นโยบายด้านเทคโนโลยีสารสนเทศ
สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย

ระบบและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญที่สามารถช่วยพัฒนาและส่งเสริมศักยภาพในการดำเนินธุรกิจ เพิ่มประสิทธิภาพการปฏิบัติงานของสมาคมฯ รวมถึงการมีมาตรการในการป้องกันปัญหาอันอาจเกิดขึ้นจากการถูกภาวะคุกคามต่าง ๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่พึงประสงค์ อีกทั้งเป็นการป้องกันการกระทำความผิดตามกฎหมายและระเบียบอื่น ๆ ที่เกี่ยวข้อง สมาคมฯ จึงเห็นสมควรกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ ให้ทราบและถือปฏิบัติ ไว้ดังนี้

ความหมายและคำจำกัดความ

คำเรียก	ความหมายและคำจำกัดความ
สมาคมฯ	สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย
ผู้ใช้งาน	ผู้บริหาร ผู้ปฏิบัติงาน ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก ที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเครือข่ายของสมาคมฯ
ผู้ใช้งานภายนอก	บุคคล หรือนิติบุคคล ซึ่งสมาคมฯ หรือหน่วยงานในสมาคมฯ อนุญาตให้มีสิทธิ์เข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิ์ตามประเภทการใช้งาน
ระบบสารสนเทศ	ระบบงานของสมาคมฯ ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศ ซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของสมาคมฯ
ระบบเครือข่าย	ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสมาคมฯ ได้ เช่น LAN Wireless Intranet Internet และระบบการสื่อสารอื่นๆ
ทรัพยากรเทคโนโลยีสารสนเทศ	ระบบเทคโนโลยีสารสนเทศ อุปกรณ์ Hardware และ Software งบประมาณ รวมถึงการจัดสรรทรัพยากรบุคคลเพื่อสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศ
ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของสมาคมฯ โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) และความน่าเชื่อถือ (Reliability)

ทรัพย์สินสารสนเทศ	ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบสารสนเทศ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์ต่อพ่วงทุกชนิด เครื่องบันทึกข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
ผู้รับดำเนินการ	บุคคลภายนอกองค์กรซึ่งสมาคมฯ ว่าจ้างเพื่อให้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง และต้องใช้ดุลพินิจหรือตัดสินใจในการปฏิบัติงานดังกล่าวแทนสมาคมฯ
ผู้ดูแลระบบ	ผู้ปฏิบัติงานที่ทำหน้าที่บริหาร จัดการระบบคอมพิวเตอร์ และระบบเครือข่ายในสมาคมฯ โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้งและปรับปรุงซอฟต์แวร์ สร้างและบำรุงรักษาบัญชีผู้ใช้งาน

นโยบายด้านเทคโนโลยีสารสนเทศมีรายละเอียด ดังนี้

หมวดที่ 1
การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร (Governance of Enterprise IT)

จุดมุ่งหมายของการกำกับดูแลด้านเทคโนโลยีสารสนเทศมี 4 ประการด้วยกัน คือ 1) เพื่อให้สมาคมฯ สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ในการจัดหาเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุนการทำงานในองค์กรให้เป็นไปอย่างมีประสิทธิภาพสูงสุด 2) เพื่อสามารถบริหารจัดการความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้ 3) เพื่อให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดี โดยมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากรและข้อมูลที่มีประสิทธิภาพ และแผนรองรับเพื่อสนับสนุนนโยบาย ยุทธศาสตร์ เป้าหมายขององค์กร และการบริหารความเสี่ยงที่เหมาะสม และ 4) เพื่อให้มีการรายงาน ติดตามการดำเนินงาน และทบทวนประสิทธิผลของการนำเทคโนโลยีมาใช้งานโดยประเมินเทียบกับวัตถุประสงค์ที่ตั้งไว้

สมาคมฯ จึงกำหนดการดำเนินการเพื่อให้บรรลุจุดมุ่งหมายข้างต้น ดังนี้

1.1 มีนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร สื่อสารสร้างความเข้าใจเพื่อทำให้ผู้เกี่ยวข้องสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในสมาคมฯ

1.2 ทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสมาคมฯ

1.3 บริหารจัดการความเสี่ยงที่เกี่ยวกับหน่วยงานเจ้าของระบบสารสนเทศหรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ดังนี้

1.3.1 ตรวจสอบและประเมินความเสี่ยงหน่วยงานเจ้าของระบบสารสนเทศหรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ เป็นระยะ

1.3.2 กำหนดให้มีการบริหารจัดการความเสี่ยงอย่างเป็นระบบ ซึ่งประกอบไปด้วยการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่สมาคมฯ ยอมรับได้

1.3.3 กำหนดให้ต้องมีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

1.3.4 กำหนดให้มีแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมทั้งในเชิงการป้องกันและการรับมือกับปัญหา

หมวดที่ 2
การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Information Technology Security)

2.1. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ

2.1.1. ฝ่ายจัดการรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของสมาคมฯ

2.1.2. ผู้ปฏิบัติงานส่วนเทคโนโลยีสารสนเทศที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator ทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบ และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดต้องดำเนินการแก้ไข และรายงานต่อผู้บังคับบัญชาอย่างทันท่วงที

2.1.3. ผู้ใช้งานและหน่วยงานทั้งภายในและภายนอกรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของสมาคมฯ และต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2.2. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่ และความรับผิดชอบในการใช้งานระบบสารสนเทศของสมาคมฯ และมีการดำเนินการต่างๆ ให้มีความมั่นคงปลอดภัยที่สุด สมาคมฯ จึงกำหนดแนวทางการดำเนินการดังนี้

2.2.1. บุคลากรในข้อนี้ หมายถึง บุคลากรภายใน และบุคลากรภายนอก

(1) บุคลากรภายใน ประกอบด้วย กรรมการสมาคมฯ ผู้บริหารและพนักงานของสมาคมฯ นักศึกษาฝึกงาน

(2) บุคลากรภายนอก ประกอบด้วย ที่ปรึกษา บุคคลที่ทำงานในโครงการแลกเปลี่ยนของสมาคมฯ บุคคลหรือหน่วยงานภายนอกที่สมาคมฯ จัดจ้างมาปฏิบัติงาน

2.2.2. การว่าจ้างหรือการรับบุคลากรภายใน หรือจัดจ้างบุคคลหรือหน่วยงานภายนอก

(1) เมื่อสมาคมฯ ว่าจ้าง จัดจ้าง หรือรับบุคคล หรือหน่วยงานมาปฏิบัติงาน สมาคมฯ จะกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของสมาคมฯ

(2) สมาคมฯ กำหนดให้บุคคลหรือหน่วยงานดังกล่าวต้องลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงานว่าจะรักษาความลับและไม่เปิดเผยข้อมูลของสมาคมฯ (สัญญารักษาความลับและไม่เปิดเผยข้อมูล)

(3) สมาคมฯ กำหนดให้บุคคลหรือหน่วยงานภายนอกที่ได้รับการว่าจ้างให้ทำงานให้สมาคมฯ และมีส่วนเกี่ยวข้องกับการเก็บ รักษา หรือประมวลผลข้อมูลใด ๆ ของสมาคมฯ ต้องลงนามในสัญญาประมวลผลข้อมูลของสมาคมฯ (สัญญาการประมวลผลข้อมูล)

2.2.3. การเคลื่อนไหวด้านบุคลากรภายในและภายนอก

เมื่อมีการเคลื่อนไหวด้านบุคลากรภายในและภายนอก หน่วยงานทรัพยากรบุคคล หรือผู้ที่ได้รับมอบหมาย หรือหน่วยงานที่เกี่ยวข้องกับการรับหรือจัดจ้างบุคคลหรือหน่วยงานมาปฏิบัติงาน ต้องแจ้งให้ผู้ดูแลเทคโนโลยีสารสนเทศทราบทันที เมื่อมีการเคลื่อนไหวดังนี้

(1) การว่าจ้างงาน การรับเข้า การจัดจ้าง

(2) การเปลี่ยนแปลงสภาพการจ้างงาน เช่น โยกย้าย เลื่อนตำแหน่ง แต่งตั้ง ถอดถอน การเปลี่ยนแปลงความรับผิดชอบ สถานที่ปฏิบัติงาน สายบังคับบัญชา หรือโครงสร้างองค์กร เป็นต้น

(3) การสิ้นสุดสภาพการจ้าง การสิ้นสุดการเป็นกรรมการ การสิ้นสุดสัญญา

2.2.4. การให้ความรู้กับบุคลากรภายในและภายนอก

(1) สมาคมฯ จะให้ผู้ใช้งานระบบสารสนเทศของสมาคมฯ ทุกคน บุคคลหรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(2) ผู้ปฏิบัติงานใหม่ของสมาคมฯ ต้องได้รับการปฐมนิเทศเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(3) ลูกจ้างและนักศึกษาฝึกงานของสมาคมฯ จะได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นปัจจุบันที่สุด และจะได้รับการอบรมเพื่อให้มีความรู้และความตระหนักต่อการเปลี่ยนแปลงที่เกี่ยวข้อง

2.3. การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

ทรัพยากรด้านเทคโนโลยีสารสนเทศ หมายรวมถึง ระบบเทคโนโลยีสารสนเทศ บุคลากรที่เกี่ยวข้อง งบประมาณ และการบริหารความเสี่ยงที่เกิดจากการไม่สามารถจัดสรรทรัพยากรเพื่อสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศ

(1) สมาคมฯ จะจัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนยุทธศาสตร์ของสมาคมฯ โดยครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ สมาคมฯ จะจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

(2) หน่วยงานเจ้าของระบบสารสนเทศมีหน้าที่รับผิดชอบโดยตรงในการวางแผนระบบ กำหนดงบประมาณ และ การบริหารจัดการเพื่อให้การบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศสอดคล้องกับแผนยุทธศาสตร์ของสมาคมฯ และของหน่วยงาน

2.4. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของสมาคมฯ ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวม ทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของสมาคมฯ

2.4.1. การจัดการข้อมูลสารสนเทศและการรักษาความลับ

(1) การรักษาความลับของข้อมูล (Confidentiality) เป็นการกำหนดชนิดและจัดลำดับของข้อมูลสารสนเทศ เพื่อป้องกันการนำข้อมูลสารสนเทศไปใช้โดยผิดวัตถุประสงค์ การจัดข้อมูลสารสนเทศ (Information Classification) กำหนดให้มีการแบ่งระดับความปลอดภัยขององค์กร โดยคำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัย ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการอาจได้รับ

(2) การสำรองข้อมูลและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

สมาคมฯ กำหนดให้หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องดำเนินการต่อไปนี้

(1) จัดทำระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ (ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญทั้ง front และ back office ได้แก่ ระบบงานจัดซื้อ ระบบงานบัญชีและการเงิน ระบบงานการตลาดและสมาชิก ระบบ CRM, ระบบงาน CGR, ระบบงาน CAC Certifications, ระบบบริหารทรัพยากรบุคคล เป็นต้น)

(2) จัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน

(3) กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(4) ให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

2.5. การควบคุมการเข้ารหัสข้อมูล

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

2.6. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องกำหนดมาตรการป้องกัน ควบคุมการใช้งาน และการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศ ซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานระบบสารสนเทศของสมาคมฯ ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

2.7. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

การควบคุมการใช้งานของผู้ใช้งานหน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องจัดให้มีการควบคุมการใช้งานทรัพย์สินสารสนเทศและระบบสารสนเทศ ดังนี้

2.7.1. กำหนดมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน

(1) กำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศใส่รหัสผ่าน

(2) ให้ผู้ใช้งานออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์ โดยทันที เมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน

(3) ให้ผู้ใช้งานล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม

2.7.2. กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกสมาคมฯ

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องกำหนดให้มีมาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของสมาคมฯรวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกสมาคมฯ

2.7.3. กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน

(Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของสมาคมฯ อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในสมาคมฯ รับทราบและปฏิบัติตาม

2.8. การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

2.8.1. การบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

2.8.2. การควบคุมการรับส่งข้อมูลสารสนเทศ

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในสมาคมฯ กับหน่วยงานภายนอกโดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) หน่วยงานเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในสมาคมฯ และระหว่างสมาคมฯ กับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

(2) หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ EDI(Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

(3) ผู้บริหารหน่วยงานและ/หรือหน่วยงานจัดซื้อจัดจ้างต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้สมาคมฯ มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของสมาคมฯ อย่างเป็นลายลักษณ์อักษร

(4) หน่วยงานทรัพยากรบุคคลต้องจัดให้บุคลากรภายในทำสัญญารักษาความลับและไม่เปิดเผยข้อมูลของสมาคมฯ เป็นลายลักษณ์อักษร

2.9. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องจัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้ และกำหนดให้มีการรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศเพื่อให้การพัฒนาหรือ แก้ไขเปลี่ยนแปลงระบบสารสนเทศประมวลผลได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมถึงการรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบงานสารสนเทศ

2.10. การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (IT Outsourcing)

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

2.11. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

หน่วยงานเจ้าของระบบเทคโนโลยีสารสนเทศ และ/หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของสมาคมฯ มีหน้าที่รับผิดชอบ

(1) กำหนดขั้นตอนและกระบวนการในการจัดการกับเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงผู้รับผิดชอบ และมาตรฐานการปฏิบัติการ (Incident Response Process) เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) รายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ผู้เกี่ยวข้องทราบ

(3) กำหนดวิธีการและขั้นตอนการรายงาน สำหรับผู้ใช้งานที่พบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ผู้พบเหตุต้องแจ้งเหตุการณ์ดังกล่าวต่อหน่วยงานเทคโนโลยีสารสนเทศ

(4) กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรง ของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว ต้องจัดทำบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย

2.12. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Business Continuity Management)

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของสมาคมฯ อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของสมาคมฯ

(1) สมาคมฯ จะมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของสมาคมฯ

(2) สมาคมฯ จะดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นกับการทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

(3) จัดให้มีการปฏิบัติตามขั้นตอนการ Incident Response Process และกำหนดขั้นตอนการจัดการปัญหาในแต่ละสถานการณ์อย่างชัดเจน และมีแนวทางในการป้องกันสถานการณ์เกิดซ้ำ

(4) จัดให้มีข้อมูล อุปกรณ์ หรือระบบที่จำเป็นสำหรับการนำออกมาใช้รับมือกับสถานการณ์ฉุกเฉิน และจัดเตรียมอุปกรณ์ หรือระบบสำรอง หรือข้อมูลหน่วยงานที่ให้การสนับสนุน โดยข้อมูลต้องมีความละเอียดเพียงพอต่อการปฏิบัติงานในภาวะฉุกเฉิน เพื่อให้การดำเนินงานของสมาคมฯ ดำเนินต่อไปได้อย่างราบรื่นและมีผลกระทบน้อยที่สุด

(5) กำหนดขั้นตอนและวิธีการสื่อสารกับคู่ค้าสำคัญในกรณีที่จำเป็น เช่น กรรมการ ลูกค้า พนักงาน เป็นต้น

ประกาศ ณ วันที่ 23 สิงหาคม 2566

(ดร.กุลภัทรา สิโรดม)

ประธานกรรมการ

สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย