

นโยบายความปลอดภัยสารสนเทศ

วัตถุประสงค์

1. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยด้านสารสนเทศ
2. สร้างความรู้ความเข้าใจของพนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวข้องกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อให้พนักงานและผู้ที่ต้องใช้เชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

ขอบเขต

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท ทั้งที่อยู่ภายในหรือภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคร่าวด์ที่บริษัทจัดหา ซึ่งครอบคลุมถึง

1. พนักงานและหน่วยงานทั้งหมดของบริษัท
2. บุคคลภายนอกบริษัทที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท
3. ยึดถือนโยบายตาม “มาตรฐานความปลอดภัยสารสนเทศ” ของบริษัทอย่างเคร่งครัด

หน้าที่และความรับผิดชอบ

หน้าที่ของผู้บังคับบัญชา

1. ชี้แจงให้พนักงานทราบถึงนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติคำแนะนำ และกระบวนการต่างๆ ของบริษัทที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ดูแล แนะนำ และตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม
3. พิจารณาลงโทษทางวินัยแก่ผู้กระทำความผิดอย่างเสมอภาค และเป็นธรรม

หน้าที่ของพนักงาน

พนักงานทุกคน ต้องปฏิบัติดังต่อไปนี้

1. ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่างๆ ของบริษัทที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศโดยเคร่งครัด
2. ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท
3. แจ้งให้บริษัททราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุกโจรกรรมทำลาย แทรกแซงการทำงาน หรือโจรกรรมที่อาจสร้างความเสียหายต่อบริษัท
4. หากพบสิ่งผิดปกติที่เกิดขึ้นกับระบบคอมพิวเตอร์ให้หยุดการทำงาน ถอดสายแลน หรือ ตัดระบบออกจากเครือข่ายคอมพิวเตอร์ของบริษัททันที และแจ้งเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเข้าตรวจสอบปัญหาที่เกิดขึ้น



พนักงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติตามดังต่อไปนี้

1. ต้องออกจากระบบ (Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน
2. ต้องล็อกหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน
3. ต้องตรวจสอบข้อมูลที่น่ามาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti virus) ที่มีข้อมูลไวรัสที่ทันสมัย
4. ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นในที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับส่วนตัวของพนักงาน ซึ่งจะต้องเก็บ รักษาไว้มิให้ผู้อื่นล่วงรู้และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้พนักงานต้องเปลี่ยนรหัสผ่านและรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อพนักงานเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน โดยตั้งรหัสผ่าน และรหัสอื่นใด ด้วยความรอบคอบ ห้ามตั้งรหัสซ้ำกับรหัสเก่า ห้ามตั้งรหัสที่ผู้อื่นสามารถคาดเดาได้ง่าย และห้ามตั้งรหัสซ้ำกันในทุกระบบที่พนักงานมีสิทธิใช้งาน ทั้งนี้มาตรฐานการตั้งรหัสผ่านอย่างปลอดภัย อ้างอิงตามเอกสาร IT Security Standard

พนักงานทุกคน ต้องห้ามทำสิ่งดังต่อไปนี้

1. นำเอกสาร ข้อมูลสารสนเทศ ช้องบริษัทที่สำคัญ ออกจากบริษัทโดยไม่ได้รับอนุญาตจากผู้มีอำนาจโดยเด็ดขาด
2. ดัดแปลงข้อมูล, เปลี่ยนแปลงข้อมูลสารสนเทศของบริษัท โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ
3. เชื่อมต่อคอมพิวเตอร์ สมาร์ทโฟน อุปกรณ์ใดๆ ที่ไม่ได้รับอนุญาตจากบริษัท หรือ หน่วยงานที่สังกัด
4. ห้ามใช้อุปกรณ์บันทึกข้อมูล เช่น แฟลชไดรฟ์, CD, DVD โดยไม่ได้รับอนุญาตจากผู้มีอำนาจหรือหน่วยงานที่สังกัด
5. นำอุปกรณ์คอมพิวเตอร์ออกจากบริษัทโดยไม่ได้รับอนุญาต
6. ติดตั้งโปรแกรมคอมพิวเตอร์ที่ไม่ได้รับอนุญาตจากบริษัท หรือ หน่วยงานที่รับผิดชอบ

การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

1. การควบคุมการใช้งานของผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องจัดให้มีการควบคุมการใช้งานทรัพย์สินสารสนเทศและระบบสารสนเทศ ดังนี้

➤ กำหนดมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องกำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่ รหัสผ่าน และให้ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์ โดย ทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มีการล็อกหน้าจอเครื่อง คอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน หรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่ กำหนดอย่างเหมาะสม

➤ กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกบริษัทฯ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องกำหนดให้มาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภท พกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัทฯ รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัทฯ



➤ **กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน**
หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องจัดทำ ขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้ง ซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และ กำหนดรายการซอฟต์แวร์ มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของ บริษัทฯ อย่างเป็นทางการเป็นลายลักษณ์ อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายใน บริษัทฯ รับทราบและปฏิบัติตาม

2. การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องจัดทำ ข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ มีความมั่นคง ปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับ ดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

การจัดการข้อมูลสารสนเทศและการรักษาความลับ

1. การจำแนกประเภททรัพย์สินสารสนเทศ

หน่วยงานเจ้าของโครงการหรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องกำหนดแนว ทิศทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้น ความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัทฯ มาร่วมพิจารณา การกำหนดชั้นความลับที่ เหมาะสม รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนว ทิศทางการดำเนินงานที่กำหนดไว้

2. การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องจัดทำ ระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบ สารสนเทศที่สำคัญ รวมทั้งจัดทำ แผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์ เพื่อให้สามารถ ใช้ งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียม ความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถ ปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการ ดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และ ความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบ สารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผน รองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถ ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และให้มีการทดสอบ สภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

3. การควบคุมการเข้าถึงข้อมูล

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องกำหนด มาตรการการเข้าถึงข้อมูลและแนวทางการเลือกมาตรฐานการเข้าถึงข้อมูล โดยให้มีความเหมาะสมกับ ความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้ง ติดตามให้มีการปฏิบัติให้เป็นไป ตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ



การป้องกันภัยคุกคามต่อระบบสารสนเทศ

1. การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สิน จากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม
2. การบริหารจัดการช่องโหว่ทางเทคนิค หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องควบคุมให้ระบบสารสนเทศของบริษัทฯ ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้

การทบทวนนโยบาย

กำหนดให้มีการทบทวนนโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างน้อย ปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ หรือเมื่อเกิดเหตุการณ์ด้านความปลอดภัย ที่มีผลกระทบต่อองค์กร เพื่อให้นโยบายความปลอดภัยด้านสารสนเทศ รวมทั้งแนวทางปฏิบัติ ข้อกำหนด ขั้นตอนปฏิบัติ และเอกสารใดๆ ที่เกี่ยวข้องกับนโยบายดังกล่าว มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง ทั้งนี้ฝ่ายเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้อง ต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลง

บทลงโทษ

1. ตักเตือนด้วยวาจา
2. ตักเตือนเป็นลายลักษณ์อักษร
3. ปลดออก
4. ไล่ออก
5. การดำเนินทางกฎหมายอาญาหรือแพ่ง

กรณีการลงโทษพนักงาน บริษัทไม่จำเป็นต้องปฏิบัติตามลำดับดังกล่าวข้างต้น บริษัทอาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

นโยบายความปลอดภัยสารสนเทศ นี้มีผลบังคับใช้ตั้งแต่วันที่ 17 พฤษภาคม 2565 เป็นต้นไป

พลตำรวจโท



(สมคิด บุญถนอม)

ประธานคณะกรรมการบริษัท