บริษัท ซัมมิท คอมพิวเตอร์ จำกัด
Summit Computer Co., Ltd.

นโยบายและแนวปฏิบัติเกี่ยวกับ
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

Information Technology Security
Policy and Guideline

จัดทำโดย

บริษัท ซัมมิท คอมพิวเตอร์ จำกัด
Summit Computer Co., Ltd.

การจัดทำเอกสาร

เวอร์ชัน	วันที่ปรับปรุง	รายละเอียด	ผู้จัดทำ
1.0	1 เม.ย. 2562	เขียนครั้งแรก	รพีพงศ์ นิสสัยสุข
2.0	28 ก.พ. 2566	ปรับปรุงให้ทันสมัย	พนิดา จงมั่นเกษมสุข
3.0	1 มี.ค. 2567	เพิ่มการควบคุมการใช้งานในระบบคลาวด์	พนิดา จงมั่นเกษมสุข

บริษัทขอยกเลิกนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เวอร์ชัน 1.0 ลงวันที่ 1 เมษายน 2562 และ เวอร์ชัน 2.0 ลงวันที่ 28 กุมภาพันธ์ 2566 และบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เวอร์ชัน 3.0 ลงวันที่ 1 มีนาคม 2567 ทั้งนี้ให้มีผลตั้งแต่วันที่ 1 มีนาคม 2567 เป็นต้นไป

(จินดา บุญลาภทวีโชค)

กรรมการผู้จัดการ

สารบัญ

หน้า

ส่วน 1 หลักการและเหตุผล

1. หลักการและเหตุผล

บริษัท ซัมมิท คอมพิวเตอร์ จำกัด ได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Technology Security Policy) เพื่อเป็นมาตรฐานและแนวปฏิบัติให้ระบบเทคโนโลยีสารสนเทศของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศ ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ทั้งจากภายในและภายนอก ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจก็ตาม อันเป็นการลดความเสียหายต่าง ๆ และรักษาไว้ซึ่งความสามารถในการดำเนินงานได้อย่างมีประสิทธิภาพ และเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยการดำเนินการดังกล่าวจะเป็นมาตรการที่ช่วยยกระดับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงการดำเนินงานตามกรอบมาตรฐานสากล ISO/IEC 27001

หลักการ

ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่บริษัทได้จัดเตรียมให้ใช้งาน จำเป็นจะต้องมีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินกิจการ มุ่งหมายไปในด้านความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ โดยอธิบายได้ ดังนี้

การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้สินทรัพย์สามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งสินทรัพย์นั้นด้วย ดังนั้นในการรักษาความลับจำเป็นจะต้องมีการควบคุมทั้งทางกายภาพและทางเทคนิค โดยผู้ที่ไม่มีสิทธิจะต้องไม่สามารถเข้าถึงสินทรัพย์นั้นได้ และสินทรัพย์จำเป็นจะต้องมีการจำแนกและกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ที่ถือครองสินทรัพย์ปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น

ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้สินทรัพย์ถูกเปลี่ยนแปลงแก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิที่จะแก้ไขสินทรัพย์เหล่านั้น ดังนั้นการควบคุมและป้องกันจึงต้องประกอบด้วยการกำหนดสิทธิในการแก้ไข กำหนดสิทธิในการเข้าถึง และจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีสินทรัพย์และการตรวจสอบทางเทคนิคด้วย

ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้มีสิทธิสามารถเข้าใช้งานสินทรัพย์นั้นได้เมื่อต้องการใช้งานทั้งในทางกายภาพและทางเทคโนโลยี ได้แก่ การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้นเมื่อผู้ใช้ต้องการจะรับหรือส่ง ระบบจำเป็นต้องสามารถให้บริการได้ตลอดเวลา เป็นต้น

นอกจากนี้จะต้องมีผู้รับผิดชอบต่อการกระทำ (Accountability) ซึ่งหมายถึง สินทรัพย์จำเป็นจะต้องมีผู้รับผิดชอบและสามารถอธิบายได้ถึงผลที่เกิดขึ้นไม่ว่าผลนั้นเกิดจากการกระทำจากบุคคลหรือสิ่งอื่นใด

1.1 วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศ ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ

บริษัทจึงเห็นสมควรกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) วิธีการปฏิบัติ (Work Instruction) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังนี้

1. เพื่อให้บริษัทมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีความสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง
2. เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ อ้างอิงตามนโยบายมาตรฐานที่บริษัทปรับใช้และนโยบายอื่นๆ ที่เกี่ยวข้อง
3. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีการปฏิบัติ ให้พนักงานตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและสามารถปฏิบัติตามอย่างเคร่งครัด
4. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงคุณภาพความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

1.2 ขอบเขต

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ มีผลบังคับใช้กับผู้บริหารและพนักงานทุกระดับ โดยมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามนโยบายอย่างเคร่งครัด ผู้ใช้งานที่เกี่ยวข้องจะต้องให้ความร่วมมือในการดำเนินการตามนโยบายนี้ หากมีการฝ่าฝืนจนเป็นเหตุให้เกิดความเสียหายแก่บริษัทหรือบุคคลหนึ่งบุคคลใด บริษัทจะพิจารณาดำเนินการทางวินัย ตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายประกอบอื่น ๆ แก่พนักงานที่ฝ่าฝืนตามความเหมาะสม

1.3 ความหมายและคำจำกัดความ

1. “บริษัท” หมายถึง บริษัท ซัมมิท คอมพิวเตอร์ จำกัด
2. “ผู้บริหาร” หมายถึง กรรมการผู้จัดการ และกรรมการบริษัท
3. “ผู้จัดการ/หัวหน้าทีม” หมายถึง ผู้จัดการแผนก ผู้จัดการโครงการ และหัวหน้าทีมพัฒนาระบบ
4. “ผู้ใช้งาน” หมายถึง ผู้บริหาร พนักงานบริษัท และผู้ใช้งานที่เกี่ยวข้อง
5. “ผู้ใช้งานภายนอก” หมายถึง บุคคลหรือนิติบุคคลที่เข้ามาดำเนินกิจกรรมภายในบริษัท ผู้รับจ้างหรือผู้ที่ได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์หรือระบบเครือข่ายของบริษัท
6. “บุคคลภายนอก” หมายถึง บุคคล หรือนิติบุคคลนอกเหนือจากข้อ (4) และ (5)
7. “ส่วนเทคโนโลยีสารสนเทศ” หมายถึง แผนกที่ดูแลรักษาอุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ ระบบเครือข่ายของบริษัท

8. “ผู้ดูแลระบบ” หมายถึง ผู้ที่มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแลการใช้ระบบงาน

9. “ระบบสารสนเทศ” หมายถึง ระบบงานของบริษัทที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศ ซึ่งทำงานประสานกันระหว่างอุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผลให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของบริษัท

10. “อุปกรณ์คอมพิวเตอร์” หมายถึง อุปกรณ์ที่มีหน่วยประมวลผล หน่วยความจำ ส่วนบันทึกข้อมูล ส่วนการเชื่อมต่อเครือข่าย ส่วนรับข้อมูล และส่วนแสดงผล ได้แก่ คอมพิวเตอร์แม่ข่าย คอมพิวเตอร์แบบตั้งโต๊ะ คอมพิวเตอร์แบบพกพา

11. “อุปกรณ์เคลื่อนที่” หมายถึง อุปกรณ์คอมพิวเตอร์แบบพกพาที่มีขนาดเล็ก สามารถใช้เพียงมือเดียวในการใช้งาน ส่วนของการรับข้อมูลเป็นแบบสัมผัสโดยไม่ต้องใช้คีย์บอร์ด และสามารถเชื่อมต่อเครือข่ายไร้สาย เครือข่ายโทรศัพท์ได้ เช่น Smartphone, Tablet เป็นต้น

12. “ระบบคลาวด์” (Cloud Computing) หมายถึง บริการเช่าใช้ระบบคอมพิวเตอร์หรือทรัพยากรด้านคอมพิวเตอร์ของผู้ให้บริการที่เป็นหน่วยงานภายนอก โดยครอบคลุมทั้งฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการประมวลผล การจัดเก็บข้อมูล และระบบออนไลน์ต่าง ๆ ผ่านอินเตอร์เน็ต โดยสามารถเลือกกำลังการประมวลผล เลือกจำนวนทรัพยากร ได้ตามความต้องการในการใช้งาน

13. “สินทรัพย์ด้านสารสนเทศ” หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตน อันมีมูลค่าหรือคุณค่าสำหรับบริษัท ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เคลื่อนที่ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก อุปกรณ์ต่อพ่วงทุกชนิด ระบบเครือข่าย ระบบสารสนเทศ ระบบคลาวด์

14. “ผู้ตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง ผู้ที่ได้รับการแต่งตั้งจากผู้บริหาร ให้ทำหน้าที่ตรวจสอบการปฏิบัติหน้าที่ของผู้ใช้งาน ให้เป็นไปตามแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ

15. “คณะดูแลความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง คณะทำงานที่ได้รับการแต่งตั้งจากผู้บริหาร ให้เป็นผู้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และกำกับ ดูแลผู้ใช้งานให้ปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

1.4 การเผยแพร่และการทบทวน

นโยบายนี้จะเผยแพร่โดยการประกาศในระบบ SPIN (Summit Personnel Information Network) เพื่อให้พนักงานทุกระดับในบริษัทได้รับทราบ และพนักงานทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด นโยบายนี้ต้องถูกทบทวนอย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ส่วน 2 นโยบายการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ

2. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(Information Technology Security Policy)

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ถูกจัดทำขึ้นเพื่อกำหนดทิศทาง หลักการและกรอบของข้อกำหนดในการป้องกันสินทรัพย์ที่เกี่ยวข้องกับสารสนเทศ ให้ปลอดภัยจากภัยคุกคามที่อาจก่อให้เกิดความเสียหายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลสารสนเทศ

เพื่อผลักดันให้มีการควบคุมภายในด้านสารสนเทศที่รัดกุมตามแนวความเสี่ยง ที่สอดคล้องกับมาตรฐานสากล และเพื่อสนับสนุนให้ผู้ใช้งานตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงความสำคัญในการบริหารจัดการความเสี่ยงด้านสารสนเทศ

2.1 นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. ผู้บริหารเป็นผู้รับผิดชอบความเสี่ยง ความเสียหายต่อระบบสารสนเทศของบริษัท ซึ่งเกิดจากการละเลย ละเว้นการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศ
2. ผู้บริหารแต่งตั้ง “คณะดูแลความมั่นคงปลอดภัยด้านสารสนเทศ” และ “ผู้ตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ”
3. ผู้บริหารต้องให้การสนับสนุนการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งด้านงบประมาณ ทรัพยากรบุคคล การบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัย
4. ผู้บริหารต้องกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยง
5. ผู้บริหารต้องจัดให้มีการประเมินความเสี่ยง และทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยการประเมินความเสี่ยงดังกล่าว ต้องพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจที่บริษัทกำหนดไว้
6. ผู้บริหารต้องประเมินผลสัมฤทธิ์ของนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ประกาศใช้ เพื่อนำมาปรับปรุงแผนกลยุทธ์ให้สอดคล้องกับภัยคุกคามในปัจจุบันและที่อาจเกิดขึ้นในอนาคต
7. ผู้บริหารต้องสนับสนุนให้มีการสร้างความตระหนักด้านความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
8. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องได้รับการอนุมัติจากกรรมการผู้จัดการเพื่อประกาศใช้และถือปฏิบัติทั้งบริษัท โดยให้มีผลบังคับใช้กับพนักงานในทุกระดับชั้นของบริษัท และบุคคลภายนอก ที่เกี่ยวข้องกับการใช้สินทรัพย์ด้านสารสนเทศของบริษัท

9. การปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องได้รับการตรวจสอบโดยผู้ตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง และรายงานผลการตรวจสอบให้ผู้บริหารทราบ ทั้งนี้ให้คณะดูแลความมั่นคงปลอดภัยด้านสารสนเทศเป็นผู้รับผิดชอบในการติดตามผลการปรับปรุงหรือแก้ไขปัญหาที่พบจากการตรวจสอบนั้น

10. ผู้ใช้งานมีสิทธิใช้ระบบสารสนเทศตามอำนาจหน้าที่ที่ได้รับมอบหมาย ภายใต้แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หากมีการฝ่าฝืนจนเป็นเหตุให้เกิดความเสียหายแก่บริษัทหรือบุคคลหนึ่งบุคคลใด บริษัทจะพิจารณาดำเนินการทางวินัย ตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายประกอบอื่น ๆ แก่พนักงานที่ฝ่าฝืนตามความเหมาะสม

11. บริษัทสงวนสิทธิ์ในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามีการละเมิดนโยบายการใช้งาน

2.2 หน้าที่ความรับผิดชอบ

1. **ผู้บริหาร** กำหนดแผนกลยุทธ์ ให้การสนับสนุน ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

2. **คณะดูแลความมั่นคงปลอดภัยด้านสารสนเทศ** จัดทำแนวปฏิบัติและหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และติดตามการปฏิบัติหน้าที่ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3. **ผู้ตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศ** ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ และการปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามความจำเป็น และรายงานผลการตรวจสอบแก่ผู้บริหาร

4. **ส่วนเทคโนโลยีสารสนเทศ** กำกับ ควบคุมดูแล ติดตั้ง/ปรับปรุงระบบสารสนเทศ ให้เป็นไปตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

5. **ผู้จัดการ/หัวหน้าทีม** พิจารณาอนุมัติและควบคุมดูแลพนักงานให้ปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

6. **ผู้ใช้งาน** ปฏิบัติหน้าที่ที่รับผิดชอบตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

ส่วน 3 แนวปฏิบัติความมั่นคงปลอดภัย ด้านสารสนเทศ

3. การบริหารจัดการทรัพยากรบุคคล
(Human Resource Management)

เพื่อให้บริษัทมีกระบวนการในการคัดเลือกบุคลากร ฝึกอบรมและควบคุมการปฏิบัติงานของบุคลากรในองค์กรอย่างเหมาะสมตลอดระยะเวลาการจ้างงาน และเพื่อให้เข้าใจถึงหน้าที่ความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศของบริษัท

3.1 ก่อนการจ้างงาน

1) แผนกทรัพยากรบุคคลต้องตรวจสอบคุณสมบัติของผู้สมัครงานทุกคน ก่อนที่จะบรรจุเป็นพนักงานของบริษัท เช่น ข้อมูลส่วนตัว, การศึกษา, การติดสารเสพติด และประวัติอาชญากรรม เป็นต้น

2) แผนกทรัพยากรบุคคลต้องกำหนดเงื่อนไขการจ้างงาน รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท และยอมรับข้อตกลงในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบ

3) พนักงานทุกคนที่ปฏิบัติงานในบริษัท ต้องลงนามรับทราบและยินยอมปฏิบัติตามข้อตกลงการรักษาข้อมูลที่เป็นความลับของบริษัท และเอกสารอื่น ๆ ที่เกี่ยวข้อง ก่อนอนุญาตให้เริ่มงานหรือเข้าถึงและใช้งานข้อมูลสารสนเทศของบริษัท

4) แผนกทรัพยากรบุคคลจัดเตรียมบัญชีผู้ใช้งาน เมื่อบรรจุเป็นพนักงานใหม่ของบริษัท

3.2 ระหว่างการจ้างงาน

1) พนักงานใหม่ของบริษัท ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการบันทึกการอบรมและเก็บรวบรวมไว้

2) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานอย่างสม่ำเสมอ

3) กรณีที่มีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนเทคโนโลยีสารสนเทศ ต้องแจ้งให้พนักงานทราบเกี่ยวกับการเปลี่ยนแปลงนั้น ๆ

3.3 การเปลี่ยนตำแหน่งหรือการสิ้นสุดการจ้างงาน

1) เมื่อมีการเปลี่ยนตำแหน่งหรือสิ้นสุดการจ้างงาน แผนกทรัพยากรบุคคลต้องรายงานการเปลี่ยนแปลงดังกล่าวให้ส่วนเทคโนโลยีสารสนเทศทราบ เพื่อดำเนินการเปลี่ยนแปลง/เพิกถอน/ยกเลิก/ระงับสิทธิการใช้งานระบบสารสนเทศของผู้ใช้งาน

2) ส่วนเทคโนโลยีสารสนเทศ ต้องดำเนินการเปลี่ยนแปลง/เพิกถอน/ยกเลิก/ระงับสิทธิการใช้งานระบบสารสนเทศของผู้ใช้งาน เพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะการว่าจ้าง โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิในระบบสารสนเทศที่เกิดขึ้นได้

3) เมื่อสิ้นสุดการจ้างงาน ผู้ใช้งานจะต้องคืนสินทรัพย์ที่เป็นของบริษัท เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์เคลื่อนที่ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออกอาคาร ให้กับแผนกทรัพยากรบุคคล สำหรับซอฟต์แวร์ที่มีลิขสิทธิ์คืนให้กับส่วนเทคโนโลยีสารสนเทศ

3.4 บทลงโทษ

ผู้ใช้งานที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จนเป็นเหตุให้เกิดความเสียหายแก่บริษัทหรือบุคคลหนึ่งบุคคลใด บริษัทจะพิจารณาดำเนินการทางวินัย ตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายประกอบอื่น ๆ แก่พนักงานที่ฝ่าฝืนตามความเหมาะสม

4. การบริหารจัดการสินทรัพย์

(Asset Management)

เพื่อให้มีการระบุสินทรัพย์ของบริษัท หรือสินทรัพย์ที่นำมาใช้งานในบริษัท และกำหนดหน้าที่ความรับผิดชอบในการปกป้องสินทรัพย์จากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นอย่างเหมาะสม

4.1 ความรับผิดชอบต่อข้อมูลสารสนเทศที่มีชั้นความลับ

1) การจัดระดับชั้นความลับต้องพิจารณาถึงข้อกำหนดทางด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวเพื่อป้องกันมิให้ข้อมูลถูกเปิดเผย หรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต โดยให้ปฏิบัติอย่างเหมาะสมตามระดับชั้นความลับของข้อมูล

2) ผู้จัดการ/หัวหน้าทีม ต้องกำหนดประเภทของข้อมูล ระดับความสำคัญ ลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง และช่องทางการเข้าถึง เป็นลายลักษณ์อักษร และมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ

3) ข้อมูลที่มีชั้นความลับ หรือข้อมูลที่มีความสำคัญมาก รวมถึงข้อมูลในคอมพิวเตอร์ ต้องเคลื่อนย้ายโดยผู้เป็นเจ้าของข้อมูลเท่านั้น ไม่เคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

4) ข้อมูลที่มีความสำคัญ มีการรักษาความลับต้องมีการเข้ารหัสเมื่อถูกจัดเก็บ

5) การแบ่งประเภทของข้อมูล

5.1) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์

5.2) ข้อมูลบุคลากร ได้แก่ ประวัติพนักงาน ประวัติการศึกษา ประวัติการอบรม

5.3) ข้อมูลงบประมาณการเงินและบัญชี

5.4) ข้อมูลสารสนเทศของโครงการต่าง ๆ

6) การแบ่งระดับชั้นความลับของข้อมูล

6.1) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

6.2) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

6.3) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

6.4) ข้อมูลใช้ภายใน หมายถึง ข้อมูลที่ใช้เฉพาะภายในบริษัทเท่านั้น

6.5) ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่แก่สาธารณะได้

7) การจัดแบ่งระดับชั้นการเข้าถึงและการใช้งานข้อมูล

7.1) การเข้าถึงและการใช้งานข้อมูลลับที่สุด กรรมการผู้จัดการเป็นผู้กำหนดสิทธิในการเข้าถึงและใช้งานข้อมูล และต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

7.2) การเข้าถึงและการใช้งานข้อมูลลับมาก กรรมการผู้จัดการเป็นผู้กำหนดสิทธิในการเข้าถึงและใช้งานข้อมูล และต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

7.3) การเข้าถึงและการใช้งานข้อมูลลับ กรรมการผู้จัดการเป็นผู้กำหนดสิทธิในการเข้าถึงและใช้งานข้อมูล และต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

7.4) การเข้าถึงและการใช้งานกลุ่มข้อมูลภายใน พนักงานของบริษัทสามารถเข้าถึงและใช้งานข้อมูลได้

7.5) การเข้าถึงและการใช้งานข้อมูลสาธารณะ ไม่มีข้อบังคับพิเศษ

4.2 ความรับผิดชอบต่อการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่

1) อุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของบริษัท ถือเป็นสินทรัพย์ของบริษัท ใช้เพื่อการดำเนินงานของบริษัทเท่านั้น

2) ห้ามมิให้ผู้ใช้งานทำการดัดแปลง/แก้ไข Configuration หรือส่วนประกอบของอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของบริษัท โดยไม่ได้รับอนุญาต

3) ไม่ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่นำมาใช้งานในบริษัท ผิดวัตถุประสงค์ ประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม

4) อุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่นำมาใช้งานในบริษัท ต้องนำอุปกรณ์ไปลงทะเบียนกับส่วนเทคโนโลยีสารสนเทศ

5) การเชื่อมต่ออุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่นำมาใช้งานในบริษัท กับเครือข่ายของบริษัท รวมทั้งการเข้าถึงระบบงานภายในต้องได้รับอนุญาตจากผู้จัดการ/หัวหน้าทีม

6) อุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่นำมาใช้งานในบริษัท ต้องติดตั้งโปรแกรมป้องกันไวรัส ห้ามปิด ยกเลิก กระทำการใด ๆ ที่อาจส่งผลต่อระบบการป้องกันไวรัสหรือระบบป้องกันมัลแวร์อื่นใด

7) หากสงสัยว่าอุปกรณ์คอมพิวเตอร์และ/หรืออุปกรณ์เคลื่อนที่ที่นำมาใช้งานในบริษัท ติดมัลแวร์หรือพบข้อมูลภัยคุกคาม ผู้ใช้งานต้องยุติการเชื่อมต่อเข้ากับระบบเครือข่าย และให้แจ้งส่วนเทคโนโลยีสารสนเทศทันที

8) อุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่นำมาใช้งานในบริษัท ต้องจัดเก็บในที่ปลอดภัย ไม่วางทิ้งไว้ในที่เสี่ยงต่อการสูญหาย ในกรณีที่อุปกรณ์สูญหาย ต้องแจ้งส่วนเทคโนโลยีสารสนเทศโดยทันที

9) ต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ในสถานที่ที่มีความร้อนชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ ไม่ใช้หรือวางใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน

10) การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับหรือโยน ไม่เคลื่อนย้ายอุปกรณ์ขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่

11) ข้อมูลที่มีชั้นความลับซึ่งถูกจัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่นำมาใช้งานในบริษัท ต้องบริหารจัดการตามระดับชั้นความลับของข้อมูลอย่างเคร่งครัด

12) ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการ ต้องคืนอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของบริษัทที่รับผิดชอบทั้งหมดต่อบริษัทในสภาพที่พร้อมใช้งาน

13) การคืน หรือส่งซ่อมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของบริษัท ให้ลบข้อมูลอย่างปลอดภัย ตามระดับความลับของข้อมูลที่อยู่ในอุปกรณ์นั้น

14) การนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไปปฏิบัติงานภายนอก ให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

4.3 ความรับผิดชอบต่อการใช้โปรแกรมคอมพิวเตอร์

1) ห้ามมิให้ผู้ใช้งานติดตั้ง หรือใช้งานโปรแกรมเพิ่มเติม หรือใช้งานโปรแกรมที่สุ่มเสี่ยงกับการกระทำผิดกฎหมาย หรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท

2) ห้ามมิให้ผู้ใช้งานครอบครอง หรือพัฒนาโปรแกรมไวรัส หรือโปรแกรมที่ก่อกวน หรือโปรแกรมที่ส่งผลต่อระบบของบริษัทหรือองค์กรอื่น ๆ โดยไม่ได้รับอนุญาต

3) ห้ามมิให้ผู้ใช้งานคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย

4) กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานไม่ว่าจะมีลิขสิทธิ์ หรือ Freeware หรือ Open source ก็ตาม ต้องได้รับความเห็นชอบจากส่วนเทคโนโลยีสารสนเทศก่อน หากฝ่าฝืนและเกิดความเสียหายหรือละเมิดเกิดขึ้น ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

4.4 ความรับผิดชอบต่อการใช้สื่อบันทึกข้อมูล

1) สื่อบันทึกข้อมูลทั้งหมด ต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูล

2) สื่อบันทึกข้อมูลที่มีชั้นความลับ หรือมีข้อมูลสำคัญ ต้องถูกจัดเก็บอย่างปลอดภัย ตามระดับชั้นความลับของข้อมูลและไม่นำไปให้บุคคลอื่นใช้งานโดยไม่ได้รับอนุญาต

3) กรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลที่มีชั้นความลับ หรือมีข้อมูลสำคัญออกนอกบริษัท ต้องได้รับการอนุมัติจากกรรมการผู้จัดการหรือผู้ที่ได้รับมอบหมาย และต้องบันทึกการโยกย้ายเพื่อใช้ในการตรวจสอบ

4) กรณีสื่อบันทึกข้อมูลไม่ได้ถูกนำมาใช้งานแล้ว ต้องทำลาย ให้ไม่สามารถกู้คืนข้อมูลเดิมกลับมาใช้ได้อีก และให้มีการจัดทำบันทึกการทำลายอย่างเหมาะสม

5) ต้องตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลต่าง ๆ ได้แก่ External Hard Disk, Flash Drive Thumb Drive ก่อนนำมาใช้งาน

5. การควบคุมการเข้าถึงระบบสารสนเทศ

(Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของบริษัท และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัทได้อย่างถูกต้อง

5.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

เพื่อให้ผู้ใช้งานและผู้ที่มีส่วนเกี่ยวข้องกับการปฏิบัติงาน รับทราบ และตระหนักถึงความสำคัญของการควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศ ให้เป็นตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสามารถปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัด ส่วนเทคโนโลยีสารสนเทศ ต้องดำเนินการอย่างน้อยดังต่อไปนี้

1) กำหนดให้มีการควบคุมการใช้งานระบบสารสนเทศ เพื่อควบคุมให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตจากบริษัทเท่านั้น

2) ต้องกำหนดสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่ความรับผิดชอบของผู้ใช้งาน

3) ต้องจัดเก็บบันทึกการใช้งานระบบสารสนเทศของผู้ใช้งาน

4) ต้องบันทึกการแก้ไขเปลี่ยนแปลงสิทธิการใช้งานของผู้ใช้งาน

5) สิทธิการใช้งานและการเข้าถึงระบบสารสนเทศ ต้องได้รับอนุญาตจากผู้จัดการ/หัวหน้าทีม ก่อนส่งให้ส่วนเทคโนโลยีสารสนเทศ ดำเนินการให้สิทธิการใช้งาน

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

เพื่อควบคุมการเข้าถึงและใช้งานระบบสารสนเทศของบริษัท ครอบคลุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ อุปกรณ์เคลื่อนที่ ระบบคลาวด์ ระบบสารสนเทศและระบบเครือข่าย เฉพาะผู้ที่ได้รับอนุญาต โดยมีการควบคุมและจัดการสิทธิการเข้าถึงและใช้งาน รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

1) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิก เพิกถอนการอนุญาต

2) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการเข้าถึงและใช้งานระบบสารสนเทศของผู้ใช้งานตามหน้าที่ความรับผิดชอบ และมีการทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

3) ผู้ใช้งานต้องได้รับการพิสูจน์ตัวตนทุกครั้ง ก่อนเข้าสู่ระบบสารสนเทศ

4) ต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย

5.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์คอมพิวเตอร์

1) ผู้ใช้งานต้องรับผิดชอบดูแลรหัสผู้ใช้งานและรหัสผ่าน สำหรับใช้งานระบบสารสนเทศ โดยไม่เปิดเผยหรือให้ผู้อื่นใช้งานโดยไม่ได้รับอนุญาตจากส่วนเทคโนโลยีสารสนเทศ

2) ผู้ใช้งานจะต้องกำหนดรหัสผ่าน ให้มีความมั่นคงปลอดภัย และเปลี่ยนรหัสผ่าน เมื่อสงสัยว่ามีผู้อื่นเข้าถึงรหัสผ่านของผู้ใช้งาน และแจ้งให้ส่วนเทคโนโลยีสารสนเทศ ช่วยตรวจสอบทันที

3) ผู้ใช้งานต้องป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์คอมพิวเตอร์ของบริษัทในขณะไม่ใช้งาน

4) ควบคุมสินทรัพย์ด้านสารสนเทศและการใช้งานอุปกรณ์คอมพิวเตอร์ ไม่ให้อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

5.4 การควบคุมการเข้าถึงเครือข่าย

เพื่อป้องกันการเข้าถึงระบบเครือข่ายของบริษัท โดยไม่ได้รับอนุญาต

1) นโยบายการใช้งานระบบเครือข่าย

1.1) ต้องควบคุมการเข้าถึงระบบเครือข่าย โดยมีอุปกรณ์รักษาความปลอดภัย (Firewall) ในการควบคุมการใช้งานตามสิทธิของผู้ใช้งาน

1.2) ต้องมีการยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบเครือข่าย เพื่อจัดเก็บข้อมูลการใช้งานระบบเครือข่ายของผู้ใช้งาน

1.3) ต้องตรวจสอบและดูแลอุปกรณ์ที่เกี่ยวข้องในระบบเครือข่ายทั้งหมด รวมทั้งอุปกรณ์ที่ใช้สำหรับการเข้าถึงระยะไกล

2) การบริหารจัดการเครือข่าย

2.1) ระบุขอบเขตของเครือข่ายและควบคุมด้วยระบบ Firewall เช่น เครือข่ายการเชื่อมต่อ Internet, เครือข่ายการเชื่อมต่อภายในบริษัท และเครือข่ายการเชื่อมต่อระยะไกล (VPN)

2.2) ต้องมีระบบยืนยันตัวตนของผู้ใช้งาน ก่อนเข้าสู่ระบบเครือข่าย

2.3) อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่าย เพื่อการทำงานภายในบริษัท

2.3.1) อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็นและการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่า Default Community, Default Username และ Default Password

2.3.2) ต้องมีแผนการบำรุงรักษาและปรับปรุงระบบเครือข่าย เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

2.4) อุปกรณ์ที่ทำหน้าที่ควบคุมระบบจากระยะไกล ได้แก่ Virtual Private Network (VPN) ต้องมีการปรับปรุงช่องโหว่อย่างสม่ำเสมอ และสำรองค่า Configuration ของอุปกรณ์ทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลง หรือตามระยะเวลาที่กำหนด

2.4.1) ต้องมีการปรับปรุงช่องโหว่อย่างสม่ำเสมอ และสำรองค่า Configuration ของอุปกรณ์ทุกครั้งที่ติดตั้ง หรือมีการเปลี่ยนแปลง หรือตามระยะเวลาที่กำหนด

2.4.2) ให้ลบบัญชีผู้ใช้งานที่ใช้ในการทดสอบหรือถูกยกเลิกสิทธิการใช้งาน ออกจากระบบเพื่อไม่ให้ผู้ไม่มีสิทธิเข้ามาใช้งาน

2.5) กำหนดให้มีวิธีปฏิบัติในการเก็บบันทึก Log และตรวจสอบสิ่งผิดปกติต่าง ๆ ภายในระบบเครือข่าย

3) การควบคุมการเข้าถึงระบบเครือข่าย

3.1) ผู้ใช้งานทุกคนจะได้รับสิทธิในการเข้าใช้งานระบบต่าง ๆ รวมถึงระบบเครือข่ายตามหน้าที่รับผิดชอบเท่าที่จำเป็นเท่านั้น โดยผู้ใช้งานที่ต้องการเข้าถึงระบบใด ๆ และระบบเครือข่าย ต้องดำเนินการขออนุมัติต่อผู้จัดการ/หัวหน้าทีม และส่วนเทคโนโลยีสารสนเทศทุกครั้ง ทั้งนี้การพิจารณาให้สิทธิในการเข้าถึงระบบจะต้องสอดคล้องตามแนวปฏิบัติเรื่องการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

3.2) การเชื่อมต่อเข้าสู่ระบบเครือข่ายของบริษัทผ่านระบบเครือข่ายไร้สาย ต้องได้รับการเข้ารหัสอย่างเหมาะสม

3.3) สิทธิการเข้าถึงของผู้ใช้งานภายนอก ต้องถอดถอนเมื่อสิ้นสุดการดำเนินงาน สิ้นสุดสัญญา หรือสิ้นสุดข้อตกลงทันที และต้องมีการปรับปรุงให้เป็นปัจจุบัน

4) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

4.1) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของบริษัทต้องได้รับอนุญาตจากส่วนเทคโนโลยีสารสนเทศ ก่อนจึงจะสามารถดำเนินการได้และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

4.2) จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username, Password หรือ MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

5) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

6) การควบคุมผู้ใช้งานในการใช้งานระบบเครือข่าย

6.1) ต้องแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานให้มีความเหมาะสม เพื่อควบคุมการเข้าถึงระบบและเครือข่ายสำคัญให้มีความมั่นคงปลอดภัยในการติดต่อสื่อสาร หรือการส่งผ่านข้อมูล เช่น เครือข่ายสำหรับผู้ใช้งานภายใน เครือข่ายสำหรับผู้ใช้งานภายนอก และกำหนดให้มีการแยกสภาพแวดล้อมสำหรับระบบสารสนเทศที่สำคัญ

6.2) การจำกัดสิทธิความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย ตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

6.3) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต โดยจัดให้มีการใช้งาน Firewall เพื่อควบคุมการเข้าใช้งานข้อมูล application และ service ต่าง ๆ บนระบบเครือข่ายให้เป็นไปตามที่

บริษัทกำหนดไว้เท่านั้น โดยส่วนเทคโนโลยีสารสนเทศ มีหน้าที่ในการตรวจสอบ ดูแล และติดตั้ง Firewall ให้เป็นไปตาม Firewall Rule ที่กำหนดไว้

7) มีการควบคุมการจัดเส้นทางบนเครือข่าย ที่ใช้ในการเชื่อมต่ออุปกรณ์คอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

7.1) ตรวจสอบความน่าเชื่อถือของต้นทางและปลายทางเพื่อควบคุมการเชื่อมต่อให้เป็นไปตามที่กำหนดไว้ใน Routing Table เท่านั้น เพื่อป้องกันการเชื่อมต่อกับเครือข่ายที่ไม่เหมาะสม

7.2) ตรวจสอบเส้นทางการเชื่อมต่อที่กำหนดไว้ใน Routing Table อย่างสม่ำเสมอ

7.3) IP Address ของเครือข่ายภายในต้องไม่ถูกเปิดเผยต่อเครือข่ายภายนอก เช่น การใช้เทคโนโลยี Network Address Translation (NAT)

5.5 การควบคุมการเข้าถึงระบบปฏิบัติการ

เพื่อรักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

1) การควบคุมการเข้าถึงระบบปฏิบัติการของบริษัท

1.1) ต้องกำหนดรหัสผู้ใช้งานและรหัสผ่าน ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของบริษัท

1.2) ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบจะปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง

2) การระบุและยืนยันตัวตนของผู้ใช้งาน ต้องมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานสำหรับระบบปฏิบัติการ ดังนี้

2.1) การสร้างบัญชีผู้ใช้ใหม่ การแก้ไข หรือยกเลิกบัญชีผู้ใช้ ต้องแจ้งให้ส่วนเทคโนโลยีสารสนเทศดำเนินการ โดยได้รับความเห็นชอบจากผู้จัดการ/หัวหน้าทีม

2.2) ผู้ใช้งานทุกคนต้องมีรหัสผู้ใช้งานของตนและไม่ซ้ำกับผู้ใช้งานคนอื่น ๆ โดยสามารถตรวจสอบและยืนยันกลับไปยังตัวผู้ใช้งานได้ ยกเว้นระบบปฏิบัติการที่ใช้ในการพัฒนาระบบ (Development) สามารถใช้งานแบบร่วมกันได้

3) การกำหนดเวลาในการใช้งานระบบ

3.1) ต้องมีวิธีการตัดเวลาการใช้งานอุปกรณ์คอมพิวเตอร์ เมื่ออุปกรณ์นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ

5.6 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศ

เพื่อกำหนดกฎเกณฑ์ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและระบบสารสนเทศของบริษัทจากผู้ที่ไม่ได้รับอนุญาต

1) การจำกัดการเข้าถึงระบบสารสนเทศ ต้องดำเนินการ ดังนี้

1.1) ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

1.2) บัญชีผู้ใช้งานที่มีสิทธิเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

1.3) การเข้าถึงระบบสารสนเทศจากผู้ใช้งานภายนอก จะต้องได้รับสิทธิและได้รับอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ส่วนเทคโนโลยีสารสนเทศจะต้องยกเลิกสิทธิที่ให้กับผู้ใช้งานภายนอก ซึ่งหากผู้ใช้งานภายนอกดำเนินการใด ๆ ที่มีผลกระทบต่อระบบ จะต้องเป็นผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้น/การกระทำนั้น ๆ

2) ส่วนเทคโนโลยีสารสนเทศ ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ออกจากระบบอื่น ๆ เช่น การแบ่งระหว่างระบบที่เชื่อมต่อภายในบริษัทกับระบบที่เชื่อมต่อจากภายนอกบริษัท เป็นต้น

5.7 การควบคุมผู้ใช้งานภายนอกเข้าถึงระบบสารสนเทศ

การใช้บริการจากผู้ใช้งานภายนอกอาจก่อให้เกิดความเสี่ยงได้ จึงกำหนดแนวทางในการควบคุมการปฏิบัติงานของผู้ใช้งานภายนอกที่ทำงานให้กับบริษัท ไม่ว่าจะทำงานอยู่ภายในบริษัทหรือนอกสถานที่

1) ผู้ใช้งานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของบริษัท ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบสารสนเทศเพื่อขออนุมัติจากผู้จัดการ/หัวหน้าทีม และส่วนเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อเครือข่าย
- กำหนดข้อตกลงการใช้งานข้อมูล เพื่อป้องกันการเปิดเผยข้อมูล

2) ผู้ใช้งานภายนอกต้องรับผิดชอบต่อการเข้าถึงข้อมูล ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และผู้ใช้งานภายนอกต้องลงนามในสัญญาหรือข้อตกลงไม่เปิดเผยข้อมูลของบริษัท โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศของบริษัท

3) ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบสารสนเทศ หรืออุปกรณ์คอมพิวเตอร์โดยผู้ใช้งานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของบริษัท

4) ต้องกำหนดให้ผู้ใช้งานภายนอกจัดทำแผนการดำเนินงาน และเอกสารที่เกี่ยวข้อง รวมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ใช้งานภายนอกได้อย่างเข้มงวด และมั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

5) บริษัทมีสิทธิในการตรวจสอบตามสัญญาหรือข้อตกลงการใช้งานระบบสารสนเทศเพื่อให้มั่นใจว่าบริษัทสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญาหรือข้อตกลงนั้น

5.8 นโยบายการบริหารจัดการรหัสผ่าน

1) การบริหารรหัสผ่าน

1.1) ไม่อนุญาตให้ผู้ใช้งานใช้รหัสผ่านร่วมกัน ชื่อผู้ใช้งานและ/หรือรหัสผ่าน ต้องไม่ถูกใช้งานร่วมกันหรือแบ่งปันกันใช้งาน ยกเว้นการใช้งานบนอุปกรณ์คอมพิวเตอร์สำหรับการพัฒนาระบบ

1.2) รหัสผ่านเบื้องต้น รหัสผ่านชั่วคราวและรหัสผ่านปริยายของระบบสารสนเทศต้องถูกเปลี่ยนโดยส่วนเทคโนโลยีสารสนเทศ ให้เป็นรหัสผ่านที่มั่นคงในทันทีที่การติดตั้งระบบเสร็จสิ้น

1.3) มีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่านไว้อย่างชัดเจน เช่น 60 วัน 90 วัน เป็นต้น

2) การกำหนดคุณภาพรหัสผ่าน

2.1) กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมผสานตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

2.2) การตั้งรหัสผ่านชั่วคราวต้องยากต่อการเดาและต้องมีความแตกต่างกัน ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

3) การใช้งานรหัสผ่าน

3.1) ห้ามใช้งานบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น

3.2) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

3.3) เปลี่ยนรหัสผ่านของตนเองทันทีที่ได้รับรหัสผ่านจากส่วนเทคโนโลยีสารสนเทศ ไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตาม และไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิมที่ได้รับมา และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

3.4) ผู้ใช้งานต้องรายงานเหตุการณ์ที่สงสัยว่ามีการเปิดเผยรหัสผ่านไปยังส่วนเทคโนโลยีสารสนเทศพร้อมทั้งเปลี่ยนรหัสผ่านทันที

3.5) ถ้าผู้ใช้งานไม่สามารถเข้าใช้งานระบบด้วยชื่อผู้ใช้และรหัสผ่านของตนเองได้ ผู้ใช้งานต้องแจ้งให้ส่วนเทคโนโลยีสารสนเทศทราบ

5.9 การควบคุมการใช้งานในระบบคลาวด์

การควบคุมการใช้งานทรัพยากรที่อยู่ในระบบคลาวด์ ซึ่งเป็นระบบที่ให้บริการในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และอุปกรณ์รักษาความปลอดภัย จากผู้ให้บริการที่เป็นหน่วยงานภายนอกเพื่อให้การใช้งานทรัพยากรมีความปลอดภัยและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

1) ต้องควบคุมการเข้าถึงระบบ โดยมีอุปกรณ์รักษาความปลอดภัย (Firewall) ในการควบคุมการใช้งานตามสิทธิของผู้ใช้งาน

2) ต้องมีการยืนยันตัวตนของผู้ใช้งานก่อนเข้าสู่ระบบ และจำกัดการเข้าถึงระบบคลาวด์เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น

3) ต้องควบคุมสิทธิการเข้าถึงระบบตามบทบาทหน้าที่ของผู้ใช้งาน

4) บัญชีผู้ใช้งานที่มีสิทธิเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

5) ต้องทำการลบบัญชีผู้ใช้งานที่ถูกยกเลิกสิทธิการใช้งานทันที เพื่อไม่ให้ผู้ไม่มีสิทธิเข้ามาใช้งาน

6) ต้องเก็บบันทึกประวัติการเข้าใช้งานระบบและตรวจสอบสิ่งผิดปกติต่าง ๆ ภายในระบบเพื่อแจ้งเตือนเจ้าหน้าที่ดูแลระบบ

6. การเข้ารหัสลับข้อมูล

(Cryptography)

เพื่อกำหนดแนวทางการใช้งานการเข้ารหัสลับข้อมูลและทำให้ระบบสารสนเทศรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และ/หรือป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและความเหมาะสม

6.1 มาตรการเข้ารหัสลับข้อมูล

ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการเข้ารหัสลับข้อมูล และแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยกำหนดกลุ่มผู้ใช้งานอย่างเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละระดับชั้นความลับที่กำหนดไว้และมีความครอบคลุมข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่กรณีที่ไม่สามารถเข้ารหัสได้ ต้องควบคุมการเข้าถึงอย่างเหมาะสมตามหน้าที่และความรับผิดชอบ

6.2 การบริหารจัดการกุญแจเข้ารหัสลับข้อมูล

ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับข้อมูล ซึ่งประกอบไปด้วย

1) การพิจารณาประเภทกลุ่มข้อมูลที่นำมาใช้เข้ารหัสให้สอดคล้องกับการจัดระดับชั้นความลับของข้อมูล และแนวทางการดำเนินการกำกับข้อมูล

2) มีการพิจารณาวิธีการเข้ารหัสแต่ละรูปแบบ รวมทั้งใช้อัลกอริทึมที่เหมาะสม การเลือกใช้การเข้ารหัสข้อมูลให้สามารถดำเนินการได้ 2 แบบ ดังนี้

2.1) แบบสมมาตร Symmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสเดียวกัน (Secret Key)

2.2) แบบอสมมาตร Asymmetric คือการเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคู่ (Public/ Private Key)

3) ดำเนินการสร้างกุญแจรหัสจากโปรแกรมที่น่าเชื่อถือ โดยมีแนวทางการสร้างกุญแจรหัส และการบริหารจัดการกุญแจรหัส (Key Management) ดังนี้

3.1) นำข้อมูลผ่านกระบวนการเข้ารหัส เพื่อนำข้อมูลที่เข้ารหัสแล้วไปใช้ตามจุดประสงค์ต่อไป

3.2) กำหนดอายุการใช้งานของกุญแจ

3.3) กำหนดมาตรการในการเก็บกุญแจ (Key)

7. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน และเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบสารสนเทศ ข้อมูลซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ

7.1 ความมั่นคงปลอดภัยสำหรับพื้นที่ใช้งานระบบสารสนเทศ

1) ห้อง Data Center

1.1) บริษัทกำหนดให้ห้อง Data Center เป็นพื้นที่มีความมั่นคงปลอดภัยสูง โดยให้อยู่ในการควบคุมดูแลของส่วนเทคโนโลยีสารสนเทศ

1.2) บริษัทต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย ประกอบด้วย กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถป้องกัน ภัยคุกคามจากผู้บุกรุก เป็นต้น เพื่อเฝ้าระวังผู้ที่ไม่ได้รับอนุญาตเข้าออกห้อง Data Center รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

1.3) บริษัทต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณห้อง Data Center

1.4) ส่วนเทคโนโลยีสารสนเทศ กำหนดมาตรการควบคุมการเข้าออกห้อง Data Center โดยให้ผ่านเข้าออกได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบที่เกี่ยวข้องเท่านั้น

2) พื้นที่ใช้งานระบบสารสนเทศ

2.1) บริษัทกำหนดให้พื้นที่ปฏิบัติงานทั้งหมดเป็นพื้นที่ใช้งานระบบสารสนเทศ และอยู่ในการควบคุมดูแลของแผนกทรัพยากรบุคคล

2.2) แผนกทรัพยากรบุคคล ต้องจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ และประกาศให้รับทราบโดยทั่วกัน

2.3) แผนกทรัพยากรบุคคล กำหนดมาตรการควบคุมการเข้าออกในบริเวณพื้นที่ใช้งานระบบสารสนเทศ โดยให้ผ่านเข้าออกได้เฉพาะผู้ใช้งานที่มีสิทธิเท่านั้น ระบุตัวผู้ใช้งานและช่วงเวลาที่มีสิทธิผ่านเข้าออกในแต่ละพื้นที่อย่างชัดเจน

3) พื้นที่สำหรับบุคคลภายนอก

3.1) แผนกทรัพยากรบุคคล ต้องจัดบริเวณส่งมอบผลิตภัณฑ์หรือบริเวณที่บุคคลภายนอกเข้าถึงได้เพื่อป้องกันการเข้าถึงสินทรัพย์ของบริษัทโดยไม่ได้รับอนุญาต และจัดเป็นบริเวณแยกออกมาต่างหาก

3.2) หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ให้ปฏิบัติตามหลักเกณฑ์การเข้าออกพื้นที่ใช้งานระบบสารสนเทศ

3.3) หากมีบุคคลอื่นใดที่มิได้เกี่ยวข้องกับกิจการของบริษัท หรือมิได้แจ้งขอเข้าพื้นที่ล่วงหน้า แผนกทรัพยากรบุคคลจะต้องตรวจสอบเหตุผลและความจำเป็นก่อนการอนุญาตหรือไม่อนุญาตเข้าพื้นที่

3.4) บุคคลภายนอก ต้องแลกบัตรที่ใช้ระบุตัวตนกับฝ่ายอาคาร ซี.ซี.ที. และต้องติดบัตรผู้ติดต่อตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในบริษัท

7.2 ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับเครื่องมือ และอุปกรณ์ต่าง ๆ

1) ความปลอดภัยของอุปกรณ์

1.1) ผู้ใช้งานต้องจัดตั้งอุปกรณ์ไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัย หรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

1.2) ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ ได้แก่ จัดให้มีการซ่อมบำรุงตามรอบที่กำหนดโดยเฉพาะระบบที่มีความสำคัญ เป็นต้น เพื่อให้สามารถใช้งานได้อย่างต่อเนื่องและมีความพร้อมใช้อยู่เสมอ

1.3) ต้องกำหนดให้มีการป้องกันสินทรัพย์ด้านสารสนเทศของบริษัท เมื่อถูกนำไปใช้งานนอกบริษัท

1.4) ต้องกำหนดให้มีวิธีการในการทำลายข้อมูลอย่างเหมาะสม ตามระดับชั้นความลับของข้อมูลที่ถูกจัดเก็บในอุปกรณ์นั้น

2) ความปลอดภัยของระบบกระแสไฟฟ้าสำรอง และระบบป้องกันภัย

2.1) ต้องมีระบบไฟฟ้าสำรองอัตโนมัติ เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง และต้องตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาอย่างน้อยปีละ 1 ครั้ง

2.2) ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย ได้แก่ ระบบดับเพลิง ระบบแจ้งเตือนอัคคีภัย

2.3) ต้องวางแผนและซักซ้อมการปฏิบัติ เพื่อรับมือกับเหตุการณ์ฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

2.4) ระบบที่สำคัญของบริษัทจะต้องปฏิบัติตามนโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ เพื่อลดผลกระทบที่จะเกิดขึ้นกับการดำเนินงานของบริษัท

3) ความปลอดภัยของการเดินสายไฟฟ้าหลัก และสายเคเบิลหลัก

3.1) การเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในบริษัท ต้องเป็นบริเวณที่ไม่สามารถเข้าถึงได้ง่าย

3.2) การติดตั้งตู้พักสายต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะผู้ดูแลระบบ หรือผู้ใช้งานที่มีสิทธิเท่านั้น

4) ความปลอดภัยของโต๊ะทำงานและการป้องกันหน้าจอคอมพิวเตอร์

4.1) ต้องควบคุมสินทรัพย์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ ฯลฯ ให้ปลอดภัยจากการเข้าถึงโดยผู้ไม่มีสิทธิ

4.2) จัดเก็บเอกสารหรือสื่อบันทึกข้อมูล ตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูล

4.3) ทุกครั้งที่ว่างเว้นจากการใช้งาน หรือไม่อยู่หน้าจอคอมพิวเตอร์ต้องล็อคหน้าจอ หรือ log off ออกจากระบบ

8. การบริหารจัดการด้านการปฏิบัติการสารสนเทศ (Operations Management)

เพื่อให้การบริหารจัดการด้านการปฏิบัติการด้านสารสนเทศ เป็นไปอย่างถูกต้องและรักษาไว้ซึ่งความมั่นคงปลอดภัยด้านสารสนเทศ

8.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน

เพื่อให้การปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์คอมพิวเตอร์ และอุปกรณ์เคลื่อนที่เป็นไปอย่างถูกต้องมั่นคงปลอดภัย จึงได้กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงานให้ชัดเจนและเหมาะสม เพื่อลดความเสียหายที่อาจเกิดกับสินทรัพย์ด้านสารสนเทศของบริษัท

ส่วนเทคโนโลยีสารสนเทศต้องจัดให้มีคู่มือปฏิบัติงาน โดยมีการดำเนินการอย่างน้อยดังต่อไปนี้

1) จัดทำและปรับปรุงคู่มือการปฏิบัติงาน เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ทั้งนี้คู่มือดังกล่าวสามารถจัดทำในรูปแบบสิ่งพิมพ์หรืออิเล็กทรอนิกส์

2) ฝึกอบรมแก่พนักงาน เมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง

3) ทดสอบการปฏิบัติงานตามคู่มือที่จัดทำขึ้น

4) ต้องกำหนดให้มีการควบคุมการเข้าถึงคู่มือการปฏิบัติงาน เพื่อป้องกันการเข้าถึงและเปิดเผยคู่มือการปฏิบัติงานโดยมิได้รับอนุญาต

8.2 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน

ส่วนเทคโนโลยีสารสนเทศ ต้องมีแนวทางบันทึกเหตุการณ์ต่าง ๆ โดยพิจารณาถึงประเด็นความต้องการทางธุรกิจและข้อกำหนดที่มีผลทางกฎหมาย โดยมีรายละเอียดครอบคลุมอย่างน้อยดังต่อไปนี้

1) รหัสผู้ใช้งาน

2) วันที่ เวลา รายละเอียดของเหตุการณ์ เช่น การ Log on และ การ Log off เป็นต้น

3) ข้อมูลที่ระบุถึงเครื่องต้นทางและปลายทาง เช่น ชื่อเครื่อง, IP Address, Protocol หรือ Port ที่ใช้งาน หรือ MAC Address เป็นต้น

4) ความสำเร็จและล้มเหลวในการพยายามเข้าถึงระบบ ข้อมูลและทรัพยากรอื่น ๆ

5) การเปลี่ยนแปลงการกำหนดค่าในระบบ (Configuration)

6) กิจกรรมที่เกิดจากการใช้สิทธิการใช้งาน

7) การเข้าถึงไฟล์ และวิธีการเข้าถึง

8) จัดเก็บบันทึกเหตุการณ์ย้อนหลังอย่างน้อย 90 วัน ไว้ในสถานที่ที่มั่นคงและปลอดภัย

9) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการป้องกันข้อมูล บันทึกเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานอุปกรณ์คอมพิวเตอร์ และระบบสารสนเทศจากการเปลี่ยนแปลงแก้ไข หรือเข้าถึงโดยมิได้รับอนุญาต

8.3 การเฝ้าระวังการใช้งาน

เพื่อให้มีการเฝ้าระวังการใช้งานระบบสารสนเทศ และมีการตรวจสอบผลการเฝ้าระวังอย่างสม่ำเสมอ ตรวจจับกิจกรรมการใช้งานที่มิได้รับอนุญาตและหาทางแก้ไขอย่างทันท่วงที

1) ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดหลักเกณฑ์ในการเฝ้าระวังการใช้งานระบบสารสนเทศของบริษัท ซึ่งประกอบไปด้วยเหตุการณ์ที่ต้องเฝ้าระวัง ช่วงเวลาและความถี่ของการเฝ้าระวัง และมีการตรวจสอบผลการเฝ้าระวังอย่างสม่ำเสมอ โดยพิจารณาถึงประเด็นต่าง ๆ อย่างน้อยดังต่อไปนี้

1.1) ความต้องการทางธุรกิจ และข้อกำหนดที่มีผลทางกฎหมาย

1.2) ระดับความลับ ระดับความสำคัญ ของข้อมูลสารสนเทศ

1.3) เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ และเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นในอดีต

1.4) ขอบเขตการเชื่อมต่อ เช่น มีการเชื่อมต่อเฉพาะภายในสำนักงาน หรือมีการเชื่อมต่อกับเครือข่ายสาธารณะ

1.5) บันทึกเหตุการณ์ของระบบซึ่งถูกระงับการใช้งาน

2) เหตุการณ์ที่ควรเฝ้าระวัง ประกอบไปด้วยเรื่องต่าง ๆ อย่างน้อยดังต่อไปนี้

2.1) การเฝ้าระวังการเข้าถึงที่ได้รับอนุญาต เช่น ช่วงวันและเวลา การเข้าถึง File ต่างๆ

2.2) การเฝ้าระวังปฏิบัติงานที่ใช้สิทธิพิเศษ เช่น การเริ่มต้นหรือการหยุดระบบ การเชื่อมต่ออุปกรณ์

2.3) การเฝ้าระวังการพยายามเข้าถึงที่ไม่ได้รับอนุญาต เช่น การกระทำที่ผิดพลาด หรือการถูกปฏิเสธ การละเมิดการเข้าถึงผ่านการเชื่อมต่อเครือข่าย การแจ้งเตือน ตรวจจับการบุกรุก

2.4) การเฝ้าระวังการแจ้งเตือนหรือข้อผิดพลาดจากระบบ เช่น การแจ้งเตือนจาก Console การบันทึกเหตุการณ์การยกเว้นในระบบ การแจ้งเตือนจากการบริหารจัดการเครือข่าย

2.5) การเฝ้าระวังการเปลี่ยนแปลง หรือความพยายามที่จะเปลี่ยนแปลงการควบคุม และค่าการติดตั้งด้านความมั่นคงปลอดภัยของระบบ

8.4 บันทึกกิจกรรมการดำเนินงานของผู้ใช้งานที่เกี่ยวข้องกับระบบ

ส่วนเทคโนโลยีสารสนเทศต้องกำหนดให้มีการบันทึกการเฝ้าระวัง และป้องกันข้อมูลกิจกรรมการดำเนินงานของผู้ใช้งานอย่างเหมาะสม โดยให้พิจารณาตามหลักเกณฑ์ในการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานและการเฝ้าระวังการใช้งาน

8.5 การบริหารจัดการช่องโหว่ทางเทคนิคของบริษัท

ส่วนเทคโนโลยีสารสนเทศต้องจัดให้มีการจัดการช่องโหว่ทางเทคนิคที่เหมาะสมและทันท่วงที เพื่อลดความเสี่ยงจากการใช้ประโยชน์จากช่องโหว่ทางเทคนิค ควบคุมช่องโหว่ในระบบปฏิบัติการและแอพพลิเคชัน โดยพิจารณาดำเนินการในเรื่องต่าง ๆ อย่างน้อยดังต่อไปนี้

1) เฝ้าระวังและติดตามข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคอย่างสม่ำเสมอ

2) หากพบช่องโหว่ทางเทคนิค ต้องหาแนวทางการแก้ไข เพื่อให้สามารถป้องกันความเสียหายได้อย่างทันท่วงที

3) ก่อนดำเนินการแก้ไขช่องโหว่ทางเทคนิค ต้องทดสอบเพื่อให้มั่นใจว่าแนวทางดังกล่าวไม่ส่งผลเสียหายต่อการดำเนินงานของระบบปฏิบัติงานจริง

4) จัดให้มีขั้นตอนควบคุมการเปลี่ยนแปลงอย่างเหมาะสม เพื่อดำเนินการแก้ไขช่องโหว่ทางเทคนิค

5) จัดให้มีการประเมินช่องโหว่ทางเทคนิคอย่างสม่ำเสมอ เพื่อเป็นการตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคด้านความมั่นคงปลอดภัย

8.6 การบริหารจัดการปรับปรุงระบบปฏิบัติการ

ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการบริหารจัดการ Patch ที่เหมาะสมและทันท่วงที เพื่อให้เป็นการปรับปรุง แก้ไขเพิ่มเติมและติดตั้งซอฟต์แวร์ที่ใช้แก้ไขระบบที่ใช้งานจริงให้ดีขึ้น และเป็นปัจจุบันที่สุด โดยพิจารณาดำเนินการในเรื่องต่าง ๆ อย่างน้อยดังต่อไปนี้

1) เก็บรวบรวมข้อมูลอุปกรณ์ทั้งหมดที่มีอยู่ในระบบ เช่น switch, router, firewall, server เป็นต้น โดยจะต้องมีรายละเอียดของอุปกรณ์นั้นใน physical เช่น serial number, รุ่นของอุปกรณ์ หรือ logical เช่น software version, windows version เป็นต้น

2) วิเคราะห์ วางแผน การทำ Patch Management เพื่อปิดช่องโหว่โดยให้มีผลกระทบต่อการใช้งานจริงน้อยที่สุดและเป็นปัจจุบันที่สุด ซึ่งควรมีระดับความเสี่ยง และผลกระทบ เป็นปัจจัยขั้นต่ำในการวิเคราะห์

3) ก่อนทำ Patch ในระบบใช้งานจริง ต้องมีการทดสอบการทำ Patch ในระบบทดสอบ ที่มีความคล้ายคลึงกับระบบใช้งานจริงที่สุด

4) ต้อง Backup ข้อมูลของอุปกรณ์ต่าง ๆ ก่อนเริ่มทำในระบบใช้งานจริง หากระบบใช้งานจริงมีความเปลี่ยนแปลงตลอดเวลา การ Backup ควรมีระยะเวลาห่างจากการทำ Patch ให้น้อยที่สุด

5) ก่อนทำ Patch ในระบบใช้งานจริง ต้องแจ้งกำหนดการและระยะเวลาในการตรวจสอบการใช้งานระบบใช้งานจริงและยืนยันกลับมายังผู้ดูแลระบบ เพื่อเป็นหลักฐานในด้านผลกระทบก่อนและหลังการทำ Patch ทุกครั้ง

6) ต้องมีระบบการบริหารจัดการ Patch ที่เหมาะสม สามารถแจ้งเตือน รายงาน สถานะปัจจุบันของทุกระบบที่มีอยู่ได้แม่นยำและถูกต้อง

7) ต้องได้รับความเห็นชอบจากส่วนเทคโนโลยีสารสนเทศ หากมีการทำ Patch ในกรณีฉุกเฉิน และต้องทำรายงานผลการดำเนินการให้ผู้บริหารทราบทันที

8.7 การตั้งเวลาของอุปกรณ์ให้ตรงกัน

เพื่อตั้งเวลาของอุปกรณ์คอมพิวเตอร์ให้ตรงกัน และเพื่อช่วยในการตรวจสอบหากอุปกรณ์คอมพิวเตอร์ของบริษัท ถูกบุกรุก โดยอ้างอิงจากแหล่งเวลาสำหรับใช้ร่วมกันทั้งบริษัท เช่น Network Time Protocol Server

(NTP Server) ของสำนักงานกรมอุทกศาสตร์ (กองทัพเรือ) และสถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี) เป็นต้น

8.8 การป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์

ส่วนเทคโนโลยีสารสนเทศมีหน้าที่ในการบริหารจัดการ ควบคุม และวางแผนป้องกันความเสียหายต่อระบบสารสนเทศของบริษัทจากโปรแกรมที่ไม่ประสงค์ดี โดยต้องดำเนินการอย่างน้อยดังต่อไปนี้

1) ติดตั้งซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดี เพื่อป้องกันระบบสารสนเทศของบริษัท และปรับปรุงซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดีให้ทันสมัยอยู่เสมอ ทั้งนี้การตรวจจับต้องครอบคลุมเรื่องอย่างน้อยดังต่อไปนี้

1.1) ตรวจสอบไฟล์ที่อยู่ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ก่อนเปิดใช้งาน

1.2) ตรวจสอบไฟล์ที่ส่งมากับข้อความอิเล็กทรอนิกส์ก่อนเปิดใช้งาน

1.3) ตรวจสอบ Web Page ก่อนเข้าถึง

1.4) ตรวจสอบสื่อบันทึกข้อมูลแบบพกพาก่อนใช้งาน

2) ควบคุมไม่ให้มีการติดตั้ง ปรับเปลี่ยนค่าการติดตั้ง และถอดถอนซอฟต์แวร์ในอุปกรณ์คอมพิวเตอร์ของบริษัทโดยมิได้รับอนุญาตจากส่วนเทคโนโลยีสารสนเทศ

3) จัดทำกระบวนการสำหรับผู้ใช้งานเมื่อตรวจพบโปรแกรมที่ไม่ประสงค์ดี รวมถึงการรายงาน และการแก้ปัญหาเบื้องต้นจากการถูกโจมตีจากโปรแกรมที่ไม่ประสงค์ดี

4) จัดทำกระบวนการและแผนความต่อเนื่องทางธุรกิจ เพื่อรับมือกับการถูกโจมตีโดยโปรแกรมที่ไม่ประสงค์ดี ทั้งนี้รวมถึงการเตรียมการต่างๆ ที่จำเป็นสำหรับการสำรองและกู้คืนซอฟต์แวร์และระบบสารสนเทศ

5) ตรวจสอบการทำงานของซอฟต์แวร์ หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดี เพื่อให้มั่นใจว่าการแจ้งเตือนและการให้ข้อมูลนั้นถูกต้อง

6) จัดทำข้อตกลงหรือสัญญาการให้บริการหลังการขายกับบริษัทคู่ค้าหรือเจ้าของผลิตภัณฑ์ เพื่อปรับปรุงให้ซอฟต์แวร์หรืออุปกรณ์สำหรับตรวจจับและกำจัดโปรแกรมที่ไม่ประสงค์ดี มีความทันสมัยอยู่เสมอ

8.9 การสำรองข้อมูล

เพื่อรักษาความถูกต้องครบถ้วนของระบบสารสนเทศ และความพร้อมใช้ของระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ จึงควรให้มีการสำรองและกู้คืนข้อมูล

1) ส่วนเทคโนโลยีสารสนเทศต้องกำหนดให้มีกระบวนการสำรองข้อมูล การทดสอบ และการกู้คืนข้อมูลที่เก็บไว้ ให้สอดคล้องกับความต้องการทางธุรกิจของบริษัทและตามข้อกำหนดที่มีผลทางกฎหมาย ดังต่อไปนี้

1.1) พิจารณาคัดเลือกและทบทวนระบบสารสนเทศ กำหนดประเภทของข้อมูลและกำหนดความถี่ในการจัดทำระบบสำรองที่เหมาะสมอย่างน้อยปีละ 1 ครั้ง

1.2) กำหนดประเภทของข้อมูลที่ควรสำรอง เช่น ระบบปฏิบัติการ บันทึกเหตุการณ์ของระบบปฏิบัติการ ระบบฐานข้อมูล ค่าการติดตั้งของอุปกรณ์คอมพิวเตอร์ เป็นต้น

1.3) จัดทำตารางการสำรองข้อมูล และระยะเวลาในการจัดเก็บ วิธีการสำรองข้อมูล เช่น การสำรองข้อมูลทั้งหมด การสำรองข้อมูลส่วนเพิ่ม และการสำรองข้อมูลที่แตกต่าง เป็นต้น โดยสำรองข้อมูลแยกจากแหล่งข้อมูลเดิมโดยสิ้นเชิง

1.4) การจัดเก็บสื่อบันทึกข้อมูลสำรองนอกพื้นที่ โดยพิจารณาตามระดับความมั่นคงปลอดภัยด้านสารสนเทศ เช่น ข้อมูลมีความมั่นคงปลอดภัยระดับสูง เป็นต้น

1.5) การจัดเก็บสื่อบันทึกข้อมูลสำรอง ในสถานที่ที่มีระดับการป้องกันด้านกายภาพ สภาพแวดล้อมที่เหมาะสม โดยพิจารณาตามระดับความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้มีการควบคุมเทียบเท่ากับสถานที่ตั้งของระบบที่ให้บริการจริง

1.6) ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากร ที่ดูแลรับผิดชอบระบบสำรองสำหรับระบบสารสนเทศ จัดทำแผนและสำรองระบบสารสนเทศ เพื่อเตรียมความพร้อมใช้งานกรณีฉุกเฉิน

1.7) ต้องจัดทำแผนเตรียมความพร้อมกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง สอดคล้องกับการใช้งานตามภารกิจ

1.8) การทดสอบสื่อบันทึกข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง สำหรับระบบสารสนเทศที่มีระดับความมั่นคงปลอดภัย "สูงสุด" เพื่อให้มั่นใจว่าสามารถนำกลับมาใช้ได้ในช่วงฉุกเฉิน

1.9) การเข้ารหัสสื่อบันทึกข้อมูลสำรอง โดยพิจารณาตามระดับความมั่นคงปลอดภัยของ ระบบสารสนเทศ

2) ส่วนเทคโนโลยีสารสนเทศ ต้องทำการสำรองซอฟต์แวร์และค่าการติดตั้งก่อนที่จะเปลี่ยนแปลงแก้ไข เพื่อให้มั่นใจว่าระบบสามารถกู้กลับคืนได้ในกรณีที่เกิดปัญหากับระบบหลังจากที่มีการเปลี่ยนแปลงแก้ไข ทั้งนี้ต้องจัดเก็บไว้อย่างน้อย 3 เวอร์ชันก่อนหน้า

3) ส่วนเทคโนโลยีสารสนเทศ ต้องบันทึกกิจกรรมและผลการสำรองข้อมูล เช่น Backup Log Sheet เป็นต้น เพื่อให้มั่นใจว่ามีการปฏิบัติตามกระบวนการสำรองข้อมูลที่กำหนดไว้

4) ต้องปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

5) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่ออุปกรณ์คอมพิวเตอร์หรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ส่วนเทคโนโลยีสารสนเทศดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้บริหารทราบโดยทันที

6) กรณีความเสียหายที่เกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานหรือผู้ดูแลระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบ เมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์

8.10 การจัดการการเปลี่ยนแปลง

เพื่อควบคุมการเปลี่ยนแปลงระบบสารสนเทศและบริการของบริษัท ให้มั่นใจว่าการเปลี่ยนแปลง ปรับปรุง แก้ไขระบบสารสนเทศ และบริการได้รับการควบคุมตลอดระยะเวลาที่มีการเปลี่ยนแปลง รวมถึงลดความเสี่ยงที่อาจเกิดความเสียหายจากการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบสารสนเทศและบริการ และเพื่อให้มี

การแยกระบบใช้งานจริงออกจากระบบสำหรับพัฒนาและการทดสอบ เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบใช้งานจริงโดยมิได้รับอนุญาต

1) ในการขอเปลี่ยนแปลงอุปกรณ์คอมพิวเตอร์ในระบบใช้งานจริง ส่วนเทคโนโลยีสารสนเทศต้องควบคุมให้มีการแจ้งความประสงค์และขออนุมัติการเปลี่ยนแปลง โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- วัตถุประสงค์ในการเปลี่ยนแปลง
- รายละเอียดการเปลี่ยนแปลง
- วันที่ต้องการใช้งาน
- ประเมินผลกระทบที่อาจจะเกิดขึ้น รวมทั้งผลกระทบความมั่นคงปลอดภัยของการเปลี่ยนแปลงนั้น ๆ
- ผลการทดสอบ
- การอนุมัติการเปลี่ยนแปลง
- การสื่อสารการเปลี่ยนแปลงให้ผู้ที่เกี่ยวข้องรับทราบ
- ขั้นตอนในการถอยกลับ รวมทั้งหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องในการกู้คืนระบบในกรณีที่การเปลี่ยนแปลงไม่เป็นไปตามแผน

2) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการกำหนดหลักเกณฑ์และวิธีปฏิบัติสำหรับการขออนุมัติการเปลี่ยนแปลงกรณีฉุกเฉิน ซึ่งไม่สามารถรอการดำเนินงานตามขั้นตอนปกติได้

3) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีกระบวนการในการจัดเก็บข้อมูลบันทึกเหตุการณ์ เมื่ออุปกรณ์คอมพิวเตอร์มีการเปลี่ยนแปลงเพื่อใช้ในการตรวจสอบ

4) หลังจากการเปลี่ยนแปลงเสร็จสิ้น ผู้อนุมัติการเปลี่ยนแปลงต้องจัดให้มีการประเมินผลหลังการเปลี่ยนแปลง เพื่อให้มั่นใจว่าการเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ และนำผลของการประเมินมาใช้ปรับปรุงกระบวนการเปลี่ยนแปลงในอนาคต

5) ส่วนเทคโนโลยีสารสนเทศ จัดให้มีการแยกระบบใช้งานจริงออกจากระบบสำหรับการพัฒนาและการทดสอบ เพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูล หรือการประมวลผลของระบบใช้งานจริง โดยต้องจัดให้มีการควบคุมอย่างน้อยดังต่อไปนี้

5.1) ให้แยกระบบสำหรับการพัฒนาและการทดสอบออกจากระบบใช้งานจริง แบบกายภาพ เช่น การแยกเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น ทั้งนี้ในกรณีที่ไม่สามารถทำได้ ต้องแยกการทำงานแบบตรรกะ เช่น แยก Directories หรือ Logical Partition ออกจากกัน เป็นต้น

5.2) การเปลี่ยนแปลงแก้ไข Source Code ต้องดำเนินการบนระบบสำหรับการพัฒนาเท่านั้น

5.3) Source Code ที่พร้อมใช้งาน หรือ Source Code ที่ได้รับจากระบบเครือข่ายภายนอกต้องผ่านการตรวจสอบจากส่วนเทคโนโลยีสารสนเทศ จึงจะสามารถโอนย้ายไปยังส่วนที่ใช้งานจริงโดยผู้ที่ได้รับอนุญาตเท่านั้น

5.4) การเปลี่ยนแปลง Source Code ที่ใช้งานจริงต้องมีการจัดเก็บอย่างเป็นระบบตามขั้นตอนการจัดระดับชั้นความลับของข้อมูลและมีการควบคุมเวอร์ชัน

5.5) จัดทำขั้นตอนปฏิบัติและการอนุมัติในการนำโปรแกรมคอมพิวเตอร์ จากระบบสำหรับการพัฒนาและการทดสอบไปยังระบบใช้งานจริง

5.6) ระบบสำหรับการทดสอบต้องจำลองมาจากระบบใช้งานจริง ให้มีความคล้ายคลึงกันมากที่สุด

5.7) ระบบสำหรับการทดสอบต้องแตกต่างระบบใช้งานจริง โดยต้องมีข้อความหรือสัญลักษณ์ที่แสดงประเภทของระบบอย่างชัดเจน เพื่อลดความเสี่ยงจากการผิดพลาดในการเข้าถึงระบบ

6) การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลอย่างเหมาะสมตามระดับชั้นความลับของข้อมูลและตามความคุ้มครองข้อมูลส่วนบุคคล

7) การดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ จำเป็นต้องขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลง แก้ไข หรือมอบให้ผู้แทนดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจให้ ซอฟต์แวร์แพ็กเกจที่แก้ไขจะต้องได้รับการทดสอบและตรวจสอบถึงผลกระทบ และความเสี่ยงที่อาจเกิดขึ้นก่อนการนำมาใช้งาน

8.11 การจัดการการให้บริการผู้ใช้งานภายนอก

เพื่อบริหารจัดการการให้บริการผู้ใช้งานภายนอกให้มีระดับความมั่นคงปลอดภัย และระดับการบริการเป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างบริษัทกับผู้ใช้งานภายนอก ประกอบไปด้วยเรื่องดังต่อไปนี้

1) บริษัทต้องกำกับดูแลให้ผู้ใช้งานภายนอกปฏิบัติตามนโยบาย และมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ตลอดจนคำสั่งหรือระเบียบบริษัทที่เกี่ยวข้อง รวมถึงควบคุมการบริการให้เป็นไปตามข้อตกลงหรือสัญญาการให้บริการ

2) ผู้ใช้งานภายนอกต้องจัดทำแผนการดำเนินงานและเอกสารที่เกี่ยวข้อง รวมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ใช้งานภายนอกได้อย่างเข้มงวด และมั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดหรือตกลงไว้

3) บริษัทต้องเฝ้าระวังและตรวจสอบการให้บริการผู้ใช้งานภายนอก เช่น การบริการกับข้อตกลงที่ได้จัดทำไว้ รายงานการให้บริการผู้ใช้งานภายนอกเพื่อสรุปการดำเนินงานตามเงื่อนไข การบันทึกเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดจากข้อตกลง เป็นต้น

4) การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ บริษัทต้องทบทวน หรือแก้ไขข้อตกลงหรือสัญญาการให้บริการกับผู้ใช้งานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้อง โดยประเมินจากผลกระทบที่เกิดขึ้นเมื่อมีการเปลี่ยนแปลงโดยบริษัท เช่น การแก้ไขนโยบาย มาตรการและขั้นตอนปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น หรือมีการเปลี่ยนแปลงโดยผู้ใช้งานภายนอก เช่น การใช้เทคโนโลยีใหม่ การเปลี่ยนคู่ค้า หรือคู่สัญญาใหม่ เป็นต้น

5) บริษัทต้องประเมินการให้บริการผู้ใช้งานภายนอกอย่างสม่ำเสมอ หรือก่อนต่ออายุข้อตกลงหรือสัญญาการให้บริการ

8.12 การจัดการทรัพยากรระบบ

เพื่อให้มีการบริหารจัดการขีดความสามารถของอุปกรณ์คอมพิวเตอร์ ให้เพียงพอต่อการใช้งาน และมีประสิทธิภาพทั้งในปัจจุบันและอนาคต

1) ผู้ดูแลระบบและส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการประมาณการหรือสำรวจความต้องการใช้งานอุปกรณ์คอมพิวเตอร์ในอนาคต เพื่อรองรับความต้องการด้านธุรกิจของบริษัท

2) ส่วนเทคโนโลยีสารสนเทศ ต้องรวบรวมความต้องการสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ พร้อมทั้งสำรวจความสามารถในการให้บริการในปัจจุบัน เพื่อจัดเตรียมโครงสร้างพื้นฐานด้านสารสนเทศในส่วนที่รับผิดชอบให้เพียงพอต่อความต้องการ โดยพิจารณาในเรื่องอย่างน้อยดังต่อไปนี้

- ความสามารถในการประมวลผล
- ความต้องการหน่วยความจำ
- ปริมาณการใช้งานและความจุของหน่วยเก็บข้อมูล และปริมาณข้อมูลในระบบเครือข่ายที่สามารถรองรับได้
- จำนวนและประเภทของสิทธิการใช้ซอฟต์แวร์
- การตั้งค่าการติดตั้งของระบบ

3) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการเฝ้าระวังการใช้งานของอุปกรณ์คอมพิวเตอร์และการปรับแต่ง เพื่อให้อุปกรณ์คอมพิวเตอร์สามารถทำงานได้อย่างมีประสิทธิภาพ

4) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดทำรายงานการใช้งานอุปกรณ์คอมพิวเตอร์สารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อรองรับการประมาณการในอนาคตได้อย่างเหมาะสม

9. การบริหารจัดการด้านการสื่อสาร (Communication Management)

เพื่อให้การบริหารจัดการด้านการสื่อสารด้านสารสนเทศเป็นไปอย่างถูกต้อง และรักษาไว้ซึ่งความมั่นคงปลอดภัยด้านสารสนเทศ บริษัทมีแนวนโยบายในเรื่องการบริหารจัดการด้านการสื่อสารด้านสารสนเทศ ดังต่อไปนี้

9.1 การใช้งานจดหมายอิเล็กทรอนิกส์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้งานต้องให้ความสำคัญ ตระหนักถึงปัญหาที่อาจจะเกิดขึ้น และต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ส่วนเทคโนโลยีสารสนเทศกำหนดไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ และต้องปฏิบัติตามอย่างเคร่งครัด โดยดำเนินการอย่างน้อยดังต่อไปนี้

1) ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัท ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

2) ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท

3) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการเข้ารหัสเพื่อรักษาความลับของข้อมูลตามระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีการยืนยันและพิสูจน์แหล่งที่มาของข้อความ มีกระบวนการเพื่อให้มั่นใจว่าผู้รับได้รับข้อความ และมีการพิสูจน์ความถูกต้องครบถ้วนของข้อความตามระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

5) สำหรับผู้ใช้รายใหม่ที่ได้รับรหัสผ่านชั่วคราว ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านทันที โดยการตั้งรหัสผ่านจะต้องเป็นไปตามนโยบายบริหารจัดการรหัสผ่านของบริษัท

6) ส่วนเทคโนโลยีสารสนเทศ ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้อย่างมาก ไม่เกิน 3 ครั้ง และควรมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่านสม่ำเสมอ เช่น 60 วัน 90 วัน เป็นต้น

7) ผู้ใช้งาน ควรออกจากระบบทุกครั้งเมื่อใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น เพื่อป้องกันบุคคลอื่นแอบอ้างและเข้าใช้งาน

8) ผู้ใช้งาน ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

9) ผู้ใช้งาน ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

10) ผู้ใช้งาน ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของบัญชี และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

11) ผู้ใช้งาน ควรตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส

12) ผู้ใช้งาน หากได้รับจดหมายอิเล็กทรอนิกส์จากผู้ส่งที่ไม่แน่ใจหรือไม่คุ้นเคย หรือเป็นที่น่าสงสัย จะต้องแจ้งผู้ดูแลระบบโดยทันที และไม่เปิดดูข้อความภายในหรือส่งต่อจดหมายอิเล็กทรอนิกส์

13) ผู้ใช้งาน ไม่ควรส่งข้อมูลที่เป็นความลับผ่านช่องทางจดหมายอิเล็กทรอนิกส์ หากมีความจำเป็นผู้ใช้งานจะต้องกำหนดและใส่รหัสผ่านเพื่อป้องกันการโจรกรรมข้อมูลผ่านช่องทางจดหมายอิเล็กทรอนิกส์ และจะต้องไม่ใส่หรือระบุข้อความลับใด ๆ ลงในจดหมายอิเล็กทรอนิกส์ และผู้ใช้ต้องแจ้งรหัสผ่านในการเปิดดูข้อมูลโดยช่องทางการสื่อสารอื่น ๆ หรือผ่านช่องทางจดหมายอิเล็กทรอนิกส์ฉบับแยกจากฉบับที่มีข้อมูล

14) ส่วนเทคโนโลยีสารสนเทศ จัดทำเงื่อนไขการใช้งานข้อความจดหมายอิเล็กทรอนิกส์และสื่อสาร ให้ผู้ใช้งานรับทราบ

15) มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน (Audit Log) และมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ

9.2 การใช้งานอินเทอร์เน็ต

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

1) ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดเส้นทางการเชื่อมต่ออินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่บริษัทจัดสรรไว้เท่านั้น

2) เครื่องคอมพิวเตอร์ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการปิดช่องโหว่ของระบบปฏิบัติการ Web Browser สม่ำเสมอ

3) การรับข้อมูลทางอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานทุกครั้ง

4) ห้ามใช้และห้ามเผยแพร่ข้อมูลในเครือข่ายของบริษัท เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือเพื่อการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือข้อมูลที่ละเมิดสิทธิของบุคคลอื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัท

5) ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

6) ห้ามผู้ใช้งาน เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัท ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

7) ห้ามกระทำการติดตั้ง Download/Upload ซอฟต์แวร์ หรือโปรแกรม ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขายที่ละเมิดทรัพย์สินทางปัญญาผ่านช่องทางอินเทอร์เน็ตของบริษัท

8) ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยของข้อมูลของบริษัท

9) ผู้ใช้งานมีหน้าที่ต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้

10) ในกรณีที่ผู้ใช้งานพบเว็บไซต์ที่ไม่เหมาะสม เป็นภัยต่อความมั่นคงปลอดภัย ขัดต่อศีลธรรม ขัดต่อชาติ ศาสนา พระมหากษัตริย์ เป็นภัยต่อสังคม หรือกระทบต่อความปลอดภัยของบริษัท ผู้ใช้งานต้องยกเลิกการติดต่อกับเว็บไซต์ดังกล่าว และแจ้งส่วนเทคโนโลยีสารสนเทศทราบทันที

11) ในการใช้งาน Social Media หรือ Web board ของผู้ใช้งาน เพื่อแลกเปลี่ยนข้อมูลในการปฏิบัติงานสามารถกระทำได้ โดยต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของบริษัท โดยความคิดเห็นนั้นให้ถือว่าเป็นความคิดเห็นส่วนบุคคลของผู้ใช้งานไม่ใช่ความคิดเห็นจากบริษัท

12) ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัท การทำลายความสัมพันธ์กับลูกค้า พันธมิตรธุรกิจ และเจ้าหน้าที่ของหน่วยงานอื่น ๆ

13) หลังใช้งานอินเทอร์เน็ตแล้ว ให้ออกจากระบบ และปิด Web Browser เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

14) ส่วนเทคโนโลยีสารสนเทศสงวนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควรหากพบว่ามีการละเมิดนโยบายการใช้งานอินเทอร์เน็ต

9.3 การใช้สื่อสังคมออนไลน์

เพื่อให้เกิดความเข้าใจและใช้งานสื่อสังคมออนไลน์ (Social Media) ได้อย่างถูกต้องและเป็นไปตามระเบียบของบริษัท เพื่อหลีกเลี่ยงผลกระทบและความเสียหายที่อาจเกิดขึ้นกับบริษัทและผู้ใช้งาน

1) ผู้ใช้งาน ต้องพึงตระหนักถึงข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง ข้อมูลต่าง ๆ หรือความคิดเห็นที่เผยแพร่บนสื่อสังคมออนไลน์ เป็นสื่อที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบทั้งทางด้านสังคมและด้านกฎหมาย

2) ผู้ใช้งาน ต้องไม่ใช้สื่อสังคมออนไลน์ในการเผยแพร่ความคิดเห็นที่อาจกระตุ้นหรือนำไปสู่การยั่วยุการโต้แย้งที่รุนแรง หรือขัดต่อจริยธรรม เช่น เรื่องเกี่ยวกับการเมือง ศาสนา ความมั่นคงของชาติ และชนชั้นในชาติเป็นต้น หรือเผยแพร่เนื้อหาที่ขัดต่อกฎหมาย ศีลธรรม กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

3) ผู้ใช้งาน ต้องระมัดระวังการใช้งานที่ผิดรูปแบบหรือจุดประสงค์โดยละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และพระราชบัญญัติความคุ้มครองข้อมูลส่วนบุคคล

4) ผู้ใช้งาน ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน และหากมีความจำเป็นต้องใช้งานอันมีลิขสิทธิ์เพื่อประกอบในการทำสื่อสังคมออนไลน์ จะต้องได้รับอนุญาตจากเจ้าของลิขสิทธิ์ก่อนการเผยแพร่

5) ผู้ใช้งาน หากประสงค์ใช้สื่อสังคมออนไลน์เพื่อเผยแพร่ข้อมูลเกี่ยวกับองค์กร ควรแยกบัญชีผู้ใช้งานระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน และหากประสงค์ใช้งานสื่อสังคมออนไลน์ที่แสดงสังกัดหน่วยงานภายในของบริษัท ต้องแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง และผู้เผยแพร่ต้องแสดงชื่อตำแหน่ง ให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ติดตามสามารถใช้ดุลยพินิจในการติดตามได้

6) ผู้ใช้งาน ต้องพึงระวังการใช้ถ้อยคำ การใช้ภาษาที่อาจก่อให้เกิดความเข้าใจคลาดเคลื่อน เข้าข่ายการดูหมิ่น หมิ่นประมาทบุคคลอื่น หรือละเมิดสิทธิส่วนบุคคล และควรใช้ภาษาให้ถูกต้อง สุภาพ และสร้างสรรค์

7) งดการใช้สื่อสังคมออนไลน์เปิดเผย วิพากษ์ วิจารณ์ ตลอดจนแสดงความคิดเห็นในเรื่องที่เป็นข้อมูลภายใน ข้อมูลที่มีความสำคัญหรือเป็นความลับของบริษัท ซึ่งอาจส่งผลกระทบต่อบริษัทได้

8) ต้องไม่ใช้งานสื่อสังคมออนไลน์ไม่ว่าด้วยช่องทางใด ๆ ณ เวลาใด ณ สถานที่ใด เพื่อด่าทอ ให้ร้าย ดูหมิ่น หมิ่นประมาท รวมถึงการสื่อสารเพื่อวิจารณ์การบังคับบัญชา การบริหารกิจการของบริษัท พนักงานทุกระดับชั้น ตลอดจนผู้ใช้บริการ ผู้ให้บริการ โดยการกระทำเช่นว่านั้นอาจหรือก่อให้เกิดความเสียหายทั้งด้านชื่อเสียง ภาพลักษณ์ การยอมรับนับถือไม่ว่าทางตรงหรือทางอ้อมแก่บริษัท หรือบุคคลอื่นดังกล่าวข้างต้น

9) การแสดงความคิดเห็นใด ๆ ที่มีการเผยแพร่บนสื่อสังคมออนไลน์ อาจกระทำได้แต่ต้องเป็นการกระทำโดยสุจริตและไม่ละเมิดสิทธิของผู้อื่น โดยผู้แสดงความคิดเห็นจะต้องรับผิดชอบในการแสดงความคิดเห็นและการเผยแพร่บนสื่อสังคมออนไลน์ทุกกรณี

10) หากพบว่ามีข้อความบนสื่อสังคมออนไลน์ที่มีการบิดเบือนข้อเท็จจริง ประเด็นขัดแย้ง หรือข้อความอื่นใดซึ่งอาจทำให้เกิดความเสื่อมเสียชื่อเสียงของบริษัท ให้ผู้ใช้งานแจ้งต่อผู้จัดการ/หัวหน้าทีมของตน หรือผู้ที่เกี่ยวข้องกับเรื่องนั้น ๆ ทราบ และทั้งนี้ส่วนเทคโนโลยีสารสนเทศต้องมอบหมายให้มีผู้เฝ้าระวังและตรวจตราข่าวสารในทุกช่องทางที่อาจส่งผลกระทบต่อชื่อเสียงของบริษัทได้

11) ป้องกันการถูกละเมิดความเป็นส่วนตัวโดยศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Setting” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสม นอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลต่อบริษัทได้ด้วย

12) ไม่เผยแพร่ข้อความที่เป็นข่าวลือ ข่าวไม่ปรากฏที่มา หรือข้อมูลที่เป็นเพียงการคาดเดา เป็นเท็จหรือข้อมูลที่ก่อให้เกิดความเข้าใจผิด หรือการยั่วยุให้เกิดความขัดแย้งขึ้นภายในบริษัท

13) การนำเสนอหรือเผยแพร่ข้อมูลต่าง ๆ ผ่านสื่อสังคมออนไลน์ หากเกิดความผิดพลาด ซึ่งอาจก่อให้เกิดผลกระทบต่อบริษัทหรือบุคคลอื่นได้ ผู้ใช้งานต้องแสดงความรับผิดชอบและดำเนินการแก้ไขในทันที

9.4 การรับส่งข้อมูลสารสนเทศ

เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในบริษัท และระหว่างระบบเครือข่ายภายในบริษัทกับระบบเครือข่ายภายนอก ประกอบไปด้วยเรื่องดังต่อไปนี้

9.4.1 การควบคุมการรับส่งข้อมูลสารสนเทศ

1) ต้องจัดให้มีการควบคุมการรับส่งข้อมูลสารสนเทศให้สอดคล้องกับระดับความมั่นคงปลอดภัยของสารสนเทศ

2) ต้องจัดให้มีการป้องกัน การดักจับข้อมูลที่รับส่ง การทำสำเนา การเปลี่ยนแปลงแก้ไข การส่งผิดเส้นทาง (Mis-Routing) และการถูกทำลาย

3) ต้องมีการตรวจจับและป้องกันโปรแกรมที่ไม่ประสงค์ดี

4) ต้องมีการป้องกันข้อมูลที่สำคัญในรูปสื่ออิเล็กทรอนิกส์ที่ส่งผ่านในรูปแบบของเอกสารแนบและการควบคุมการส่งต่อ เช่น การส่งต่อจดหมายอิเล็กทรอนิกส์ภายในบริษัท ไปจดหมายอิเล็กทรอนิกส์ภายนอกโดยอัตโนมัติ

5) ต้องมีการควบคุมในช่องทางการสื่อสารแบบไร้สาย โดยจะต้องคำนึงถึงความเสี่ยงเฉพาะด้านที่เกี่ยวข้อง

6) ต้องมีการกำกับดูแลหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของผู้ใช้งาน ผู้ใช้งานภายนอก ที่ปฏิบัติงานให้บริษัท

7) ต้องมีการควบคุมการใช้เทคนิคการเข้ารหัส เพื่อป้องกันสารสนเทศที่เป็นความลับให้สารสนเทศมีความถูกต้องและระบุตัวตนได้

8) ต้องมีการเก็บรักษาและทำลายเอกสารเพื่อให้เป็นไปตามข้อกำหนดที่มีผลทางกฎหมาย

9) ต้องมีการป้องกันอุปกรณ์คอมพิวเตอร์ที่ไม่มีผู้ดูแล

9.4.2 ข้อตกลงในการรับส่งข้อมูลสารสนเทศ

การรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ของบริษัทกับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากผู้จัดการ/หัวหน้าทีม โดยต้องทำข้อตกลงหรือสัญญากับหน่วยงานภายนอก ให้มีข้อกำหนดหรือเงื่อนไขอย่างเหมาะสม อย่างน้อยดังต่อไปนี้

1) การรักษาความลับ กรรมสิทธิ์ การป้องกันสิทธิและทรัพย์สินทางปัญญาของสารสนเทศและซอฟต์แวร์

2) ข้อตกลงในการฝากข้อมูลหรือ Source Code ไว้ที่หน่วยงานภายนอกซึ่งไม่ใช่คู่สัญญา เพื่อให้บริษัทสามารถเข้าถึงข้อมูลดังกล่าวได้ ในกรณีที่หน่วยงานคู่สัญญาหรือหน่วยงานที่ได้รับการว่าจ้างให้พัฒนาซอฟต์แวร์ไม่สามารถให้บริการได้

3) หน้าที่ความรับผิดชอบของบริษัทและคู่สัญญาในการควบคุมสารสนเทศและซอฟต์แวร์ระหว่างการส่งผ่าน (Transmission) การกระจายต่อ (Dispatch) และการได้รับ (Receive) สารสนเทศ

4) ความรับผิดชอบ และการใช้เมื่อสารสนเทศสูญหาย ถูกแก้ไข หรือถูกเปิดเผยโดยมิชอบ

5) กำหนดข้อตกลงร่วมกันในการจัดทำป้ายชื่อ ตามระดับความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มีความเข้าใจตรงกันและสามารถดำเนินการป้องกันได้อย่างเหมาะสม

6) มาตรฐานทางเทคนิคอื่น ๆ สำหรับ รูปแบบของข้อมูล การจัดเก็บ การประมวลผล และการส่งสารสนเทศที่มีการรับส่งข้อมูล

7) กระบวนการติดตาม และป้องกันการปฏิเสธความรับผิด (Non-Repudiation)

9.4.3 การรับส่งสื่อบันทึกข้อมูล

1) ต้องมีการใช้บริการผู้จัดส่งที่มีความน่าเชื่อถือซึ่งได้รับอนุญาตเท่านั้น

2) กำหนดให้มีกระบวนการในการระบุตัวตน เพื่อให้สามารถติดตามเจ้าหน้าที่ผู้จัดส่งได้

3) มีการบรรจุหีบห่ออย่างเหมาะสมและเป็นไปตามคำแนะนำของผู้ผลิต เพื่อป้องกันความเสียหายทางกายภาพที่อาจเกิดขึ้นในช่วงขนส่ง เช่น การถูกความร้อน ความชื้น หรือคลื่นแม่เหล็กไฟฟ้า เป็นต้น

4) มีการป้องกันการเปิดเผยหรือดัดแปลงสารสนเทศอย่างเหมาะสม เช่น การปิดผนึกและลงนามกำกับ การใช้บรรจุภัณฑ์ที่สามารถล็อคได้ และการส่งมอบด้วยตนเอง เป็นต้น

5) ผู้จัดการ/หัวหน้าทีม ต้องจัดให้มีกระบวนการรับส่งที่เหมาะสมเพื่อให้มั่นใจว่าผู้รับได้รับของถูกต้องครบถ้วน โดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ

9.4.4 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

1) จัดให้มีการควบคุมทางกายภาพ เพื่อป้องกันการเข้าถึงอุปกรณ์ที่ให้บริการข้อความทางอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

2) จัดให้มีการบริหารจัดการการเข้าถึงของผู้ใช้อย่างเหมาะสม เพื่อควบคุมการเข้าถึงระบบเฉพาะผู้ที่ได้รับอนุญาต

3) จัดทำหลักเกณฑ์การใช้งานแอพพลิเคชันทางธุรกิจและสื่อสารให้ผู้ใช้งานทราบเรื่องการรับส่งข้อมูลสารสนเทศระหว่างแอพพลิเคชัน

4) จัดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน และมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ

5) จัดให้มีการปฏิบัติตามข้อกำหนดที่มีผลทางกฎหมาย เช่น การสำรองข้อมูล การควบคุมการเปลี่ยนแปลง และการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น

6) ต้องมีการเข้ารหัสเพื่อรักษาความลับของข้อมูล ตามระดับความมั่นคงปลอดภัยของสารสนเทศ

7) ต้องจัดให้มีการยืนยันและพิสูจน์ตัวตนของแหล่งที่มาของสารสนเทศและพิสูจน์ความถูกต้องครบถ้วนของสารสนเทศที่ส่งระหว่างแอพพลิเคชัน ตามระดับความมั่นคงปลอดภัยของสารสนเทศ

10. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

(Information System Acquisition, Development and Maintenance)

เพื่อให้ความมั่นคงปลอดภัยด้านสารสนเทศเป็นองค์ประกอบสำคัญของระบบ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะ

1) ความต้องการด้านความมั่นคงปลอดภัยของระบบ

1.1) ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศต้องมีการพิจารณาร่วมกับความต้องการสำหรับระบบใหม่หรือระบบที่มีอยู่แล้ว

1.2) สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันอย่างเหมาะสมจากการเปิดเผย เปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต

1.3) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตและการส่งข้อมูลซ้ำ โดยปฏิบัติตามแนวปฏิบัติงานการจัดระดับชั้นความลับของข้อมูล

2) ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน

2.1) กฎเกณฑ์ในการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดขั้นตอนการปฏิบัติงานเพื่อเป็นแนวปฏิบัติสำหรับการพัฒนาระบบ

2.2) การเปลี่ยนแปลงระบบหรือการพัฒนาระบบ ต้องมีการควบคุมโดยปฏิบัติตามนโยบายการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management) และขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลง

2.3) เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบที่สำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน หรือต่อความมั่นคงปลอดภัยของบริษัท

2.4) ต้องพิจารณาสภาพแวดล้อมที่เหมาะสมต่อการพัฒนาระบบที่ต้องการความมั่นคงปลอดภัย ได้แก่ พื้นที่ปฏิบัติงานไม่อยู่ในพื้นที่พลุกพล่าน หรือเข้าถึงได้ง่าย

2.5) ต้องจัดให้มีการแยกระบบใช้งานจริงออกจากระบบสำหรับการพัฒนาและการทดสอบ เพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูล หรือการประมวลผลของระบบที่ให้บริการจริง

2.6) การจ้างพัฒนาระบบจากผู้ใช้งานภายนอก ต้องมีการควบคุม เฝ้าระวัง ติดตามการดำเนินงานอย่างใกล้ชิดเพื่อให้เป็นไปตามขอบเขตการดำเนินงาน และสอดคล้องกับนโยบาย ขั้นตอนปฏิบัติของบริษัทที่กำหนดไว้

2.7) ผู้พัฒนาระบบควรมีการจัดทำคู่มือหรือขั้นตอนการทดสอบระบบ และจะต้องมีการปรับปรุงคู่มือการใช้งาน หรือคู่มืออบรมผู้ใช้งาน เมื่อการขอเปลี่ยนแปลงนั้น ๆ มีผลต่อคู่มือฉบับเดิม

2.8) ควรมีการทดสอบการใช้งานระบบ เพื่อเป็นการสอบทานคู่มือหรือขั้นตอนการทดสอบระบบ รวมถึงการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชันใหม่

2.9) ควรมีการยืนยันผลการทดสอบจากผู้ที่เกี่ยวข้อง และมีการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจก่อนย้ายระบบงานที่ได้จัดทำเรียบร้อยแล้ว จากระบบทดสอบเข้าสู่ระบบใช้งานจริง

2.10) ต้องมีการควบคุม กำหนดสิทธิการเข้าถึง Source Code อย่างเหมาะสมให้สอดคล้อง ตามบทบาทหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

2.11) ในกระบวนการพัฒนาระบบสารสนเทศ จะต้องมีการตรวจทานความถูกต้องของข้อมูลที่ดีเพื่อลดความเสี่ยงที่อาจเกิดจากความผิดพลาดในการนำเข้าข้อมูลและความผิดพลาดของข้อมูลที่เกิดจากประมวลผลข้อมูล

2.12) ควรมีการควบคุมและตรวจสอบการทำงานของแอปพลิเคชัน เพื่อป้องกันความเสี่ยงที่อาจเกิดจากการทำงานหรือการประมวลผลข้อมูลที่ผิดพลาดอันจะส่งผลเสียต่อระบบโดยรวม

2.13) ควรจัดทำข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง และความถูกต้องครบถ้วนของข้อมูลในแอปพลิเคชัน รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

3) การควบคุมข้อมูลในการทดสอบ

ผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบใช้งานจริงมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบ ต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง และต้องมีการควบคุมข้อมูลในระบบทดสอบให้เป็นไปตามชั้นความลับและการคุ้มครองข้อมูลส่วนบุคคล

11. ความมั่นคงปลอดภัยระบบสารสนเทศด้านความสัมพันธ์กับผู้ใช้งานภายนอก

(Information Security in Third Party Relationship)

การใช้บริการจากผู้ใช้งานภายนอก อาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น จึงจำเป็นต้องมีการควบคุมผู้ใช้งานภายนอกที่มีการเข้าใช้งานระบบสารสนเทศของบริษัทให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางการคัดเลือก ควบคุมการปฏิบัติงานของผู้ใช้งานภายนอก

1) บริษัทต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับผู้ใช้งานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาหรือประเมินความเสี่ยงที่อาจเกิดขึ้น และกำหนดแนวทางป้องกัน เพื่อลดความเสี่ยงนั้นก่อนอนุญาตให้ผู้ใช้งานภายนอก หรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของบริษัท

2) ผู้ดูแลระบบและแผนกต่าง ๆ ที่รับผิดชอบในการประสานงานกับผู้ใช้งานภายนอก ต้องกำกับดูแลผู้ใช้งานภายนอก ให้ปฏิบัติตามที่ว่าจ้างในสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

3) การควบคุมการเข้าใช้งานของผู้ใช้งานภายนอก

3.1) ผู้ดูแลระบบและแผนกต่าง ๆ ต้องประเมินความเสี่ยงจากการเข้าถึงระบบสารสนเทศ และมีมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบได้

3.2) ผู้ใช้งานภายนอกที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของบริษัท จะต้องทำเรื่องขออนุมัติจากผู้จัดการ/หัวหน้าทีม ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าวเป็นลายลักษณ์อักษร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์เชื่อมต่อเครือข่าย
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

3.3) ผู้ใช้งานภายนอก ไม่ว่าจะปฏิบัติงานอยู่ภายในบริษัทหรือนอกบริษัท ต้องลงนามในสัญญาการรักษาข้อมูลที่เป็นความลับของบริษัท

3.4) ส่วนเทคโนโลยีสารสนเทศมีหน้าที่กำหนดและทบทวนสิทธิของการเข้าใช้งานระบบสารสนเทศเฉพาะบุคคลที่จำเป็นเท่านั้น และมีการทบทวนสิทธิให้เป็นปัจจุบัน

3.5) บริษัทต้องพิจารณาการเข้าประเมินความเสี่ยง หรือจัดทำการควบคุมภายในของผู้ใช้งานภายนอกทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศ

3.6) บริษัทมีสิทธิในการตรวจสอบตามสัญญาจ้าง เพื่อให้มั่นใจได้ว่าบริษัทสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

3.7) ในกรณีที่มีการเปลี่ยนแปลงการดำเนินงาน ผู้ใช้งานภายนอกต้องแจ้งให้บริษัทรับทราบและอนุมัติการเปลี่ยนแปลงนั้นก่อนการดำเนินงาน เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

3.8) เมื่อสิ้นสุดระยะเวลาการใช้งาน บริษัทจะดำเนินการยกเลิกสิทธิการเข้าใช้งานระบบสารสนเทศทันที

3.9) หากพบเหตุละเมิดด้านความมั่นคงปลอดภัยด้านสารสนเทศ ให้แจ้งส่วนเทคโนโลยีสารสนเทศยกเลิกสิทธิการเข้าใช้งานระบบสารสนเทศทันที

3.10) ผู้ใช้งานภายนอกต้องยอมรับและดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่บริษัทประกาศไว้อย่างเคร่งครัด

3.11) บริษัทมีสิทธิที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของผู้ใช้งานภายนอก

12. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ

(Information Security Incident Management)

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัท ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และมีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของบริษัท

1) การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุละเมิดด้านความมั่นคงปลอดภัย

1.1) บริษัทต้องกำหนดหน้าที่ความรับผิดชอบ และกำหนดขั้นตอนปฏิบัติเพื่อให้สามารถรับมือกับเหตุละเมิดด้านความมั่นคงปลอดภัยอย่างทันท่วงที

1.2) บริษัทต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ออกจากเหตุการณ์ด้านการปฏิบัติงานทั่วไป เพื่อกำหนดแนวทางแก้ไขที่ถูกต้องเหมาะสม

1.3) บริษัทต้องกำหนดช่องทาง และเกณฑ์ในการรายงานเหตุการณ์ หรือจุดอ่อนหรือเหตุการณ์ความมั่นคงสารสนเทศ หรือสื่อสารให้บุคลากรในบริษัท และบุคคลภายนอกรับทราบ

2) การรายงานเหตุการณ์น่าสงสัย หากผู้ใช้งานพบเหตุการณ์ที่น่าสงสัย ให้รายงานต่อส่วนเทคโนโลยีสารสนเทศและผู้จัดการ/หัวหน้าทีมทันที ได้แก่ เหตุการณดังนี้

2.1) พบว่ารหัสผ่านไม่สามารถใช้งานได้ โดยไม่ทราบสาเหตุ

2.2) เวลาการเข้าใช้งานระบบครั้งล่าสุด (Last Login Time) ที่ผิดปกติ

2.3) พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน ได้แก่ พบไฟล์ที่น่าสงสัยว่าเป็นไวรัสการเปลี่ยนแปลงของค่าต่าง ๆ

2.4) พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

2.5) พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไข หรือลบทิ้ง

2.6) ความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธี ไม่ว่าจะสำเร็จหรือไม่

2.7) การให้บริการของระบบเกิดการหยุดชะงัก หรือไม่สามารถให้บริการ

2.8) เกิดการละเมิดสิทธิเข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

2.9) การแก้ไขค่าความปลอดภัยในระบบโดยไม่ได้รับอนุญาต

3) ผู้ใช้งานต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทต่อส่วนเทคโนโลยีสารสนเทศ และผู้จัดการ/หัวหน้าทีม อย่างรวดเร็วที่สุด

4) ส่วนเทคโนโลยีสารสนเทศต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ จัดแยกกลุ่มเหตุการณ์ หรือจุดอ่อนด้านความมั่นคงปลอดภัย จัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้ ในกรณีที่พบว่าเหตุการณ์ หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยด้านสารสนเทศให้แจ้งผู้ที่เกี่ยวข้องทราบเพื่อแก้ไข

5) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศและการทำงานที่บกพร่องของระบบสารสนเทศ

5.1) หากพบเห็นเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศหรือการทำงานที่บกพร่อง หรือการทำงานผิดปกติ ต้องรายงานสิ่งที่เกิดขึ้นให้แก่ส่วนเทคโนโลยีสารสนเทศทราบโดยทันที

5.2) กรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนเทคโนโลยีสารสนเทศต้องร่วมกับผู้ที่รับผิดชอบ ประเมินขอบเขตและความรุนแรงของปัญหา หากพบว่าเป็นปัญหาที่จะมีผลกระทบรุนแรง หรือมีผลต่อชื่อเสียงของบริษัท จะต้องรายงานให้ผู้บริหารทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันต่อไป

6) การเรียนรู้จากเหตุละเมิดด้านความมั่นคงปลอดภัย

6.1) ส่วนเทคโนโลยีสารสนเทศ ต้องบันทึกเหตุละเมิดด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขจากเหตุการณ์ที่เกิดขึ้น เพื่อเตรียมการป้องกันไว้ล่วงหน้า

6.2) ส่วนเทคโนโลยีสารสนเทศ ต้องมีการทบทวนเหตุละเมิดความมั่นคงปลอดภัย และจัดทำรายการเฝ้าระวังล่วงหน้าจากเหตุละเมิดความมั่นคง เพื่อป้องกันการเกิดปัญหาเดิมซ้ำ

6.3) ส่วนเทคโนโลยีสารสนเทศ ต้องวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

7) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบบริษัท และกฎหมายที่เกี่ยวข้อง

13. การบริหารความต่อเนื่องในการดำเนินงาน

(Business Continuity Management)

เพื่อเป็นแนวทางในการบริหารจัดการความต่อเนื่องในการดำเนินงานของบริษัทเมื่ออยู่ภายใต้สภาวะวิกฤตและเหตุฉุกเฉินต่าง ๆ ทำให้มั่นใจได้ว่าขั้นตอนการดำเนินงานและระบบสารสนเทศต่าง ๆ ที่สำคัญของบริษัท มีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP) และแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan หรือ DRP) อย่างเหมาะสม เพื่อให้การดำเนินงานของบริษัทเป็นไปอย่างต่อเนื่อง

1) ขั้นตอนการเตรียมแผนรองรับเหตุการณ์ฉุกเฉิน

1.1) บริษัทต้องจัดตั้งคณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากแผนก/ทีมพัฒนา

1.2) คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษรและปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อย ปีละ 1 ครั้ง

1.3) กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ประกอบด้วย

- การวิเคราะห์ผลกระทบทางการดำเนินงานของบริษัท (Business Impact Analysis)
- การประเมินความเสี่ยงและการควบคุม (Risk Analysis & Control)
- แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan หรือ BCP) แผนการกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Plan หรือ DRP)
- การประชาสัมพันธ์และการฝึกอบรม การทดสอบ การปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉิน

1.4) แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

- ป้องกันผลกระทบและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อการให้บริการของบริษัท
- กำหนดแนวทางในการจัดการต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย
- กิจกรรมเพื่อให้กระบวนการดำเนินงานเป็นไปได้อย่างต่อเนื่อง ได้แก่ การสำรองข้อมูล การกู้คืนระบบ เป็นต้น
- ต้องมีแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ

2) การตอบสนองต่อเหตุการณ์ฉุกเฉินเพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง

2.1) ระบุขั้นตอนการดำเนินการ ประเมินสถานการณ์เบื้องต้น สถานที่ สาเหตุ และขอบเขตความเสียหาย เพื่อระงับเหตุการณ์ความเสียหาย และวิธีการดำเนินงานต่าง ๆ ที่เกี่ยวข้อง ได้แก่ แนวทางการเก็บรักษาข้อมูล เอกสาร ความปลอดภัยของผู้ปฏิบัติงาน การเคลื่อนย้ายอพยพพนักงาน ผู้ใช้งานและสินทรัพย์ที่จำเป็น

2.2) ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร กำหนดวิธีการสื่อสาร และประสานงานกับหน่วยงาน หรือบุคคลที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งสถานการณ์และแนวทางการดำเนินงาน หรือสถานที่ติดต่อ

ฉุกเฉิน รวมทั้งจัดทำรายชื่อผู้ที่รับผิดชอบในการดำเนินการ ช่วยเหลือ ยุติเหตุการณ์ความเสียหายทั้งภายในและภายนอกบริษัท

2.3) ระบุความต้องการทรัพยากรต่าง ๆ ที่มีความจำเป็น งบประมาณ จำนวนแรงงาน สถานที่ ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค อุปกรณ์และเครื่องมือต่าง ๆ ให้ชัดเจน

3) การกลับคืนสู่การทำงานปกติ

3.1) ระบุขั้นตอนการปฏิบัติงานเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ การควบคุมการติดตั้ง การตั้งค่าและทดสอบระบบที่ถูกกู้คืนมาหรือทดแทนใหม่ การรายงานสรุปความเสียหายต่อผู้บริหาร

3.2) จัดทำรายชื่อผู้ที่รับผิดชอบทั้งจากภายในและภายนอก เพื่อการดำเนินการช่วยเหลือ ฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ

3.3) การกำหนดกระบวนการป้องกันและควบคุมความเสี่ยง เพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ความเสียหายในอนาคต

4) คณะทำงานรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศต้องระบุขั้นตอนและวิธีการประชาสัมพันธ์ให้แก่ผู้บริหาร พนักงาน และจัดฝึกอบรมให้แก่ผู้มีส่วนเกี่ยวข้องให้รับทราบถึงวัตถุประสงค์ ขั้นตอนการปฏิบัติงาน การประสานงาน การติดต่อสื่อสาร ขั้นตอนการรายงาน ระบบรักษาความปลอดภัยและหน้าที่ความรับผิดชอบตามแผนอย่างชัดเจน

5) การทดสอบแผนรองรับเหตุการณ์ฉุกเฉิน

5.1) กำหนดเวลาการทดสอบแผนกู้คืนที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้นจนสิ้นสุดกระบวนการทดสอบ

5.2) กำหนดเหตุการณ์จำลองและรายละเอียดของเหตุการณ์ที่จะใช้ทดสอบ ต้องระบุวัตถุประสงค์ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน

5.3) กำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบแผน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุมประสานงาน และรับผิดชอบในการจัดการทดสอบแผน รวมถึงสถานที่และอุปกรณ์เครื่องมือต่าง ๆ และงบประมาณที่ต้องใช้

5.4) กำหนดเกณฑ์การประเมินผลและผู้รับผิดชอบในการประเมินผล เกณฑ์การประเมินผล ซึ่งอาจมีความแตกต่างกันไปตามลักษณะของระบบงาน กระบวนการทำงาน และวัตถุประสงค์ของการทดสอบในแต่ละครั้ง

5.5) ต้องมีการทดสอบสภาพพร้อมใช้งานระบบสารสนเทศ และระบบสำรองอย่างน้อยปีละ 1 ครั้ง

6) การปรับปรุงและตรวจสอบแผนรองรับเหตุการณ์ฉุกเฉิน

6.1) กำหนดแนวทาง และระยะเวลาในการปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

6.2) กำหนดผู้รับผิดชอบในการตรวจสอบแผน เพื่อยืนยันความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผน

7) รายละเอียดเพิ่มเติมอื่น ๆ

7.1) รายชื่อ ที่อยู่ หมายเลขโทรศัพท์ของพนักงาน และผู้ใช้งานที่มีหน้าที่รับผิดชอบในการปฏิบัติตามแผน

7.2) รายชื่อหน่วยงาน สถานที่ตั้ง และหมายเลขโทรศัพท์ของผู้ใช้งานภายนอกที่เกี่ยวข้อง

7.3) รายละเอียดการปฏิบัติตามแผน (Checklist)

7.4) รูปแบบรายงานต่าง ๆ ที่จำเป็น

8) สภาพความพร้อมใช้ของอุปกรณ์คอมพิวเตอร์สารสนเทศ

8.1) ส่วนเทคโนโลยีสารสนเทศต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งานของระบบสารสนเทศที่มีความสำคัญสูง

8.2) ส่วนเทคโนโลยีสารสนเทศต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

14. การปฏิบัติตามข้อกำหนด
(Compliance)

เพื่อป้องกันการละเมิดที่เกี่ยวข้องกับการปฏิบัติงาน ระเบียบ ข้อบังคับ เงื่อนไขในสัญญา และข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นแนวทางในการปฏิบัติงานของบริษัท ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

14.1 การนำนโยบายไปสู่การปฏิบัติ

1) แผนกทรัพยากรบุคคล ต้องระบุแนวทางหรือมาตรการทางกฎหมาย ระเบียบปฏิบัติ และสัญญาว่าจ้าง รวมทั้งสัญญาที่ทำกับผู้ใช้งานภายนอกที่เกี่ยวข้องเพื่อทำให้มีการปฏิบัติตามนโยบายฉบับนี้

2) ส่วนเทคโนโลยีสารสนเทศต้องปรับปรุงแนวทางหรือมาตรการให้ทันสมัยอยู่เสมอ

14.2 การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานทรัพย์สินทางปัญญา

1) การนำซอฟต์แวร์ของบุคคลที่สามมาใช้ในบริษัท ต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

2) ผู้ใช้งานซอฟต์แวร์บนระบบสารสนเทศของบริษัท ต้องยึดถือและปฏิบัติตามกฎหมาย ข้อกำหนดของผู้ผลิตซอฟต์แวร์ สิทธิเรื่องทรัพย์สินทางปัญญา และสิทธิผู้ใช้งานข้อมูลสำคัญอย่างเคร่งครัด

3) ต้องควบคุมการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ โดยมีการบันทึกข้อมูลการใช้งาน เพื่อเก็บเป็นหลักฐาน และมีการตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง ถ้าหากพบว่ามีการละเมิดข้อตกลงจะต้องยกเลิกการติดตั้งหรือลบทิ้งทันที

4) ซอฟต์แวร์หรือระบบงานพัฒนาขึ้นเพื่อบริษัท และซอฟต์แวร์ที่ถูกพัฒนาโดยพนักงาน ถือเป็นสินทรัพย์ของบริษัท

5) การติดตั้งซอฟต์แวร์ใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการปรับปรุงระบบหรือซ่อมแซมแก้ไขระบบต่าง ๆ จากผู้ใช้งานภายนอกต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

6) ถ้ามีการติดตั้งซอฟต์แวร์ใด ๆ ในเครื่องคอมพิวเตอร์ของพนักงานโดยไม่ได้รับอนุญาต แล้วเกิดข้อพิพาททางกฎหมาย หรือข้อกำหนดและเงื่อนไขของผู้ผลิตซอฟต์แวร์นั้น ๆ ทางบริษัทขอสงวนสิทธิ์ที่จะไม่รับผิดชอบในการดำเนินการดังกล่าวไม่ว่าจะกรณีใด ๆ

7) ซอฟต์แวร์ที่เป็นสินทรัพย์ของบริษัท ห้ามมิให้ผู้ใช้งานคัดลอก แก้ไข ปรับแต่ง หรือนำไปให้ผู้อื่นใช้งานโดยไม่ได้รับอนุญาต

14.3 การป้องกันข้อมูลสำคัญของบริษัท

1) ข้อมูลสำคัญของบริษัท ต้องได้รับการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึง และการเผยแพร่โดยไม่ได้รับอนุญาต

2) การปฏิบัติงานต้องสอดคล้องกับกฎหมาย นโยบาย ระเบียบข้อบังคับที่เกี่ยวข้อง

14.4 การป้องกันข้อมูลส่วนบุคคลและการเข้ารหัส

1) ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล ต้องดำเนินการให้สอดคล้องกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

2) ส่วนเทคโนโลยีสารสนเทศ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนบุคคลของผู้ใช้งาน ได้แก่ ข้อมูลในจดหมายอิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น

3) ส่วนเทคโนโลยีสารสนเทศ ต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายภายในประเทศ และต่างประเทศ เกี่ยวกับการเข้ารหัสข้อมูล กรณีมีเหตุจำเป็นในการโยกย้ายข้อมูลที่เข้ารหัสไปยังอีกประเทศหนึ่ง ให้ศึกษาและปฏิบัติตามข้อกำหนด หรือกฎหมายของประเทศนั้นด้วย

14.5 การป้องกันการใช้งานอุปกรณ์คอมพิวเตอร์สารสนเทศผิดวัตถุประสงค์

1) อุปกรณ์คอมพิวเตอร์สารสนเทศของบริษัท มีไว้เพื่อใช้ในกิจการของบริษัทเท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหาร หรือผู้จัดการ/หัวหน้าทีม

2) ต้องกำหนดให้มีผู้รับผิดชอบ รวมถึงการจัดทำบัญชีรายการของอุปกรณ์คอมพิวเตอร์สารสนเทศที่ซื้อหรือเช่ามาใช้งาน

3) ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของบริษัท

4) การดำเนินการใด ๆ ที่เป็นการติดตั้งซอฟต์แวร์หรืออุปกรณ์เพิ่มเติมต้องได้รับการอนุมัติจากผู้จัดการ/หัวหน้าทีม และส่วนเทคโนโลยีสารสนเทศ เพื่อป้องกันการใช้งานที่ผิดวัตถุประสงค์หรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้

5) การใช้งานอุปกรณ์คอมพิวเตอร์ในระบบเครือข่ายและสารสนเทศของบริษัท จะต้องพิสูจน์ตัวตนก่อนการใช้งานด้วยการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน

14.6 การทบทวนความมั่นคงปลอดภัยด้านสารสนเทศ

1) ผู้จัดการ/หัวหน้าทีม ต้องกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ใต้บังคับบัญชา ให้ปฏิบัติตามแนวปฏิบัติด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบ ทั้งนี้เพื่อให้การปฏิบัติงานเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

2) วิธีการในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย วัตถุประสงค์ นโยบาย ขั้นตอนการปฏิบัติ การประเมินความเสี่ยง ต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

3) ส่วนเทคโนโลยีสารสนเทศ ต้องมีการทบทวนความสอดคล้องทางเทคนิคของระบบอย่างสม่ำเสมอ เพื่อพิจารณาความสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

14.7 การตรวจประเมินระบบสารสนเทศ

ส่วนเทคโนโลยีสารสนเทศ ต้องมีการวางแผนการตรวจประเมินระบบสารสนเทศ เพื่อลดผลกระทบต่อระบบและกระบวนการดำเนินงานของบริษัท อย่างน้อยปีละ 1 ครั้ง

14.8 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ

ส่วนเทคโนโลยีสารสนเทศ ต้องมีแนวทางป้องกันเครื่องมือที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำเครื่องมือไปใช้ในทางที่ผิด และป้องกันการเข้าถึงข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยเครื่องมือ