคโนโลยีสารสนเทศภายในองค์กร ตามคำสั่งแต่งตั้งของสมาคม ดังนี้

- กำกับ ดูแลการพัฒนาระบบดิจิทัลของสมาคม เพื่อเพิ่มประสิทธิภาพในการดำเนินงานและในการให้บริการแก่ผู้ประกอบการ ให้ระบบมีความมั่นคงและปลอดภัย
- กำกับ ดูแลระบบดิจิทัลของสมาคม ให้สอดคล้องกับนโยบาย และเชื่อมโยงกับระบบดิจิทัลของภาครัฐ ด้านส่งเสริมการลงทุนอย่างมีประสิทธิภาพ
- เสนอแนะการพัฒนาระบบดิจิทัลของสมาคม แก่คณะอนุกรรมการบริหาร และคณะกรรมการสมาคม

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน มีหน้าที่รายงาน และมีสายงานขึ้นตรงต่อคณะกรรมการสมาคมสโมสรนักลงทุน การปรับเปลี่ยนหน้าที่ และสถานะของคณะอนุกรรมการต้องได้รับอนุมัติจากประธานคณะอนุกรรมการพัฒนาระบบสารสนเทศสมาคมสโมสรนักลงทุน จะมีการประชุมตามที่ประธานของคณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน กำหนด

หมายเหตุ: รายชื่อคณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน ตามคำสั่งแต่งตั้งของกรรมการสมาคมสโมสรนักลงทุนในแต่ละสมัย

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ฝ่ายเทคโนโลยีสารสนเทศ

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่สรรหาระบบสารสนเทศ และเทคโนโลยี ตามวัตถุประสงค์ และนโยบาย ของหน่วยงานในสมาคมสโมสรนักลงทุน

คำจำกัดความ

โครงสร้างของ ฝ่ายเทคโนโลยีสารสนเทศแบ่งเป็น 2 กลุ่ม ดังนี้

1. กลุ่มซอฟต์แวร์ระบบงาน และ ธุรกิจ
2. กลุ่มเครือข่ายเน็ตเวิร์คและเทคโนโลยี

ความรับผิดชอบ

ฝ่ายเทคโนโลยีสารสนเทศมีบทบาทในการกำกับดูแลการปฏิบัติงานทั้งหมดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศภายในองค์กร โดยมีหน้าที่ดังนี้

- เป็นผู้นำในการกำหนดนโยบายและกลยุทธ์ในระยะยาว ที่เอื้อประโยชน์ชัดเจนต่อธุรกิจ และดูแลให้ระบบเทคโนโลยีสารสนเทศในอนาคตสามารถรองรับการขยายตัวขององค์กร
- สนับสนุนการทำงานร่วมกันของทุกหน่วยงานที่มีหน้าที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ โดยการสร้างเอกภาพทางด้านแนวความคิดที่เสริมสร้างคุณค่าและแนวทางการทำงาน
- แสวงหาโอกาสและช่องทางในการสนับสนุนการใช้เทคโนโลยี ที่เป็นประโยชน์ต่อองค์กรโดยรวม
- จัดหาผู้เชี่ยวชาญ ผู้ช่วยเหลือ และผู้ประสานงานเพื่อพัฒนา และปรับปรุงเทคโนโลยีสารสนเทศขององค์กร
- สรรหาระบบเทคโนโลยีสารสนเทศที่สามารถใช้ร่วมกันได้อย่างมีประสิทธิภาพ และคุ้มค่าต่อการลงทุน ทั้งนี้หมายถึงการจัดหาระบบอุปกรณ์ และการพัฒนาบุคลากรให้กับหน่วยธุรกิจ
- เป็นผู้นำในการพัฒนานโยบายระบบเทคโนโลยีสารสนเทศ ตลอดจนกำหนดมาตรฐานและขั้นตอนการทำงาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

หน้าที่หลัก

โดยทั่วไป ฝ่ายเทคโนโลยีสารสนเทศจะต้องทำหน้าที่เกี่ยวกับ

- ดูแล บริหารจัดการระบบเครื่องคอมพิวเตอร์ อุปกรณ์ฮาร์ดแวร์ และอุปกรณ์เสริมต่างๆ เพื่อให้การใช้งานประจำวันเป็นไปอย่างมีประสิทธิภาพ
- ดูแล บริหารจัดการระบบเครือข่ายเน็ตเวิร์คเช่นระบบ LAN และ WAN
- บริการให้ความช่วยเหลือและแก้ไขปัญหาในการใช้งานระบบคอมพิวเตอร์
- ดูแลรักษาและแก้ไขปัญหาาระบบซอฟต์แวร์ที่ใช้งานประจำวันให้ใช้งานได้อย่างมีประสิทธิภาพ
- แนะนำและจัดการระบบซอฟต์แวร์ใหม่ วางแผนการประยุกต์ใช้งาน เพื่อเพิ่มประสิทธิภาพในการทำงานขององค์กร
- ตรวจสอบและอนุมัติ ข้อกำหนดทางเทคนิคของระบบ (Specification)
- บริการกู้/แก้ไขความเสียหายของข้อมูล (ตามรายละเอียดในหัวข้อความปลอดภัยของอุปกรณ์และข้อมูล)
- ให้คำปรึกษาและบริการเชื่อมต่อระหว่างระบบงานเพื่อสามารถให้ใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพและลดความซ้ำซ้อนของข้อมูล

สายบังคับบัญชา

ฝ่ายเทคโนโลยีสารสนเทศซึ่งบริหารโดยหัวหน้าฝ่ายเทคโนโลยีสารสนเทศจะต้องอยู่ในความรับผิดชอบและรายงานต่อ ผู้จัดการสมาคมสโมสรนักลงทุน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ความปลอดภัยของอุปกรณ์ และข้อมูล

หลักการ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้แนวทางด้านความมั่นคงปลอดภัยของสารสนเทศ โดยพิจารณาองค์ประกอบ 3 ข้อหลัก ได้แก่

องค์ประกอบ	คำอธิบาย
ความลับ (Confidentiality)	การรักษาไว้ซึ่งความลับของสารสนเทศ ไม่ถูกเปิดเผยแก่ระบบ คน และ/หรือหน่วยงานที่ไม่ได้มีส่วนเกี่ยวข้อง
ความสมบูรณ์ (Integrity)	การรักษาไว้ซึ่งความถูกต้องเสถียรภาพของสารสนเทศ ไม่ถูกแก้ไขหรือนำไปใช้อย่างผิดวิธี และสามารถตรวจสอบความถูกต้องของสารสนเทศก่อนการนำไปใช้งานได้
ความพร้อมใช้ (Availability)	การรักษาไว้ซึ่งความพร้อมใช้งานของสารสนเทศ

โดยองค์ประกอบข้างต้น จะถูกนำมาพิจารณาเป็นมูลค่าของทรัพย์สินสารสนเทศในเชิงความมั่นคงปลอดภัย อันรวมไปถึงทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับสารสนเทศ

เป้าหมายสำคัญของการดำเนินกิจกรรมตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือ การลดและหลีกเลี่ยงปัญหาการละเมิดความมั่นคงปลอดภัยสารสนเทศ อันส่งผลต่อภาพลักษณ์และความเชื่อมั่นของผู้ใช้งานระบบ โดยมีการวางเป้าหมายเชิงธุรกิจ คือ ระบบสารสนเทศของสมาคมสโมสรนักลงทุนที่เป็นมืออาชีพในการให้บริการด้วยระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย (Information Security)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

แนวทาง

- 1) แนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดเกณฑ์ในการยอมรับความเสี่ยง

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ยึดแนวทางการพิจารณาความเสี่ยงที่มีผลกระทบต่อทรัพย์สินสารสนเทศทั้งทางตรงและทางอ้อม ผ่านการประเมินมูลค่าความเสียหาย และโอกาสการเกิดขึ้นของภัยคุกคามที่อาศัยช่องโหว่ของทรัพย์สินหรือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ที่ไม่มีประสิทธิภาพ รวมถึงการจัดการการเกิดการเปลี่ยนแปลง (Change) และการร้องขอเหตุผิดปกติ (Incident)

- 2) การลงทะเบียนทรัพย์สิน

ระบบสารสนเทศ หรืออุปกรณ์ที่อยู่ภายในขอบเขตการดำเนินงาน จะต้องได้รับการจำแนกประเภทของทรัพย์สิน ซึ่งจะทำให้ผู้ประเมินใช้ในการพิจารณาวิเคราะห์จุดอ่อนหรือช่องโหว่ (Vulnerability) ตลอดจนภัยคุกคาม (Threat) ได้อย่างครอบคลุม โดยแบ่งออกเป็น 5 ประเภทหลัก ได้แก่

ประเภทของทรัพย์สิน	ตัวอย่าง
Hardware Asset	เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์สนับสนุนโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวข้อง
Software Asset	ระบบปฏิบัติการ ระบบสารสนเทศ โปรแกรมประยุกต์
Information Asset	ข้อมูลในฐานข้อมูล เอกสาร ข้อมูลการตั้งค่าระบบ ข้อมูล Log คู่มือการปฏิบัติงาน
People Asset	พนักงานและผู้ที่เกี่ยวข้อง
Service Asset	บริการจากหน่วยงานภายนอก หรือหน่วยงานภายใน
Process Asset	กระบวนการ กระบวนการย่อย หรือกิจกรรมที่สำคัญที่หากเสียหาย สูญเสียไปแล้วจะมีผลต่อการปฏิบัติงานตามภารกิจขององค์กร
Site Asset	อาคาร สถานที่ตั้ง พื้นที่การแบ่งเขตโซนภายในสถานที่ เช่น ห้องเซิร์ฟเวอร์ พื้นที่ปฏิบัติงานของเจ้าหน้าที่ เป็นต้น

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

3) การจัดกลุ่มทรัพย์สิน (Asset Grouping)

ในกรณีที่ทรัพย์สินหลายรายการมีความคล้ายคลึงกันหรือเป็นชนิดเดียวกัน เจ้าของทรัพย์สินสามารถจัดกลุ่มทรัพย์สิน โดยการจัดทำรายการทรัพย์สินแยกย่อย เพื่อลดจำนวนรายการทรัพย์สินในการประเมินความเสี่ยง (ประเมินเป็นกลุ่มของทรัพย์สินแทน) และสามารถบริหารจัดการง่ายขึ้น ตัวอย่างกลุ่มของทรัพย์สิน กลุ่มเครื่องคอมพิวเตอร์แม่ข่าย (Server), กลุ่มอุปกรณ์เครือข่าย (Network Device), กลุ่มอุปกรณ์ที่เกี่ยวข้อง (Facility) เป็นต้น โดยรายละเอียดนิยามและรูปแบบข้อมูลที่บ้านที่ลงในแบบฟอร์มบัญชีทรัพย์สิน (IT-2FM-05) ให้อ้างอิงจาก IT-2PR-03 กระบวนการจัดองค์ประกอบ (Configuration Management Procedure)

4) ประเมินมูลค่าของทรัพย์สิน (Asset Value Evaluation)

ในการประเมินมูลค่าของทรัพย์สินนั้น กำหนดให้ใช้องค์ประกอบด้านความมั่นคงปลอดภัย (Security Components) เป็นเกณฑ์ในการพิจารณา โดยอย่างน้อยประกอบด้วย

- **การรักษาความลับ (Confidentiality):** ทรัพย์สินหรือข้อมูลจะเป็นความลับ อนุญาตให้ผู้ที่มีสิทธิ์เท่านั้นที่จะสามารถเข้าถึงได้
- **การรักษาความถูกต้อง ครบถ้วนสมบูรณ์ (Integrity):** ทรัพย์สินหรือข้อมูลที่จัดเก็บ หรือที่ผ่านการประมวลผลจะต้องมีความถูกต้อง ครบถ้วนสมบูรณ์ ไม่ถูกเปลี่ยนแปลง โดยไม่ได้รับอนุญาต
- **ความพร้อมใช้งาน (Availability):** ทรัพย์สินหรือข้อมูลจะต้องพร้อมใช้งานในเวลาที่ต้องการ

$$\text{Asset Value} = \sum_{i=1}^n (\text{loss value of security components} \times \text{weight})$$

สมาคมสโมสรนักลงทุน กำหนดให้มีการพิจารณาผลกระทบของการสูญเสียคุณลักษณะ C-I-A ในแต่ละด้านมุมของการให้บริการภายใต้ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยอย่างน้อยครอบคลุม ดังนี้

- ความสามารถในการให้บริการ หรือปฏิบัติงานของหน่วยงาน (Operation Perspective)
- ผลกระทบด้านชื่อเสียงองค์กรและภาพลักษณ์ (Reputation)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

มูลค่าทรัพย์สิน (Total Asset Value) จะถูกแบ่งระดับชั้นความสำคัญ โดยการแบ่งช่วงสัดส่วนของค่าเต็มของมูลค่าทรัพย์สิน (100%) กำหนดเกณฑ์พิจารณา ดังนี้

ระดับ	ค่า Total Asset Value (weight = 1)	
High	มากกว่าหรือเท่ากับ 4	4.0-5.0
Medium	มากกว่า 2 และน้อยกว่า 4	2.1-3.9
Low	น้อยกว่าหรือเท่ากับ 2	1.0-2.0

ทรัพย์สินที่มีระดับตั้งแต่ High ขึ้นไปจะเข้าสู่กระบวนการประเมินความเสี่ยง

ตัวอย่างการกำหนดมูลค่าทรัพย์สินของอุปกรณ์ระบบ eMT โดยมุ่งเน้นความสามารถในการให้บริการ (Operation) และภาพลักษณ์ชื่อเสียง (Reputation)

ชื่อทรัพย์สิน	Operation Perspective (50%)			รวม	Reputation Perspective (50%)			รวม
	C (0.33)	I (0.33)	A (0.33)		C (0.33)	I (0.33)	A (0.33)	
ระบบ eMT	1	4	5	3.33	5	5	5	5.00

$$\text{Total Asset Value} = (0.5 * 3.33) + (0.5 * 5.0) = 4.165 \text{ (High)}$$

ทั้งนี้ การเลือกใช้มุมมอง (Perspective) และการกำหนดน้ำหนักของคุณลักษณะของความมั่นคงปลอดภัยสารสนเทศ (Security Component) ให้พิจารณาตามวัตถุประสงค์และเป้าหมายขององค์กร (Mission) เพื่อสร้างความสอดคล้องกับความต้องการทางธุรกิจ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

5) การระบุภัยคุกคามที่เกี่ยวข้อง (Threat Identification)

การระบุภัยคุกคามที่เกี่ยวข้อง โดยพิจารณาจากเหตุการณ์ที่เคยเกิดขึ้น หรือพิจารณาจากช่องโหว่ที่มีในทรัพย์สินสารสนเทศ ทำให้ทางสมาคมสโมสรนักลงทุนทราบว่าภัยคุกคามใดบ้างที่อาจเกิดขึ้นได้กับทรัพย์สินสารสนเทศของสมาคมสโมสรนักลงทุน โดยทั่วไปภัยคุกคามอาจมีที่มาจากแหล่งต่างๆ ต่อไปนี้

ประเภท	ตัวอย่าง
ภัยคุกคามทางธรรมชาติ หรือสถานการณ์ฉุกเฉิน	เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติ หรือสถานการณ์ร้ายแรง ที่ก่อให้เกิดความเสียหายร้ายแรงกับทรัพย์สินสารสนเทศ เช่น น้ำท่วม แผ่นดินไหว พายุ อาคารถล่ม สภาพแวดล้อมเป็นพิษ สถานที่ตั้งอยู่ในพื้นที่มีน้ำรั่ว หรือขาดระบบไฟฟ้า ไฟไหม้ การประชุมชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
ภัยคุกคามจากมนุษย์ หรือผู้ปฏิบัติงาน	เป็นภัยคุกคามที่อาจเกิดจากการโจรกรรมทรัพย์สินของสมาคมสโมสรนักลงทุน การโจมตีระบบเครือข่าย การบุกรุกระบบ การปล่อย Virus หรือ Malware ในระบบ การก่ออาชญากรรมทางคอมพิวเตอร์ ผู้ก่อการร้าย เป็นต้น
ภัยคุกคามด้านการบริหารจัดการหรือกระบวนการภายในหน่วยงาน	เป็นภัยคุกคามที่อาจเกิดจากแผนนโยบายในการบริหารจัดการ ที่อาจส่งผลกระทบต่อการทำงานด้านการสารสนเทศ
ภัยคุกคามด้านไอที/เทคนิค	เป็นภัยคุกคามที่อาจเกิดจากช่องโหว่ของแอปพลิเคชัน หรือช่องโหว่ของเทคโนโลยีที่สมาคมสโมสรนักลงทุนนำมาใช้ เช่น ระบบคอมพิวเตอร์ เครื่องมือ และอุปกรณ์

6) การระบุช่องโหว่หรือจุดอ่อนของทรัพย์สิน (Vulnerability Identification)

การระบุช่องโหว่ที่มีในทรัพย์สิน พิจารณาจาก

- ผลการประเมินความเสี่ยงที่ผ่านมา (Previous risk assessment result)
- ผลการประเมินภายใน (Internal audit report)
- ผลการทดสอบความสอดคล้องทางเทคนิคของระบบ (system compliance testing)

ผลการดำเนินงาน จะทำให้องค์กรทราบช่องโหว่ที่มีในทรัพย์สิน ซึ่งช่องโหว่ดังกล่าวอาจเป็นช่องทางในการบุกรุกหรือละเมิด นำไปสู่เหตุการณ์อันไม่พึงประสงค์ได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

7) การวิเคราะห์และระบุมาตรการควบคุมในปัจจุบันขององค์กร (Control Analysis)

ช่องโหว่ที่พบในทรัพย์สินสารสนเทศ ผู้ประเมินต้องพิจารณามาตรการที่ทางสมาคมสโมสรนักลงทุน ใช้ควบคุมในปัจจุบัน โดยมาตรการจะช่วยลดผลกระทบหรือโอกาสที่จะเกิดภัยคุกคามได้ มาตรการแบ่งออกเป็นสองประเภท ดังต่อไปนี้

- มาตรการในการป้องกัน (Preventive Controls) มาตรการที่ถูกนำมาใช้ เพื่อป้องกันหรือลดโอกาสที่จะเกิดภัยคุกคาม
- มาตรการในการเฝ้าระวัง (Detective Controls) มาตรการที่ถูกนำมาใช้ เพื่อเฝ้าระวังหรือแจ้งเตือนเมื่อเกิดเหตุการณ์ที่เป็นภัยคุกคาม

8) การพิจารณาโอกาสที่จะเกิดภัยคุกคาม (Likelihood Determination)

โอกาสที่จะเกิดเหตุการณ์ภัยคุกคามที่มีผลต่อความมั่นคงปลอดภัยของทรัพย์สิน พิจารณาจากมาตรการที่มีในปัจจุบัน โดยมีรายละเอียด ดังนี้

Likelihood Level	รายละเอียด
5- มีโอกาสเกิดขึ้นสูงมาก (Almost certain)	ภัยคุกคามมีโอกาสดังเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 1 เดือนเนื่องจากขาดมาตรการในการควบคุม
4- มีโอกาสเกิดขึ้นสูง (Likely)	ภัยคุกคามมีโอกาสดังเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 3 เดือน เนื่องจากมาตรการในการควบคุมไม่เพียงพอต่อการป้องกันภัยคุกคาม
3- มีโอกาสเกิดขึ้นปานกลาง (Possible)	ภัยคุกคามมีโอกาสดังเกิดขึ้น หรือเคยเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 6 เดือน เนื่องจากมาตรการในการควบคุมไม่เพียงพอและขาดประสิทธิภาพในการป้องกันภัยคุกคาม
2- มีโอกาสเกิดขึ้นน้อย (Unlikely)	ภัยคุกคามมีโอกาสดังเกิดขึ้นหรือเคยเกิดขึ้นประมาณ 1 ครั้ง ภายใน 1 ปี เนื่องจากมีมาตรการในการควบคุมเพียงพอต่อการป้องกันภัยคุกคาม
1- มีโอกาสเกิดขึ้นน้อยมาก (Rare)	ภัยคุกคามมีโอกาสดังเกิดขึ้น หรือเคยเกิดขึ้นประมาณ 1 ครั้ง ภายใน 5 ปี เนื่องจากมีมาตรการในการควบคุมเพียงพอและมีประสิทธิภาพต่อการป้องกันภัยคุกคาม

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

9) การพิจารณาผลกระทบ (Impact)

พิจารณาระดับของผลกระทบที่มีต่อบริการหรือธุรกิจ หากเกิดภัยคุกคาม โดยมีรายละเอียด ดังนี้

ระดับของผลกระทบ	รายละเอียด
5- รุนแรง (Critical)	มีผลกระทบอย่างรุนแรง ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศและความต่อเนื่องในการให้บริการ (Service Continuity) ส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในระดับสูงที่สุดของทรัพย์สินนั้นๆ (อาจต้องประกาศแผน BCP)
4- มาก (Major)	มีผลกระทบมาก ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ และระดับการให้บริการ (Service Level) อาจส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในระดับสูงของทรัพย์สินนั้นๆ (กระทบกับระบบหลักบางส่วนยังสามารถให้บริการได้)
3-ปานกลาง (Moderate)	มีผลกระทบปานกลาง ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ และระดับการให้บริการ (Service Level) อาจส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในระดับปานกลางของทรัพย์สินนั้นๆ (กระทบกับระบบที่สนับสนุนระบบหลัก)
2- เล็กน้อย (Minor)	มีผลกระทบเล็กน้อย ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ แต่ไม่กระทบต่อระดับการให้บริการ (Service Level) อาจส่งผลกระทบต่อการสูญเสียคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศในทรัพย์สินนั้นๆ
1-ไม่มีผลกระทบ (Insignificant)	ไม่มีผลกระทบ ต่อความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ และระดับการให้บริการ (Service Level)

10) การพิจารณาระดับความเสี่ยง (Risk Determination)

ดำเนินการประเมินความเสี่ยงของทรัพย์สินและกำหนดระดับความเสี่ยงที่สมาคมสโมสรนักลงทุนยอมรับได้ (Acceptable Risk Level) รวมถึงการกำหนดแนวทางในการจัดการความเสี่ยงที่สูงกว่าระดับความเสี่ยงที่ยอมรับได้

11) การพิจารณาระดับความเสี่ยงของทรัพย์สิน

การพิจารณาระดับความเสี่ยงของทรัพย์สินแต่ละรายการ ใช้เกณฑ์การพิจารณาดังตารางต่อไปนี้

Likelihood	ผลกระทบ				
	1- Insignificant	2 - Minor	3- Moderate	4- Major	5- Critical
5- Almost Certain	M	H	H	E	E
4- Likely	M	M	H	H	E
3- Possible	L	M	M	H	E
2- Unlikely	L	M	M	M	H
1- Rare	L	L	L	M	H

คำอธิบาย E: ระดับสูงมาก (Extremely High)

H: ระดับสูง (High)

M: ระดับปานกลาง (Medium)

L: ระดับต่ำ (Low)

12) การพิจารณาระดับความเสี่ยงที่ยอมรับได้

ระดับความเสี่ยงที่สมาคมสโมสรนักลงทุนยอมรับได้นั้น กำหนดให้ต้องเป็นทรัพย์สินที่มีระดับความเสี่ยงน้อยกว่าระดับสูง (H) สำหรับทรัพย์สินที่มีความเสี่ยงตั้งแต่ระดับสูง “H” ขึ้นไป ให้เจ้าของทรัพย์สินร่วมกับเจ้าของความเสี่ยงกำหนดแนวทางในการจัดการทรัพย์สินต่อไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

13) การจัดการความเสี่ยงและมาตรการควบคุมที่นำมาใช้ (Risk Treatment and Control Recommendation)

เมื่อทราบผลการประเมินความเสี่ยงของทรัพย์สิน และพบว่าค่าความเสี่ยงของทรัพย์สินสูงกว่าระดับความเสี่ยงที่สมาคมสโมสรนักลงทุนยอมรับได้ ให้เจ้าของทรัพย์สินดังกล่าว พิจารณาแนวทางในการจัดการความเสี่ยงโดยมี 4 แนวทาง ได้แก่

- การยอมรับความเสี่ยง (Accept Risk)
- การลดความเสี่ยง (Reduce Risk)
- การถ่ายโอนความเสี่ยง (Transfer Risk)
- การหลีกเลี่ยงความเสี่ยง (Avoid Risk)

เมื่อเลือกแนวทางในการจัดการความเสี่ยงได้แล้ว เจ้าของความเสี่ยง จะต้องกำหนดมาตรการควบคุม และแผนการดำเนินงานในการจัดการความเสี่ยง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การรักษาความปลอดภัย

หลักการ

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อแจกแจงระเบียบปฏิบัติสำหรับผู้ใช้อุปกรณ์คอมพิวเตอร์ ข้อห้ามทั่วไปที่จะนำมาประยุกต์ใช้ และอ้างอิงข้อมูลเพิ่มเติมอื่นๆ ที่จะนำมาใช้ในบางสถานการณ์

ขอบเขต

ทรัพยากรที่บริหาร และดูแลโดยฝ่ายเทคโนโลยีสารสนเทศภายใต้นโยบายฉบับนี้ครอบคลุมอุปกรณ์และโปรแกรมคอมพิวเตอร์ เอกสาร และสื่อที่ใช้อ้างอิง ข้อมูลที่เก็บบนอุปกรณ์คอมพิวเตอร์แม่ข่าย ตลอดจนข้อมูลอื่น ๆ ของสมาคมสโมสรนักลงทุนที่เก็บบนสื่ออื่น ๆ เช่น ซีดีรอม เทป รวมถึงอุปกรณ์จัดเก็บประเภทต่าง ๆ ที่อยู่ในการครอบครองของฝ่ายเทคโนโลยีสารสนเทศหรือหน่วยงานใดภายใต้สมาคมสโมสรนักลงทุน

แนวทาง

การเชื่อมต่อทั้งที่เป็นการชั่วคราวและถาวรผ่านระบบเครือข่ายต้องเป็นไปตามที่กำหนดไว้ในนโยบายฉบับนี้ ซึ่งครอบคลุมถึงการเชื่อมต่อถึงในระดับข้อมูลของเครื่องคอมพิวเตอร์แต่ละเครื่องที่ต่อเชื่อมกับเครือข่าย และอุปกรณ์โทรศัพท์ที่ใช้เชื่อมต่อด้วย

อุปกรณ์คอมพิวเตอร์ที่สมาคมสโมสรนักลงทุนไม่ได้เป็นเจ้าของ จะเชื่อมต่อกับระบบเครือข่ายของสมาคมฯ ได้ต่อเมื่อได้รับการอนุมัติโดยผู้จัดการสมาคมฯ โดยฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิ์ในการติดตามเนื้อหาของข้อมูลที่มีการส่งผ่านระบบเครือข่าย และหากมีความจำเป็นในการตรวจสอบเนื้อหาที่ส่งก็สามารถแจ้งให้หัวหน้าฝ่ายที่รับผิดชอบกิจกรรมที่มีความจำเป็นในการเชื่อมต่อ เพื่อรับทราบการติดตามการตรวจสอบ

นโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy)

- การอนุญาตให้มีการเข้าถึงระบบและข้อมูลสารสนเทศใด ๆ ก็ตาม ต้องขึ้นอยู่กับความจำเป็นในการทำงาน
- การเข้าถึงระบบและข้อมูลสารสนเทศต้องมีการยืนยันตัวตนก่อนจึงจะเข้าใช้งานได้ เช่น การยืนยันตัวตนโดยใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นต้น
- ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ และต้องมีการกำหนดสิทธิ์ผู้ใช้งานในระดับสูง
- ในการเข้าใช้งานของผู้ใช้งานในระดับสูงจะต้องมีการร้องขอใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงในแต่ละครั้ง
- ผู้ดูแลระบบสามารถถอดสิทธิ์หรือเปลี่ยนแปลงสิทธิ์ในกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการทำงานของระบบและข้อมูลสารสนเทศได้ตามความเหมาะสม

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- ไม่อนุญาตให้มีการใช้งานรหัสผ่านตั้งต้น (Default Password) ที่ติดมากับอุปกรณ์หรือที่มีมากับการตั้งค่าจากโรงงาน
- เจ้าของระบบหรือผู้ดูแลระบบควรมีการทบทวนสิทธิที่ได้มีการอนุญาตให้กับผู้ใช้งานอย่างสม่ำเสมอ
- ควรมีการจัดทำเอกสารแสดงสิทธิที่ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศต่างๆ เพื่อใช้ในการทบทวนและตรวจสอบการเข้าถึง
- พนักงานที่มีความประสงค์ร้องขอเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Account) ต้องจัดทำแบบฟอร์มร้องขอบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Request Form) (IT-2FM-07)
- ผู้ดูแลระบบบันทึกทะเบียนบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privileged Account Inventory) (IT-2FM-09) สำหรับใช้ในการอ้างอิง

สถานะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน

ปัจจุบันนี้ฝ่ายเทคโนโลยีสารสนเทศดำเนินการดูแลการปฏิบัติงานระบบคอมพิวเตอร์ภายในองค์กร โดยทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศจะทำหน้าที่ดูแลจัดการสัญญาการว่าจ้างจากภายนอกกับสมาคม ฯ เพื่อให้สัญญาเป็นไปตามเวลาที่กำหนดอย่างมีประสิทธิภาพและต้นทุนที่เหมาะสม พนักงานที่ได้รับการอนุมัติจะสามารถเข้าใช้ระบบเครือข่ายและทรัพยากรคอมพิวเตอร์ได้ตลอดเวลา

ฝ่ายเทคโนโลยีสารสนเทศได้จัดให้มีหน่วยสนับสนุน และช่วยเหลือการใช้งานคอมพิวเตอร์ให้กับผู้ใช้งานที่ต้องการให้เพิ่มรายชื่อผู้ใช้งาน หรือเข้ารับการอบรม หรือต้องการเอกสารประกอบการใช้งานระบบคอมพิวเตอร์

บัญชีรายชื่อผู้ใช้งานในระบบอยู่ภายใต้ข้อกำหนดต่อไปนี้

- รายชื่อผู้ใช้งานจะถูกตั้งค่าปิดการใช้งานบัญชีล่วงหน้าและตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานลาออก
- ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการตรวจสอบวันที่เข้าสู่ระบบล่าสุดของพนักงานที่ลาออก (Check Last Logon Date) ในกรณีที่มีการแจ้งลาออกล่าช้าหรือมีการเลิกจ้างฐานละทิ้งหน้าที่โดยระบุในส่วนรายละเอียดเพิ่มเติมของแบบฟอร์มการเพิกถอนสิทธิใช้งานบัญชีผู้ใช้ พร้อมบันทึกหลักฐานการตรวจสอบ
- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการระงับการใช้งาน หรือลบรายชื่อผู้ใช้งาน เมื่อมีความจำเป็น และในกรณีดังกล่าว หัวหน้าฝ่ายเทคโนโลยีสารสนเทศจะทำการอนุมัติล่วงหน้าก่อนที่จะสั่งการให้ระงับหรือการลบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ให้ผู้ใช้งานตรวจสอบ หรือให้เปลี่ยนรหัสการเข้าสู่ระบบใด ๆ ทั้งนี้ขึ้นอยู่กับข้อจำกัดของระบบแต่ละระบบ อนึ่ง กรณีดังกล่าวจะเกิดขึ้นก็ต่อเมื่อได้มีการพิจารณาแล้วว่าอาจจะมีการละเมิดมาตรการความปลอดภัยของระบบคอมพิวเตอร์เท่านั้น
- ฝ่ายเทคโนโลยีสารสนเทศสงวนสิทธิในการระงับสิทธิในการเข้าสู่ระบบใด ๆ เมื่อได้มีการพิจารณาแล้วว่าอาจจะมีการละเมิดมาตรฐานการรักษาความปลอดภัยระบบคอมพิวเตอร์
- ฝ่ายเทคโนโลยีสารสนเทศกำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที
- ฝ่ายเทคโนโลยีสารสนเทศกำหนดการตั้งรหัสผ่าน (Password Management) ต้องมีรูปแบบดังนี้
 - มีความยาวไม่ต่ำกว่า 8 ตัวอักษร
 - ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว
 - ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กอย่างน้อย 1 ตัว
 - ประกอบด้วยตัวเลขอย่างน้อย 1 ตัว
 - ต้องเปลี่ยนรหัสผ่านทุก 90 วัน
 - รหัสผ่านที่เปลี่ยนใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม
- แผนกบุคคลมีความรับผิดชอบในการแจ้งฝ่ายเทคโนโลยีสารสนเทศทราบทันทีที่มีการว่าจ้าง การโยกย้ายหรือพ้นสภาพของพนักงานใด ๆ ที่มีรายชื่ออยู่ในทะเบียนผู้ใช้งานระบบคอมพิวเตอร์
- ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของสมาคมฯ ได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง

ข้อห้ามและการใช้งานอย่างเหมาะสม

การกระทำที่ต้องห้าม มีดังนี้

- การปฏิเสธไม่ให้บริการต่อพนักงานผู้ใช้งานของสมาคมสโมสรนักลงทุน
- การแสวงหาประโยชน์จากบัญชีรายชื่อหรือทรัพยากรที่ถูกปล่อยปละละเลย หรือผู้ใช้งานที่ด้อยความรู้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- การพยายามคาดเดา เจาะ หรือหารหัสผ่านในการเข้าสู่ระบบของผู้ใช้งานอื่นๆ
- การใช้อุปกรณ์ หรือโปรแกรม เพื่อลักลอบตัดต่อข้อมูลที่ส่งผ่านระบบเครือข่าย
- การปลอมแปลงจดหมายอิเล็กทรอนิกส์ หรือข่าวสารอิเล็กทรอนิกส์ หรือการจงใจให้เกิดความเข้าใจผิดผ่านการสื่อสารอิเล็กทรอนิกส์

ผู้ใช้งานทุกคนจะต้องใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุนอย่างเหมาะสม ซึ่งรวมถึงข้อดังต่อไปนี้

- จัดการรักษารหัสผ่านในการเข้าสู่ระบบอย่างเหมาะสม เช่น ไม่ให้ยืมใช้ร่วมกัน ไม่เปิดเผยให้เห็น เป็นต้น
- ดูแลให้การเข้าสู่ระบบ และการออกจากระบบเป็นไปอย่างสมบูรณ์ หรือไม่ละทิ้งเครื่องคอมพิวเตอร์ในขณะที่เปิดโปรแกรมค้างไว้
- เคารพในลิขสิทธิ์ของโปรแกรม
- บริหารจัดการข้อมูลที่เป็นความลับอย่างเหมาะสม

บุคคลที่ไม่ใช่พนักงานที่เข้าใช้เครื่องคอมพิวเตอร์โดยลำพัง และไม่มีพนักงานของบริษัทคอยดูแลอยู่ หากถูกพบจะถูกบังคับให้ออกจากระบบทันที โดยที่เครื่องคอมพิวเตอร์ที่ใช้งาน และบัญชีผู้ใช้งานที่เปิดค้างไว้ ให้บุคคลใช้อยู่ขณะตรวจพบจะถูกยึด และระงับไม่ให้ใช้งานต่อไป ในเหตุการณ์ดังกล่าว จะต้องแจ้งให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและผู้บริหารของหน่วยงานที่ครอบคลุมอุปกรณ์คอมพิวเตอร์และข้อมูลนั้นรับทราบ เพื่อดำเนินการต่อไป

นอกจากนี้ ผู้ใช้งานไม่ควรที่จะถือโอกาสอ่านข้อมูลที่เป็นความลับ อันเนื่องมาจากความบังเอิญ หรือจากความผิดพลาดของผู้ละเมิดเข้าสู่ระบบ หรือจากการถือสิทธิในการเข้าสู่ข้อมูลที่เหนือกว่า เป็นต้น เมื่อทราบว่าข้อมูลที่เป็นความลับถูกเปิดเผยก็ไม่ควรที่จะอ่านต่อ และจะต้องรายงานให้ผู้บริหารของฝ่ายเทคโนโลยีสารสนเทศทราบทันที เช่นเดียวกับการเขียนทับข้อมูลที่ไม่ใช่ของตนโดยตั้งใจ และไม่ได้รับอนุญาต ถือเป็นความผิด

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and Operations Management)

การแบ่งหน้าที่ในการปฏิบัติงานและการจัดทำเอกสารประกอบการปฏิบัติงาน

- การกำหนดบทบาทหน้าที่ในการปฏิบัติงาน หน้าที่ในการบริหารจัดการระบบสารสนเทศและระบบเครือข่ายจะต้องแยกออกจากกัน ไม่ควรให้พนักงานคนเดียวกันทำงานที่สำคัญในกระบวนการเดียวกัน เพื่อป้องกันการทุจริตและการสะกดหยุดชะงักของงาน หากพนักงานดังกล่าวไม่สามารถมาปฏิบัติงานได้ ยกเว้นแต่มีข้อจำกัดเรื่องจำนวนของผู้ปฏิบัติงาน
- การบริหารการเปลี่ยนแปลงใด ๆ ในระบบเครือข่าย และระบบสารสนเทศของสมาคมสโมสรนักลงทุน จะต้องปฏิบัติตามขั้นตอนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure) ของสมาคมสโมสรนักลงทุน
- การแบ่งแยกระบบสารสนเทศ เพื่อลดความผิดพลาดหรือผลกระทบอันเกิดจากการดำเนินการทดสอบ ควรมีการแยกระบบสารสนเทศที่ให้บริการจริง ออกจากระบบสารสนเทศที่ใช้ในการพัฒนา และทดสอบ (เฉพาะระบบที่สามารถดำเนินการได้)

หน้าที่ความรับผิดชอบของผู้ใช้

- การใช้รหัสผ่านและการกำหนดรหัสผ่านจะต้องปฏิบัติตามแนวทางการจัดการรหัสผ่าน (Password Management)
- การจัดการด้านความปลอดภัยของอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended Equipment) เมื่อไม่ต้องการใช้งานอุปกรณ์หรือเครื่องคอมพิวเตอร์แล้ว ให้ทำการยกเลิกการเชื่อมต่อกับระบบเครือข่าย หรือระบบสารสนเทศ จัดเก็บอุปกรณ์หรือเครื่องคอมพิวเตอร์ไว้ในตู้ที่สามารถปิดล็อกได้ เพื่อป้องกันไม่ให้บุคคลอื่นเข้ามาใช้อุปกรณ์ดังกล่าวโดยไม่ได้รับอนุญาต
- เครื่องคอมพิวเตอร์ทุกเครื่องจะต้องถูกล็อกหน้าจอทุกครั้งเมื่อไม่มีการใช้งาน
- การจัดเก็บเอกสารข้อมูลสำคัญของสมาคมสโมสรนักลงทุน ข้อมูลที่อยู่ในสื่อบันทึกข้อมูลไว้ในสถานที่ที่สามารถปิดล็อกหรือเข้ารหัสข้อมูลดังกล่าวได้ พนักงานจะต้องไม่ทิ้งเอกสารสำคัญไว้บนโต๊ะทำงาน และจัดเก็บโต๊ะทุกครั้งก่อนเลิกงาน
- ข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์หรือส่งออกภายนอกองค์กรต้องจัดให้มีการเข้ารหัสข้อมูลโดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ ทั้งนี้ ต้องพิจารณาเลือกใช้เทคนิคต่าง ๆ ที่มีระดับความมั่นคงปลอดภัยตามมาตรฐานสากล
- การจัดทำการจัดเก็บ การส่งต่อ ลบทำลายข้อมูล จะต้องดำเนินการตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล (Information Classification Labelling and Media Disposal Procedure)



- ต้องควบคุมให้มีมาตรการการปิดบังข้อมูลสารสนเทศเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน และปฏิบัติตามข้อกำหนดทางกฎหมาย กฎหมาย ข้อบังคับ และสัญญา แนวทางและมาตรการความปลอดภัยในการปิดบังข้อมูลเพื่อไม่ให้อาสาสมัครสามารถระบุตัวตนได้ มีดังนี้
 - การปิดบังข้อมูล (Data Masking) เช่น แทนที่เลขบัตรประจำตัวประชาชน 10 หลักแรก ด้วยเครื่องหมาย x แสดงเพียง 4 หลักสุดท้าย (x-xxxx-xxxxx-12-3)
 - การใช้นามแฝง (Pseudonymization) เช่น แทนที่ชื่อลูกค้าด้วยเลขรหัสลูกค้า (ลูกค้าหมายเลข 12345)
 - การทำข้อมูลนิรนาม (Anonymization) เช่น รวมกลุ่มข้อมูลที่มีลักษณะคล้ายคลึงกัน เข้าด้วยกัน (ลูกค้ากลุ่มอายุ 20-30 ปี, เพศชาย, อาชีพพนักงานออฟฟิศ)
 - การเข้ารหัส (Encryption) เช่น การเข้ารหัสการส่งอีเมล
 - การลบหรือเปลี่ยนเป็นค่า null เช่น การลบข้อมูลออกจากระบบ หรือแทนที่ด้วยค่าว่าง (null)
 - การแทนที่ (Substitution) เช่น แทนที่ชื่อจริงด้วยชื่อปลอม หรือแทนที่ที่อยู่จริงด้วยที่อยู่ปลอม
 - การแทนที่ด้วยค่าแฮช (Hashing) เช่น เก็บรหัสผ่านในรูปแบบค่าแฮช เพื่อป้องกันการถูกขโมยและนำไปใช้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การเข้าสู่ห้องเซิร์ฟเวอร์

หลักการ

ห้องเซิร์ฟเวอร์เป็นแหล่งเก็บอุปกรณ์คอมพิวเตอร์ส่วนใหญ่ขององค์กร ระบบความปลอดภัยที่เหมาะสมจึงมีความจำเป็นเพื่อปกป้องสินทรัพย์เหล่านี้ การจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์ เป็นไปเพื่อป้องกันสินทรัพย์คอมพิวเตอร์จากการละเมิดใช้ อุบัติเหตุ หรือเจตนาให้เกิดความเสียหาย หรือการขโมย การอนุมัติเพื่อจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์จะทำเมื่อเห็นว่ามี ความจำเป็น เนื่องจากการกำหนดเงื่อนไขเพื่อบังคับใช้ข้อจำกัดดังกล่าวเฉพาะกลุ่มบุคคล หรือเป็นรายบุคคล เป็นสิ่งที่ทำได้ยากและไม่เหมาะสม ดังนั้นจึงได้กำหนดแนวทางดังต่อไปนี้เพื่อช่วยในการตัดสินใจกรณีที่ต้องจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์

แนวทาง

พนักงานที่ต้องปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์ทุกวัน ซึ่งได้รับสิทธิเข้าสู่ห้องเซิร์ฟเวอร์ ได้แก่

- พนักงานดูแลซอฟต์แวร์
- พนักงานดูแลเครือข่ายเน็ตเวิร์คและเทคโนโลยี
- พนักงานสำนักงานคณะกรรมการส่งเสริมการลงทุนที่ได้รับมอบหมายให้ดูแลฝ่ายเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน

ผู้ได้รับสิทธิอื่นนอกเหนือจากที่กล่าวข้างต้น ยังประกอบไปด้วยบุคคลที่ต้องเข้าไปปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์เป็นประจำ ได้แก่

- พนักงานดูแลโปรแกรมคอมพิวเตอร์ที่มีความรับผิดชอบเกี่ยวข้องกับการทำงานบนเครื่องเซิร์ฟเวอร์ หรืองานนั้นต้องทำบนเครื่องเซิร์ฟเวอร์ ณ ห้องเซิร์ฟเวอร์ การทำงานในห้องเซิร์ฟเวอร์จะถูกจำกัดเฉพาะสถานการณ์ที่จำเป็นเท่านั้น
- พนักงานฝ่ายเทคโนโลยีสารสนเทศอื่น ๆ ซึ่งต้องเข้าไปปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์เป็นประจำ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

โดยหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ (หรือผู้แทน) จะเป็นผู้อนุมัติการเข้าทำงานดังกล่าวข้างต้น ในกรณีที่บุคคลอื่น ๆ ดังกล่าวข้างล่างนี้ มีความจำเป็นต้องเข้าไปทำงานในห้องเซิร์ฟเวอร์ จะต้องกรอกแบบคำขออนุญาตเข้าพื้นที่ห้องเซิร์ฟเวอร์ บุคคลเหล่านั้นจะได้รับอนุญาต โดยมีพนักงานฝ่ายปฏิบัติการคอมพิวเตอร์มีส่วนรับรู้ในการเข้าไปทำงานในจุดนั้น เช่น

- ผู้ขายที่เข้ามาทำงานบำรุงรักษา และช่างระบบคอมพิวเตอร์
- พนักงานฝ่ายงานระบบอื่น ๆ ในองค์กร
- บุคคลอื่น ๆ ที่ได้รับอนุญาต และติดตามโดยพนักงานฝ่ายปฏิบัติการคอมพิวเตอร์

ข้อจำกัดอื่น ๆ ภายในบริเวณห้องเซิร์ฟเวอร์

- ห้ามนำอาหารและเครื่องดื่มเข้ามาบริเวณห้องเซิร์ฟเวอร์
- ห้ามนำอุปกรณ์สื่อสารเข้ามาในบริเวณห้องเซิร์ฟเวอร์ เว้นแต่จะได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- ห้ามนำกล้องถ่ายรูปเข้ามา เว้นแต่จะได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- ห้ามนำวัตถุระเบิด เชื้อเพลิง วัสดุติดเพลิงง่าย อาวุธ สารเคมี หรือสิ่งอื่นใดที่อาจก่อให้เกิดความเสียหายทั้งต่อชีวิตและทรัพย์สิน เข้ามาบริเวณห้องเซิร์ฟเวอร์

การติดตามการเข้า-ออกบริเวณห้องเซิร์ฟเวอร์จะใช้ระบบการบันทึกการเข้า-ออกห้องเซิร์ฟเวอร์

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

กรรมสิทธิ์ในข้อมูล

หลักการ

ระบบเทคโนโลยีสารสนเทศขององค์กร ข้อมูล รวมถึงสินทรัพย์ต่าง ๆ ในระบบคอมพิวเตอร์ ถือเป็นกรรมสิทธิ์ของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน และถือเป็นทรัพย์สินที่มีค่าขององค์กร และข้อมูลทั้งหมดที่เก็บอยู่ในสินทรัพย์เหล่านี้ถือเป็นกรรมสิทธิ์ของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน โดยฝ่ายเทคโนโลยีสารสนเทศมีความรับผิดชอบต่อข้อมูลที่เก็บไว้บนระบบเครือข่าย และระบบข้อมูลกลางอื่น ๆ ที่อยู่ภายใต้การครอบครองและดูแล ในขณะที่ผู้ใช้งานแต่ละคนจะรับผิดชอบข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายคอมพิวเตอร์แต่ละเครื่องที่ตนเองใช้งานอยู่ และอุปกรณ์การจัดเก็บประเภทต่าง ๆ ที่อยู่ในการครอบครอง

แนวทาง

ระบบคอมพิวเตอร์และข้อมูลต่าง ๆ ที่เกี่ยวข้องถือเป็นสินทรัพย์ที่มีมูลค่าขององค์กร และข้อมูลทั้งหมดที่เก็บอยู่ในสินทรัพย์เหล่านี้ถือเป็นสมบัติของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน โดยผู้ใช้งานแต่ละคนจะรับผิดชอบข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายคอมพิวเตอร์แต่ละเครื่องที่ตนเองใช้งานอยู่

ระบบข้อมูลที่สำคัญ และตัวข้อมูลควรจะถูกเก็บรักษาไว้ที่เครื่องแม่ข่ายคอมพิวเตอร์ เพื่อประโยชน์ในการสำรองข้อมูล ข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายเป็นความรับผิดชอบโดยตรงของผู้ใช้งานแต่ละคน ดังนั้นผู้ใช้งานแต่ละคนที่เก็บข้อมูลไว้ที่เครื่องลูกข่ายจะต้องทำสำเนาแฟ้มข้อมูลด้วยตนเอง ข้อมูลใด ๆ ที่ละเมิดต่อกฎหมายไทยและกฎหมายลิขสิทธิ์ แต่ถูกจัดเก็บ รักษา และสามารถเข้าถึงได้ทางเครื่องลูกข่าย จะถือว่าละเมิดต่อนโยบายขององค์กรด้วย

การใช้ข้อมูลและระบบสารสนเทศขององค์กรจะทำได้ก็ต่อเมื่อได้รับอนุมัติโดยผู้จัดการของสมาคมสโมสรนักลงทุนเท่านั้น การมอบสิทธิในการเข้าถึงข้อมูลและระบบสารสนเทศของพนักงานแต่ละคน ควรสอดคล้องกับหน้าที่และงานที่รับผิดชอบ การเปิดเผยข้อมูลควรเป็นไปตามข้อกำหนดในนโยบายว่าด้วยความลับของสมาคมสโมสรนักลงทุน (โปรดดูข้อตกลงว่าด้วยการรักษาความลับขององค์กร หรือ Mutual Confidentiality Agreement ตามเอกสารแนบ 2) การละเมิดนโยบายดังกล่าวนี้จะต้องรายงานให้คณะกรรมการสารสนเทศของสมาคมสโมสรนักลงทุนหรือฝ่ายเทคโนโลยีสารสนเทศทราบทันที ผู้รับเหมาทุกรายที่ต้องเข้าใช้งานระบบสารสนเทศขององค์กรจะต้องเซ็นยอมรับตามข้อตกลงในเอกสารข้อตกลงว่าด้วยการรักษาความลับขององค์กร (Confidential Agreement)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้อินเทอร์เน็ต

หลักการ

สมาคมสโมสรนักลงทุนจะเชื่อมต่ออินเทอร์เน็ตและเปิดให้พนักงานที่ได้รับการอนุมัติใช้งาน โดยหน่วยงานต้นสังกัดจะต้องดำเนินการตามขั้นตอนการแจ้งขอใช้อินเทอร์เน็ตของฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเปิดให้ใช้งานได้ระหว่างเวลาทำการขององค์กรโดยมีวัตถุประสงค์เพื่อประโยชน์ในการปฏิบัติงาน และต้องสอดคล้องโดยตรงกับหน้าที่ และความรับผิดชอบของพนักงาน โดยหัวหน้าฝ่าย/หัวหน้าแผนก ของหน่วยงาน นั้น มีหน้าที่สอดส่องและดูแลให้สอดคล้องกับวัตถุประสงค์ดังกล่าว

แนวทาง

ถึงแม้การใช้อินเทอร์เน็ตส่งผลให้ค่าใช้จ่ายขององค์กรสูงขึ้น แต่ก็ถือว่าเป็นเทคโนโลยีทันสมัยที่มีประโยชน์สำหรับการใช้งาน และถือเป็นหนึ่งในภารกิจขององค์กร เฉพาะพนักงานที่ได้รับอนุมัติเท่านั้นจึงจะเข้าใช้งานอินเทอร์เน็ตได้ ทั้งนี้พนักงานต้องปฏิบัติให้ถูกต้องเหมาะสมตามกฎหมายกำหนด ดังที่มีกำหนดไว้ในหลักการว่าด้วยสิ่งลามกอนาจาร และ นโยบายลิขสิทธิ์โปรแกรมและการสั่งซื้อโปรแกรมคอมพิวเตอร์ เพื่อที่จะป้องกันไม่ให้สมาคมสโมสรนักลงทุนตกเป็นเป้าหมายโจมตีของไวรัสคอมพิวเตอร์ การใช้งานอินเทอร์เน็ตต้องเป็นไปเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับธุรกิจขององค์กร

เพื่อป้องกันไม่ให้ระบบเครือข่ายมีไวรัสคอมพิวเตอร์และโปรแกรมที่ไม่ถูกต้องตามลิขสิทธิ์ จึงห้ามมิให้มีการนำโปรแกรมที่ส่งผ่านมาทางจดหมายอิเล็กทรอนิกส์ หรือโปรแกรมที่ Download จากระบบเครือข่ายภายนอกมาติดตั้ง ในกรณีที่ต้องใช้โปรแกรมหมาจะต้องได้รับการอนุมัติจากหัวหน้าฝ่ายของหน่วยงานนั้น ๆ ก่อน และประสานฝ่ายเทคโนโลยีสารสนเทศเพื่อดำเนินการต่อไป ผู้ละเมิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

การควบคุมการใช้งานระบบเครือข่าย

- ในการขอเข้าใช้งานระบบเครือข่ายนั้นจะต้องได้รับอนุมัติจากหัวหน้าฝ่ายของผู้ที่มีความประสงค์ การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ตต้องเชื่อมต่อผ่านระบบเครือข่ายที่สมาคมสโมสรนักลงทุนจัดไว้เท่านั้น
- ไม่เปิดเผยข้อมูลเวอร์ชันของระบบปฏิบัติการและหมายเลข IP Address ให้บุคคลที่ไม่เกี่ยวข้องทราบ
- การควบคุมการเชื่อมต่อระบบเครือข่าย ควรแบ่งโซนของระบบเครือข่ายตามลักษณะการให้บริการของระบบ ควรกำหนดให้มี Demilitarized Zone (DMZ) คั่นระหว่างการเชื่อมต่อภายนอกกับระบบเครือข่ายของสมาคมสโมสรนักลงทุน แต่โซนของระบบเครือข่ายควรแยกออกจากกัน (ถ้าเป็นไปได้)

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- การควบคุมการเลือกเส้นทางข้อมูลของเครือข่ายควรใช้ไฟร์วอลล์ (Firewall) เพื่อจำกัดการเข้าถึงผ่านระบบเครือข่าย ควรมีอุปกรณ์ป้องกันการบุกรุกจากภายนอก การจำกัดการเชื่อมต่อผ่านระบบเครือข่ายต้องเป็นไปตามนโยบายด้านการควบคุมการเข้าถึง และข้อกำหนดสำหรับระบบ/แอปพลิเคชัน โดยข้อกำหนดนี้ควรจะมีการปรับปรุงเมื่อจำเป็น
- ระบบเครือข่ายที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอกจะต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ เพื่อตรวจสอบและป้องกันการบุกรุกจากภายนอก จะต้องจำกัดการเชื่อมต่อจากภายนอก โดยกำหนดให้สามารถเข้าถึง Network Zone หรือระบบสารสนเทศที่กำหนดไว้เท่านั้น
- ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของสมาคมฯ ให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ อาทิจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับ (ฉบับที่ 2) พ.ศ. 2560

การเชื่อมต่ออินเทอร์เน็ตจะต้องไม่เป็นไปเพื่อโอนถ่ายข้อมูลดังต่อไปนี้

- ที่ละเมิดต่อกฎหมายไทย หรือกฎหมายลิขสิทธิ์ หรือขัดต่อศีลธรรมหรือขัดต่อเนื้อหาหรือวัตถุประสงค์ของนโยบายฉบับนี้
- ที่มีวัตถุประสงค์ในเชิงพาณิชย์ที่นอกเหนือจากผลประโยชน์ขององค์กร
- ห้ามมิให้ใช้อินเทอร์เน็ตเพื่อเข้าสู่โปรแกรมระบบอื่น ๆ ที่ไม่มีสิทธิเข้าใช้
- การละเมิดเข้าใช้งานอินเทอร์เน็ตไม่ว่ากรณีใด จะต้องรายงานให้ผู้จัดการสมาคม ฯ ทราบ มิฉะนั้นจะถือว่าละเมิดนโยบายขององค์กร
- ห้ามใช้อินเทอร์เน็ตเพื่อเยี่ยมชมเว็บไซต์ (Website) ที่ลามกอนาจาร หรือขัดต่อศีลธรรมอันดีงาม หรือเพื่อโอนถ่ายข้อมูลหรือรูปภาพที่ลามกอนาจาร หรือขัดต่อศีลธรรม ซึ่งผู้กระทำความผิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน และอาจถูกดำเนินคดีอาญา และ/หรือคดีแพ่ง หากการกระทำดังกล่าวถือว่าขัดต่อกฎหมายของประเทศไทยเช่นกัน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้จดหมายอิเล็กทรอนิกส์ หรืออีเมล

หลักการ

ระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail System) ถือเป็นทรัพย์สินขององค์กร บุคคลที่สามารถใช้งานได้จะต้องได้รับอนุมัติ โดยแจ้งขอใช้จดหมายอิเล็กทรอนิกส์ (Electronic Mail) ตามวิธีการที่ฝ่ายบุคคลกำหนด โดยบุคคลที่ได้รับสิทธิดังกล่าวจะต้องใช้จดหมายอิเล็กทรอนิกส์ด้วยวัตถุประสงค์ที่เป็นประโยชน์ต่อสมาคมสโมสรนักลงทุน และเกี่ยวเนื่องกับงานในหน้าที่ของตนเท่านั้น

คำจำกัดความ

“ข้อมูลอิเล็กทรอนิกส์ (Electronic Data)” หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

“จดหมายอิเล็กทรอนิกส์ (Electronic Mail) หรืออีเมล (E-Mail)” หมายถึง การสื่อสารหรือการส่งข้อมูลในรูปของข้อความอิเล็กทรอนิกส์ (Messages) บันทึกหรือเอกสารประกอบ (Attached Files) จากคอมพิวเตอร์ของผู้ส่งไปยังคอมพิวเตอร์ของผู้รับผ่านระบบโทรคมนาคมสื่อสาร หรืออีกนัยหนึ่งจดหมายอิเล็กทรอนิกส์ คือ วิธีการรับส่งข้อความหรือข้อมูลระหว่างคอมพิวเตอร์เครือข่าย (Network) ของสมาคมสโมสรนักลงทุน และให้หมายความรวมถึง การรับและ/หรือส่งข้อความหรือข้อมูลผ่านเครือข่ายอินเทอร์เน็ต (Internet) ด้วย “ผู้ใช้ (User)” หมายถึง พนักงานของสมาคมสโมสรนักลงทุน

แนวทาง

สมาคมสโมสรนักลงทุนจัดให้มีระบบจดหมายอิเล็กทรอนิกส์เพื่อใช้สำหรับติดต่อสื่อสารในเรื่องที่เกี่ยวข้องกับงานขององค์กร หรือของสมาคมสโมสรนักลงทุน เป็นหลัก การใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารส่วนบุคคลจึงควรอยู่บนพื้นฐานของความเหมาะสมและความพอดี

ข้อมูลอิเล็กทรอนิกส์ที่รับส่งผ่านระบบจดหมายอิเล็กทรอนิกส์ ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน หรือระบบอินเทอร์เน็ต ถือเป็นพยานหลักฐานที่สามารถนำมาใช้ในการฟ้องร้องดำเนินคดีกับผู้ก่อการในภายหลังได้ ในกรณีที่มีการใช้ที่ขัดต่อนโยบายหรือก่อให้เกิดความเสียหายต่อสมาคมสโมสรนักลงทุน และ/หรือพนักงาน และ/หรือผู้บริหารของสมาคมสโมสรนักลงทุน แม้ว่าผู้ใช้นั้นจะพ้นสภาพการเป็นพนักงาน หรือสิ้นสุดสัญญาว่าจ้างกับสมาคมสโมสรนักลงทุนแล้วหรือไม่ก็ตาม โดยฝ่ายเทคโนโลยีสารสนเทศจะทำการจัดเก็บข้อมูลดังกล่าวไว้จนกว่าจะสิ้นสุดอายุความในการฟ้องร้องคดี

องค์กรไม่มีนโยบายที่จะเปิดอ่านข้อมูลอิเล็กทรอนิกส์ของผู้ใช้ที่ถูกส่งหรือได้รับผ่านระบบจดหมายอิเล็กทรอนิกส์หรือระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน เว้นแต่

(1) กรณีที่มีเหตุจำเป็น เช่น มีเหตุอันควรสงสัยว่า มีบุคลากรขององค์กรนำข้อมูลความลับขององค์กรออกไปเปิดเผยภายนอกโดยผ่านทางระบบจดหมายอิเล็กทรอนิกส์ หรือมีเหตุอันควรสงสัยว่า บุคลากรของ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

องค์กรใช้จดหมายอิเล็กทรอนิกส์ในทางที่ไม่ถูกต้อง ฯลฯ ซึ่งผู้ที่มีสิทธิตรวจสอบข้อมูลอิเล็กทรอนิกส์ของผู้ใช้แต่ละรายได้จะต้องเป็นผู้บริหารหรือเป็นบุคคลที่ได้รับแต่งตั้งจากคณะกรรมการขององค์กรเท่านั้น หรือ

(2) ในกรณีที่ สมาคมสโมสรนักลงทุนได้รับคำสั่งจากศาลหรือหน่วยงานที่มีอำนาจตามบทบัญญัติแห่งกฎหมายสั่งให้ส่งข้อมูลอิเล็กทรอนิกส์และ/หรือตรวจสอบการสื่อสารในรูปแบบจดหมายอิเล็กทรอนิกส์

เพื่อมิให้เกิดปัญหาในเรื่องของความปลอดภัย การปฏิบัติผิดกฎหมาย และประสิทธิภาพในการทำงาน ผู้ใช้ทุกรายพึงมีความรับผิดชอบดังนี้

- ในฐานะที่เป็นผู้มีส่วนเกี่ยวข้องกับการใช้จดหมายอิเล็กทรอนิกส์ ผู้ใช้แต่ละรายต้องปฏิบัติตามนโยบายที่เกี่ยวข้องกับการใช้จดหมายอิเล็กทรอนิกส์ โดยในการใช้ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน รวมถึงระบบอื่น ๆ ที่สมาคมสโมสรนักลงทุนจัดไว้ให้ นั้น ผู้ใช้ต้องปฏิบัติตามนโยบายที่สมาคมสโมสรนักลงทุนกำหนด
- เนื้อหาของข้อความ เอกสารประกอบ หรือรูปภาพประกอบ และอื่น ๆ ที่ส่งโดยใช้จดหมายอิเล็กทรอนิกส์ควรเป็นไปด้วยความเหมาะสม ไม่ขัดต่อบทบัญญัติของกฎหมาย และสอดคล้องกับนโยบายฉบับนี้ และอยู่ภายใต้ข้อจำกัดเดียวกันกับการติดต่อสื่อสารในรูปแบบอื่น ๆ ที่สมาคมสโมสรนักลงทุนกำหนด
- ข้อมูลอิเล็กทรอนิกส์ที่ผู้ใช้แต่ละรายเก็บสะสมไว้ ต้องใช้เนื้อที่บนเครื่องแม่ข่ายในการเก็บซึ่งฝ่ายเทคโนโลยีสารสนเทศจะกำหนดขนาดของเนื้อที่ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ (Mail Box) ของผู้ใช้แต่ละราย ผู้ใช้ต้องลบข้อมูลอิเล็กทรอนิกส์ที่ไม่จำเป็นและไม่เกี่ยวกับงานขององค์กรออก รวมทั้งข้อมูลอิเล็กทรอนิกส์ที่ไม่ใช้แล้วทิ้งไป แต่หากมีความจำเป็นที่จะต้องใช้เนื้อที่ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์มากกว่านโยบายที่กำหนด ให้หัวหน้าฝ่ายส่งแจ้งความจำเป็นและเหตุผลถึงหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
- ปฏิบัติตามนโยบายที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน และระบบคอมพิวเตอร์ที่เกี่ยวข้องที่สมาคมสโมสรนักลงทุนกำหนด
- รักษาความสุภาพ และมารยาทในการสื่อสาร
- ปกป้องความเป็นส่วนตัว และความลับของผู้อื่น
- ช่วยดูแลรับผิดชอบการจำกัดขนาดของข้อมูลอิเล็กทรอนิกส์ที่ใช้งานอยู่
- ใช้เทคโนโลยีสารสนเทศให้มีประสิทธิภาพและก่อให้เกิดประโยชน์แก่งานที่รับผิดชอบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้จดหมายอิเล็กทรอนิกส์ที่ถูกต้อง

การใช้จดหมายอิเล็กทรอนิกส์ที่ถูกต้อง ต้องใช้ให้สอดคล้องกับวัตถุประสงค์ เป้าหมาย และภารกิจขององค์กร ตลอดจนสอดคล้องกับหน้าที่และความรับผิดชอบของผู้ใช้แต่ละราย ตัวอย่างต่อไปนี้แสดงให้เห็นถึงการใช้งานที่ถูกต้อง

- ใช้เพื่อการสื่อสาร รวมถึงการแลกเปลี่ยนข้อมูลสำหรับพัฒนาสายอาชีพ หรือเพื่อศึกษาหาความรู้ หรือทักษะในสายงาน
- ใช้เพื่อการสื่อสารกับหุ้นส่วนทางธุรกิจ เพื่อส่งเอกสาร หรือเพื่อโอนย้ายเอกสารประกอบการทำงาน หรือร่างเอกสารต่าง ๆ
- ใช้เพื่อค้นคว้า หรือรวบรวมข้อมูลเพื่อสนับสนุนคำแนะนำ มาตรฐาน การวิเคราะห์ หรือเพื่อพัฒนาสายอาชีพที่เกี่ยวข้องกับหน้าที่ของผู้ใช้
- ใช้เพื่อการสื่อสาร หรือแลกเปลี่ยนข้อมูลเพื่อสนับสนุนการทำงาน หรือโครงการที่รับผิดชอบร่วมกัน

การใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง และขัดต่อนโยบาย

ตัวอย่างต่อไปนี้แสดงให้เห็นถึงการใช้งานที่ไม่ถูกต้อง

- การใช้ที่เป็นการละเมิดบทบัญญัติแห่งกฎหมาย
- การใช้ที่เป็นการให้ข้อมูลภายในขององค์กร หรือข้อมูลที่เกี่ยวข้องกับความสามารถขององค์กรในด้านต่าง ๆ ซึ่งยังไม่ได้เป็นที่เปิดเผยต่อสาธารณชนแก่บุคคลอื่น โดยไม่ได้รับความเห็นชอบจากผู้บริหาร
- การใช้เพื่อเผยแพร่สิ่งลามกอนาจาร หรือขัดต่อศีลธรรม หรือนโยบายของสมาคมสโมสรนักลงทุน
- การใช้เพื่อส่งข้อความที่ส่อเสียด ยุยง ก่อให้เกิดความแตกแยก หรือความเกลียดชัง หรือก่อให้เกิดความเสื่อมเสีย/เสียหายแก่สมาคมสโมสรนักลงทุน รวมทั้งพนักงาน คณะกรรมการ และคณะกรรมการของสมาคมสโมสรนักลงทุน
- การส่งข้อความ หรือเอกสารแนบที่ไม่มีสาระเกี่ยวข้องกับการดำเนินการ หรือก่อให้เกิดประโยชน์กับสมาคมสโมสรนักลงทุน ที่เกินขอบเขตที่ยอมรับได้ หรือการใช้เพื่อธุรกิจส่วนตัวที่เกินขอบเขตที่ยอมรับได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ผู้ใช้อยู่ได้ก็ตามที่ใช้งานจดหมายอิเล็กทรอนิกส์ หรือส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์ เครือข่ายของสมาคมสโมสรนักลงทุนด้วยวิธีการอื่น ๆ ที่ขัดต่อนโยบายและหรือข้อตกลงหมายอาจถูกลงโทษ โดยการตัดสินใจต่าง ๆ อันพึงได้รับ จนถึงขั้นให้พ้นสภาพการเป็นพนักงาน และ/หรือถูกดำเนินคดีทางแพ่งและทางอาญาได้

ผู้ใช้งานจะต้องตระหนักว่า (1) ข้อมูลอิเล็กทรอนิกส์ โดยเฉพาะที่มีเนื้อหาในเชิงลบต่อองค์กรสามารถส่ง พิมพ์ หรือทำสำเนาได้โดยง่าย และพึงระมัดระวังว่า การส่งข้อความโดยจดหมายอิเล็กทรอนิกส์ทุกครั้งจะมีชื่อขององค์กรปรากฏอยู่ (2) สมาคมสโมสรนักลงทุนไม่อาจรับประกันได้ว่าจดหมายอิเล็กทรอนิกส์จะมีความเป็นส่วนตัว เนื่องจากบุคคลที่สามอาจจะละเมิดเข้ามาเปิดอ่านข้อมูลอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน เพื่อจุดประสงค์ในการล้วงความลับของสมาคมสโมสรนักลงทุนได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ลิขสิทธิ์โปรแกรม และการสั่งซื้อ หรือการเช่าใช้

หลักการ

นโยบายนี้กำหนดขึ้นเพื่อให้สอดคล้องกับกฎหมายลิขสิทธิ์และเพื่อปกป้องโปรแกรมที่เป็นสินทรัพย์ขององค์กร ถึงแม้ว่านโยบายนี้จะมีมาตรการช่วยในการบังคับใช้ แต่ความสำเร็จในท้ายสุดขึ้นอยู่กับความเข้าใจและความร่วมมือของพนักงานทุกคน ฝ่ายเทคโนโลยีสารสนเทศได้รับมอบหมายให้รับผิดชอบให้บังคับใช้นโยบายนี้อย่างต่อเนื่อง

ลิขสิทธิ์ของโปรแกรม

นโยบายของสมาคมสโมสรนักลงทุนในที่นี้คือ การเคารพในลิขสิทธิ์โปรแกรม และปฏิบัติตามสิทธิ์ที่ได้รับในการใช้โปรแกรมตามที่ระบุไว้ในเอกสารลิขสิทธิ์ ผู้ละเมิดต่อนโยบายนี้ถือว่ามีความผิดและอาจถูกลงโทษทางวินัย พนักงานจะต้องไม่ทำสำเนาของโปรแกรมหรือเอกสารที่เกี่ยวข้อง เพื่อนำมาใช้ภายในสำนักงานหรือที่อื่น ๆ โดยพลการ ยกเว้นเสียแต่ว่าได้รับการยินยอมโดยเจ้าของลิขสิทธิ์เป็นลายลักษณ์อักษร การทำสำเนาโปรแกรมโดยการละเมิดอาจส่งผลให้พนักงานและสมาคมสโมสรนักลงทุนถูกลงโทษทางอาญาและทางแพ่งตามที่กฎหมายระบุ พนักงานจะต้องไม่นำโปรแกรมไปให้บุคคลหรือนิติบุคคลที่สาม หมายรวมถึงผู้ขาย ผู้รับเหมา และลูกค้า พนักงานสามารถใช้โปรแกรมที่ติดตั้งบนระบบเครือข่ายหรือบนเครื่องคอมพิวเตอร์ตามที่ระบุไว้ในสัญญาลิขสิทธิ์เท่านั้น

การซื้อโปรแกรม

โปรแกรมที่ซื้อมาถือเป็นสินทรัพย์ที่มีมูลค่าสูง และต้องบันทึกไว้เป็นสินทรัพย์ขององค์กร เพื่อติดตามตรวจสอบ ดังนั้นการซื้อโปรแกรมจึงควรปฏิบัติให้สอดคล้องกับกระบวนการอนุมัติสั่งซื้อขององค์กร เพื่อให้การบันทึกสินทรัพย์เป็นไปอย่างถูกต้องตามที่ได้ระบุไว้ในนโยบายการสั่งซื้อทรัพยากรทางเทคโนโลยีสารสนเทศ โปรแกรมทั้งหมดต้องได้รับการอนุมัติใช้โดยฝ่ายเทคโนโลยีสารสนเทศ จำนวนผู้มีสิทธิในการสั่งซื้อได้ถูกจำกัดไว้ เพื่อให้มั่นใจว่าโปรแกรมที่สั่งซื้อทั้งหมดได้รับการบันทึกอย่างถูกต้อง ฝ่ายเทคโนโลยีสารสนเทศจะระงับการสั่งซื้อโปรแกรมใด ๆ ที่จะส่งผลเสียหายต่อระบบเครือข่าย หรือไม่เหมาะสมกับการใช้งานของหน่วยธุรกิจ หน่วยธุรกิจจะต้องปรึกษารื้อกับฝ่ายเทคโนโลยีสารสนเทศก่อนที่จะทำการสั่งซื้อ เนื่องจากฝ่ายเทคโนโลยีสารสนเทศจะสามารถแจ้งได้ว่าการติดตั้งโปรแกรมดังกล่าวไว้แล้วหรือไม่

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การจดทะเบียนโปรแกรม

ภายหลังจากที่ได้รับโปรแกรม ฝ่ายเทคโนโลยีสารสนเทศจะติดต่อกับผู้ขายเพื่อยืนยันการจดทะเบียนอย่างถูกต้อง โปรแกรมที่สั่งซื้อจะได้รับการจดทะเบียนในนามขององค์กร และจะไม่มี การจดทะเบียนในนามส่วนบุคคลโดยเด็ดขาด ภายหลังจากการจดทะเบียนแล้วเสร็จ โปรแกรมจะได้รับการติดตั้งโดยฝ่ายเทคโนโลยีสารสนเทศหรือบุคคล/นิติบุคคลที่ได้รับการมอบหมายอย่างเป็นทางการจากหน่วยงานฝ่ายเทคโนโลยีสารสนเทศเท่านั้น โดยที่ฝ่ายเทคโนโลยีสารสนเทศจะรับผิดชอบเก็บต้นฉบับของสัญญาลิขสิทธิ์และการสั่งซื้อ และแผนกจัดซื้อรับผิดชอบเก็บสำเนา จนกว่าฝ่ายเทคโนโลยีสารสนเทศและแผนกจัดซื้อเห็นสมควรว่าโปรแกรมดังกล่าวไม่สมควรจะนำมาใช้งานอีก โดยให้ปฏิบัติตามขั้นตอนและระเบียบการตัดจำหน่ายทรัพย์สิน

โปรแกรม

สินทรัพย์คอมพิวเตอร์ขององค์กรจะต้องได้มาอย่างถูกกฎหมาย และปราศจากไวรัสคอมพิวเตอร์ เฉพาะโปรแกรมที่สั่งซื้อและได้รับอนุมัติอย่างถูกต้องเท่านั้นที่สามารถนำมาใช้กับระบบคอมพิวเตอร์ขององค์กร หากปราศจากความเห็นชอบจากฝ่ายเทคโนโลยีสารสนเทศ พนักงานไม่สามารถจะนำโปรแกรมอื่นใดมาใช้กับระบบคอมพิวเตอร์ขององค์กรได้ เป็นที่ตระหนักว่า มีโปรแกรมที่มักจะถูกส่งมาพร้อมกับจดหมายอิเล็กทรอนิกส์ หรือ Download จากเครือข่ายภายนอก หรือ แผ่น CD ถูกนำมาติดตั้งลงเครื่องคอมพิวเตอร์ หากทางฝ่ายเทคโนโลยีสารสนเทศตรวจพบโปรแกรมที่ไม่ถูกต้องเหล่านั้นจะถูกตรวจจับและลบทิ้งอัตโนมัติในระหว่างการตรวจสอบภายใน ผู้ละเมิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

การตรวจสอบภายใน

ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องเป็นระยะ ๆ เพื่อดูแลให้สอดคล้องตามนโยบายที่กำหนด ฝ่ายเทคโนโลยีสารสนเทศสามารถตรวจจับรายงาน และลบโปรแกรมที่ได้มาอย่างไม่ต้องบนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายขององค์กร นอกจากนี้ฝ่ายเทคโนโลยีสารสนเทศอาจจะตรวจสอบเครื่องคอมพิวเตอร์ที่ไม่เชื่อมต่อกับระบบเครือข่ายขององค์กร และทำการลบโปรแกรมที่ไม่จดทะเบียนทันที โดยพนักงานจะต้องให้ความร่วมมือกับฝ่ายเทคโนโลยีสารสนเทศในระหว่างที่มีการตรวจสอบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์

หลักการ

การใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องมีวัตถุประสงค์เพื่อประโยชน์ต่อองค์กร และเกี่ยวข้องกับงานในหน้าที่ของพนักงานเท่านั้น

แนวทาง

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ถือเป็นทรัพย์สินขององค์กร มีใช้ทรัพย์สินส่วนตัว การใช้อุปกรณ์และระบบดังกล่าวต้องมีวัตถุประสงค์ที่เป็นประโยชน์โดยตรงต่อองค์กร

ข้อห้ามในการใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ มีต่อไปนี้

- เป็นการละเมิดต่อกฎหมายไทย
- ให้ข้อมูลของสมาคมสโมสรนักลงทุนโดยที่ไม่ได้รับความเห็นชอบจากผู้จัดการสมาคม ฯ
- เผยแพร่ข้อมูล หรือเอกสารที่ขัดแย้ง และละเมิดนโยบายของสมาคมสโมสรนักลงทุน
- ดำเนินธุรกิจส่วนตัว เกินความเหมาะสมผลในช่วงเวลาทำงาน

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องไม่มีวัตถุประสงค์ในเชิงพาณิชย์ นอกเหนือไปจากที่ได้รับมอบหมาย หรือต้องเป็นไปเพียงเพื่อประโยชน์ของสมาคมสโมสรนักลงทุนเท่านั้น อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์อาจนำมาใช้เพื่อช่วยกิจกรรมต่าง ๆ ขององค์กรมีส่วนร่วม หรืองานกุศลต่าง ๆ ที่องค์กรเป็นผู้สนับสนุน เฉพาะบุคคลที่ได้รับอนุมัติจากสมาคมสโมสรนักลงทุนเท่านั้น จึงจะสามารถใช้งานอุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์

การเข้าใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต จะต้องแจ้งให้ผู้จัดการสมาคม ฯ ทราบในทันที ค่าใช้จ่ายที่อาจเกิดขึ้นจะต้องแจ้งต่อผู้จัดการสมาคม ฯ หรือฝ่ายเทคโนโลยีสารสนเทศ และต้องดำเนินการสอบสวนโดยเร่งด่วน กรณีที่ไม่มีการแจ้งเรื่องเข้าใช้อุปกรณ์ดังกล่าวโดยไม่ได้รับมอบหมาย ถือเป็นการละเมิดนโยบายขององค์กรและต้องมีโทษทางวินัย

เนื้อหาที่ใช้ในการสื่อสารด้วยเสียงต้องดำรงไว้ซึ่งความเป็นมืออาชีพ และมีความเหมาะสม ห้ามมิให้ใช้เนื้อหาที่ไม่มีสาระสำคัญ ไม่สุภาพ สบประมาท แบ่งแยกเชื้อชาติ ล่วงเกินทางเพศ โจมตี ทำลายชื่อเสียง บังคับ ชูเชิญ ช่มชู้ โดยเด็ดขาด

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

ข้อความที่สนทนาผ่านอุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ถือเป็นทรัพย์สินขององค์กร มิใช่ทรัพย์สินส่วนบุคคล สมาคมสโมสรนักลงทุนจึงขอสงวนสิทธิในการติดตามตรวจสอบเนื้อหาของการสนทนา รวมทั้งแฟ้มเสียงที่ถูกบันทึกไว้

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องเป็นไปอย่างเหมาะสม หากค่าใช้จ่ายที่เกิดขึ้นมากเกินความสมเหตุสมผลอาจทำให้บุคคลนั้น ๆ สูญสิทธิในการใช้งาน หรือบุคคลนั้นอาจต้องรับผิดชอบค่าใช้จ่ายทั้งหมดหรือส่วนหนึ่ง หรืออาจถือว่ามีความผิดทางวินัยขั้นรุนแรง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การแจ้งให้ทราบเรื่องการระงับให้บริการชั่วคราว

หลักการ

นโยบายนี้ครอบคลุมขั้นตอนที่ฝ่ายเทคโนโลยีสารสนเทศจะแจ้งให้ผู้เกี่ยวข้องรับทราบถึงแผนงานที่อาจจะส่งผล หรือมีผลกระทบต่อให้บริการต่าง ๆ บนระบบเครือข่าย และทำให้การบริการดังกล่าวต้องถูกระงับชั่วคราว ตัวอย่างเช่น การปรับปรุงประสิทธิภาพของเครื่องเซิร์ฟเวอร์ การบำรุงรักษาเครื่องเซิร์ฟเวอร์ หรือแผนบำรุงรักษาอื่นๆ ที่จะส่งผลกระทบต่อระบบไฟฟ้า หรือระบบสื่อสาร ที่หล่อเลี้ยงการทำงานของอุปกรณ์คอมพิวเตอร์ในห้องเซิร์ฟเวอร์

สำหรับการระงับใช้บริการที่มีสาเหตุอื่น ๆ อันได้แก่ ไฟฟ้า คมนาคมก่อสร้างตัดสายไฟฟ้า หรืออุบัติเหตุ และอุบัติเหตุที่อยู่เหนือการควบคุมของทางฝ่ายเทคโนโลยีสารสนเทศ จะแจ้งให้ผู้เกี่ยวข้องทราบทันทีที่เกิด

แนวทาง

สื่อหลักที่ใช้เพื่อแจ้งให้ทราบ คือ จดหมายอิเล็กทรอนิกส์หรืออีเมลหรือการโทรแจ้งถึงพนักงานทุกคน โดยฝ่ายเทคโนโลยีสารสนเทศจะแจ้งให้ทราบล่วงหน้าอย่างน้อย 48 ชั่วโมง กรณีที่เกิดจากการวางแผนงานล่วงหน้า ตามด้วยการแจ้งให้ทราบในกรณีที่ใช้เวลาเกินกว่ากำหนดการที่วางไว้เป็นระยะ ๆ ตามนโยบายแล้ว การดำเนินแผนงานที่มีผลกระทบดังกล่าวจะหลีกเลี่ยงไปทำนอกเวลางาน อย่างไรก็ตาม ในบางกรณีก็ไม่สามารถหลีกเลี่ยงได้

ในกรณีที่เกิดอุบัติเหตุหรืออุบัติเหตุที่ทำให้การบริการต้องหยุดชะงัก พนักงานของฝ่ายเทคโนโลยีสารสนเทศจะได้จัดให้มีหน่วยช่วยเหลือ และให้ข้อมูลโดยย่อเกี่ยวกับขอบเขตของปัญหา ระยะเวลา สาเหตุ และผลกระทบที่อาจเกิดขึ้นให้ผู้ใช้งานที่ได้รับผลกระทบได้รับทราบ นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศจะชี้แจงให้ทราบถึงปัญหาต่อเนื่องที่จะเกิดขึ้นอันเป็นผลจากหรือเกี่ยวข้องกับการหยุดชะงักของระบบ ข้อสงสัยใด ๆ ที่เกิดขึ้นอันเนื่องมาจากแผนงาน หรือจากเหตุสุดวิสัย สามารถสอบถามได้จากพนักงานประจำหน่วยช่วยเหลือผู้ใช้คอมพิวเตอร์ การติดต่อที่นอกเหนือหน่วยนี้ ทางฝ่ายเทคโนโลยีสารสนเทศจะได้แจ้งให้ทราบเป็นกรณี ๆ ไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การใช้อุปกรณ์คอมพิวเตอร์

หลักการ

พนักงานทุกคนในสมาคมสโมสรนักลงทุนที่ใช้ระบบปฏิบัติงานและอุปกรณ์ในระบบการสื่อสารที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ของสมาคมสโมสรนักลงทุน มีหน้าที่รับผิดชอบในการใช้ระบบดังกล่าวอย่างผู้มีจรรยาบรรณ มีความเป็นมืออาชีพ โดยเป็นไปอย่างถูกต้องตามกฎหมาย ทั้งนี้ผู้ใช้ระบบทุกท่านต้องปฏิบัติตามแนวนโยบายซึ่งได้วางไว้เพื่อการใช้อุปกรณ์ในระบบต่าง ๆ ดังกล่าว

แนวทาง

พนักงานทุกคนในองค์กรควรยึดถือแนวทางปฏิบัติดังต่อไปนี้

- ต้องยึดถือในความเป็นอันหนึ่งอันเดียวกันของระบบต่างๆ ขององค์กร
- ต้องไม่แทรกแซงสิทธิส่วนบุคคลของผู้ใช้คนอื่นใด
- ต้องตระหนักว่า พนักงานต้องจำกัดการเข้าใช้ข้อมูลอันเป็นข้อมูลลับเฉพาะ ซึ่งอยู่นอกเหนืออำนาจหน้าที่ของตน
- ต้องปฏิบัติตามกฎระเบียบข้อบังคับต่าง ๆ ซึ่งควบคุมการใช้งานระบบและอุปกรณ์คอมพิวเตอร์
- ไม่ได้รับอนุญาตให้เข้าสู่ระบบหรือข้อมูลของผู้ใช้รายอื่น
- ไม่ได้รับอนุญาตให้ใช้ข้อมูลต่างๆ ของสมาคม ฯ โดยจุดประสงค์เพื่อการทำวิจัย การอบรม และการจัดทำเอกสารที่ไม่เกี่ยวข้องกับงานของสมาคม ฯ
- จะทำความคุ้นเคยและปฏิบัติตามแนวทางการใช้งานระบบต่าง ๆ รวมถึงระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานอยู่ได้อย่างถูกต้องเหมาะสม

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การควบคุมการเข้าใช้งานระบบปฏิบัติการ

- กระบวนการในการเข้าใช้งานระบบอย่างปลอดภัย จะต้องมีการตรวจสอบสิทธิ์ในการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และจะต้องมีการจัดเก็บ Log ของผู้ใช้งานในระบบ
- การตรวจสอบยืนยันผู้ใช้ระบบปฏิบัติการ จะต้องมีการระบุและตรวจสอบยืนยันตัวบุคคลของผู้ใช้ ผู้ใช้งานแต่ละคนต้องมี User Account ที่ไม่ซ้ำกัน และไม่สามารถใช้ร่วมกันหรือโอนให้กันได้ ทั้งนี้ User Account จะต้องไม่แสดงให้รู้ถึงระดับของการเข้าถึงระบบของผู้ใช้งาน ในกรณีที่จำเป็นต้องใช้ User Account ร่วมกันภายในกลุ่ม เนื่องจากข้อกำหนดบางประการจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร และการนำไปใช้ต้องอยู่ในความควบคุมอย่างเคร่งครัด
- การบริหารจัดการรหัสผ่าน ระบบปฏิบัติการจะต้องมีกลไกเพื่อให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากสามารถเข้าใช้งานครั้งแรกได้ รหัสผ่านที่ได้รับการกำหนดจากเจ้าของผลิตภัณฑ์จะต้องได้รับการเปลี่ยนทันทีเมื่อติดตั้งระบบแล้ว การบริหารจัดการรหัสผ่านในระบบปฏิบัติการจะต้องสอดคล้องกับแนวทางการจัดการรหัสผ่าน (Password Management) ของสมาคมสโมสรนักลงทุน
- การจัดการระยะเวลาในการใช้งาน เครื่องคอมพิวเตอร์ทุกเครื่องต้องมีการตั้งค่าล็อกหน้าจออัตโนมัติที่ระยะเวลา 15 นาที

การควบคุมการเข้าใช้งานแอปพลิเคชันและข้อมูล

- การจำกัดการเข้าใช้งานข้อมูล การควบคุมการเข้าถึงแอปพลิเคชันต้องเป็นไปตามข้อกำหนดและสอดคล้องกับนโยบายด้านการควบคุมการเข้าถึงของสมาคมสโมสรนักลงทุน กำหนดสิทธิ์ในการเข้าถึงข้อมูลตามความรับผิดชอบในการทำงาน
- การแยกระบบข้อมูลที่มีความสำคัญ ระบบที่มีความสำคัญควรจะแยกออกจากการเข้าถึงของบุคคลทั่วไป การให้บริการของแอปพลิเคชันที่มีความสำคัญควรใช้เซิร์ฟเวอร์ที่แยกต่างหาก ในกรณีที่อาจต้องใช้ทรัพยากรร่วมกัน เจ้าของแอปพลิเคชันทั้งสองฝ่ายต้องประเมินความสำคัญของข้อมูลก่อนจะตกลงกันเรื่องใช้ทรัพยากรร่วมกัน

การใช้คอมพิวเตอร์แบบพกพาและการเชื่อมต่อระบบเครือข่าย

- การป้องกันทางกายภาพ (Physical) อุปกรณ์ของสมาคมสโมสรนักลงทุนใด ๆ ที่ต้องนำไปใช้นอกสถานที่ในกิจกรรมของสมาคมสโมสรนักลงทุน จะต้องได้รับการอนุมัติจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ โดยอุปกรณ์ดังกล่าวจะต้องมีการควบคุมด้านความมั่นคงปลอดภัยในระดับเดียวกับอุปกรณ์ที่ใช้ในสำนักงาน เมื่อต้องเดินทางควรเก็บเครื่องคอมพิวเตอร์ในกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์ เพื่อป้องกันการกระแทกกระเทือนในระหว่างการเดินทาง ไม่ควรวางอุปกรณ์ทิ้งไว้ในที่สาธารณะโดยที่ไม่มีคนดูแล (Unattended) ต้องมีการจัดเก็บสื่อที่ใช้ในการเก็บข้อมูลไว้อย่างปลอดภัย เมื่อไม่มีการใช้งาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

- การป้องกันการเข้าถึงระบบ (Logical) อุปกรณ์ควรได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต สำหรับเครื่องคอมพิวเตอร์แบบพกพาต้องควบคุมกำหนดการเข้าถึงด้วย User and Password ข้อมูลสารสนเทศของสมาคมสโมสรนักลงทุนที่อยู่ในเครื่องคอมพิวเตอร์แบบพกพาจะต้องทำการสำรองข้อมูลไว้อย่างสม่ำเสมอ พนักงานที่ทำงานจากที่บ้านหรือทำงานนอกสถานที่จัดเก็บเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้งานไว้ในที่ปลอดภัย และจะต้องปฏิบัติตามข้อกำหนดในการทำลายสื่อบันทึกข้อมูลที่หมดอายุการใช้งานหรือชำรุดตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล อย่างเคร่งครัด ทั้งนี้สื่อบันทึกข้อมูลที่สามารถทำลายได้จะต้องได้รับอนุมัติการทำลายจากผู้มีอำนาจก่อนทุกครั้ง หากทำลายสื่อบันทึกข้อมูล โดยผู้ให้บริการภายนอก จะต้องมีการทำสัญญาข้อตกลงเรื่องการรักษาความลับ
- การเชื่อมต่อกับระบบเครือข่ายให้มีความปลอดภัย (Secure Connection) กำหนดให้การเชื่อมต่อระหว่างระบบเครือข่ายของสมาคมสโมสรนักลงทุน และเครื่องคอมพิวเตอร์แบบพกพาต้องเชื่อมต่อผ่านระบบ Virtual Private Network หรือโปรแกรมที่ได้รับอนุญาตเท่านั้น เครื่องคอมพิวเตอร์แบบพกพาจะต้องอัปเดต Antivirus ให้เป็นปัจจุบันที่สุด ก่อนที่จะเชื่อมต่อเข้ากับระบบเครือข่าย ควรดำเนินการอัปเดต Patch ที่เครื่องคอมพิวเตอร์แบบพกพาก่อนที่จะเชื่อมต่อกับระบบเครือข่าย
- ควรอัปเดต Antivirus และ Virus Signature ให้เป็นปัจจุบันอยู่เสมอ

การใช้งานคอมพิวเตอร์แบบพกพาในการปฏิบัติงานจากภายนอกและการแก้ไขปัญหาจากระยะทางไกล

- การปฏิบัติงานจากภายนอกอนุญาตให้บุคลากรของสมาคม ที่จำเป็นต้องปฏิบัติงานจากภายนอกสมาคม ให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy) และวิธีปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศตามแบบฟอร์ม HR-2FM-01 การลงทะเบียนและเพิกถอนสิทธิผู้ใช้ (User Registration-De Registration Form) เพื่อให้มีการตรวจพิสูจน์ตัวตนและควบคุมการทำงานจากระยะไกล โดยการแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินเทอร์เน็ตภายในที่ใช้งานในสมาคม และใช้งานเครือข่ายส่วนตัวเสมือน (Virtual Private Network)
- การแก้ไขปัญหาจากระยะไกลอนุญาตให้บุคลากรของสมาคม สามารถทำการเปิดโปรแกรมรีโมทเพื่อให้พนักงานสารสนเทศเข้าตรวจสอบ เมื่อดำเนินการแล้วเสร็จให้ทำการปิดทันที

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

พนักงานอาจถูกเพิกถอนสิทธิ์การเข้าใช้ระบบปฏิบัติงานคอมพิวเตอร์และอุปกรณ์การสื่อสารต่าง ๆ ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ของสมาคมสโมสรนักลงทุน เนื่องด้วยเหตุผลต่าง ๆ ได้แก่ การคุกคามระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ การดัดแปลงหรือเปิดเผยข้อมูลลับ เช่น ไฟล์ข้อมูลหรือเนื้อหาที่ปรากฏในจดหมาย โดยไม่ได้รับความยินยอมจากผู้ใช้นอกจากนี้ยังหมายถึง การดัดแปลงหรือการทำลายข้อมูลขององค์กร หรือการใช้ระบบเครือข่ายของสมาคมสโมสรนักลงทุนในลักษณะที่ขัดแย้งกับแนวทางที่ได้วางไว้

ฝ่ายเทคโนโลยีสารสนเทศสามารถเพิกถอนหรือยกเลิกการเข้าใช้ระบบได้ตลอดเวลา ทั้งนี้เป็นไปเพื่อรักษาความปลอดภัยของข้อมูลและเพื่อปกป้องสิทธิประโยชน์ของสมาคมสโมสรนักลงทุน พนักงานสามารถขออุทธรณ์การเพิกถอนสิทธิ์เข้าใช้ระบบโดยยื่นต่อผู้จัดการสมาคม ฯ ในกรณีที่มีการใช้ระบบคอมพิวเตอร์ในทางที่ก่อให้เกิดความเสียหาย ผู้ก่อเหตุต้องรับผิดชอบและอาจถูกดำเนินการทางวินัย ซึ่งผู้กระทำผิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การกู้คืนข้อมูล และระบบคอมพิวเตอร์ที่ได้รับความเสียหาย

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการจัดหาแผนกู้คืนข้อมูลที่ได้รับ ความเสียหายที่มีประสิทธิภาพและต้นทุนเหมาะสม แผนนี้มีวัตถุประสงค์เพื่อให้อุปกรณ์และระบบคอมพิวเตอร์ที่สนับสนุนกิจกรรมสำคัญๆ ในการดำเนินธุรกิจขององค์กรสามารถกู้คืนมาได้ตามที่ต้องการ งานที่เกี่ยวข้องกับแผนกู้คืนจะต้องสอดคล้องกับแนวทางที่กำหนดไว้ และความต่อเนื่องของธุรกิจของสมาคมสโมสรนักลงทุน

ขอบเขต

แผนงานนี้จะครอบคลุมการกู้คืนการประมวลผลข้อมูลสำคัญ ๆ ที่เกิดขึ้นในเครื่องแม่ข่ายของฝ่ายเทคโนโลยีสารสนเทศและเครื่องแม่ข่ายที่ห้องเซิร์ฟเวอร์กลาง กรณีเกิดความเสียหายขึ้น และส่งผลกระทบต่อโครงสร้างระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน

แนวทาง

กลยุทธ์ที่ใช้ในแผนกู้คืนข้อมูลที่ได้รับ ความเสียหาย มีดังต่อไปนี้

- ดูแลให้มีอุปกรณ์หรือระบบคอมพิวเตอร์สำรองการทำงาน กรณีที่อุปกรณ์หรือระบบหลักหยุดทำงานกะทันหัน
- มีการสำรองข้อมูลอย่างสม่ำเสมอ
- จัดทำทะเบียนรายการอุปกรณ์ โปรแกรม และข้อตกลงในการบำรุงรักษา รวมถึงนิติบุคคลที่เข้ามาดูแล
- จัดระบบรักษาความปลอดภัย เพื่อปกป้องทรัพย์สินบนระบบเครือข่ายให้พ้นจากการถูกลักขโมย การสับเปลี่ยน และป้องกันมิให้ความลับขององค์กรรั่วไหล

การสำรองข้อมูล

ระบบทุกระบบและข้อมูลของผู้ใช้งานในเครื่องแม่ข่ายจะได้รับการสำรองไว้เป็นประจำทุกวัน และสำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลง โดยข้อมูลสำรองนี้จะถูกจัดเก็บไว้ในที่ที่ปลอดภัย และทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง สำหรับหน่วยงานที่ต้องการการสำรองข้อมูลที่แตกต่างเพิ่มเติมจากที่กล่าวข้างต้นตามข้อบังคับของกฎหมาย ฝ่ายเทคโนโลยีสารสนเทศจะได้ปรึกษาร่วมกับแต่ละหน่วยงานเพื่อวางแผนสำรองข้อมูลให้เป็นกรณีพิเศษต่อไป

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การกู้คืนข้อมูลบนเครื่องแม่ข่ายคอมพิวเตอร์

ในกรณีเหตุสุดวิสัยที่ทำให้อุปกรณ์และโปรแกรมคอมพิวเตอร์ของแม่ข่ายเสียหายจนไม่สามารถใช้งานได้ ฝ่ายเทคโนโลยีสารสนเทศจะนำข้อมูลสำรองชุดล่าสุดกลับมาติดตั้งให้ใช้งานบนเครื่องแม่ข่ายที่กู้ขึ้นมาใหม่

การกู้คืนข้อมูลบนเครื่องลูกข่ายคอมพิวเตอร์

การสำรองข้อมูลบนเครื่องลูกข่ายเป็นความรับผิดชอบของผู้ใช้งาน ในกรณีที่มีความเสียหายของแฟ้มข้อมูลบนเครื่องลูกข่าย ฝ่ายเทคโนโลยีสารสนเทศจะไม่ถือว่าเป็นความรับผิดชอบที่จะกู้ข้อมูลคืน แต่จะติดตั้งโปรแกรมระบบเพื่อใช้งานต่อไป

การตอบสนองกรณีฉุกเฉิน

แผนงานในรายละเอียดเพื่อกู้คืนข้อมูลที่เสียหายสามารถแจกแจงได้ เมื่อเหตุการณ์ดังกล่าวเกิดขึ้น ทั้งนี้ขึ้นอยู่กับลักษณะของความเสียหาย เวลาที่เกิดความเสียหาย และระยะเวลาโดยประมาณที่เกิดการหยุดชะงักของระบบ

ความรับผิดชอบ

- หน่วยงานบริการระบบเครือข่ายคอมพิวเตอร์ และหน่วยงานบริการระบบคอมพิวเตอร์ ของฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการพัฒนา ปรับปรุง และทบทวนกิจกรรมที่เกี่ยวข้องกับการกู้คืนข้อมูล และระบบคอมพิวเตอร์ที่ได้รับความเสียหาย
- หน่วยงานบริการโปรแกรมระบบ รับผิดชอบในการพัฒนา ปรับปรุง และทบทวนขั้นตอนในการกู้คืนที่เกี่ยวข้องกับโปรแกรมระบบ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศหรือเจ้าของโครงการรับผิดชอบในการระบุรายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศตั้งแต่เริ่มต้น จนถึงสิ้นสุดโครงการ เพื่อให้การดำเนินงานโครงการมีความมั่นคงปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้น

แนวทาง

แนวทางที่ใช้ในการดำเนินงานโครงการด้านความมั่นคงปลอดภัยสารสนเทศ มีดังต่อไปนี้

- ต้องระบุรายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศ
- ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัย ตั้งแต่ระยะเริ่มต้น ตลอดจนจบโครงการอย่างสม่ำเสมอ ทั้งที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก เช่น ความปลอดภัยของด้านการสื่อสารภายในและภายนอกได้รับการพิจารณาและปฏิบัติของโครงการ รวมถึงดำเนินการจัดการความเสี่ยง
- ต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัย เช่น ข้อกำหนดด้านความปลอดภัยของแอปพลิเคชัน ข้อกำหนดสำหรับการปฏิบัติตามสิทธิ์ในทรัพย์สินทางปัญญา ในช่วงเริ่มต้นของโครงการ
- ต้องมีการทบทวนและติดตามแผนการจัดการความเสี่ยงที่เกี่ยวข้องกับโครงการ รวมถึงมีการวัดผลการจัดการความเสี่ยงดังกล่าว

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การบริหารจัดการ Configuration

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการบริหารจัดการ Configuration เพื่อเป็นการตั้งค่าด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งในฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่าย อย่างถูกต้องตามการตั้งค่าที่กำหนด และไม่ได้ถูกเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

แนวทาง

แนวทางการบริหารจัดการ Configuration มีดังต่อไปนี้

- ต้องจัดให้มีมาตรฐานในการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Configuration Baseline) สำหรับเครื่องแม่ข่าย เครื่องลูกข่าย และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ โดยจัดทำเป็นเอกสาร นำไปปฏิบัติ ฝ่้าติดตามและทบทวนอย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบให้มั่นใจว่ามีการกำหนดค่าการรักษาความมั่นคงปลอดภัยที่จำเป็น
- ต้องกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ เพื่อสามารถตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ การเปลี่ยนแปลงแก้ไข Baseline ของอุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน ต้องผ่านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเพียงพอ และได้รับการอนุมัติก่อนดำเนินการ
- ต้องมีการจัดเก็บการเปลี่ยนแปลงของการกำหนดค่าระบบของทุกอุปกรณ์และระบบงาน โดยมีการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอ

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

การบริหารจัดการคลาวด์

หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการบริหารจัดการคลาวด์ เพื่อให้มีกระบวนการที่ชัดเจนสำหรับการเลือกใช้บริการคลาวด์ การจัดการการใช้งาน การควบคุมการเข้าถึง และการยกเลิกการใช้งานให้สอดคล้องกับข้อกำหนดความมั่นคงปลอดภัยของข้อมูลของสมาคมฯ

แนวทาง

แนวทางการบริหารจัดการคลาวด์ มีดังต่อไปนี้

- ต้องมีการคัดเลือกประเภท รูปแบบการติดตั้งคลาวด์ โดยจะต้องคำนึงถึงปริมาณข้อมูล ความเร็วของการรับส่งข้อมูลระหว่างระบบ และความเชี่ยวชาญของผู้รับผิดชอบ
- ต้องกำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการใช้และการบริหารจัดการการใช้บริการคลาวด์
- ต้องมีกำหนดสิทธิการเข้าถึงระบบคลาวด์ และควรกำหนดให้เข้าถึงได้น้อยที่สุดตามหน้าที่ที่จำเป็นเท่านั้น
- ต้องมีการติดตามเหตุการณ์การละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดกับระบบคลาวด์ และแจ้งเหตุเมื่อเกิดความผิดปกติ รวมถึงตอบสนองต่อเหตุการณ์ที่ไม่ปกติ
- ต้องมีการติดตาม ตรวจสอบ และประเมินผลระหว่างการใช้บริการคลาวด์ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- กรณีมีการยกเลิกหรือย้ายระบบคลาวด์ต้องจัดทำแผน รวมถึงประเมินความเป็นไปได้ของแผนการยกเลิกหรือย้ายการใช้บริการ และต้องดำเนินการให้มั่นใจว่าข้อมูลได้ทำการสำรองก่อนการยกเลิก และข้อมูลทุกส่วนของระบบที่เกี่ยวข้องทั้งหมดที่อยู่บนคลาวด์ ถูกทำลายโดยไม่สามารถกู้คืนกลับมาได้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

เอกสารแนบ 1

ACKNOWLEDGEMENT STATEMENT

(ตัวอย่าง)

ข้าพเจ้าได้อ่านเอกสารและทำความเข้าใจนโยบายเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน และยืนยันที่จะปฏิบัติตามเงื่อนไขและ/หรือกฎเกณฑ์ที่มีระบุในเอกสารดังกล่าว ข้าพเจ้าเข้าใจเช่นกันว่า การเซ็นรับรองในเอกสารนี้ไม่ถือว่าการทำสัญญาหรือถูกทำให้เข้าใจว่าเป็นการทำสัญญาในอนาคต แต่เป็นการรับรองว่าข้าพเจ้าได้อ่านและเข้าใจนโยบายและกฎเกณฑ์ต่าง ๆ ที่ได้ระบุในเอกสารดังกล่าวแล้ว

ชื่อ : _____

ลายเซ็น : _____

วันที่ : _____

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

เอกสารแนบ 2

MUTUAL CONFIDENTIALITY AGREEMENT

(ตัวอย่าง)

ระหว่าง

สมาคมสโมสรนักลงทุน

1 อาคารทีพีแอนด์ที ชั้น 12 ถนนวิภาวดี-รังสิต

แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

และ

เพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับของทั้งสองหน่วยงานในระหว่างการหารือในประเด็นทางธุรกิจหรือระบบเทคโนโลยีสารสนเทศระหว่างกัน ทั้งสองฝ่ายมีข้อตกลงดังต่อไปนี้

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

1. คำจำกัดความ

- 1.1 “ข้อมูลข่าวสารที่เป็นความลับ” หมายถึงข้อมูลทั้งทางวาจาหรือเอกสารหรือข้อมูลอิเล็กทรอนิกส์ที่มาจากผู้เปิดเผย ทั้งนี้รวมถึงเอกสารและ/หรือ ข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องเช่น โปรแกรมซอฟต์แวร์ ข้อมูลไฟล์อิเล็กทรอนิกส์ต่างๆ คู่มือผู้ใช้งานและคู่มืออื่นๆ
- 1.2 “ผู้เปิดเผย” หมายถึง องค์กรในสัญญาที่ เป็นผู้ให้ข้อมูล
- 1.3 “ผู้รับ” หมายถึง องค์กรให้สัญญาที่ เป็นผู้รับข้อมูล
- 1.4 “โครงการ” หมายถึง _____

2. หน้าที่ของผู้รับ

- 2.1 ผู้รับจะใช้ข้อมูลข่าวสารที่เป็นความลับเพื่อวัตถุประสงค์เฉพาะโครงการนั้นเท่านั้น และจะไม่ใช้เพื่อวัตถุประสงค์อื่น ๆ ยกเว้นจะได้รับคามยินยอมเป็นลายลักษณ์อักษร
- 2.2 ผู้รับตกลงจะไม่เปิดเผยข้อมูลข่าวสารที่เป็นความลับที่ได้รับจากผู้เปิดเผยในรูปแบบใด ๆ ก็ตาม ทั้งนี้ข้อมูลดังกล่าวจะต้องไม่อยู่ภายใต้ข้อ 2.3
- 2.3 ข้อตกลงนี้ไม่ผูกมัดเกี่ยวกับข้อมูลข่าวสารที่เป็นความลับกรณี (ก) ข้อมูลดังกล่าวได้รับรู้โดยสาธารณะอันเนื่องมาจากทางอื่นที่นอกเหนือจากผู้รับ หรือ (ข) ข้อมูลดังกล่าวเป็นข้อมูลที่ได้รับได้ข้อมูลมาจากทางอื่นก่อนที่จะได้รับจากผู้เปิดเผย หรือ (ค) ข้อมูลดังกล่าวเป็นข้อมูลที่ได้รับได้จากองค์กรอื่นซึ่งไม่เป็นการละเมิดข้อตกลงเกี่ยวกับข้อมูลที่เป็นความลับจากผู้เปิดเผย หรือ (ง) ข้อมูลดังกล่าวได้มาหรือคิดค้นมา โดยอยู่นอกเหนือจากข้อมูลที่อยู่ในข้อตกลงนี้ หรือ (จ) ข้อมูลดังกล่าวจำเป็นต้องเปิดเผยโดยข้อบังคับทางกฎหมาย
- 2.4 ข้อมูลข่าวสารที่เป็นความลับที่ได้รับมาเป็นทรัพย์สินของผู้เปิดเผยข้อมูล ในกรณีที่ผู้เปิดเผยข้อมูลต้องการข้อมูลดังกล่าวกลับคืนโดยแจ้งมาเป็นลายลักษณ์อักษร ผู้รับจะต้องส่งข้อมูลดังกล่าวคืน หรือทำลายข้อมูลดังกล่าว ซึ่งรวมทั้งสำเนาต่าง ๆ ตามที่ผู้เปิดเผยข้อมูลร้องขอมา
- 2.5 ทั้งสองฝ่ายยอมรับว่าข้อตกลงนี้ไม่มีผลต่อการโอนย้ายทรัพย์สินทางปัญญาระหว่างฝ่ายใดฝ่ายหนึ่ง

 สมาคมสโมสรนักลงทุน Investor Club Association	เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management) รหัส : IT-1PC-01 วันที่ประกาศใช้ : 3 ธันวาคม 2567
--	--

3. ข้อตกลงทั่วไป

- 3.1 ข้อตกลงนี้ไม่ก่อให้เกิดความสัมพันธ์ทางธุรกิจอื่นใด นอกเหนือจากการเข้าใจร่วมกันในเรื่องการรักษาความลับของข้อมูล
- 3.2 ผู้รับข้อมูลยอมรับว่าความเสียหายทางการเงินอาจไม่เพียงพอต่อการละเมิดข้อตกลงดังกล่าวและตกลงว่า ผู้เปิดเผยข้อมูลสามารถเสนอทางเลือกหรือแนวทางจ่ายค่าเสียหายในกรณีที่มีการละเมิดข้อตกลงดังกล่าวขึ้น
- 3.3 ผู้รับข้อมูลยอมรับว่าข้อมูลที่ได้รับจากผู้เปิดเผยข้อมูลไม่ได้เป็นการรับประกันหรือแสดงให้เห็นว่าข้อมูลดังกล่าวมีความถูกต้องหรือครบถ้วนสมบูรณ์ของข้อมูลที่เป็นความลับดังกล่าว
- 3.4 ผู้รับข้อมูลจะไม่นำส่งข้อมูลดังกล่าวออกนอกประเทศไทยไม่ว่าจะเป็นทางตรงหรือทางอ้อม ยกเว้นจะได้รับการยินยอมเป็นลายลักษณ์อักษรจากผู้เปิดเผยข้อมูล
- 3.5 ผู้รับข้อมูลจะต้องดำเนินการลบข้อมูลที่เป็นข้อมูล Sensitive ภายในระยะเวลา 3 เดือนหลังจากสิ้นสุดระยะเวลาการดำเนินงานของโครงการและรายงานกลับ เพื่อให้ทราบว่าการดำเนินการแล้วตามมาตรฐาน
- 3.6 การเพิ่มเติมหรือแก้ไขข้อตกลงนี้จะต้องจัดทำเป็นลายลักษณ์อักษรพร้อมทั้งเซ็นรับรองโดยทั้งสองฝ่าย
- 3.7 ข้อตกลงนี้ถูกจัดทำขึ้นภายใต้กฎหมายข้อบังคับในประเทศไทย
- 3.8 ทั้งสองฝ่ายยอมรับว่า การเซ็นยินยอมในข้อตกลงนี้และดำเนินการส่งข้อตกลงทางโทรสารเพื่อให้อีกฝ่ายหนึ่งได้รับรู้เป็นการกระทำที่ยอมรับได้และถือว่ามีผลผูกพันได้ทันที

รับรองโดย _____

รับรองโดย สมาคมสโมสรนักลงทุน

ลงนาม: _____

ลงนาม: _____

ชื่อ: _____

ชื่อ: _____

ตำแหน่ง: _____

ตำแหน่ง: _____

วันที่: _____

วันที่: _____

การตรวจสอบการตั้งค่าตามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (Secure Configuration Baseline)

หมายเลขเอกสาร : IT-2FM-10 หมายเลขการปรับปรุงเอกสาร : 1.0 ระดับชั้น : ใช้ภายใน วันที่บังคับใช้ : 10 ม.ค. 68 วันที่ทบทวนข้อมูล : xx/xx/xx

* หมายถึง ข้อกำหนดดังกล่าวเป็นข้อแนะนำตามที่นโยบายกำหนด
/ หมายถึง บังคับให้มีการตั้งค่าตามข้อกำหนด | ○ หมายถึง ไม่บังคับการตั้งค่า

เอกสารแนบ 1.8

No.	รายละเอียดนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ	IT Policy	Server	Network Device/ Network Security Device	Client	Application
1	* กำหนดให้รหัสผ่านมีความยาวไม่ต่ำกว่า 8 ตัวอักษร ประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว ตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กอย่างน้อย 1 ตัว และตัวเลขอย่างน้อย 1 ตัว	การรักษาความปลอดภัย	/	/	/	/
2	* กำหนดให้เปลี่ยนรหัสผ่านทุก 90 วัน	การรักษาความปลอดภัย	/	/	/	/
3	รหัสผ่านที่เปลี่ยนใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม 10 ครั้งล่าสุด		○	○	○	
4	ล็อกสิทธิ์การเข้าถึงของผู้ใช้ 30 นาที เมื่อมีการป้อนรหัสผ่านผิดเกิน 5 ครั้ง		○	○	○	
5	* กำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที	การรักษาความปลอดภัย	/	/		/
6	* ติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัส	การใช้อุปกรณ์คอมพิวเตอร์	/		/	
7	ตรวจสอบการอัปเดตระบบปฏิบัติการ และแพตช์		○	○	○	
8	ตั้งสัญญาณนาฬิกาของระบบเทคโนโลยีสารสนเทศให้ตรงตามมาตรฐานสากล		○	○	○	
9	ปิดการใช้งาน Protocol ที่ไม่มีการเข้ารหัส เช่น "Telnet" และ "HTTP" เว้นแต่จำเป็นสำหรับการดำเนินงาน		○	○		/
10	ต้องจัดให้มีการบันทึกกิจกรรมของผู้ใช้งานระบบสารสนเทศ อุปกรณ์เครือข่าย และเหตุการณ์ความปลอดภัยต่าง ๆ (Logs)		○	○	○	○
11	* เครื่องคอมพิวเตอร์ต้องถูกล็อกหน้าจอเมื่อไม่มีการใช้งานเป็นเวลา 15 นาที	การรักษาความปลอดภัย			/	
12	ตรวจสอบซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ติดตั้ง ในเครื่องคอมพิวเตอร์ที่ใช้งานของ IC				○	

"ผู้ดำเนินการตรวจสอบ"

ลงชื่อ
ตำแหน่ง (.....)
วันที่ :

"ผู้อนุมัติการตรวจสอบ"

ลงชื่อ
ตำแหน่ง (.....)
วันที่ :

***Reference from CIS Controls V8.1