



แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
บริษัท สหพัฒน์อินเตอร์โฮลดิ้ง จำกัด (มหาชน)
ฉบับปรับปรุง ครั้งที่ 1

1. คำนำ

ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท เป็นระบบที่มีความสำคัญต่อการให้บริการกับกรรมการบริษัท ผู้บริหาร พนักงาน และรวมถึงบุคคลภายนอกซึ่งได้รับอนุญาต ดังนั้น เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์ การปฏิบัติงาน และบริหารงานได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยเชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง บริษัทฯ จึงได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติ

2. วัตถุประสงค์

2.1 เพื่อให้การดำเนินงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทมีความมั่นคง ปลอดภัยสามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพอันจะทำให้การดำเนินธุรกรรมมีความถูกต้อง เชื่อถือได้ตามมาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

2.2 เพื่อกำหนดแนวทางปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ใช้งานระบบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

2.3 เพื่อป้องกันเจ้าหน้าที่ผู้ใช้งานและผู้เกี่ยวข้องไม่ให้เกิดความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

3. กำหนดคำนิยาม คำนิยามที่ใช้ในแนวปฏิบัตินี้ ประกอบด้วย

“บริษัทฯ” หมายถึง บริษัท สหพัฒน์อินเตอร์โฮลดิ้ง จำกัด (มหาชน)

“ผู้ใช้งาน” หมายถึง บุคคลที่ได้รับอนุญาต ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบ เทคโนโลยีสารสนเทศและการสื่อสารของบริษัทโดยมีสิทธิและหน้าที่ตามที่บริษัทฯ กำหนด

“ผู้บริหาร” หมายถึง ผู้บริหารของบริษัทฯ

“ผู้ดูแลระบบ” หมายถึงผู้จัดการฝ่ายสารสนเทศ หรือผู้ได้รับมอบหมายให้ควบคุม ดูแล บริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

“เจ้าหน้าที่” หมายถึง บุคลากรในสังกัดบริษัทฯ

“สินทรัพย์” หมายถึง ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์และทรัพย์สินด้านเทคโนโลยี สารสนเทศและการสื่อสารของบริษัท เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่บริษัทฯซื้อมา เพื่อใช้งานที่ถูกต้องตามกฎหมาย เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การควบคุมและจำกัดสิทธิการใช้งานระบบ เทคโนโลยีสารสนเทศและการสื่อสารของบริษัทที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็นในการใช้งาน มีการป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่ได้สิทธิทั้งจากภายในและภายนอกบริษัทฯ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การคงไว้ซึ่งความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูลในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท



“เหตุการณ์ด้านความมั่นคงปลอดภัย” (Security incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และการสื่อสารของบริษัท หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน หรือสร้างความเสียหายได้ในที่สุด ซึ่งส่งผลให้เป็นการละเมิด นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท เช่น การอนุญาตให้ผู้อื่นเข้าใช้งานระบบ การไม่กำหนดรหัสผ่าน ในการเข้าใช้งานระบบ การเปิดเผยเอกสารสำคัญให้กับบุคคลภายนอกองค์กร โปรแกรมไม่พึงประสงค์ระบบถูกบุกรุกทางเครือข่าย หรือ การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” ได้แก่ สถานการณ์ที่ผู้ดูแลระบบไม่ต้องการ ให้เกิดขึ้นหรือสร้างความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท โดยผู้ดูแลระบบไม่ได้คาดการณ์ไว้ว่าจะ เกิดขึ้น เช่น โปรแกรมไม่พึงประสงค์ โปรแกรมทำงานผิดพลาดหรือไม่ถูกต้อง ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย เว็บไซต์ผิดถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต ระบบถูกโจมตีจนไม่สามารถให้บริการได้ การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยี สารสนเทศ

“ฝ่ายสารสนเทศ” หมายถึง หน่วยงาน และ/หรือ ผู้รับผิดชอบ ที่มีหน้าที่ดำเนินการเกี่ยวกับระบบสารสนเทศ และระบบงาน คอมพิวเตอร์และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศของบริษัท ในการศึกษา วิเคราะห์เพื่อพัฒนาระบบสารสนเทศและระบบงาน คอมพิวเตอร์ของบริษัท และปฏิบัติงานร่วมกันหรือ สนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ศูนย์สารสนเทศ” หมายถึง ห้องเครื่องแม่ข่าย (Server Room) ห้องสำรองข้อมูล (Backup Room) ห้องควบคุม (Control Room) ห้องเครือข่าย (Network Room) และส่วนระบบปรับอากาศ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือ ชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่ายสื่อสาร” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการเชื่อมโยง หรือ การส่งข้อมูลสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัท ซึ่งการเชื่อมโยงเป็นได้ ทั้งในรูปแบบใช้สายและแบบไร้สาย โดยระบบเครือข่าย สื่อสาร ได้แก่ ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Area Network: WAN) ระบบ อินทราเน็ต (Intranet) และ ระบบอินเทอร์เน็ต (Internet)

“ระบบเครือข่ายสื่อสารระยะใกล้” หมายถึง เครือข่ายที่เชื่อมโยงกันในพื้นที่ใกล้เคียงกัน

“ระบบเครือข่ายสื่อสารระยะไกล” หมายถึง เครือข่ายเชื่อมโยงกันในระยะทางที่ห่างไกล

“ระบบอินทราเน็ต” หมายถึง ระบบเครือข่ายสื่อสารภายในที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูล และสารสนเทศภายในบริษัท

“ระบบอินเทอร์เน็ต” หมายถึง ระบบเครือข่ายสื่อสารที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ของบริษัทเข้ากับระบบเครือข่าย สื่อสารอินเทอร์เน็ตทั่วโลก

“สารสนเทศ” หมายถึง ข้อมูลที่ผ่านการประมวลผล การจัดระเบียบ ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้ เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง ระบบงานของบริษัทฯ ที่ประกอบด้วย ระบบคอมพิวเตอร์ ระบบ ฐานข้อมูล ระบบเครือข่ายสื่อสาร เจ้าหน้าที่ผู้ใช้ระบบ เจ้าหน้าที่ผู้พัฒนาระบบ เจ้าหน้าที่ผู้จัดการดูแลระบบ และผู้บริหารของบริษัท นำมาทำงานร่วมกัน เพื่อกำหนดวัตถุประสงค์ รวบรวมจัดเก็บข้อมูล ประมวลผลข้อมูล และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้ ระบบและผู้บริหารของบริษัท สามารถนำมาใช้ประโยชน์ในการวางแผน เพื่อช่วยสนับสนุนการปฏิบัติงาน การตัดสินใจ การบริหาร การวิเคราะห์ และติดตามผลการดำเนินงานของหน่วยงานระดับต่างๆ ของบริษัทฯ



“รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยัน ตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การดำเนินการรักษาความมั่นคง ปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ประกอบด้วย คุณสมบัติพื้นฐาน 3 ประการ ดังนี้

(1) การรักษาความลับ (Confidentiality) คือ การเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

(2) บูรณภาพ (Integrity) คือ การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

(3) ความพร้อมใช้งาน (Availability) คือ การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

“ชุดคำสั่งไม่พึงประสงค์” (Malware) หมายถึง ชุดคำสั่งที่มีผลทำให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสาร เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรง ตามคำสั่งที่กำหนดไว้

“จดหมายอิเล็กทรอนิกส์” (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายสื่อสารที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP3 หรือ IMAP

4. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศบริษัทฯ

4.1 การรักษาความมั่นคงปลอดภัยของการเข้าถึงและการควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

4.1.1 การควบคุมการเข้าถึงสิทธิของผู้ใช้งาน

(1) มีการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบ โดยพิจารณาจากหน้าที่ความรับผิดชอบในการเข้าถึงและการใช้งานข้อมูลของผู้ใช้งานแต่ละกลุ่มงาน

(2) ผู้ใช้งานต้องทำหนังสือขอมิสิทธิเป็นลายลักษณ์อักษรให้กับฝ่ายสารสนเทศ หรือหน่วยงานที่ได้รับมอบหมาย

(3) ผู้จัดการฝ่ายสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เป็นผู้พิจารณาอนุญาต

4.1.2 การบริหารจัดการสิทธิผู้ใช้งาน

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ได้กำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้นๆ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นไปตามระเบียบที่บริษัทฯ กำหนด และทบทวนสิทธิอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือในกรณีฝ่ายทรัพยากรบุคคลมีการแจ้งย้าย/เปลี่ยนตำแหน่งงานใหม่/ออกจากงาน/เกษียณ หรือในกรณีที่หน่วยงานต้นสังกัด ยื่นทำขอต่อฝ่ายสารสนเทศเพื่อให้มีสิทธิหรือยกเลิกสิทธิต่าง ๆ ในการใช้งาน

(2) ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(3) เมื่อเจ้าหน้าที่ออกจากงาน หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้ฝ่ายทรัพยากรบุคคล แจ้งฝ่ายสารสนเทศทันที เพื่อถอดถอนสิทธิของผู้ที่ออกจากงานหรือเปลี่ยนสิทธิในระบบทันทีที่ได้รับแจ้ง



(4) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องมีการพิจารณาการควบคุมผู้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานต้องเปลี่ยนรหัสผ่านทุก 3 เดือน และต้องได้รับความเห็นชอบและอนุมัติจากผู้จัดการฝ่ายสารสนเทศหรือผู้ได้รับมอบหมาย

(5) ห้ามผู้ใช้งานซึ่งไม่ได้รับสิทธิให้เข้าใช้งาน บุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่ว่าด้วยวิธีการใด

4.1.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

(1) ผู้ดูแลระบบมีการกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ และระบบต้องไม่แสดงรหัสผ่านให้เห็นบนหน้าจอ

(2) ระบบต้องกำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเมื่อเข้าระบบครั้งแรก

(3) ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยกำหนดให้ระบบมีการบันทึกประวัติการเปลี่ยนรหัสผ่าน เพื่อป้องกันการใช้รหัสซ้ำ เช่น ระบบงาน SAP ในบริษัทฯ ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 90 วัน

(4) การแจ้งปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ผู้ใช้งานติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน

4.1.4 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

(1) ผู้ใช้ต้องใช้ชื่อผู้ใช้งาน และรหัสผ่านของตนเองในการใช้งานระบบ เพื่อป้องกันการปฏิเสธความรับผิดชอบ

(2) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

(3) ผู้ใช้งานต้องกำหนดรหัสผ่าน และเปลี่ยนรหัสผ่านของตนเองในการใช้งาน อย่างน้อยทุกๆ 90 วัน หรือตามหลักเกณฑ์ที่ผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใดๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(4) ผู้ใช้งานต้องเก็บรักษาบัตรรหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใดๆ ทั้งสิ้น เว้นแต่กรณีผู้ใช้งานที่มีอำนาจอนุมัติใดๆ ในระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถปฏิบัติงานอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในชวงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้ว ให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

(5) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(6) ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น "abcdef" "aaaaaa" "123456"

(7) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

(8) ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(9) ผู้ใช้งานต้องออกจากระบบ (Log off) ทันที เมื่อไม่ใช้งาน เพื่อป้องกันผู้ใช้งานอื่นลักลอบใช้สิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร



4.1.5 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

- (1) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน
- (2) เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบ
- (3) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน ในการขออนุญาตเข้าระบบงานนั้น ต้องทำบันทึกและกรอกแบบฟอร์มตามที่ฝ่ายสารสนเทศกำหนด และให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้มีอำนาจที่เป็นเจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน เพื่อเก็บไว้เป็นหลักฐาน
- (4) การลงทะเบียนเจ้าหน้าที่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ หรือเมื่อย้าย/เปลี่ยนตำแหน่งงานใหม่/ออกจากงาน/เกษียณ ภายในบริษัทฯ หน่วยงาน/ผู้ใช้งานต้องทำบันทึก และกรอกแบบฟอร์มตามที่ฝ่ายสารสนเทศกำหนด เพื่อให้มีสิทธิหรือยกเลิกสิทธิต่างๆ ในการใช้งาน

- 1) ผู้ใช้งานรายใหม่ ต้องทำการบันทึกข้อมูลเพื่อขอลงทะเบียนในแบบฟอร์ม **“ขออนุญาตเข้าใช้ระบบ”**
- 2) แบบฟอร์ม **“ขออนุญาตเข้าใช้ระบบ”** ที่ผู้ใช้งานรายใหม่ได้ทำการแจ้ง ต้องได้รับการอนุมัติจากผู้บังคับบัญชาของผู้ขอ และผู้จัดการฝ่ายสารสนเทศ
- 3) ผู้ดูแลระบบจะกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน โดยได้รับความเห็นชอบจากผู้มีอำนาจ และทบทวนสิทธิอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือในกรณีฝ่ายทรัพยากรบุคคลมีการแจ้งย้าย/เปลี่ยนตำแหน่งงานใหม่/ออกจากงาน/เกษียณ หรือในกรณีที่หน่วยงานต้นสังกัด ยื่นทำขอต่อฝ่ายสารสนเทศ เพื่อให้มีสิทธิหรือยกเลิกสิทธิต่างๆ ในการใช้งาน
- (5) การจัดเก็บรักษาชื่อผู้ใช้และรหัสผ่านบัญชีผู้ใช้งานที่มีสิทธิสูงสุด (Highest Privilege Users)
 - 1) ผู้ดูแลระบบจัดเก็บชื่อผู้ใช้และรหัสผ่านในช่องปิดผนึกในที่ปลอดภัย
 - 2) ผู้ดูแลระบบทำการบันทึกประวัติการเปิดของทุกครั้ง
 - 3) ช่องชื่อผู้ใช้และรหัสผ่านจะถูกเปิดใช้งานได้ในกรณีฉุกเฉินเท่านั้น
 - 4) ผู้ดูแลระบบจะต้องมีการตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิสูงสุดอย่างสม่ำเสมอ เพื่อตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิสูงสุดให้สามารถเข้าใช้งานได้ตามปกติ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

4.1.6 การควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร

เป็นการควบคุมบุคคลที่เข้าสู่ระบบเครือข่ายสื่อสาร รวมถึงการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น โดยผู้ดูแลระบบจะต้องทำการออกแบบระบบเครือข่ายสื่อสารตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ Internal Zone, External Zone และ DMZ Zone เป็นต้น จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย ดังนี้

- (1) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- (2) เจ้าหน้าที่ที่รับผิดชอบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบริการเครือข่ายสื่อสารในระบบจัดการทรัพยากรสารสนเทศบริษัทฯ



- (3) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายสื่อสารในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน ในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายสื่อสาร
- (4) ผู้ดูแลระบบจัดให้มีซอฟต์แวร์สำหรับบริหารจัดการและควบคุมระบบเครือข่าย (Network Management System) ซึ่งสามารถระบุอุปกรณ์บนเครือข่าย (Equipment Identification) ถึงระดับ IP address, Computer name, MAC address และสามารถสร้างผังการเชื่อมโยงเครือข่าย (Network Diagram)
- (5) ผู้ดูแลระบบมีการจัดทำผังการเชื่อมโยงเครือข่าย และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- (6) ผู้ดูแลระบบมีการบริหารจัดการเครือข่ายสื่อสาร ดังนี้
 - 1) มีการแบ่งแยกเครือข่ายสื่อสารเป็นเครือข่ายสื่อสารภายใน เครือข่ายสื่อสารภายนอกและเครือข่ายสื่อสารแบบไร้สาย
 - 2) มีการจัดแบ่งแยกส่วนเครือข่ายสื่อสาร/กลุ่ม เพื่อป้องกันและควบคุมการเข้าถึง ได้แก่ ส่วนที่เป็นสาธารณะ ส่วนที่เชื่อมต่อภายใน ส่วนที่เกี่ยวข้องกับสินทรัพย์สำคัญหรือที่เป็นอันตรายกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
 - 3) มีการติดตั้งอุปกรณ์ Gateway กันไว้ระหว่างเครือข่ายสื่อสาร เพื่อเป็นตัวควบคุมข้อมูลที่สื่อสารกันระหว่างเครือข่ายสื่อสาร
 - 4) อุปกรณ์ในเครือข่ายสื่อสารมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่าย
- (7) ผู้ดูแลระบบมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- (8) ผู้ดูแลระบบมีการสำรองข้อมูลการตั้งค่าของอุปกรณ์เครือข่ายสื่อสาร

4.1.7 การควบคุมการเข้าถึงระบบปฏิบัติการ

เป็นการควบคุมบุคคลเข้าสู่ระบบปฏิบัติการที่อยู่ภายใต้ระบบเครือข่ายสื่อสารของบริษัท เพื่อรักษาความปลอดภัยของข้อมูล และทรัพยากร จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย

- (1) การติดตั้งโปรแกรมอรรถประโยชน์ (Utility Program/Software) เพื่อใช้งานร่วมกับระบบ ปฏิบัติการ
 - 1) ต้องไม่ติดตั้งโปรแกรมซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
 - 2) ต้องติดตั้งโปรแกรมตามภารกิจและไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน
- (2) ฝ่ายสารสนเทศ กำหนดมาตรการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Limitation of connection time) สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือแอปพลิเคชัน (Application) ที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย ดังนี้
 - 1) กำหนดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือแอปพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูงเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้ได้ 30 นาทีต่อการเชื่อมต่อ 1 ครั้ง เฉพาะในช่วงเวลาทำการของหน่วยงานเท่านั้น

4.2 การบริหารจัดการศูนย์สารสนเทศ โดยมีการควบคุมการเข้า-ออก (Physical entry controls) ศูนย์สารสนเทศ ดังนี้

- (1) มีขั้นตอนการขออนุญาต การกำหนดสิทธิ และควบคุมการเข้าศูนย์สารสนเทศ และพื้นที่สำคัญภายในศูนย์สารสนเทศ
- (2) มีระบบการบันทึกวันและเวลาการเข้า-ออกพื้นที่ในศูนย์สารสนเทศโดยอัตโนมัติเกี่ยวกับตัวบุคคลและเวลาที่ผ่านเข้า-ออก เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น



(3) มีการควบคุมการเข้าออกศูนย์สารสนเทศ และพื้นที่สำคัญภายในศูนย์สารสนเทศ ด้วยการใช้บัตร ประจำตัวและลายนิ้วมือ หรือใช้บัตรประจำตัวและรหัสผ่าน เพื่อพิสูจน์ตัวตนของผู้มีสิทธิ

(4) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในศูนย์สารสนเทศ จนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(5) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญในศูนย์สารสนเทศ

4.3 การรักษาความมั่นคงปลอดภัยการใช้งานเครื่องคอมพิวเตอร์

4.3.1 การใช้งานของผู้ใช้งาน

(1) ให้มีการกำหนดรหัสผ่าน เปลี่ยนรหัสผ่านและเก็บรักษาารหัสผ่าน เป็นไปตาม ข้อ 4.1.4 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

(2) ให้ผู้ใช้งานออกจากระบบ (Log off) ทันทีในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันบุคคลอื่นมาใช้ระบบต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที

(3) ผู้ไม่ได้รับสิทธิให้เข้าใช้งาน ห้ามบุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศไม่ว่าด้วยวิธีการใดๆ

(4) ห้ามติดตั้งซอฟต์แวร์ หรือโปรแกรมอื่นใดลงบนเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน หรือติดตั้งอุปกรณ์เชื่อมต่อเครือข่ายเพิ่มเติม หรือเชื่อมต่อเครือข่ายคอมพิวเตอร์ที่ใช้ปฏิบัติงานกับเครือข่ายอื่นนอกจากเครือข่ายของบริษัท หรือนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานกับระบบเทคโนโลยีสารสนเทศ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

(5) ไม่เปิดให้มีการแชร์ไฟล์ในเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน เว้นแต่ในกรณีที่เป็นระบบงานที่บริษัทกำหนดไว้ หากมีความจำเป็นให้กำหนดระยะเวลาเท่าที่ใช้งานและยกเลิกการแชร์ไฟล์ทันทีที่ใช้งานเสร็จ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และข้อมูล

(6) ไม่ดาวน์โหลด (Download) ข้อมูลหรือโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน หรือ จากเว็บไซต์ซึ่งไม่น่าเชื่อถือ หรือไม่มั่นใจว่าจะปลอดภัย

4.4 การรักษาความมั่นคงปลอดภัยการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

4.4.1 การใช้งานอินเทอร์เน็ต

(1) ผู้ใช้งานต้องไม่ใช้ระบบอินเทอร์เน็ตในการใช้งานข้อมูลมัลติมีเดีย หรือดาวน์โหลดข้อมูลที่ไม่เกี่ยวกับการปฏิบัติงานและยึดครองช่องสัญญาณการสื่อสารข้อมูล

(2) ให้ผู้ดูแลระบบ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS, IDS เป็นต้น

(3) เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์คอมพิวเตอร์แบบพกพาก่อนทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

(4) ผู้ใช้งานต้องไม่ใช้งานอินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์เชิงธุรกิจส่วนตัว หรือการเข้าใช้เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

(5) ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัทโดยผ่านความเห็นชอบจากผู้ดูแลระบบ

(6) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต



(7) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

(8) ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

4.4.2 การใช้งานจดหมายอิเล็กทรอนิกส์

(1) ผู้ใช้งานต้องลงทะเบียนเป็นผู้ได้รับสิทธิการใช้งานและรหัสผ่าน เพื่อเป็นเครื่องมือในการตรวจสอบยืนยันตัวตนบุคคลในการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัท ซึ่งผู้ใช้งานแต่ละคนจะต้องดูแลรักษาสิทธิการใช้งานและรหัสผ่านของตนเองไม่ให้ผู้อื่นนำไปใช้งานได้ หากมีการกระทำใดซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เจ้าของสิทธิต้องรับผิดชอบผลจากความเสียหายที่เกิดขึ้นโดยไม่อาจปฏิเสธได้

(2) ผู้ใช้งานต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทในการรับ-ส่งจดหมายอิเล็กทรอนิกส์ซึ่งเกี่ยวกับกาปฏิบัติงาน

(3) ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทฯ สร้างความน่ารำคาญต่อผู้อื่น หรือขัดต่อศีลธรรม และไม่แสวงหาประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ของบริษัท

(4) ผู้ใช้งานต้องออกจากระบบจดหมายอิเล็กทรอนิกส์ทันทีหลังจากการเลิกใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

(5) ก่อนเปิดเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องใช้โปรแกรมป้องกันไวรัส ตรวจสอบเอกสารแนบเสนอ

(6) ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(7) ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(8) ผู้ใช้งานต้องสำรองข้อมูลที่มีความสำคัญในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ

4.5 การรักษาความมั่นคงปลอดภัยการบริหารจัดการสินทรัพย์และเครือข่าย

4.5.1 การบริหารจัดการระบบคอมพิวเตอร์

(1) จัดทำทะเบียนคุมสินทรัพย์ในระบบจัดการทรัพย์สินสารสนเทศ

(2) การรักษาความปลอดภัยระบบคอมพิวเตอร์โดย

1) กำหนดชื่อและ IP Address ในระบบคอมพิวเตอร์

2) กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

3) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์

4) ในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้ดูแลรับผิดชอบโดยทันที

5) เปิดให้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องมีความเสี่ยงต่อระบบการรักษาความปลอดภัย ต้องมีมาตรการเพิ่มเติม

6) มีการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web server อย่างสม่ำเสมอ

7) ทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งาน โดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา



(3) บำรุงรักษาอุปกรณ์ ในระบบคอมพิวเตอร์ให้สามารถทำงานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาอุปกรณ์ในระบบคอมพิวเตอร์ตามระยะเวลาที่กำหนด

4.5.2 การบริหารจัดการโปรแกรม

- (1) จัดทำทะเบียนคุมโปรแกรม
- (2) มีการติดตั้งโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือโปรแกรมสำหรับใช้งานฟรี (Freeware, Open Source)

และติดตั้งเท่าที่จำเป็นต่อการใช้งาน

4.5.3 การบริหารจัดการเครือข่ายสื่อสาร

- (1) มีการจัดแบ่งแยกส่วนเครือข่าย/กลุ่ม (VLAN / Zone)
- (2) จัดทำทะเบียนคุมการใช้งานเครือข่ายสื่อสาร
- (3) จัดทำแผนผังและขอบเขตของระบบเครือข่ายสื่อสาร
- (4) ตรวจสอบการใช้งานเครือข่ายสื่อสารให้สามารถใช้งานได้อย่างมีประสิทธิภาพ
- (5) ควบคุมการจัดเส้นทางบนเครือข่ายสื่อสารและกำหนดวิธีการเข้าถึงเครือข่ายสื่อสารบริษัทฯ
- (6) จัดทำระบบป้องกันการบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่ายสื่อสาร
- (7) ทดสอบการบุกรุกโจมตีเครือข่ายสื่อสาร และจัดทำรายงานการโจมตี
- (8) กำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายสื่อสาร

และอุปกรณ์ที่เชื่อมต่อ

- (9) ทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ 1 ครั้ง
- (10) ทำการบำรุงรักษาระบบเครือข่ายสื่อสารเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแล

ให้มีการบำรุงรักษาระบบเครือข่ายตามระยะเวลาที่กำหนด

4.5.4 การบริหารจัดการสินทรัพย์

- (1) จัดทำทะเบียนคุมสินทรัพย์
 - 1) กำหนดผู้รับผิดชอบต่อสินทรัพย์
 - 2) จัดหมวดหมู่สินทรัพย์
- (2) การเบิกใช้ทรัพย์สินคอมพิวเตอร์และเครือข่าย
 - 1) ผู้ใช้ที่ต้องการขอเบิกใช้ทรัพย์สินต้องกรอกข้อมูลคำขอลงในแบบฟอร์ม “การขอเบิกใช้ทรัพย์สินคอมพิวเตอร์และเครือข่าย” โดยระบุรายการทรัพย์สินที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ
 - 2) เจ้าหน้าที่ผู้รับผิดชอบพิจารณาตามขั้นตอนและความเหมาะสมในการขอเบิกใช้งานทรัพย์สินดังกล่าว โดยขอความเห็นชอบจากผู้บริหารหน่วยงานเจ้าของสินทรัพย์ หรือผู้ที่ได้รับมอบหมาย
 - 3) เมื่อมีการอนุมัติให้เบิกใช้ทรัพย์สิน เจ้าหน้าที่ผู้รับผิดชอบต้องบันทึกข้อมูลสถานที่จัดเก็บหรือติดตั้งใหม่ของทรัพย์สินดังกล่าว แบบคำขอลงทะเบียนทรัพย์สินคอมพิวเตอร์และเครือข่ายสื่อสารเพื่อจัดเก็บเป็นประวัติทรัพย์สิน
- (3) การแจ้งซ่อมบำรุงทรัพย์สินคอมพิวเตอร์และเครือข่าย
 - 1) เมื่อผู้ใช้งานพบการทำงานที่ผิดปกติของทรัพย์สิน หรือไม่สามารถใช้งานทรัพย์สินในการดำเนินงานได้ ผู้ใช้งานต้องแจ้งให้ดำเนินการซ่อมบำรุง โดยกรอกข้อมูลทรัพย์สินที่ต้องการแจ้งลงในแบบฟอร์ม “แจ้งซ่อม”



- 2) เจ้าหน้าที่ผู้รับผิดชอบวิเคราะห์อาการเสียหายของทรัพย์สิน จากข้อมูลในรูปแบบฟอร์ม **“แจ้งซ่อม”** และจากการทดสอบการทำงานด้วยตนเอง รวมถึงพิจารณาข้อมูลประกอบโดยเฉพาะในส่วนของระยะเวลาประกันของทรัพย์สินดังกล่าว ซึ่งหากอยู่ในระยะเวลาประกันเจ้าหน้าที่สามารถส่งทรัพย์สินเข้ารับการซ่อมบำรุงที่ศูนย์บริการของบริษัทผู้ผลิตทรัพย์สินได้ โดยไม่เสียค่าใช้จ่ายในส่วนที่ระบุในประกัน หากทรัพย์สินดังกล่าวไม่อยู่ในระยะเวลาประกัน เจ้าหน้าที่ผู้รับผิดชอบต้องพิจารณาจากความเสียหายของทรัพย์สิน หากความเสียหายของทรัพย์สินสามารถแก้ไขได้ให้ดำเนินการแก้ไข หรือหากเสียหายมากอาจจำเป็นต้องจำหน่ายทรัพย์สินดังกล่าว
 - 3) ในระหว่างที่เจ้าหน้าที่ผู้รับผิดชอบส่งทรัพย์สินเข้ารับการซ่อมบำรุงนั้น หากมีทรัพย์สินอื่นที่สามารถใช้งานทดแทนทรัพย์สินดังกล่าวได้ ให้เจ้าหน้าที่ดำเนินการแจ้งแก่ผู้ใช้ โดยให้ผู้ใช้ทำเรื่องเบิกใช้งานทรัพย์สิน โดยกรอกข้อมูลลงในแบบฟอร์ม **“การขอเบิกใช้ทรัพย์สินคอมพิวเตอร์และเครือข่าย”** โดยระบุรายการทรัพย์สินที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ และเจ้าหน้าที่ผู้ดูแลทะเบียนทรัพย์สินทำการบันทึกข้อมูลทรัพย์สินใหม่ลงในแบบฟอร์ม **“ทะเบียนทรัพย์สินคอมพิวเตอร์และเครือข่าย”** เพื่อจัดเก็บเป็นประวัติทรัพย์สินของบริษัท
 - 4) หลังจากที่เจ้าหน้าที่ผู้รับผิดชอบส่งทรัพย์สินที่พบความเสียหายเข้ารับการแก้ไขเรียบร้อยแล้ว ต้องดำเนินการทดสอบในส่วนที่พบความเสียหายอีกครั้ง ก่อนจัดส่งทรัพย์สินคืนผู้ใช้โดยเจ้าหน้าที่ผู้รับผิดชอบกรอกข้อมูลรายละเอียดการซ่อมบำรุง และการทดสอบทรัพย์สินลงในแบบฟอร์ม **“แจ้งซ่อม”** และส่งคืนทรัพย์สินดังกล่าวให้กับผู้ใช้
 - 5) ผู้ใช้ทำการตรวจสอบทรัพย์สิน หากสามารถใช้งานได้ตามปกติให้ลงลายมือชื่อเพื่อรับทรัพย์สินกลับไปใช้งาน แต่หากยังพบว่ามีความเสียหายในส่วนเดิมหรือส่วนอื่น ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบ เพื่อดำเนินการแก้ไขตามขั้นตอนต่อไป
- (4) การนำสินทรัพย์ของบริษัทฯออกนอกสถานที่ ให้มีการบันทึกขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกสถานที่ เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน
- (5) การจำหน่ายทรัพย์สินคอมพิวเตอร์และเครือข่าย
- 1) กรณีที่ทรัพย์สินเสียหายเกินกว่าที่จะแก้ไขได้ รวมถึงไม่อยู่ในระยะเวลาประกันประกอบกับเมื่อพิจารณาถึงมูลค่าของทรัพย์สินกับค่าใช้จ่ายในการซ่อมบำรุงแล้ว จำเป็นต้องดำเนินการจำหน่ายทรัพย์สินดังกล่าว ให้เจ้าหน้าที่ผู้รับผิดชอบกรอกรายละเอียดทรัพย์สินลงในแบบฟอร์ม **“การส่งคืนทรัพย์สินคอมพิวเตอร์และเครือข่าย”** ให้เจ้าหน้าที่ผู้เป็นเจ้าของงาน/โครงการ ซึ่งเป็นผู้ใช้หรือผู้จัดหาทรัพย์สินรับทราบและพิจารณาเห็นชอบ
 - 2) เจ้าหน้าที่ผู้เป็นเจ้าของงาน/โครงการ พิจารณาเรื่องการส่งคืนทรัพย์สิน หากเห็นชอบให้ลงลายมือชื่อในแบบฟอร์ม **“การส่งคืนทรัพย์สินคอมพิวเตอร์และเครือข่าย”** หากไม่เห็นชอบให้ระบุเหตุผลและส่งเรื่องคืนเจ้าหน้าที่ผู้รับผิดชอบ
 - 3) ส่งเรื่องให้หน่วยงานที่มีอำนาจอนุมัติการจำหน่ายทรัพย์สินพิจารณาดำเนินการต่อไป



4.6 การควบคุมความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

4.6.1 ควรมีการจัดทำตารางงาน ลำดับของงานก่อนหลัง สำหรับการส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการข้อผิดพลาดที่เกิดขึ้น (Job Schedule) ทั้งนี้การจัดตารางงานนั้น ควรมีการทดสอบการทำงานว่าเป็นไปตามลำดับของงานตามที่กำหนดไว้

4.6.2 ควรมีการกำหนดบทบาทและหน้าที่ของผู้รับผิดชอบในการปฏิบัติงาน และ/หรือบุคคลที่เกี่ยวข้องกับการปฏิบัติงานในขั้นตอนต่างๆ และผู้มีอำนาจอนุมัติ

4.7 การรักษาความมั่นคงปลอดภัยการสำรองข้อมูลและกู้คืนข้อมูล

4.7.1 มีระบบจัดเก็บและสำรองข้อมูล ตามประเภทของข้อมูล ได้แก่ โปรแกรมระบบปฏิบัติการโปรแกรมประยุกต์หรือแอปพลิเคชัน (Application Software) ชุดคำสั่ง และข้อมูล อย่างน้อย 1 ชุด แยกสถานที่จัดเก็บแยกจากกัน เพื่อความมั่นคงปลอดภัยและใช้งานได้อย่างต่อเนื่อง

4.7.2 กำหนดผู้รับผิดชอบในการสำรองข้อมูล ตรวจสอบความมืออยู่อย่างถูกต้อง ครบถ้วนของข้อมูล อย่างน้อยปีละ 1 ครั้ง และมีการบันทึกรายละเอียดการตรวจสอบ ในกรณีตรวจพบข้อมูลสูญหายไม่ถูกต้องครบถ้วน ให้ดำเนินการปรับปรุง แก้ไขข้อมูลให้มีความสมบูรณ์ครบถ้วนในทันที

4.7.3 กำหนดความถี่ในการสำรองข้อมูลของระบบงาน และทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ (ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรจะมีความถี่ในการสำรองข้อมูลมากขึ้น) และมีการนำข้อมูลที่สำรองไปเก็บไว้ในสถานที่อย่างน้อย 1 ชุด

- (1) กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์
- (2) ทำการตรวจสอบว่าการสำรองข้อมูลที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่
- (3) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่

4.7.4 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะเวลาที่กำหนด โดยมีแนวทางปฏิบัติสำหรับการกู้คืนข้อมูลจากภัยพิบัติ โดย

(1) มีกำหนดระบบงานที่มีความสำคัญทั้งหมดของบริษัทฯ และจัดทำเป็นบัญชีรายชื่อของระบบงานดังกล่าว รวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

(2) ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงที่พบ และให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

(3) กำหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบงาน หรือข้อมูลในฐานข้อมูล

(4) กำหนดความถี่ในการสำรองข้อมูลและวิธีการสำรอง เช่น แบบ Full Backup หรือ Incremental Backup ของระบบงานที่มีความสำคัญเหล่านั้น

(5) จัดทำแผนกู้คืนเพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้นได้ แผนกู้คืนต้องมีรายละเอียดดังต่อไปนี้

- 1) การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
- 2) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้
- 3) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
- 4) การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้
- 5) การทดสอบตามแผนเตรียมความพร้อมฯ อย่างน้อยปีละ 1 ครั้ง



- 6) การกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการ เครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์
- 7) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(6) ให้ทำการทบทวนแผนกู้คืนอย่างน้อยปีละ 1 ครั้ง

(7) ให้ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่าง

สม่ำเสมอว่าข้อมูลที่สำคัญไปนั้นมีความครบถ้วน

(8) ให้ทำการทดสอบกู้คืนข้อมูลที่สำคัญไว้แล้วว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ อย่างน้อยปีละ 1 ครั้ง

ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

4.7.5 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ เพื่อให้การปฏิบัติงานเป็นไปอย่างต่อเนื่อง

(1) ให้เตรียมแบบฟอร์ม/แบบพิมพ์ที่สามารถใช้ทดแทนแบบฟอร์ม/แบบพิมพ์ที่พิมพ์ได้จากระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(2) ให้ปฏิบัติงานตามกระบวนการงานเดิมก่อนที่จะนำระบบเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันมาใช้ เช่น การใช้ระบบมือ (Manual System)

(3) เมื่อระบบเทคโนโลยีสารสนเทศและการสื่อสารสามารถใช้งานได้ตามปกติให้นำข้อมูลที่เกิดขึ้นระหว่างที่เกิดเหตุฉุกเฉินฯ เข้าระบบ

4.8 การประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

4.8.1 มีคณะทำงานบริหารความเสี่ยงของฝ่ายสารสนเทศ เพื่อดำเนินการ

(1) จัดลำดับความสำคัญของความเสี่ยง

(2) จัดทำแผนบริหารความเสี่ยง

(3) ดำเนินการตามแผนบริหารความเสี่ยง

4.8.2 มีการตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง

4.8.3 มีการรายงานการตรวจสอบและประเมินความเสี่ยงเสนอผู้รับผิดชอบ และหน่วยงานที่รับผิดชอบ และจะดำเนินการปรับปรุงตามคำแนะนำหน่วยงานที่รับผิดชอบนั้นโดยทันที

4.8.4 มีการกำหนดความรับผิดชอบของผู้ใช้งานหรือผู้บริหาร ให้ผู้ใช้งานและผู้บริหารรับผิดชอบในกรณีเกิดความเสียหายหรืออันตรายอันเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่องหรือไม่ปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แล้วแต่กรณี

4.9 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

4.9.1 มีการเผยแพร่ประชาสัมพันธ์และฝึกอบรม ให้เจ้าหน้าที่บริษัทฯ รับทราบ เข้าใจและไม่กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงมีความรับผิดชอบในการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศของบริษัทอย่างเหมาะสม

4.9.2 มีการทบทวนปรับปรุงนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้มีความทันสมัย และเป็นมาตรฐานที่ยอมรับอย่างน้อยปีละ 1 ครั้ง



5. บทลงโทษ

บริษัทฯ จะดำเนินการลงโทษทางวินัยแก่ผู้ฝ่าฝืนหรือเพิกเฉยต่อการกระทำผิด ตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และ/หรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จะต้องได้รับโทษตามที่กฎหมายกำหนด (ถ้ามี)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้รับอนุมัติโดยมติที่ประชุมคณะกรรมการธรรมาภิบาลและบริหารความเสี่ยง ครั้งที่ 2 (ชุดที่ 7) เมื่อวันที่ 28 กุมภาพันธ์ 2565 เป็นต้นไป โดยยกเลิกแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีผลใช้บังคับเมื่อวันที่ 28 กุมภาพันธ์ 2563 ที่ได้รับอนุมัติจากที่ประชุมคณะกรรมการธรรมาภิบาลและบริหารความเสี่ยง ครั้งที่ 3 (ชุดที่ 5) เมื่อวันที่ 27 กุมภาพันธ์ 2563

นายพนพร พงษ์เวช

(นายพนพร พงษ์เวช)

ประธานกรรมการธรรมาภิบาลและบริหารความเสี่ยง