สมาคมสโมสรนักลงทุน
Investor Club Association

# นโยบายและการบริหารเทคโนโลยีสารสนเทศ

# (IT Policy and Management)

| | |
|---|---|
| **รหัสเอกสาร:** | IT-1PC-01 |
| **หมายเลขปรับปรุงเอกสาร:** | 7.0 |
| **วันที่เอกสารมีผลบังคับใช้:** | 30 กรกฎาคม 2568 |
| **เจ้าของเอกสาร:** | ฝ่ายเทคโนโลยีสารสนเทศ |

| สมาคมสโมสรนักลงทุน Investor Club Association | **เรื่อง : นโยบายและการบริหารเทคโนโลยีสารสนเทศ (IT Policy and Management)**<br>**รหัส : IT-1PC-01**<br>**วันที่ประกาศใช้ : 30 กรกฎาคม 2568** |
|---|---|

**ลายเซ็นรับรองเอกสาร**

| หน้าที่ | ชื่อ-นามสกุล | ตำแหน่ง | ลายเซ็น | วันที่ |
|---|---|---|---|---|
| ผู้จัดทำ | สมโภช เผือกจันทึก | หัวหน้าแผนก บริหารระบบ |  | 25 ก.ค. 2568 |
| ผู้ทบทวน | สิริวรรณ ฉลากรไชยา | หัวหน้าฝ่าย เทคโนโลยีสารสนเทศ |  | 25 ก.ค. 2568 |
| ผู้อนุมัติ | กรองกนก มานะกิจจงกล | ผู้จัดการ สมาคมสโมสรนักลงทุน |  | 25 กรกฎาคม 2568 |

**ประวัติการปรับปรุงเอกสาร**

| หมายเลขปรับปรุงเอกสาร (version): | วันที่ปรับปรุงเอกสาร | ปรับปรุงโดย (ชื่อ-สกุล) | คำอธิบายและเหตุผลในการแก้ไข |
|---|---|---|---|
| 2.0 | 4 พ.ค. 64 | สิริวรรณ ฉลากรไชยา | แก้ไขเนื้อหาให้มีความชัดเจนยิ่งขึ้น<br>1. การรักษาความปลอดภัย - แนวทาง<br>2. การใช้อินเตอร์เน็ต<br>3. การใช้อุปกรณ์คอมพิวเตอร์ - แนวทาง<br>4.การใช้คอมพิวเตอร์แบบพกพาและการเชื่อมต่อระบบเครือข่าย<br>5.แก้ไข ผู้ให้ข้อมูล เป็น ผู้เปิดเผยข้อมูลให้ถูกต้องตามคำจำกัดความ |
| 3.0 | 26 ก.ค. 66 | สิริวรรณ ฉลากรไชยา | เพิ่มเติมเนื้อหา<br>1.การจัดกลุ่มทรัพย์สิน (Asset Grouping)<br>2.การใช้งานคอมพิวเตอร์แบบพกพาในการปฏิบัติงานจากภายนอกและการแก้ไขปัญหาจากระยะทางไกล |

| หมายเลขปรับปรุงเอกสาร (version): | วันที่ปรับปรุงเอกสาร | ปรับปรุงโดย (ชื่อ-สกุล) | คำอธิบายและเหตุผลในการแก้ไข |
|---|---|---|---|
| 4.0 | 20 พ.ย. 66 | สิริวรรณ ฉลากรไชยา | เพิ่มเติมเนื้อหา เอกสารแนบ 2 ข้อ 3 ข้อตกลงทั่วไป<br>เพิ่มข้อ 3.5 ผู้รับข้อมูลจะต้องดำเนินการลบข้อมูลที่เป็นข้อมูล Sensitive ภายในระยะเวลา 3 เดือนหลังจากสิ้นสุดระยะเวลาการดำเนินงานของโครงการและรายงานกลับเพื่อให้ทราบว่าดำเนินการแล้วตามมาตรฐาน |
| 5.0 | 25 เม.ย. 67 | สิริวรรณ ฉลากรไชยา | 1.นโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy)<br>1.1 <u>แก้ไขข้อความ</u><br>● ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ<br><u>เป็น</u><br>● ต้องมีการกำหนดสิทธิ์ผู้ใช้ในการเข้าถึงระบบและข้อมูลสารสนเทศ และต้องมีการกำหนดสิทธิ์ผู้ใช้งานในระดับสูง<br>1.2 <u>เพิ่มข้อความ</u><br>● ในการเข้าใช้งานของผู้ใช้งานในระดับสูงจะต้องมีการร้องขอใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูงในแต่ละครั้ง<br>● พนักงานที่มีความประสงค์ร้องขอเบิกใช้งานบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Account) ต้องจัดทำแบบฟอร์มร้องขอบัญชีผู้ใช้งานที่มีสิทธิ์สูง (Privileged Request Form) (IT-2FM-07) |

| หมายเลขปรับปรุงเอกสาร (version): | วันที่ปรับปรุงเอกสาร | ปรับปรุงโดย (ชื่อ-สกุล) | คำอธิบายและเหตุผลในการแก้ไข |
|---|---|---|---|
| | | | ● ผู้ดูแลระบบบันทึกทะเบียนบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privileged Account Inventory) (IT-2FM-09) สำหรับใช้ในการอ้างอิง<br>2. สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน<br>2.1 <u>แก้ไขข้อความ</u><br>● รายชื่อผู้ใช้งานจะถูกตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานออก<br><u>เป็น</u><br>● รายชื่อผู้ใช้งานจะถูกตั้งค่าปิดการใช้งานบัญชีล่วงหน้าและตัดสิทธิการเข้าระบบโดยฝ่ายเทคโนโลยีสารสนเทศทันทีเมื่อได้รับเอกสารแจ้งพนักงานพ้นสภาพ (User Account Termination) เป็นลายลักษณ์อักษรจากแผนกบุคคล และฝ่ายเทคโนโลยีสารสนเทศสามารถที่จะระงับรายชื่อผู้ใช้งานพร้อมข้อมูลของพนักงานโดยมีผล ณ วันที่พนักงานลาออก<br><u>เพิ่มข้อความ</u> |

| หมายเลขปรับปรุงเอกสาร (version): | วันที่ปรับปรุงเอกสาร | ปรับปรุงโดย (ชื่อ-สกุล) | คำอธิบายและเหตุผลในการแก้ไข |
|---|---|---|---|
| | | | • ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการตรวจสอบวันที่เข้าสู่ระบบล่าสุดของพนักงานที่ลาออก (Check Last Logon Date) ในกรณีที่มีการแจ้งลาออกล่าช้าหรือมีการเลิกจ้างฐานละทิ้งหน้าที่ โดยระบุในส่วนรายละเอียดเพิ่มเติมของแบบฟอร์มการเพิกถอนสิทธิ์ใช้งานบัญชีผู้ใช้ พร้อมบันทึกหลักฐานการตรวจสอบ<br>• ฝ่ายเทคโนโลยีสารสนเทศกำหนด Session Timeout ในการใช้งานระบบเป็นมาตรฐานที่ระยะเวลา 20 นาที |
| 6.0 | 29 พ.ย. 67 | สมโภช เผือกจันทึก | 1. แก้ไขข้อมูล “ศูนย์ข้อมูล” เป็น “ห้องเซิร์ฟเวอร์”<br>2. การลงทะเบียนทรัพย์สิน เพิ่มเติม ประเภทของทรัพย์สิน 2 รายการ ได้แก่ Process Asset และ Site Asset<br>3. สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน เพิ่มเติม ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของสมาคม ฯ ได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง<br>4. เพิ่มเติมข้อความ การแบ่งแยกระบบสารสนเทศ เพื่อลดความผิดพลาดหรือผลกระทบอันเกิดจากการดำเนินการ |

| หมายเลขปรับปรุงเอกสาร (version): | วันที่ปรับปรุงเอกสาร | ปรับปรุงโดย (ชื่อ-สกุล) | คำอธิบายและเหตุผลในการแก้ไข |
|---|---|---|---|
| | | | ทดสอบ ควรมีการแยกระบบสารสนเทศที่ให้บริการจริง ออกจากระบบสารสนเทศที่ใช้ในการพัฒนา และทดสอบ (เฉพาะระบบที่สามารถดำเนินการได้)<br>5. เพิ่ม การจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and Operations Management) ในหน้าที่ความรับผิดชอบของผู้ใช้ในหัวข้อ ดังนี้<br>● ข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์หรือส่งออกไปภายนอกองค์กรต้องจัดให้มีการเข้ารหัสข้อมูล<br>● การจัดทำ การจัดเก็บ การส่งต่อ ลบทำลายข้อมูล จะต้องดำเนินการตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล<br>● ต้องควบคุมให้มีมาตรการการปิดบังข้อมูลสารสนเทศเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน<br>6. แนวทางการเข้าสู่ห้องเซิร์ฟเวอร์ เพิ่มเติมข้อความ ดังนี้<br>6.1 จะต้องกรอกแบบคำขออนุญาตเข้าพื้นที่ห้องเซิร์ฟเวอร์<br>6.2 ห้ามนำวัตถุระเบิด เชื้อเพลิง วัสดุติดเพลิงง่าย อาวุธ สารเคมี หรือสิ่งอื่น |

| หมายเลขปรับปรุงเอกสาร (version): | วันที่ปรับปรุงเอกสาร | ปรับปรุงโดย (ชื่อ-สกุล) | คำอธิบายและเหตุผลในการแก้ไข |
|---|---|---|---|
| | | | ใดที่อาจก่อให้เกิดความเสียหายทั้งต่อชีวิตและทรัพย์สิน เข้ามาบริเวณห้องเซิร์ฟเวอร์<br>7. <u>เพิ่มข้อความ</u> ในหัวข้อการควบคุมการใช้งานระบบเครือข่าย ดังนี้<br>● ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของสมาคม ฯ ให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับอาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับ (ฉบับที่ 2) พ.ศ. 2560<br>8. <u>เพิ่มข้อความ</u> ในหัวข้อการใช้คอมพิวเตอร์แบบพกพาและการเชื่อมต่อระบบเครือข่าย ดังนี้<br>● การทำลายสื่อบันทึกข้อมูล โดยผู้ให้บริการภายนอก จะต้องมีการทำสัญญาข้อตกลงเรื่องการรักษาความลับ<br>9. <u>เพิ่มข้อความ</u> ในหัวข้อการสำรองข้อมูล ดังนี้<br>● สำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลง โดยข้อมูลสำรองนี้จะถูกจัดเก็บไว้ในที่ที่ปลอดภัย<br>● ทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง |

| หมายเลขปรับปรุงเอกสาร (version): | วันที่ปรับปรุงเอกสาร | ปรับปรุงโดย (ชื่อ-สกุล) | คำอธิบายและเหตุผลในการแก้ไข |
|---|---|---|---|
| | | | 10. เพิ่มหัวข้อการจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ<br>11. เพิ่มหัวข้อการบริหารจัดการ Configuration<br>12. เพิ่มหัวข้อการบริหารจัดการคลาวด์ |
| 7.0 | 25 ก.ค. 68 | สมโภช เผือกจันทึก | 1. เพิ่มหัวข้อ นโยบายการใช้ปัญญาประดิษฐ์ภายในสมาคมสโมสรนักลงทุน<br>2. ปรับแก้ไขสารบัญ<br>3. แก้ไขเอกสารแนบ 2 หัวข้อ 3. ข้อตกลงทั่วไป ในส่วนที่เกี่ยวข้องกับข้อตกลงช่องทางที่กำหนด ในข้อ 3.8<br><u>เดิม</u> ทางโทรสาร<br><u>แก้ไขเป็น</u> การส่งด้วยมือ ทางไปรษณีย์ หรือ ทางอิเล็กทรอนิกส์ |

# สารบัญ

**เรื่อง** **หน้า**

## บทนำ

นโยบายเทคโนโลยีสารสนเทศที่จัดทำขึ้นครอบคลุมระบบการปฏิบัติงานคอมพิวเตอร์ ระบบโทรศัพท์ รวมถึงอุปกรณ์ต่าง ๆ ในระบบเครือข่ายคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน เพื่อให้บริการพนักงานและบริษัทภายนอก โดยคำนึงถึงความรับผิดชอบด้านกฎหมาย และได้รับความไว้วางใจจากภาคธุรกิจหลากหลายประเภท

เอกสารฉบับนี้จะกล่าวถึงนโยบายระบบเทคโนโลยีสารสนเทศขององค์กร หน้าที่ความรับผิดชอบของผู้ใช้ระบบคอมพิวเตอร์ และฝ่ายเทคโนโลยีสารสนเทศ

## วัตถุประสงค์

เพื่อวางแนวนโยบายระบบเทคโนโลยีสารสนเทศให้กับสมาคมสโมสรนักลงทุน และเพื่อให้ฝ่ายต่าง ๆ รวมทั้งหน่วยงานที่เกี่ยวข้องได้ทราบถึงแนวทางการดำเนินงานของพนักงานฝ่ายเทคโนโลยีสารสนเทศและพนักงานสมาคมสโมสรนักลงทุน

## ขอบเขตและความรับผิดชอบ

การบริหารการใช้ข้อมูลระบบสารสนเทศภายในองค์กรเป็นความรับผิดชอบหลักของแต่ละฝ่ายในสมาคม ฯ อย่างไรก็ตาม ฝ่ายเทคโนโลยีสารสนเทศยังคงมีอำนาจหน้าที่ควบคุมดูแลระบบสารสนเทศของฝ่ายต่าง ๆ ในองค์กรโดยรวม

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบงานด้านการบริหารจัดการนโยบายในระบบเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน ทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้มีอำนาจหน้าที่ในการตรวจสอบมอบหมาย และประสานงานในการปฏิบัติงานด้านต่าง ๆ ในระบบเทคโนโลยีสารสนเทศของทั้งองค์กร

**ระเบียบว่าด้วยขอบเขตอำนาจหน้าที่และความรับผิดชอบ**

สมาคมสโมสรนักลงทุนมีความต้องการให้อุปกรณ์และการใช้งานในระบบเทคโนโลยีสารสนเทศขององค์กรคงสภาพดี และพร้อมใช้งานในเครือขององค์กร 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

เป็นที่ทราบว่า บทบาทของฝ่ายเทคโนโลยีสารสนเทศในองค์กรนั้นแตกต่างจากหน่วยงานอื่น ๆ ตรงที่นอกเหนือจากผลงานโดยตรงที่เกิดขึ้นภายในฝ่ายเอง เช่น การซ่อมแซมและดูแลรักษาอุปกรณ์คอมพิวเตอร์แล้ว ผลงานของฝ่ายเทคโนโลยีสารสนเทศยังประกอบด้วยผลงานอันเกิดจากความร่วมมือกับฝ่ายอื่น ๆ โดยไม่สามารถแยกเป็นผลสำเร็จที่เป็นเฉพาะของตนเองได้ หากแต่ว่าภารกิจของฝ่ายเทคโนโลยีสารสนเทศจะบรรลุก็ด้วยความความร่วมมือ และการใช้บริการจากฝ่ายธุรกิจอื่น ๆ ขององค์กร มาตรวัดความสำเร็จของฝ่ายเทคโนโลยีสารสนเทศจึงมาจากทั้งผลการปฏิบัติงานภายในฝ่ายและความสำเร็จในการเพิ่มมูลค่าให้กับธุรกิจขององค์กรด้วยการนำเสนอระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและได้ประสิทธิผล

อีกหนึ่งบทบาทของฝ่ายเทคโนโลยีสารสนเทศเพื่อสนับสนุนเป้าหมายดังกล่าวข้างต้น คือ การมีส่วนร่วมในการให้คำเสนอแนะสำหรับการจัดทำงบประมาณเพื่อลงทุนในระบบเทคโนโลยีสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศจะทำการประเมินถึงผลกระทบในทางเทคนิค การบริหารจัดการ การให้บริการ และการเงินของเทคโนโลยีสารสนเทศที่จะมีต่อการดำเนินธุรกิจขององค์กรอย่างเหมาะสม ทันต่อสถานการณ์ และด้วยความถูกต้อง

ในหน่วยงานที่ฝ่ายเทคโนโลยีสารสนเทศเข้าไปให้บริการ ฝ่ายเทคโนโลยีสารสนเทศจะมีบทบาทในการจัดเตรียม และดูแลกำกับแผนระยะยาวให้เป็นไปตามวัตถุประสงค์ โดยแผนนี้จะรวบรวมแผนระยะสั้นและเป้าหมายที่ต้องบรรลุ นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศจะต้องจัดเตรียม เก็บรักษา และปรับปรุงมาตรฐานและขั้นตอนในการปฏิบัติงาน เพื่อสะดวกในการใช้อ้างอิงกรณีที่มีการปรับเปลี่ยนระบบในอนาคต ในขณะเดียวกันก็ไม่ละเลยที่จะให้บริการที่ตอบสนองความต้องการเร่งด่วนที่ร้องขอมา

## นโยบายระบบเทคโนโลยีสารสนเทศ

### หลักการ

ระบบสารสนเทศ ข้อมูล ทรัพย์สินคอมพิวเตอร์ ซึ่งรวมถึงเครื่องคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ การสื่อสารด้วยข้อมูลและเสียง (ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์) เครื่องพิมพ์และอุปกรณ์/ระบบต่อพ่วง ทั้งหมดนี้ถือเป็นทรัพย์สินของสมาคมสโมสรนักลงทุน ผู้ที่ได้รับสิทธิในการใช้ พึงใช้ด้วยความสมเหตุสมผลเพื่อรักษาความถูกต้องของระบบคอมพิวเตอร์ และข้อมูล และเพื่อความปลอดภัยของทรัพย์สิน อนึ่งการใช้ทรัพย์สินเหล่านี้จะต้องใช้เพื่องานที่เกี่ยวข้องกับการดำเนินงานของสมาคม ฯ เท่านั้น

การสื่อสารทุกรูปแบบที่เกิดขึ้นภายในสมาคมสโมสรนักลงทุน หรือส่งออกจากสมาคมสโมสรนักลงทุน ถือเสมือนหนึ่งเป็นตัวแทนและภาพลักษณ์ขององค์กร พนักงาน คณะกรรมการบริหาร และผู้ได้รับสิทธิ์ใช้งาน 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) การจัดหาระบบเทคโนโลยีสารสนเทศต้องดำเนินตามขั้นตอนการ จัดตั้งงบประมาณ และการสั่งซื้อ หาก ทรัพย์สินทางด้านเทคโนโลยีสารสนเทศใด ที่ไม่ได้มีการจัดตั้งงบประมาณไว้ ให้คณะกรรมการของสมาคมสโมสรนักลงทุน เป็นผู้ทำการอนุมัติตามอำนาจการสั่งจ่าย ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการควบคุมการใช้ทรัพยากรดังกล่าว ให้ใช้ได้อย่างมีประสิทธิภาพและคงไว้ซึ่งความปลอดภัยของข้อมูล

**บทสงวนสิทธิ**

ฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการติดตาม ตรวจสอบ กลั่นกรอง ปกป้องข้อมูลตามความเหมาะสม เพื่อให้สอดคล้องกับนโยบายขององค์กร การเผยแพร่ข้อมูลขององค์กรโดยพละการ การละเมิดสิทธิเข้าใช้งานระบบ และการใช้ประโยชน์จากทรัพย์สินโดยไม่ได้รับอนุญาตถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมายได้

**บทลงโทษทางวินัย**

การละเมิดกฎระเบียบที่กำหนดในนโยบายระบบเทคโนโลยีสารสนเทศถือว่าเป็นความผิดทางวินัย ซึ่งผู้กระทำผิดอาจถูกลงโทษโดยการตัดสิทธิต่างๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

**คณะอนุกรรมการสารสนเทศสมาคมสโมรสรนักลงทุน**

**หลักการ**

คณะอนุกรรมการสารสนเทศสมาคมสโมสรนักลงทุน มีบทบาทหน้าที่ในการให้คำแนะนำ วางแผน และมีบทบาทในการอนุมัติเรื่องที่เกี่ยวกับการใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศทั้งหมดเพื่อประโยชน์ในการใช้งานสูงสุดของสมาคมสโมสรนักลงทุน

**ความรับผิดชอบ**

คณะอนุกรรมการสนเทศสมาคมสโมสรนักลงทุน 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

**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 ทั้งนี้หมายรวมถึงการจัดหาระบบอุปกรณ์ และการพัฒนาบุคลากรให้กับหน่วยธุรกิจ
- เป็นผู้นำในการพัฒนานโยบายระบบเทคโนโลยีสารสนเทศ ตลอดจนกำหนดมาตรฐานและขั้นตอนการทำงาน

**หน้าที่หลัก**

โดยทั่วไป ฝ่ายเทคโนโลยีสารสนเทศจะต้องทำหน้าที่เกี่ยวกับ

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

**สายบังคับบัญชา**

ฝ่ายเทคโนโลยีสารสนเทศซึ่งบริหารโดยหัวหน้าฝ่ายเทคโนโลยีสารสนเทศจะต้องอยู่ในความรับผิดชอบและรายงานต่อ ผู้จัดการสมาคมสโมสรนักลงทุน

**ความปลอดภัยของอุปกรณ์ และข้อมูล**

**หลักการ**

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้แนวทางด้านความมั่นคงปลอดภัยของสารสนเทศ โดยพิจารณาองค์ประกอบ 3 ข้อหลัก ได้แก่

| องค์ประกอบ | คำอธิบาย |
|---|---|
| ความลับ (Confidentiality) | การรักษาไว้ซึ่งความลับของสารสนเทศ ไม่ถูกเปิดเผยแก่ระบบ คน และ/หรือ หน่วยงานที่ไม่ได้มีส่วนเกี่ยวข้อง |
| ความสมบูรณ์ (Integrity) | การรักษาไว้ซึ่งความถูกต้องเสถียรภาพของสารสนเทศ ไม่ถูกแก้ไขหรือนำไปใช้อย่างผิดวิธี และสามารถตรวจสอบความถูกต้องของสารสนเทศก่อนการนำไปใช้งานได้ |
| ความพร้อมใช้ (Availability) | การรักษาไว้ซึ่งความพร้อมใช้งานของสารสนเทศ |

โดยองค์ประกอบข้างต้น จะถูกนำมาพิจารณาเป็นมูลค่าของทรัพย์สินสารสนเทศในเชิงความมั่นคงปลอดภัย อันรวมไปถึงทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับสารสนเทศ

เป้าหมายสำคัญของการดำเนินกิจกรรมตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือ การลดและหลีกเลี่ยงปัญหาการละเมิดความมั่นคงปลอดภัยสารสนเทศ อันส่งผลต่อภาพลักษณ์และความเชื่อมั่นของผู้ใช้งานระบบ โดยมีการวางเป้าหมายเชิงธุรกิจ คือ ระบบสารสนเทศของสมาคมสโมสรนักลงทุนที่เป็นมืออาชีพในการให้บริการด้วยระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย (Information Security)

**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 |

**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):** ทรัพย์สินหรือข้อมูลที่จัดเก็บหรือที่ผ่านการประมวลผลจะต้องมีความถูกต้อง ครบถ้วนสมบูรณ์ ไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- **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)

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 |

Total Asset Value = (0.5 * 3.33) + (0.5 * 5.0) = 4.165 (High)

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

### 5) การระบุภัยคุกคามที่เกี่ยวข้อง (Threat Identification)

การระบุภัยคุกคามที่เกี่ยวข้อง โดยพิจารณาจากเหตุการณ์ที่เคยเกิดขึ้น หรือพิจารณาจากช่องโหว่ที่มีในทรัพย์สินสารสนเทศ ทำให้ทางสมาคมสโมสรนักลงทุนทราบได้ว่ามีภัยคุกคามใดบ้างที่อาจเกิดขึ้นได้กับทรัพย์สินสารสนเทศของสมาคมสโมสรนักลงทุน โดยทั่วไปภัยคุกคามอาจมีที่มาจากแหล่งต่างๆ ต่อไปนี้

| ประเภท | ตัวอย่าง |
|---|---|
| ภัยคุกคามทางธรรมชาติหรือสถานการณ์ฉุกเฉิน | เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติ หรือสถานการณ์ร้ายแรง ที่ก่อให้เกิดความเสียหายร้ายแรงกับทรัพย์สินสารสนเทศ เช่น น้ำท่วม แผ่นดินไหว พายุ อาคารถล่ม สภาพแวดล้อมเป็นพิษ สถานที่ตั้งอยู่ในพื้นที่มีน้ำรั่ว หรือขาดระบบไฟฟ้า ไฟไหม้ การประชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น |
| ภัยคุกคามจากมนุษย์หรือผู้ปฏิบัติงาน | เป็นภัยคุกคามที่อาจเกิดจากการโจรกรรมทรัพย์สินของสมาคมสโมสรนักลงทุน การโจมตีระบบเครือข่าย การบุกรุกระบบ การปล่อย Virus หรือ Malware ในระบบ การก่ออาชญากรรมทางคอมพิวเตอร์ ผู้ก่อการร้าย เป็นต้น |
| ภัยคุกคามด้านการบริหารจัดการหรือกระบวนการภายในหน่วยงาน | เป็นภัยคุกคามที่อาจเกิดจากแนวนโยบายในการบริหารจัดการ ที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ |
| ภัยคุกคามด้านไอที/เทคนิค | เป็นภัยคุกคามที่อาจเกิดจากช่องโหว่ของแอพลิเคชั่น 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

**7) การวิเคราะห์และระบุมาตรการควบคุมในปัจจุบันขององค์กร (Control Analysis)**

ช่องโหว่ที่พบในทรัพย์สินสารสนเทศ ผู้ประเมินต้องพิจารณามาตรการที่ทางสมาคมสโมสรนักลงทุน ใช้ควบคุมในปัจจุบัน โดยมาตรการจะช่วยลดผลกระทบหรือโอกาสที่จะเกิดภัยคุกคามได้ มาตรการแบ่งออกเป็นสองประเภท ดังต่อไปนี้

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

**8) การพิจารณาโอกาสที่จะเกิดภัยคุกคาม (Likelihood Determination)**

โอกาสที่จะเกิดเหตุการณ์ภัยคุกคามที่มีผลต่อความมั่นคงปลอดภัยของทรัพย์สิน พิจารณาจากมาตรการที่มีในปัจจุบัน โดยมีรายละเอียด ดังนี้

| Likelihood Level | รายละเอียด |
| --- | --- |
| 5-มีโอกาสเกิดขึ้นสูงมาก (Almost certain) | ภัยคุกคามมีโอกาสที่จะเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 1 เดือน เนื่องจากขาดมาตรการในการควบคุม |
| 4- มีโอกาสเกิดขึ้นสูง (Likely) | ภัยคุกคามมีโอกาสที่จะเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 3 เดือน เนื่องจากมาตรการในการควบคุมไม่เพียงพอต่อการป้องกันภัยคุกคาม |
| 3- มีโอกาสเกิดขึ้นปานกลาง (Possible) | ภัยคุกคามมีโอกาสที่จะเกิดขึ้น หรือเคยเกิดขึ้นมากกว่า 1 ครั้ง ภายใน 6 เดือน เนื่องจากมาตรการในการควบคุมไม่เพียงพอและขาดประสิทธิภาพในการป้องกันภัยคุกคาม |
| 2- มีโอกาสเกิดขึ้นน้อย (Unlikely) | ภัยคุกคามมีโอกาสที่จะเกิดขึ้นหรือเคยเกิดขึ้นประมาณ 1 ครั้ง ภายใน 1 ปี เนื่องจากมีมาตรการในการควบคุมเพียงพอต่อการป้องกันภัยคุกคาม |
| 1- มีโอกาสเกิดขึ้นน้อยมาก (Rare) | ภัยคุกคามมีโอกาสที่จะเกิดขึ้น หรือเคยเกิดขึ้นประมาณ 1 ครั้ง ภายใน 5 ปี เนื่องจากมีมาตรการในการควบคุมเพียงพอและมีประสิทธิภาพต่อการป้องกันภัยคุกคาม |

**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) สำหรับทรัพย์สินที่มี**ความเสี่ยงตั้งแต่ระดับสูง “H” ขึ้นไป** ให้เจ้าของทรัพย์สินร่วมกับเจ้าของความเสี่ยงกำหนดแนวทางในการจัดการทรัพย์สินต่อไป

### 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

**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 จะเชื่อมต่อกับระบบเครือข่ายของสมาคม ฯ ได้ต่อเมื่อได้รับการอนุมัติโดยผู้จัดการสมาคม ฯ โดยฝ่ายเทคโนโลยีสารสนเทศขอสงวนสิทธิในการติดตามเนื้อหาของข้อมูลที่มีการส่งผ่านระบบเครือข่าย และหากมีความจำเป็นในการตรวจสอบเนื้อหาที่ส่งก็สามารถแจ้งให้หัวหน้าฝ่ายที่รับผิดชอบกิจกรรมที่มีความจำเป็นในการเชื่อมต่อ เพื่อรับทราบการติดตามการตรวจสอบ

**นโยบายการควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ (Access Control Policy)**

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

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

**สภาวะแวดล้อมการใช้งานระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน**

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

- 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

- 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 และบัญชีผู้ใช้งานที่เปิดค้างไว้ให้บุคคลใช้อยู่ขณะตรวจพบจะถูกยึด และระงับไม่ให้ใช้งานต่อไป ในเหตุการณ์ดังกล่าว จะต้องแจ้งให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและผู้บริหารของหน่วยงานที่ครอบคลุมอุปกรณ์คอมพิวเตอร์และข้อมูลนั้นรับทราบเพื่อดำเนินการต่อไป

นอกจากนี้ ผู้ใช้งานไม่ควรที่จะถือโอกาสอ่านข้อมูลที่เป็นความลับ อันเนื่องมาจากความบังเอิญ หรือจากความผิดพลาดของผู้ละเมิดเข้าสู่ระบบ หรือจากการถือสิทธิในการเข้าสู่ข้อมูลที่เหนือกว่า เป็นต้น เมื่อทราบว่าข้อมูลที่เป็นความลับถูกเปิดเผยก็ไม่ควรที่จะอ่านต่อ และจะต้องรายงานให้ผู้บริหารของฝ่ายเทคโนโลยีสารสนเทศทราบทันที เช่นเดียวกันการเขียนทับข้อมูลที่ไม่ใช่ของตนโดยตั้งใจ และไม่ได้รับอนุญาต ถือเป็นความผิด

## การจัดการด้านการสื่อสารและการปฏิบัติการ (Communications and Operations Management)

### การแบ่งหน้าที่ในการปฏิบัติงานและการจัดทำเอกสารประกอบการปฏิบัติงาน

- การกำหนดบทบาทหน้าที่ในการปฏิบัติงาน หน้าที่ในการบริหารจัดการระบบสารสนเทศและระบบเครือข่ายจะต้องแยกออกจากกัน ไม่ควรให้พนักงานคนเดียวกันทำงานที่สำคัญในกระบวนการเดียวกัน เพื่อป้องกันการทุจริตและการสะดุดหยุดชะงักของงาน 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 จัดเก็บอุปกรณ์หรือเครื่องคอมพิวเตอร์ไว้ในตู้ที่สามารถปิดล็อคได้ เพื่อป้องกันไม่ให้บุคคลอื่นเข้ามาใช้อุปกรณ์ดังกล่าวโดยไม่ได้รับอนุญาต
- เครื่องคอมพิวเตอร์ทุกเครื่องจะต้องถูกล็อคหน้าจอทุกครั้งเมื่อไม่มีการใช้งานเป็นเวลา 15 นาที
- การจัดเก็บเอกสารข้อมูลสำคัญของสมาคมสโมสรนักลงทุน ข้อมูลที่อยู่ในสื่อบันทึกข้อมูล ไว้ในสถานที่ที่สามารถปิดล็อคหรือเข้ารหัสข้อมูลดังกล่าวได้ พนักงานจะต้องไม่ทิ้งเอกสารสำคัญไว้บนโต๊ะทำงาน และจัดเก็บโต๊ะทุกครั้งก่อนเลิกงาน
- ข้อมูลที่จัดเก็บในเครื่องคอมพิวเตอร์หรือส่งออกไปภายนอกองค์กรต้องจัดให้มีการเข้ารหัสข้อมูลโดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ ทั้งนี้ ต้องพิจารณาเลือกใช้เทคนิคต่าง ๆ ที่มีระดับความมั่นคงปลอดภัยตามมาตรฐานสากล

- การจัดทำ การจัดเก็บ การส่งต่อ ลบทำลายข้อมูล จะต้องดำเนินการตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ การจัดทำป้าย และการจัดการสื่อบันทึกข้อมูล (Information Classification Labelling and Media Disposal Procedure)
- ต้องควบคุมให้มีมาตรการการปิดบังข้อมูลสารสนเทศเพื่อจำกัดการเปิดเผยข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน และปฏิบัติตามข้อกำหนดทางกฎหมาย กฎหมาย ข้อบังคับและสัญญา

  แนวทางและมาตรการความปลอดภัยในการปิดบังข้อมูลเพื่อไม่ให้สามารถระบุตัวตนได้ มีดังนี้

  - การปิดบังข้อมูล (Data Masking) เช่น แทนที่เลขบัตรประจำตัวประชาชน 10 หลักแรกด้วยเครื่องหมาย x แสดงเพียง 4 หลักสุดท้าย ( x-xxxx-xxxxx-12-3)
  - การใช้นามแฝง (Pseudonymization) เช่น แทนที่ชื่อลูกค้าด้วยเลขรหัสลูกค้า (ลูกค้าหมายเลข 12345)
  - การทำข้อมูลนิรนาม (Anonymization) เช่น รวมกลุ่มข้อมูลที่มีลักษณะคล้ายคลึงกันเข้าด้วยกัน (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

**การเข้าสู่ห้องเซิร์ฟเวอร์**

**หลักการ**

ห้องเซิร์ฟเวอร์เป็นแหล่งเก็บอุปกรณ์คอมพิวเตอร์ส่วนใหญ่ขององค์กร ระบบความปลอดภัยที่เหมาะสมจึงมีความจำเป็นเพื่อปกป้องสินทรัพย์เหล่านี้ การจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์ เป็นไปเพื่อป้องกันสินทรัพย์คอมพิวเตอร์จากการละเมิดใช้ อุบัติเหตุ หรือเจตนาให้เกิดความเสียหาย หรือการขโมย การอนุมัติเพื่อจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์จะทำเมื่อเห็นว่ามีความจำเป็น เนื่องจากการกำหนดเงื่อนไขเพื่อบังคับใช้ข้อจำกัดดังกล่าวเฉพาะกลุ่มบุคคล หรือเป็นรายบุคคล เป็นสิ่งที่ทำได้ยากและไม่เหมาะสม ดังนั้นจึงได้กำหนดแนวทางดังต่อไปนี้เพื่อช่วยในการตัดสินใจกรณีที่ต้องจำกัดการเข้าสู่ห้องเซิร์ฟเวอร์

**แนวทาง**

พนักงานที่ต้องปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์ทุกวัน ซึ่งได้รับสิทธิเข้าสู่ห้องเซิร์ฟเวอร์ ได้แก่

- พนักงานดูแลซอฟต์แวร์
- พนักงานดูแลเครือข่ายเน็ตเวิร์คและเทคโนโลยี
- พนักงานสำนักงานคณะกรรมการส่งเสริมการลงทุนที่ได้รับมอบหมายให้ดูแลฝ่ายเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน

ผู้ได้รับสิทธินอกเหนือจากที่กล่าวข้างต้น ยังประกอบไปด้วยบุคคลที่ต้องเข้าไปปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์เป็นประจำ ได้แก่

- พนักงานดูแลโปรแกรมคอมพิวเตอร์ที่มีความรับผิดชอบเกี่ยวข้องกับการทำงานบนเครื่องเซิร์ฟเวอร์ หรืองานนั้นต้องทำบนเครื่องเซิร์ฟเวอร์ ณ ห้องเซิร์ฟเวอร์ การทำงานในห้องเซิร์ฟเวอร์จะถูกจำกัดเฉพาะสถานการณ์ที่จำเป็นเท่านั้น
- พนักงานฝ่ายเทคโนโลยีสารสนเทศอื่น ๆ ซึ่งต้องเข้าไปปฏิบัติหน้าที่ในห้องเซิร์ฟเวอร์เป็นประจำ

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-ออกบริเวณห้องเซิร์ฟเวอร์จะใช้ระบบการบันทึกลงสมุดการเข้า-ออกห้องเซิร์ฟเวอร์

## กรรมสิทธิ์ในข้อมูล

### หลักการ

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

### แนวทาง

ระบบคอมพิวเตอร์และข้อมูลต่าง ๆ ที่เกี่ยวข้องถือเป็นสินทรัพย์ที่มีมูลค่าขององค์กร และข้อมูลทั้งหมดที่เก็บอยู่ในสินทรัพย์เหล่านี้ถือเป็นสมบัติของสำนักงานคณะกรรมการส่งเสริมการลงทุนและสมาคมสโมสรนักลงทุน โดยผู้ใช้งานแต่ละคนจะรับผิดชอบข้อมูลที่เก็บไว้ที่เครื่องลูกข่ายคอมพิวเตอร์แต่ละเครื่องที่ตนเองใช้งานอยู่

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

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

**การใช้อินเตอร์เน็ต**

**หลักการ**

สมาคมสโมสรนักลงทุนจะเชื่อมต่ออินเตอร์เน็ตและเปิดให้พนักงานที่ได้รับการอนุมัติใช้งาน โดยหน่วยงานต้นสังกัดจะต้องดำเนินการตามขั้นตอนการแจ้งขอใช้อินเตอร์เน็ตของฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเปิดให้ใช้งานได้ระหว่างเวลาทำการขององค์กรโดยมีวัตถุประสงค์เพื่อประโยชน์ในการปฏิบัติงาน และต้องสอดคล้องโดยตรงกับหน้าที่ และความรับผิดชอบของพนักงาน โดยหัวหน้าฝ่าย/หัวหน้าแผนก ของหน่วยงานนั้น มีหน้าที่สอดส่องและดูแลให้สอดคล้องกับวัตถุประสงค์ดังกล่าว

**แนวทาง**

ถึงแม้การใช้อินเตอร์เน็ตส่งผลให้ค่าใช้จ่ายขององค์กรสูงขึ้น แต่ก็ถือว่าเป็นเทคโนโลยีทันสมัยที่มีประโยชน์สำหรับการใช้งาน และถือเป็นหนึ่งในภารกิจขององค์กร เฉพาะพนักงานที่ได้รับอนุมัติเท่านั้นจึงจะเข้าใช้งานอินเตอร์เน็ตได้ ทั้งนี้พนักงานต้องปฏิบัติให้ถูกต้องเหมาะสมตามกฎหมายกำหนด ดังที่มีกำหนดไว้ในหลักการว่าด้วยสิ่งลามกอนาจาร และ นโยบายลิขสิทธิ์โปรแกรมและการสั่งซื้อโปรแกรมคอมพิวเตอร์ เพื่อที่จะป้องกันไม่ให้สมาคมสโมสรนักลงทุนตกเป็นเป้าหมายโจมตีของไวรัสคอมพิวเตอร์ การใช้งานอินเตอร์เน็ตต้องเป็นไปเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับธุรกิจขององค์กร

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

**การควบคุมการใช้งานระบบเครือข่าย**

- ในการขอเข้าใช้งานระบบเครือข่ายนั้นจะต้องได้รับอนุมัติจากหัวหน้าฝ่ายของผู้ที่มีความประสงค์
- การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเตอร์เน็ตต้องเชื่อมต่อผ่านระบบเครือข่ายที่สมาคมสโมสรนักลงทุนจัดไว้เท่านั้น
- ไม่เปิดเผยข้อมูลเวอร์ชั่นของระบบปฏิบัติการและหมายเลข IP Address ให้บุคคลที่ไม่เกี่ยวข้องทราบ

- การควบคุมการเชื่อมต่อระบบเครือข่าย ควรแบ่งโซนของระบบเครือข่ายตามลักษณะการให้บริการของระบบ ควรกำหนดให้มี Demilitarized Zone (DMZ) คั่นระหว่างการเชื่อมต่อภายนอกกับระบบเครือข่ายของสมาคมสโมสรนักลงทุน แต่ละโซนของระบบเครือข่ายควรแยกออกจากกัน (ถ้าเป็นไปได้)
- การควบคุมการเลือกเส้นทางข้อมูลของเครือข่ายควรใช้ไฟร์วอลล์ (Firewall) เพื่อจำกัดการเข้าถึงผ่านระบบเครือข่าย ควรมีอุปกรณ์ป้องกันการบุกรุกจากภายนอก การจำกัดการเชื่อมต่อผ่านระบบเครือข่ายต้องเป็นไปตามนโยบายด้านการควบคุมการเข้าถึง และข้อกำหนดสำหรับระบบ/แอพพลิเคชั่น โดยข้อกำหนดนี้ควรจะมีการปรับปรุงเมื่อจำเป็น
- ระบบเครือข่ายที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอกจะต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ เพื่อตรวจสอบและป้องกันการบุกรุกจากภายนอก จะต้องจำกัดการเชื่อมต่อจากภายนอก โดยกำหนดให้สามารถเข้าถึง Network Zone หรือระบบสารสนเทศที่กำหนดไว้เท่านั้น
- ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของสมาคมฯ ให้เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ อาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับ (ฉบับที่ 2) พ.ศ. 2560

**การเชื่อมต่ออินเตอร์เน็ตจะต้องไม่เป็นไปเพื่อโอนถ่ายข้อมูลดังต่อไปนี้**

- ที่ละเมิดต่อกฎหมายไทย หรือกฎหมายลิขสิทธิ์ หรือขัดต่อศีลธรรมหรือขัดต่อเนื้อหาหรือวัตถุประสงค์ของนโยบายฉบับนี้
- ที่มีวัตถุประสงค์ในเชิงพาณิชย์ที่นอกเหนือจากผลประโยชน์ขององค์กร
- ห้ามมิให้ใช้อินเตอร์เน็ตเพื่อเข้าสู่โปรแกรมระบบอื่น ๆ ที่ไม่มีสิทธิเข้าใช้
- การละเมิดเข้าใช้งานอินเตอร์เน็ตไม่ว่ากรณีใด จะต้องรายงานให้ผู้จัดการสมาคม ฯ ทราบ มิฉะนั้นจะถือว่าละเมิดนโยบายขององค์กร
- ห้ามใช้อินเตอร์เน็ตเพื่อเยี่ยมชมเว็บไซต์ (Website) ที่ลามกอนาจาร หรือขัดต่อศีลธรรมอันดีงาม หรือเพื่อโอนถ่ายข้อมูลหรือรูปภาพที่ลามกอนาจาร หรือขัดต่อศีลธรรม ซึ่งผู้กระทำผิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน และอาจถูกดำเนินคดีอาญา และ/หรือคดีแพ่ง หากการกระทำดังกล่าวถือว่าขัดต่อกฎหมายของประเทศไทยเช่นกัน

## 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/หรือส่งข้อความหรือข้อมูลผ่านเครือข่ายอินเตอร์เน็ต (Internet) ด้วย “ผู้ใช้ (User)” หมายถึง พนักงานของสมาคมสโมสรนักลงทุน

### แนวทาง

สมาคมสโมสรนักลงทุนจัดให้มีระบบจดหมายอิเล็กทรอนิกส์เพื่อใช้สำหรับติดต่อสื่อสารในเรื่องที่เกี่ยวข้องกับงานขององค์กร หรือของสมาคมสโมสรนักลงทุน เป็นหลัก การใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารส่วนบุคคลจึงควรอยู่บนพื้นฐานของความเหมาะสมและความพอดี

ข้อมูลอิเล็กทรอนิกส์ที่รับส่งผ่านระบบจดหมายอิเล็กทรอนิกส์ ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน หรือระบบอินเตอร์เน็ต ถือเป็นพยานหลักฐานที่สามารถนำมาใช้ในการฟ้องร้องดำเนินคดีกับผู้ใช้ต่อศาลในภายหลังได้ ในกรณีที่มีการใช้ที่ขัดต่อนโยบายหรือก่อให้เกิดความเสียหายต่อสมาคมสโมสรนักลงทุน และ/หรือพนักงาน และ/หรือผู้บริหารของสมาคมสโมสรนักลงทุน แม้ว่าผู้ใช้รายนั้นจะพ้นสภาพการเป็นพนักงาน หรือสิ้นสุดสัญญาว่าจ้างกับสมาคมสโมสรนักลงทุนแล้วหรือไม่ก็ตาม โดยฝ่ายเทคโนโลยีสารสนเทศจะทำการจัดเก็บข้อมูลดังกล่าวไว้จนกว่าจะสิ้นสุดอายุความในการฟ้องร้องคดี

องค์กรไม่มีนโยบายที่จะเปิดอ่านข้อมูลอิเล็กทรอนิกส์ของผู้ใช้ที่ถูกส่งหรือได้รับผ่านระบบจดหมายอิเล็กทรอนิกส์หรือระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน เว้นแต่

(1) กรณีที่มีเหตุจำเป็น เช่น มีเหตุอันควรสงสัยว่า มีบุคลากรขององค์กรนำข้อมูลความลับขององค์กรออกไปเปิดเผยภายนอกโดยผ่านทางระบบจดหมายอิเล็กทรอนิกส์ หรือมีเหตุอันควรสงสัยว่า บุคลากรขององค์กรใช้จดหมายอิเล็กทรอนิกส์ในทางที่ไม่ถูกต้อง ฯลฯ ซึ่งผู้ที่มีสิทธิตรวจสอบข้อมูลอิเล็กทรอนิกส์ของผู้ใช้แต่ละรายได้จะต้องเป็นผู้บริหารหรือเป็นบุคคลที่ได้รับแต่งตั้งจากคณะกรรมการขององค์กรเท่านั้น หรือ

(2) ในกรณีที่ สมาคมสโมสรนักลงทุนได้รับคำสั่งจากศาลหรือหน่วยงานที่มีอำนาจตามบทบัญญัติแห่งกฎหมายสั่งให้ส่งข้อมูลอิเล็กทรอนิกส์และ/หรือตรวจสอบการสื่อสารในรูปแบบจดหมายอิเล็กทรอนิกส์

เพื่อมิให้เกิดปัญหาในเรื่องของความปลอดภัย การปฏิบัติผิดกฎหมาย และประสิทธิภาพในการทำงาน ผู้ใช้ทุกรายพึงมีความรับผิดชอบดังนี้

- ในฐานะที่เป็นผู้มีส่วนเกี่ยวข้องกับการใช้จดหมายอิเล็กทรอนิกส์ ผู้ใช้แต่ละรายต้องปฏิบัติตามนโยบายที่เกี่ยวข้องกับการใช้จดหมายอิเล็กทรอนิกส์ โดยในการเข้าใช้ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุน รวมถึงระบบอื่น ๆ ที่สมาคมสโมสรนักลงทุนจัดไว้ให้นั้น ผู้ใช้ต้องปฏิบัติตามนโยบายที่สมาคมสโมสรนักลงทุนกำหนด

- เนื้อหาของข้อความ เอกสารประกอบ หรือรูปภาพประกอบ และอื่น ๆ ที่ส่งโดยใช้จดหมายอิเล็กทรอนิกส์ควรเป็นไปด้วยความเหมาะสม ไม่ขัดต่อบทบัญญัติของกฎหมาย และสอดคล้องกับนโยบายฉบับนี้ และอยู่ภายใต้ข้อจำกัดเดียวกันกับการติดต่อสื่อสารในรูปแบบอื่น ๆ ที่สมาคมสโมสรนักลงทุนกำหนด

- ข้อมูลอิเล็กทรอนิกส์ที่ผู้ใช้แต่ละรายเก็บสะสมไว้ ต้องใช้เนื้อที่บนเครื่องแม่ข่ายในการเก็บซึ่งฝ่ายเทคโนโลยีสารสนเทศจะกำหนดขนาดของเนื้อที่ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ (Mail Box) ของผู้ใช้แต่ละราย ผู้ใช้ต้องลบข้อมูลอิเล็กทรอนิกส์ที่ไม่จำเป็นและไม่เกี่ยวกับงานขององค์กรออก รวมทั้งข้อมูลอิเล็กทรอนิกส์ที่ไม่ใช้แล้วทิ้งไป แต่หากมีความจำเป็นที่จะต้องใช้เนื้อที่ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์มากกว่านโยบายที่กำหนด ให้หัวหน้าฝ่ายส่งแจ้งความจำเป็นและเหตุผลถึงหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

- ปฏิบัติตามนโยบายที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุนและระบบคอมพิวเตอร์ที่เกี่ยวข้องที่สมาคมสโมสรนักลงทุนกำหนด

- รักษาความสุภาพ และมารยาทในการสื่อสาร
- ปกป้องความเป็นส่วนตัว และความลับของผู้อื่น
- ช่วยดูแลรับผิดชอบการจำกัดขนาดของข้อมูลอิเล็กทรอนิกส์ที่ใช้งานอยู่
- ใช้เทคโนโลยีสารสนเทศให้มีประสิทธิภาพและก่อให้เกิดประโยชน์แก่งานที่รับผิดชอบ

**การใช้จดหมายอิเล็กทรอนิกส์ที่ถูกต้อง**

การใช้จดหมายอิเล็กทรอนิกส์ที่ถูกต้อง ต้องใช้ให้สอดคล้องกับวัตถุประสงค์ เป้าหมาย และภารกิจขององค์กร ตลอดจนสอดคล้องกับหน้าที่และความรับผิดชอบของผู้ใช้แต่ละราย ตัวอย่างต่อไปนี้แสดงให้เห็นถึงการใช้งานที่ถูกต้อง

- ใช้เพื่อการสื่อสาร รวมถึงการแลกเปลี่ยนข้อมูลสำหรับพัฒนาสายอาชีพ หรือเพื่อศึกษาหาความรู้หรือทักษะในสายงาน
- ใช้เพื่อการสื่อสารกับหุ้นส่วนทางธุรกิจ เพื่อส่งเอกสาร หรือเพื่อโอนย้ายเอกสารประกอบการทำงาน หรือร่างเอกสารต่าง ๆ
- ใช้เพื่อค้นคว้า หรือรวบรวมข้อมูลเพื่อสนับสนุนคำแนะนำ มาตรฐาน การวิเคราะห์ หรือเพื่อพัฒนาสายอาชีพที่เกี่ยวเนื่องกับหน้าที่ของผู้ใช้
- ใช้เพื่อการสื่อสาร หรือแลกเปลี่ยนข้อมูลเพื่อสนับสนุนการทำงาน หรือโครงการที่รับผิดชอบร่วมกัน

**การใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง และขัดต่อนโยบาย**

ตัวอย่างต่อไปนี้แสดงให้เห็นถึงการใช้งานที่ไม่ถูกต้อง

- การใช้ที่เป็นการละเมิดบทบัญญัติแห่งกฎหมาย
- การใช้ที่เป็นการให้ข้อมูลภายในขององค์กร หรือข้อมูลที่เกี่ยวกับความสามารถขององค์กรในด้านต่าง ๆ ซึ่งยังไม่ได้เป็นที่เปิดเผยต่อสาธารณชนแก่บุคคลอื่น โดยไม่ได้รับความเห็นชอบจากผู้บริหาร

- การใช้เพื่อเผยแพร่สิ่งลามกอนาจาร หรือขัดต่อศีลธรรม หรือนโยบายของสมาคมสโมสรนักลงทุน
- การใช้เพื่อส่งข้อความที่ส่อเสียด ยุยง ก่อให้เกิดความแตกแยก หรือความเกลียดชัง หรือก่อให้เกิดความเสื่อมเสีย/เสียหายแก่สมาคมสโมสรนักลงทุน รวมทั้งพนักงาน คณะกรรมการ และคณะอนุกรรมการของสมาคมสโมสรนักลงทุน
- การส่งข้อความ หรือเอกสารแนบที่ไม่มีสาระเกี่ยวข้องกับการดำเนินการ หรือก่อให้เกิดประโยชน์กับสมาคมสโมสรนักลงทุน ที่เกินขอบเขตที่ยอมรับได้ หรือการใช้เพื่อธุรกิจส่วนตัวที่เกินขอบเขตที่ยอมรับได้

ผู้ใช้รายใดก็ตามที่ใช้งานจดหมายอิเล็กทรอนิกส์ หรือส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์เครือข่ายของสมาคมสโมสรนักลงทุนด้วยวิธีการอื่น ๆ ที่ขัดต่อนโยบายและหรือขัดต่อกฎหมายอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ จนถึงขั้นให้พ้นสภาพการเป็นพนักงาน และ/หรือถูกดำเนินคดีทางแพ่งและทางอาญาได้

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

## ลิขสิทธิ์โปรแกรม และการสั่งซื้อ หรือการเช่าใช้

### หลักการ

นโยบายนี้กำหนดขึ้นเพื่อให้สอดคล้องกับกฎหมายลิขสิทธิ์และเพื่อปกป้องโปรแกรมที่เป็นสินทรัพย์ขององค์กร ถึงแม้ว่านโยบายนี้จะมีมาตรการช่วยในการบังคับใช้ แต่ความสำเร็จในท้ายสุดขึ้นอยู่กับความเข้าใจและความร่วมมือของพนักงานทุกคน ฝ่ายเทคโนโลยีสารสนเทศได้รับมอบหมายให้รับผิดชอบให้บังคับใช้นโยบายนี้อย่างต่อเนื่อง

### ลิขสิทธิ์ของโปรแกรม

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

### การซื้อโปรแกรม

โปรแกรมที่ซื้อมาถือเป็นสินทรัพย์ที่มีมูลค่าสูง และต้องบันทึกไว้เป็นสินทรัพย์ขององค์กร เพื่อติดตามตรวจสอบ ดังนั้นการซื้อโปรแกรมจึงควรปฏิบัติให้สอดคล้องกับกระบวนการอนุมัติสั่งซื้อขององค์กร เพื่อให้การบันทึกสินทรัพย์เป็นไปอย่างถูกต้องตามที่ได้ระบุไว้ในการนโยบายการสั่งซื้อทรัพยากรทางเทคโนโลยีสารสนเทศ โปรแกรมทั้งหมดต้องได้รับการอนุมัติใช้โดยฝ่ายเทคโนโลยีสารสนเทศ จำนวนผู้มีสิทธิในการสั่งซื้อได้ถูกจำกัดไว้ เพื่อให้มั่นใจว่าโปรแกรมที่สั่งซื้อทั้งหมดได้รับการบันทึกอย่างถูกต้อง ฝ่ายเทคโนโลยีสารสนเทศจะระงับการสั่งซื้อโปรแกรมใด ๆ ที่จะส่งผลเสียหายต่อระบบเครือข่าย หรือไม่เหมาะกับการใช้งานของหน่วยธุรกิจ หน่วยธุรกิจจะต้องปรึกษาหารือกับฝ่ายเทคโนโลยีสารสนเทศก่อนที่จะทำการสั่งซื้อ เนื่องจากฝ่ายเทคโนโลยีสารสนเทศจะสามารถแจ้งได้ว่ามีการติดตั้งโปรแกรมดังกล่าวไว้แล้วหรือไม่

**การจดทะเบียนโปรแกรม**

ภายหลังจากที่ได้รับโปรแกรม ฝ่ายเทคโนโลยีสารสนเทศจะติดต่อกับผู้ขายเพื่อยืนยันการจดทะเบียนอย่างถูกต้อง โปรแกรมที่สั่งซื้อจะได้รับการจดทะเบียนในนามขององค์กร และจะไม่มีการจดทะเบียนในนามส่วนบุคคลโดยเด็ดขาด ภายหลังจากการจดทะเบียนแล้วเสร็จ โปรแกรมจะได้รับการติดตั้งโดยฝ่ายเทคโนโลยีสารสนเทศหรือบุคคล/นิติบุคคลที่ได้รับการมอบหมายอย่างเป็นทางการจากหน่วยงานฝ่ายเทคโนโลยีสารสนเทศเท่านั้น โดยที่ฝ่ายเทคโนโลยีสารสนเทศจะรับผิดชอบเก็บต้นฉบับของสัญญาลิขสิทธิ์และการสั่งซื้อและแผนกจัดซื้อรับผิดชอบเก็บสำเนา 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 และลบโปรแกรมที่ได้มาอย่างไม่ถูกต้องบนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายขององค์กร นอกจากนี้ฝ่ายเทคโนโลยีสารสนเทศอาจจะตรวจสอบเครื่องคอมพิวเตอร์ที่ไม่เชื่อมต่อกับระบบเครือข่ายขององค์กร และทำการลบโปรแกรมที่ไม่จดทะเบียนทันที โดยพนักงานจะต้องให้ความร่วมมือกับฝ่ายเทคโนโลยีสารสนเทศในระหว่างที่มีการตรวจสอบ

**อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์**

**หลักการ**

การใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องมีวัตถุประสงค์เพื่อประโยชน์ต่อองค์กร และเกี่ยวข้องกับงานในหน้าที่ของพนักงานเท่านั้น

**แนวทาง**

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ถือเป็นทรัพยากรขององค์กร มิใช่ทรัพย์สินส่วนตัว การใช้อุปกรณ์และระบบดังกล่าวต้องมีวัตถุประสงค์ที่เป็นประโยชน์โดยตรงต่อองค์กร

ข้อห้ามในการใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ มีต่อไปนี้

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

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องไม่มีวัตถุประสงค์ในเชิงพาณิชย์ นอกเหนือไปจากที่ได้รับมอบหมาย หรือต้องเป็นไปเพียงเพื่อประโยชน์ของสมาคมสโมสรนักลงทุนเท่านั้น อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์อาจนำมาใช้เพื่อช่วยกิจกรรมต่าง ๆ ของที่องค์กรมีส่วนร่วม หรืองานกุศลต่าง ๆ ที่องค์กรเป็นผู้สนับสนุน เฉพาะบุคคลที่ได้รับอนุมัติจากสมาคมสโมสรนักลงทุนเท่านั้น จึงจะสามารถใช้งานอุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์

การเข้าใช้อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาตจะต้องแจ้งให้ผู้จัดการสมาคม ฯ ทราบในทันที ค่าใช้จ่ายที่อาจเกิดขึ้นจะต้องแจ้งต่อผู้จัดการสมาคม ฯ หรือฝ่ายเทคโนโลยีสารสนเทศ และต้องดำเนินการสอบสวนโดยเร่งด่วน กรณีที่ไม่มีการแจ้งเรื่องเข้าใช้อุปกรณ์ดังกล่าวโดยไม่ได้รับมอบหมาย ถือเป็นการละเมิดนโยบายขององค์กรและต้องมีโทษทางวินัย

เนื้อหาที่ใช้ในการสื่อสารด้วยเสียงต้องดำรงไว้ซึ่งความเป็นมืออาชีพ และมีความเหมาะสม ห้ามมิให้ใช้เนื้อหาที่ไม่มีสาระสำคัญ ไม่สุภาพ สบประมาท แบ่งแยกเชื้อชาติ ล่วงเกินทางเพศ โจมตี ทำลายชื่อเสียง บังคับขู่เข็ญ ข่มขู่ โดยเด็ดขาด

ข้อความที่สนทนาผ่านอุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ถือเป็นทรัพย์สินขององค์กร มิใช่ทรัพย์สินส่วนบุคคล สมาคมสโมสรนักลงทุนจึงของสงวนสิทธิในการติดตามตรวจสอบเนื้อหาของบทสนทนา รวมทั้งแฟ้มเสียงที่ถูกบันทึกไว้

อุปกรณ์สื่อสารด้วยเสียงที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ต้องเป็นไปอย่างเหมาะสม หากค่าใช้จ่ายที่เกิดขึ้นมากเกินความสมเหตุสมผลอาจทำให้บุคคลนั้น ๆ สูญสิทธิในการใช้งาน หรือบุคคลนั้นอาจต้องรับผิดชอบค่าใช้จ่ายทั้งหมดหรือส่วนหนึ่ง หรืออาจถือว่ามีความผิดทางวินัยขั้นรุนแรง

**การแจ้งให้ทราบเรื่องการระงับให้บริการชั่วคราว**

**หลักการ**

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

สำหรับการระงับใช้บริการที่มีสาเหตุอื่น ๆ อันได้แก่ ฟ้าผ่า คนงานก่อสร้างตัดสายไฟฟ้า หรืออุบัติเหตุและอุบัติภัยที่อยู่เหนือการควบคุมของทางฝ่ายเทคโนโลยีสารสนเทศ จะแจ้งให้ผู้เกี่ยวข้องทราบทันทีที่เกิด

**แนวทาง**

สื่อหลักที่ใช้เพื่อแจ้งให้ทราบ คือ จดหมายอิเลคทรอนิกส์หรืออีเมลหรือการโทรแจ้งถึงพนักงานทุกคน โดยฝ่ายเทคโนโลยีสารสนเทศจะแจ้งให้ทราบล่วงหน้าอย่างน้อย 48 ชั่วโมง กรณีที่เกิดจากการวางแผนงานล่วงหน้า ตามด้วยการแจ้งให้ทราบในกรณีที่ใช้เวลาเกินกว่ากำหนดการที่วางไว้เป็นระยะ ๆ ตามนโยบายแล้วการดำเนินแผนงานที่มีผลกระทบดังกล่าวจะหลีกเลี่ยงไปทำนอกเวลางาน อย่างไรก็ตาม ในบางกรณีก็ไม่สามารถหลีกเลี่ยงได้

ในกรณีที่เกิดอุบัติเหตุหรืออุบัติภัยที่ทำให้การบริการต้องหยุดชะงัก พนักงานของฝ่ายเทคโนโลยีสารสนเทศจะได้จัดให้มีหน่วยช่วยเหลือ และให้ข้อมูลโดยย่อเกี่ยวกับขอบเขตของปัญหา ระยะเวลา สาเหตุ และผลกระทบที่อาจเกิดขึ้นให้ผู้ใช้งานที่ได้รับผลกระทบได้รับทราบ นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศจะชี้แจงให้ทราบถึงปัญหาต่อเนื่องที่จะเกิดขึ้นอันเป็นผลจากหรือเกี่ยวข้องกับการหยุดชะงักของระบบ ข้อสงสัยใด ๆ ที่เกิดขึ้นอันเนื่องมาจากแผนงาน หรือจากเหตุสุดวิสัย สามารถสอบถามได้จากพนักงานประจำหน่วยช่วยเหลือผู้ใช้คอมพิวเตอร์ การติดต่อที่นอกเหนือหน่วยนี้ ทางฝ่ายเทคโนโลยีสารสนเทศจะได้แจ้งให้รับทราบเป็นกรณี ๆ ไป

**การใช้อุปกรณ์คอมพิวเตอร์**

**หลักการ**

พนักงานทุกคนในสมาคมสโมสรนักลงทุนที่ใช้ระบบปฏิบัติงานและอุปกรณ์ในระบบการสื่อสารที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ของสมาคมสโมสรนักลงทุน มีหน้าที่รับผิดชอบในการใช้ระบบดังกล่าวอย่างผู้มีจรรยาบรรณ มีความเป็นมืออาชีพ โดยเป็นไปอย่างถูกต้องตามกฎหมาย ทั้งนี้ผู้ใช้ระบบทุกท่านต้องปฏิบัติตามแนวนโยบายซึ่งได้วางไว้เพื่อการใช้อุปกรณ์ในระบบต่าง ๆ ดังกล่าว

**แนวทาง**

พนักงานทุกคนในองค์กรควรยึดถือแนวทางปฏิบัติดังต่อไปนี้

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

**การควบคุมการเข้าใช้งานระบบปฏิบัติการ**

- กระบวนการในการเข้าใช้งานระบบอย่างปลอดภัย จะต้องมีระบบตรวจสอบสิทธิ์ในการเข้าถึงระบบปฏิบัติการ 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 เครื่องคอมพิวเตอร์ทุกเครื่องต้องมีการตั้งค่าล็อคหน้าจออัตโนมัติ

**การควบคุมการเข้าใช้งานแอพพลิเคชั่นและข้อมูล**

- การจำกัดการเข้าใช้งานข้อมูล การควบคุมการเข้าถึงแอพพลิเคชั่นต้องเป็นไปตามข้อกำหนดและสอดคล้องกับนโยบายด้านการควบคุมการเข้าถึงของสมาคมสโมสรนักลงทุน กำหนดสิทธิ์ในการเข้าถึงข้อมูลตามความรับผิดชอบในการทำงาน
- การแยกระบบข้อมูลที่มีความสำคัญ ระบบที่มีความสำคัญควรจะแยกออกจากการเข้าถึงของบุคคลทั่วไป การให้บริการของแอพพลิเคชั่นที่มีความสำคัญควรใช้เซิร์ฟเวอร์ที่แยกต่างหาก ในกรณีที่อาจต้องใช้ทรัพยากรร่วมกัน เจ้าของแอพพลิเคชั่นทั้งสองฝ่ายต้องประเมินความสำคัญของข้อมูลก่อนจะตกลงกันเรื่องใช้ทรัพยากรร่วมกัน

**การใช้คอมพิวเตอร์แบบพกพาและการเชื่อมต่อระบบเครือข่าย**

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

- 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 เครื่องคอมพิวเตอร์แบบพกพาจะต้องอัพเดท Antivirus ให้เป็นปัจจุบันที่สุด ก่อนที่จะเชื่อมต่อเข้ากับระบบเครือข่าย ควรดำเนินการอัพเดท Patch ที่เครื่องคอมพิวเตอร์แบบพกพาก่อนที่จะเชื่อมต่อกับระบบเครือข่าย

- ควรอัพเดท Antivirus และ Virus Signature ให้เป็นปัจจุบันอยู่เสมอ

**การใช้งานคอมพิวเตอร์แบบพกพาในการปฏิบัติงานจากภายนอกและการแก้ไขปัญหาจากระยะทางไกล**

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

พนักงานอาจถูกเพิกถอนสิทธิ์การเข้าใช้ระบบปฏิบัติงานคอมพิวเตอร์และอุปกรณ์การสื่อสารต่าง ๆ ที่ผ่านระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ของสมาคมสโมสรนักลงทุน เนื่องด้วยเหตุผลต่าง ๆ ได้แก่ การคุกคามระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ การดัดแปลงหรือเปิดเผยข้อมูลลับ เช่น ไฟล์ข้อมูลหรือเนื้อหาที่ปรากฏในจดหมาย โดยไม่ได้รับความยินยอมจากผู้ใช้ นอกจากนี้ยังหมายรวมถึง การดัดแปลงหรือการทำลายข้อมูลขององค์กร หรือการใช้ระบบเครือข่ายของสมาคมสโมสรนักลงทุนในลักษณะที่ขัดแย้งกับแนวทางที่ได้วางไว้

ฝ่ายเทคโนโลยีสารสนเทศสามารถเพิกถอนหรือยกเลิกการเข้าใช้ระบบได้ทุกเวลา ทั้งนี้เป็นไปเพื่อรักษาความปลอดภัยของข้อมูลและเพื่อปกป้องสิทธิประโยชน์ของสมาคมสโมสรนักลงทุน พนักงานสามารถขออุทธรณ์การเพิกถอนสิทธิ์เข้าใช้ระบบโดยยื่นต่อผู้จัดการสมาคม ฯ ในกรณีที่มีการใช้ระบบคอมพิวเตอร์ในทางที่ก่อให้เกิดความเสียหาย ผู้ก่อเหตุต้องรับผิดชอบและอาจถูกดำเนินการทางวินัย ซึ่งผู้กระทำผิดอาจถูกลงโทษโดยการตัดสิทธิต่าง ๆ อันพึงได้รับ หรือถึงขั้นให้พ้นสภาพการเป็นพนักงาน

## การกู้คืนข้อมูล และระบบคอมพิวเตอร์ที่ได้รับความเสียหาย

### หลักการ

ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบในการจัดหาแผนกู้คืนข้อมูลที่ได้รับความเสียหายที่มีประสิทธิภาพและต้นทุนเหมาะสม แผนนี้มีวัตถุประสงค์เพื่อดูแลให้อุปกรณ์และระบบคอมพิวเตอร์ที่สนับสนุนกิจกรรมสำคัญๆ ในการดำเนินธุรกิจขององค์กรสามารถกู้กลับคืนมาได้ตามที่ต้องการ งานที่เกี่ยวข้องกับแผนกู้คืนจะต้องสอดคล้องกับแนวทางที่กำหนดไว้ และความต่อเนื่องของธุรกิจของสมาคมสโมสรนักลงทุน

### ขอบเขต

แผนงานนี้จะครอบคลุมการกู้คืนการประมวลผลข้อมูลสำคัญ ๆ ที่เกิดขึ้นในเครื่องแม่ข่ายของฝ่ายเทคโนโลยีสารสนเทศและเครื่องแม่ข่ายที่ห้องเซิร์ฟเวอร์กลาง กรณีเกิดความเสียหายขึ้น และส่งผลกระทบต่อโครงสร้างระบบคอมพิวเตอร์ของสมาคมสโมสรนักลงทุน

### แนวทาง

กลยุทธ์ที่ใช้ในแผนกู้คืนข้อมูลที่ได้รับความเสียหาย มีดังต่อไปนี้

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

**การสำรองข้อมูล**

ระบบทุกระบบและข้อมูลของผู้ใช้งานในเครื่องแม่ข่ายจะได้รับการสำรองไว้เป็นประจำทุกวัน และสำรองข้อมูลการตั้งค่าอุปกรณ์เครือข่ายทุกครั้งที่มีการเปลี่ยนแปลง โดยข้อมูลสำรองนี้จะถูกจัดเก็บไว้ในที่ที่ปลอดภัย และทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง สำหรับหน่วยงานที่ต้องการการสำรองข้อมูลที่แตกต่างเพิ่มเติมจากที่กล่าวข้างต้นตามข้อบังคับของกฎหมาย ฝ่ายเทคโนโลยีสารสนเทศจะได้ปรึกษาร่วมกับแต่ละหน่วยงานเพื่อวางแผนสำรองข้อมูลให้เป็นกรณีพิเศษต่อไป

**การกู้คืนข้อมูลบนเครื่องแม่ข่ายคอมพิวเตอร์**

ในกรณีเหตุสุดวิสัยที่ทำให้อุปกรณ์และโปรแกรมคอมพิวเตอร์ของแม่ข่ายเสียหายจนไม่สามารถใช้การได้ ฝ่ายเทคโนโลยีสารสนเทศจะนำข้อมูลสำรองชุดล่าสุดกลับมาติดตั้งให้ใช้งานบนเครื่องแม่ข่ายที่กู้ขึ้นมาใหม่

**การกู้คืนข้อมูลบนเครื่องลูกข่ายคอมพิวเตอร์**

การสำรองข้อมูลบนเครื่องลูกข่ายเป็นความรับผิดชอบของผู้ใช้งาน ในกรณีที่มีความเสียหายของแฟ้มข้อมูลบนเครื่องลูกข่าย ฝ่ายเทคโนโลยีสารสนเทศจะไม่ถือว่าเป็นความรับผิดชอบที่จะกู้ข้อมูลคืน แต่จะติดตั้งโปรแกรมระบบเพื่อใช้งานต่อไป

**การตอบสนองกรณีฉุกเฉิน**

แผนงานในรายละเอียดเพื่อกู้คืนข้อมูลที่เสียหายสามารถแจกแจงได้ เมื่อเหตุการณ์ดังกล่าวเกิดขึ้น ทั้งนี้ขึ้นอยู่กับลักษณะของความเสียหาย เวลาที่เกิดความเสียหาย และระยะเวลาโดยประมาณที่เกิดการหยุดชะงักของระบบ

**ความรับผิดชอบ**

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

**การจัดทำโครงการที่เกี่ยวข้องกับระบบสารสนเทศ**

**หลักการ**

ฝ่ายเทคโนโลยีสารสนเทศหรือเจ้าของโครงการรับผิดชอบในการระบุรายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศตั้งแต่เริ่มต้น จนไปถึงสิ้นสุดโครงการ เพื่อให้การดำเนินงานโครงการมีความมั่นคงปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้น

**แนวทาง**

แนวทางที่ใช้ในการดำเนินงานโครงการด้านความมั่นคงปลอดภัยสารสนเทศ มีดังต่อไปนี้

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

## 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 เฝ้าติดตามและทบทวนอย่างน้อยปีละ 1 ครั้ง เพื่อตรวจสอบให้มั่นใจว่ามีการกำหนดค่าการรักษาความมั่นคงปลอดภัยที่จำเป็น

- ต้องกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ เพื่อสามารถตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ การเปลี่ยนแปลงแก้ไข Baseline ของอุปกรณ์คอมพิวเตอร์ โปรแกรม ระบบงาน ต้องผ่านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเพียงพอ และได้รับการอนุมัติก่อนดำเนินการ

- ต้องมีการจัดเก็บการเปลี่ยนแปลงของการกำหนดค่าระบบของทุกอุปกรณ์และระบบงาน โดยมีการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอ

**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

## นโยบายการใช้ปัญญาประดิษฐ์ภายในสมาคมสโมสรนักลงทุน

### บทนำ

สมาคมสโมสรนักลงทุนตระหนักถึงศักยภาพอันยิ่งใหญ่ของปัญญาประดิษฐ์ (AI)ในการเพิ่มประสิทธิภาพการดำเนินงาน สร้างสรรค์นวัตกรรม และยกระดับการบริการลูกค้า อย่างไรก็ตาม การใช้ AI อย่างมีความรับผิดชอบและมีจริยธรรมเป็นสิ่งสำคัญยิ่ง เพื่อให้มั่นใจว่าเทคโนโลยีนี้จะถูกนำมาใช้เพื่อประโยชน์สูงสุดของสมาคมและสังคมโดยรวม

การนำ AI มาใช้ในองค์กรอย่างมีประสิทธิภาพจำเป็นต้องอาศัยความร่วมมือจากทุกฝ่ายในองค์กร ตั้งแต่ผู้นำจนถึงพนักงานทุกคน การเปลี่ยนแปลงวัฒนธรรมองค์กร การเสริมสร้างความรู้ความเข้าใจเกี่ยวกับ AI และการปรับตัวให้เข้ากับเทคโนโลยีใหม่ๆ เป็นสิ่งสำคัญที่จะทำให้องค์กรสามารถเดินหน้าไปได้พร้อมกันและมั่นคง

### วัตถุประสงค์

นโยบายนี้มีวัตถุประสงค์เพื่อ:

1. กำหนดแนวทางการใช้ AI ที่ชัดเจนและมีจริยธรรมภายในสมาคม
2. ส่งเสริมความเข้าใจและความตระหนักเกี่ยวกับการใช้ AI อย่างมีความรับผิดชอบ
3. สร้างความเชื่อมั่นให้กับพนักงาน ลูกค้า และผู้มีส่วนได้ส่วนเสียทุกฝ่ายว่าสมาคมใช้ AIอย่างโปร่งใสและเป็นธรรม
4. สนับสนุนการพัฒนาและใช้ AI ที่สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง

### ขอบเขต

ขอบเขตการใช้งานปัญญาประดิษฐ์ของสมาคมสโมสรนักลงทุน จะส่งเสริมการใช้ AI เป็นหลักในการดำเนินงานและการตัดสินใจในทุกระดับของสมาคม ในการพัฒนาและปรับปรุงกระบวนการทำงาน ผลิตภัณฑ์และบริการ โดยมีการบูรณาการ AI เข้ากับโครงสร้างพื้นฐานและวัฒนธรรมสมาคมอย่างเป็นระบบ และครอบคลุมการใช้ AI ในทุกรูปแบบภายในสมาคม

1. การใช้ AIในการตัดสินใจ: สมาคมจะนำ AI มาใช้ในการวิเคราะห์ข้อมูลและสร้างแบบจำลองเพื่อสนับสนุนการตัดสินใจในทุกระดับ ตั้งแต่การบริหารจัดการจนถึงการพัฒนาผลิตภัณฑ์และบริการ
2. การเรียนรู้และปรับปรุงตนเอง: สมาคมจะมีระบบที่สามารถเรียนรู้จากข้อมูลและผลลัพธ์ที่ได้รับอย่างต่อเนื่อง เพื่อพัฒนาความแม่นยำและประสิทธิภาพของ AI ในการดำเนินงาน
3. การสร้างวัฒนธรรมที่เน้นข้อมูล (Data-Driven Culture): สมาคมจะมีการสะสมและใช้ข้อมูลเป็นศูนย์กลางในการดำเนินธุรกิจ ทำให้ AI สามารถสร้างมูลค่าและนวัตกรรมใหม่ๆ ได้
4. การผสาน AI เข้ากับกระบวนการทำงาน: AI จะถูกรวมเข้ากับทุกขั้นตอนของกระบวนการทำงาน ตั้งแต่การประมวลผล ไปจนถึงการบริการลูกค้า เพื่อเพิ่มประสิทธิภาพและลดต้นทุน
5. การพัฒนาความสามารถของพนักงาน: สมาคมจะมุ่งเน้นในการฝึกอบรมและพัฒนาทักษะของพนักงานให้มีความสามารถในการใช้ AI ในการทำงาน และการทำงานร่วมกับ AI
6. การกำกับดูแลและความโปร่งใส: สมาคมจะมีมาตรการในการกำกับดูแลการใช้ AI อย่างมีจริยธรรมและโปร่งใส เพื่อให้มั่นใจว่า AI ถูกใช้อยางเหมาะสมและสอดคล้องกับนโยบายและค่านิยมของสมาคม

**หลักการพื้นฐาน**

การใช้ AI ในสมาคมของเราจะอยู่ภายใต้หลักการพื้นฐานดังต่อไปนี้:

1. **ความรับผิดชอบ:** จะรับผิดชอบต่อผลกระทบที่เกิดขึ้นจากการใช้ AI ทั้งหมด
2. **ความโปร่งใส:** จะเปิดเผยข้อมูลเกี่ยวกับการใช้ AI ของสมาคมอย่างชัดเจนและเข้าใจได้
3. **ความเป็นธรรม:** จะใช้ AI อย่างเป็นธรรมและไม่เลือกปฏิบัติ
4. **ความปลอดภัย:** จะให้ความสำคัญกับความปลอดภัยของข้อมูลและระบบ AI ของสมาคม
5. **ความเป็นส่วนตัว:** จะเคารพความเป็นส่วนตัวของบุคคลที่เกี่ยวข้องกับข้อมูลที่ใช้ในการพัฒนาและใช้งาน AI
6. **ความยั่งยืน:** จะใช้ AI ในลักษณะที่ส่งเสริมความยั่งยืนของสมาคมและสังคม

**แนวปฏิบัติ**

1. **การพัฒนาและใช้งานระบบ** AI:
    - การพัฒนาและใช้งานระบบ AI จะต้องได้รับอนุมัติจากผู้บริหารที่เกี่ยวข้อง
    - ระบบ AI จะต้องได้รับการทดสอบและประเมินอย่างละเอียดก่อนนำไปใช้งานจริง
    - จะต้องมีกระบวนการตรวจสอบและติดตามการทำงานของระบบ AI อย่างสม่ำเสมอ
2. **การจัดเก็บและประมวลผลข้อมูล:**
    - การจัดเก็บและประมวลผลข้อมูลที่เกี่ยวข้องกับ AI จะต้องเป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง
    - ข้อมูลส่วนบุคคลจะได้รับการปกป้องอย่างเหมาะสม
    - การเข้าถึงข้อมูลจะถูกจำกัดเฉพาะผู้ที่ได้รับอนุญาต
3. **การตัดสินใจโดยใช้** AI:
    - การตัดสินใจที่สำคัญจะไม่ถูกมอบหมายให้กับ AI โดยลำพัง
    - มนุษย์จะมีส่วนร่วมในการตัดสินใจเสมอ
    - เหตุผลในการตัดสินใจโดยใช้ AI จะต้องสามารถอธิบายได้
4. **การกำกับดูแลและตรวจสอบ:**
    - มีคณะกรรมการกำกับดูแลการใช้ AI ภายในสมาคม
    - การใช้ AI จะได้รับการตรวจสอบอย่างสม่ำเสมอเพื่อให้มั่นใจว่าเป็นไปตามนโยบายนี้
    - มีกระบวนการรับเรื่องร้องเรียนเกี่ยวกับการใช้ AI

**บทบาทและความรับผิดชอบ**

- **ผู้บริหาร**: มีหน้าที่รับผิดชอบในการกำหนดนโยบายและแนวทางการใช้ AI
- **คณะกรรมการกำกับดูแล**: มีหน้าที่กำกับดูแลการใช้ AI ให้เป็นไปตามนโยบาย
- **พนักงาน**: มีหน้าที่ปฏิบัติตามนโยบายและแนวทางการใช้ AI
- **ผู้พัฒนา** AI: มีหน้าที่พัฒนา AI ที่มีความปลอดภัย มีจริยธรรม และเป็นไปตามนโยบาย
- **ผู้ใช้** AI: มีหน้าที่ใช้ AIอย่างมีความรับผิดชอบและเป็นไปตามนโยบาย

**การฝึกอบรมและการสื่อสาร**

สมาคมจะจัดให้มีการฝึกอบรมที่เหมาะสมแก่พนักงานทุกคนเกี่ยวกับการใช้ AI อย่างมีความรับผิดชอบและเป็นไปตามนโยบาย นอกจากนี้ สมาคมจะสื่อสารนโยบายนี้ให้แก่พนักงาน ลูกค้า และผู้มีส่วนได้ส่วนเสียทุกฝ่ายได้รับทราบ

**การสร้างเครือข่ายการเรียนรู้และการแลกเปลี่ยนความรู้** (Creating Learning Networks and Knowledge Sharing)

- การสร้างชุมชนการเรียนรู้ (Learning Communities) การสร้างชุมชนการเรียนรู้ที่ประกอบด้วยพนักงานจากแผนกต่างๆ ที่สนใจในการใช้ AI จะช่วยส่งเสริมการแลกเปลี่ยนความรู้และประสบการณ์ในการใช้ AI ในบริบทต่างๆ
- การจัดตั้งเครือข่ายผู้เชี่ยวชาญด้าน AI ภายในองค์กร การสร้างเครือข่ายผู้เชี่ยวชาญด้าน AI ที่พนักงานสามารถเข้าถึงและขอคำปรึกษาได้ จะช่วยเพิ่มความมั่นใจในการใช้ AI และสนับสนุนการเรียนรู้ที่ต่อเนื่อง
- การส่งเสริมการเรียนรู้ร่วมกันระหว่างองค์กร การสร้างความร่วมมือกับองค์กรภายนอกที่มีความเชี่ยวชาญด้าน AI เช่น สถาบันการศึกษา ศูนย์วิจัย หรือบริษัทเทคโนโลยี จะช่วยให้พนักงานสามารถเข้าถึงแหล่งความรู้และทรัพยากรที่มีคุณภาพ

**การประเมินและปรับปรุงโปรแกรมการฝึกอบรม** (Evaluating and Improving Training Programs)

- การประเมินผลการฝึกอบรม การประเมินผลการฝึกอบรมอย่างสม่ำเสมอ โดยใช้เกณฑ์ที่ชัดเจนเช่น ความพึงพอใจของผู้เรียน ความเข้าใจและการนำความรู้ไปใช้ การวัดประสิทธิภาพในการทำงานที่เพิ่มขึ้น จะช่วยให้องค์กรสามารถปรับปรุงโปรแกรมฝึกอบรมให้มีคุณภาพและเหมาะสมกับความต้องการของพนักงานมากขึ้น
- การปรับปรุงโปรแกรมฝึกอบรมตาม Feedback การรับฟังข้อเสนอแนะจากผู้เรียนและการนำข้อเสนอแนะเหล่านั้นมาใช้ในการปรับปรุงโปรแกรมฝึกอบรม จะช่วยให้การฝึกอบรมมีประสิทธิภาพและตอบโจทย์ความต้องการของพนักงานได้ดียิ่งขึ้น

**การปรับปรุงนโยบาย**

นโยบายนี้จะได้รับการทบทวนและปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีและกฎหมายที่เกี่ยวข้อง

**บทลงโทษ**

การไม่ปฏิบัติตามนโยบายนี้อาจมีบทลงโทษทางวินัย

**บทสรุป**

นโยบายนี้เป็นแนวทางสำคัญในการใช้ AI อย่างมีความรับผิดชอบและมีจริยธรรมภายในสมาคม โดยมุ่งมั่นที่จะใช้ AI เพื่อประโยชน์สูงสุดของสมาคมและสังคมโดยรวม

**เอกสารแนบ 1**

ACKNOWLEDGEMENT STATEMENT

(ตัวอย่าง)

ข้าพเจ้าได้อ่านเอกสารและทำความเข้าใจนโยบายเทคโนโลยีสารสนเทศของสมาคมสโมสรนักลงทุน และยืนยันที่จะปฏิบัติตามเงื่อนไขและ/หรือกฎเกณฑ์ที่มีระบุในเอกสารดังกล่าว ข้าพเจ้าเข้าใจเช่นกันว่า การเซ็นรับรองในเอกสารนี้ไม่ถือว่าเป็นการทำสัญญาหรือถูกทำให้เข้าใจว่าเป็นการทำสัญญาในอนาคต แต่เป็นการรับรองว่าข้าพเจ้าได้อ่านและเข้าใจนโยบายและกฎเกณฑ์ต่าง ๆ ที่ได้ระบุในเอกสารดังกล่าวแล้ว

**ชื่อ :** _____

**ลายเซ็น :** _____

**วันที่ :** _____

**เอกสารแนบ 2**

MUTUAL CONFIDENTIALITY AGREEMENT

(ตัวอย่าง)

ระหว่าง

**สมาคมสโมสรนักลงทุน**

1 อาคารทีพีแอนด์ที ชั้น 12 ถนนวิภาวดี-รังสิต

แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

และ

---

---

---

เพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับของทั้งสองหน่วยงานในระหว่างการหารือในประเด็นทางธุรกิจหรือระบบเทคโนโลยีสารสนเทศระหว่างกัน ทั้งสองฝ่ายมีข้อตกลงดังต่อไปนี้

1. **คำจำกัดความ**

1.1 “ข้อมูลข่าวสารที่เป็นความลับ” หมายถึงข้อมูลทั้งทางวาจาหรือเอกสารหรือข้อมูลอิเล็กทรอนิกส์ที่มาจากผู้เปิดเผย ทั้งนี้รวมถึงเอกสารและ/หรือ ข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องเช่น โปรแกรมซอฟต์แวร์ ข้อมูลไฟล์อิเล็กทรอนิกส์ต่างๆ คู่มือผู้ใช้งานและคู่มืออื่นๆ

1.2 “ผู้เปิดเผย” หมายถึง องค์กรในสัญญานี้ที่เป็นผู้ให้ข้อมูล

1.3 “ผู้รับ” หมายถึง องค์กรให้สัญญานี้ที่เป็นผู้รับข้อมูล

1.4 “โครงการ” หมายถึง _____

2. **หน้าที่ของผู้รับ**

2.1 ผู้รับจะใช้ข้อมูลข่าวสารที่เป็นความลับเพื่อวัตถุประสงค์เฉพาะโครงการนั้นเท่านั้น และจะไม่ใช้เพื่อวัตถุประสงค์อื่น ๆ ยกเว้นจะได้รับความยินยอมเป็นลายลักษณ์อักษร

2.2 ผู้รับตกลงจะไม่เปิดเผยข้อมูลข่าวสารที่เป็นความลับที่ได้รับจากผู้เปิดเผยในรูปแบบใด ๆ ก็ตาม ทั้งนี้ข้อมูลดังกล่าวจะต้องไม่อยู่ภายใต้ข้อ 2.3

2.3 ข้อตกลงนี้ไม่ผูกมัดเกี่ยวกับข้อมูลข่าวสารที่เป็นความลับกรณี (ก) ข้อมูลดังกล่าวได้รับรู้โดยสาธารณะอันเนื่องจากทางอื่นที่นอกเหนือจากผู้รับ หรือ (ข) ข้อมูลดังกล่าวเป็นข้อมูลที่ผู้รับได้ข้อมูลมาจากทางอื่นก่อนที่จะได้รับจากผู้เปิดเผย หรือ (ค) ข้อมูลดังกล่าวเป็นข้อมูลที่ผู้รับได้รับจากองค์กรอื่นซึ่งไม่เป็นการละเมิดข้อตกลงเกี่ยวกับข้อมูลที่เป็นความลับจากผู้เปิดเผย หรือ (ง) ข้อมูลดังกล่าวได้มาหรือคิดค้นมา โดยอยู่นอกเหนือจากข้อมูลที่อยู่ในข้อตกลงนี้ หรือ (จ) ข้อมูลดังกล่าวจำเป็นต้องเปิดเผยโดยข้อบังคับทางกฎหมาย

2.4 ข้อมูลข่าวสารที่เป็นความลับที่ได้รับมาเป็นทรัพย์สินของผู้เปิดเผยข้อมูล ในกรณีที่ผู้เปิดเผยข้อมูลต้องการข้อมูลดังกล่าวกลับคืนโดยแจ้งมาเป็นลายลักษณ์อักษร ผู้รับจะต้องส่งข้อมูลดังกล่าวคืน หรือทำลายข้อมูลดังกล่าว ซึ่งรวมทั้งสำเนาต่าง ๆ ตามที่ผู้เปิดเผยข้อมูลร้องขอมา

2.5 ทั้งสองฝ่ายยอมรับว่าข้อตกลงนี้ไม่มีผลต่อการโอนย้ายทรัพย์สินทางปัญญาระหว่างฝ่ายใดฝ่ายหนึ่ง

## 3. ข้อตกลงทั่วไป

3.1 ข้อตกลงนี้ไม่ก่อให้เกิดความสัมพันธ์ทางธุรกิจอื่นใด นอกเหนือจากการเข้าใจร่วมกันในเรื่องการรักษาความลับของข้อมูล

3.2 ผู้รับข้อมูลยอมรับว่าความเสียหายทางการเงินอาจไม่เพียงพอต่อการละเมิดข้อตกลงดังกล่าว และตกลงว่า ผู้เปิดเผยข้อมูลสามารถเสนอทางเลือกหรือแนวทางจ่ายค่าเสียหายในกรณีที่มีการละเมิดข้อตกลงดังกล่าวขึ้น

3.3 ผู้รับข้อมูลยอมรับว่าข้อมูลที่ได้รับจากผู้เปิดเผยข้อมูลไม่ได้เป็นการรับประกันหรือแสดงให้ เห็นว่าข้อมูลดังกล่าวมีความถูกต้องหรือครบถ้วนสมบูรณ์ของข้อมูลที่เป็นความลับดังกล่าว

3.4 ผู้รับข้อมูลจะไม่นำส่งข้อมูลดังกล่าวออกนอกประเทศไทยไม่ว่าจะเป็นทางตรงหรือทางอ้อม ยกเว้นจะได้รับการยินยอมเป็นลายลักษณ์อักษรจากผู้เปิดเผยข้อมูล

3.5 ผู้รับข้อมูลจะต้องดำเนินการลบข้อมูลที่เป็นข้อมูล Sensitive ภายในระยะเวลา 3 เดือน หลังจากสิ้นสุดระยะเวลาการดำเนินงานของโครงการและรายงานกลับ เพื่อให้ทราบว่าดำเนินการแล้วตามมาตรฐาน

3.6 การเพิ่มเติมหรือแก้ไขข้อตกลงนี้จะต้องจัดทำเป็นลายลักษณ์อักษรพร้อมทั้งเซ็นรับรองโดยทั้งสองฝ่าย

3.7 ข้อตกลงนี้ถูกจัดทำขึ้นภายใต้กฎหมายข้อบังคับในประเทศไทย

3.8 ทั้งสองฝ่ายยอมรับว่า การเซ็นยินยอมในข้อตกลงนี้และดำเนินการส่งข้อตกลงการส่งด้วยมือทางไปรษณีย์ หรือ ทางอิเล็กทรอนิกส์ เพื่อให้อีกฝ่ายหนึ่งได้รับรู้นั้นเป็นการกระทำที่ยอมรับได้และถือว่ามีผลผูกพันได้ทันที

**รับรองโดย** _____ **รับรองโดย สมาคมสโมสรนักลงทุน**

ลงนาม: _____ ลงนาม: _____

ชื่อ: _____ ชื่อ: _____

ตำแหน่ง:_____ ตำแหน่ง:_____

วันที่: _____ วันที่: _____