บริษัท คิน คอร์ปอเรชั่น จำกัด

KIN CORPORATION CO., LTD

นโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

รหัสเอกสาร : P-COM-028 วันที่บังคับใช้ : 01 กุมภาพันธ์ 2568 แก้ไขครั้งที่ : 01

1. บทนำ

บริษัท คิน คอร์ปอเรชั่น จำกัด กำหนดให้เทคโนโลยีสารสนเทศและการสื่อสาร เป็นปัจจัยสำคัญที่ช่วยส่งเสริมการดำเนินธุรกิจและเพิ่มประสิทธิภาพการทำงาน ฉะนั้น จึงเป็นความรับผิดชอบร่วมกันของพนักงานทุกคน ที่จะต้องใช้เทคโนโลยีสารสนเทศและการสื่อสารภายใต้ข้อบังคับของกฎหมาย คำสั่งบริษัท และ ตามมาตรฐานที่บริษัทกำหนด และบริษัทได้จัดให้มีการบริหารความปลอดภัยของระบบสารสนเทศ ซึ่งหมายถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ตามมาตรฐานสากล (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือกฎหมายอื่นที่เกี่ยวข้อง) ทั้งนี้ พนักงานบริษัททุกคนรวมถึง บุคคลภายนอก คู่ค้า และผู้ที่มีส่วนได้ส่วนเสียมีหน้าที่และข้อปฏิบัติตามระเบียบปฏิบัติฉบับนี้

2. วัตถุประสงค์

1. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท ทำให้ดำเนินงาน ได้อย่างมีประสิทธิภาพ และประสิทธิผลตามวัตถุประสงค์ที่กำหนดไว้
2. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีการปฏิบัติให้ผู้ใช้งานและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท
3. เพื่อป้องกันไม่ให้ระบบสารสนเทศ และสารสนเทศของบริษัท ถูกบุกรุก เปลี่ยนแปลง ขโมย ทำลายหรือการกระทำอื่น ๆ ที่อาจสร้างความเสียหายต่อบริษัท
4. เพื่อสร้างความมั่นใจให้กับบุคคลภายนอกที่เป็นคู่ค้า หรือผู้มีส่วนได้เสียต่าง ๆ ว่าข้อมูลส่วนบุคคลจะได้รับการปกป้องตามมาตรฐานความปลอดภัยของบริษัท
5. เพื่อเผยแพร่ให้ผู้ใช้งาน และบุคคลภายนอก ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศได้รับทราบและถือปฏิบัติอย่างเคร่งครัด
6. นโยบายนี้จะต้องทำการเผยแพร่ให้พนักงานทุกระดับในบริษัทได้รับทราบ และพนักงานทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

3. ขอบเขต

นโยบายฉบับนี้ใช้กับบริษัท คิน คอร์ปอเรชั่น จำกัด และ (“ผู้ใช้งาน”) และ (“บุคคลภายนอก”) ที่ได้รับอนุญาตให้ใช้ระบบเครือข่ายคอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคม เพื่อเข้าถึงสารสนเทศของบริษัท

4. ความหมายและคำจำกัดความ

"บริษัท" หมายถึง บริษัท คิน คอร์ปอเรชั่น จำกัด

"ผู้ใช้งาน" หมายถึง กรรมการ / พนักงาน หรือผู้ที่ได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์หรือระบบเครือข่ายของบริษัท

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูล เป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเสียหาย

"ทรัพย์สินด้านสารสนเทศ" ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟท์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด

"ระบบสารสนเทศ" หมายถึง ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้ระบบ พนักงานที่เกี่ยวข้อง และข้อมูล ซึ่งทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์ที่ได้ให้ผู้ใช้เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวิเคราะห์และติดตามผลการดำเนินงานของบริษัท

"สารสนเทศ" หมายถึง ข้อมูลในรูปแบบต่าง ๆ เช่น ตัวอักษร รูปภาพ สัญลักษณ์หรือเสียง ที่ผ่านกระบวนการประมวลผลด้วยวิธีการต่าง ๆ เช่น การคำนวณ การเปรียบเทียบ การวิเคราะห์ การเรียงลำดับ และการสรุปผล เป็นต้น แล้วจึงมีการบันทึกไว้อย่างเป็นระบบ เพื่อสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ต่อไป

"บุคคลภายนอก" หมายถึง บุคคล / นิติบุคคล ซึ่งบริษัทหรือหน่วยงานในบริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศ โดยได้รับสิทธิ์ตามประเภทการใช้งาน และต้องรับผิดชอบการเปิดเผยความลับของบริษัทโดยไม่ได้รับอนุญาต

"ผู้รับการว่าจ้าง" หมายถึง บุคคล / บริษัท หรือหน่วยงานภายนอก ซึ่งได้รับการว่าจ้างจากบริษัทให้ทำงานให้ในช่วงระยะเวลาหนึ่ง หรือทำงานในฐานะเป็นผู้ใช้งานของบริษัท ซึ่งรวมถึงลูกจ้างชั่วคราว โดยทั่วไปการว่าจ้างจะมีการทำสัญญาจ้างเพื่อควบคุมให้ผู้รับจ้างปฏิบัติตามเงื่อนไข หรือข้อตกลงการจ้างงานนั้น

"ทรัพย์สินซอฟต์แวร์ (Software Asset)" หมายถึง โปรแกรมที่ใช้ในการใช้งานคอมพิวเตอร์และทำงานเฉพาะเจาะจง โดยอาจจะเป็นได้ทั้งซื้อสิทธิขาด เช่น SAP, OS, Office หรือเช่าใช้ เช่น M365, Cloud, Hosting, Domain

"ทรัพย์สินอุปกรณ์ (Hardware Asset)" หมายถึง เครื่องมือ เครื่องจักร ชิ้นส่วน และอุปกรณ์ต่าง ๆ ที่สามารถมองเห็นและจับต้องได้ ในระบบคอมพิวเตอร์นั้น เช่น PC / Notebook / Monitor / Printer เป็นต้น

"ทรัพย์สินบริการ (Service Asset)" หมายถึง งานบริการ MA ต่าง ๆ เช่น SAP, Printer / การตั้งค่าติดตั้งระบบ / รายการซ่อม / ที่ปรึกษา

"ทรัพย์สินข้อมูล (Data Inventory)" หมายถึง ชุดข้อมูลที่ถูกจัดเก็บ และนำมาใช้ผ่านระบบคอมพิวเตอร์ เช่น Database เป็นต้น

"การเข้ารหัส (Encryption)" หมายถึง การเปลี่ยนข้อความหรือเครื่องหมายธรรมดา ให้เป็นข้อความหรือเครื่องหมายลับด้วยวิธีใดวิธีหนึ่ง

5. หน้าที่ความรับผิดชอบ

1. **<u>หน้าที่ของประธานเจ้าหน้าที่บริหาร</u>**
    1. กำหนดกลยุทธ์ในภาพรวม นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
2. **<u>หน้าที่ของกรรมการผู้จัดการ</u>**
    2. กำหนดเป้าหมาย นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท
    3. ควบคุมการปฏิบัติงานในบริษัทให้สอดคล้องกับกลยุทธ์ในภาพรวม
3. **<u>หน้าที่ของรองกรรมการผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ</u>**
    1. ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท
    2. ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายใน อย่างมีประสิทธิภาพ
4. **<u>หน้าที่ของผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ</u>**
    1. จัดการพัฒนานโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ Policy, มาตรฐาน (Standard), ขั้นตอนการปฏิบัติ (Procedure) และแนวทางปฏิบัติ (Guideline) เพื่อให้บริษัทได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Data Integrity) และเสถียรภาพความมั่นคงของระบบ (System Stability)
    2. จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจ เพื่อกู้ระบบยามฉุกเฉิน
    3. มีการบริหารความเสี่ยง และการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหา กระทบกับ การดำเนินธุรกิจของบริษัท
    4. นำเสนอผู้บริหารระดับสูง
    5. เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ ๆ ทางด้านการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศอย่างสม่ำเสมอ
5. **<u>หน้าที่ของผู้จัดการฝ่าย</u>**
    1. ชี้แจงและส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และตักเตือนลงโทษทางวินัย กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม
    2. ร่วมร่างนโยบายและระเบียบการดำเนินการด้านนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
    3. ดูแลให้พนักงานปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
    4. ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศและระบบคอมพิวเตอร์ภายใต้หน้าที่ และความรับผิดชอบ
    5. แจ้ง “เจ้าหน้าที่เทคโนโลยีสารสนเทศ” เพื่อลบ / เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงาน / อำนาจหน้าที่ / โอนย้าย

6. **<u>หน้าที่ของผู้ใช้งาน</u>**
    1. ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทโดยเคร่งครัด
    2. ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัทให้มีความปลอดภัย
    3. รายงานต่อบริษัททันที เมื่อพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรม สารสนเทศ รวมถึง ระบบสารสนเทศที่อาจสร้างความเสียหายต่อบริษัท

6. การกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

ระเบียบปฏิบัติสำคัญที่เกี่ยวกับการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) จะแบ่งเป็น 14 หมวดดังนี้

หมวดที่ 1 ระเบียบปฏิบัติความมั่นคงปลอดภัยของบริษัท
หมวดที่ 2 ความมั่นคงปลอดภัยสารสนเทศ
หมวดที่ 3 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
หมวดที่ 4 การบริหารจัดการทรัพย์สิน
หมวดที่ 5 การควบคุมการเข้าถึง
หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)
หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินการ
หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล
หมวดที่ 10 การจัดหา พัฒนา และดูแลระบบสารสนเทศ
หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก
หมวดที่ 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
หมวดที่ 13 การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ
หมวดที่ 14 ความสอดคล้อง

หมวดที่ 1 ระเบียบปฏิบัติความมั่นคงปลอดภัยของบริษัท (Information Security Policy)

จุดประสงค์และขอบเขต :

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

ระเบียบปฏิบัติความปลอดภัยสารสนเทศ ครอบคลุมถึงการปกป้องข้อมูลของบริษัทเป็นหลัก ข้อมูลในระเบียบปฏิบัตินี้ หมายถึง ข้อมูลในรูปแบบอิเล็กทรอนิกส์ เอกสาร สิ่งพิมพ์ ฟิล์ม หรือแม้แต่ในรูปของการสนทนา อย่างไรก็ตามการปกป้องข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ จะกล่าวถึงเป็นส่วนใหญ่เนื่องจากข้อมูลของบริษัทนั้นจะอยู่ในรูปอิเล็กทรอนิกส์

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

การจัดทำระเบียบปฏิบัติความปลอดภัยสารสนเทศ (Information Security Policy)

- ต้องจัดทำระเบียบปฏิบัติระบบบริหารความมั่นคงปลอดภัยสารสนเทศไว้เป็นลายลักษณ์อักษรหรือในรูปแบบอิเล็กทรอนิกส์ เพื่อให้เกิดความเชื่อมั่น และมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยระเบียบปฏิบัติดังกล่าวจะต้องได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการ โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของบริษัท ตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สินสารสนเทศของบริษัท
- ต้องจัดให้มีการสื่อสาร/ประกาศใช้ระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้บุคลากรภายในบริษัท หน่วยงานภายนอก และผู้ที่เกี่ยวข้องรับทราบ โดยมีหน้าที่จะต้องสนับสนุน ดำเนินการตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและ การสื่อสารอย่างเคร่งครัด การฝ่าฝืนระเบียบปฏิบัตินี้ ถือเป็นความผิดที่ร้ายแรง โดยมีบทลงโทษถึงขั้นสูงสุดตามระเบียบของบริษัท

การทบทวนระเบียบปฏิบัติความปลอดภัยสารสนเทศ (Review of the Information Security Policy)

- ต้องดำเนินการตรวจสอบ ทบทวน และประเมินระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร อย่างน้อย 1 ครั้งต่อปี โดยสอดคล้องกับรอบการทบทวนนโยบายของบริษัท หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อบริษัท เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศของบริษัท เช่น การเปลี่ยนแปลงกลยุทธ์หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงที่สำคัญต่อบริษัท

หมวดที่ 2 ความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศภายในบริษัท (Internal Organization)

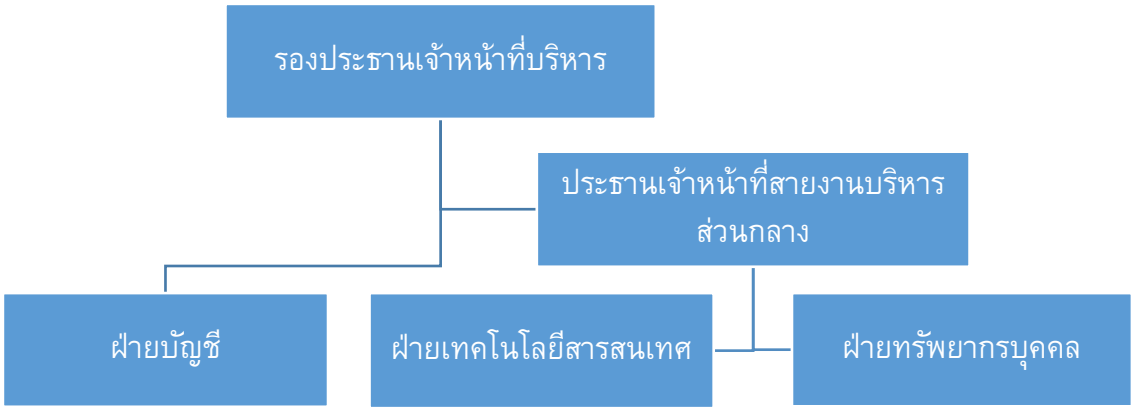
จุดประสงค์และขอบเขต :

เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสารสนเทศของบริษัท ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย บริษัทจึงได้จัดทำโครงสร้างความปลอดภัยสารสนเทศ รวมถึงการกำหนดบทบาท และหน้าที่ในการบริหารจัดการความปลอดภัยของสารสนเทศภายในบริษัท

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

- ตัวแทนฝ่ายบริหารระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMR: Information Security Management Representative) ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทไว้อย่างชัดเจน
- ผู้บริหารให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ โดยอนุมัติให้มีการจัดตั้งคณะทำงาน หรือกลุ่มผู้ทำงานหลักด้านความปลอดภัยสารสนเทศ ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารและจัดการความมั่นคงปลอดภัยสารสนเทศของบริษัท ดังนี้



โครงสร้างของคณะทำงานความปลอดภัยสารสนเทศ

- คณะทำงานความปลอดภัยสารสนเทศ ประกอบจากผู้บริหารของหน่วยงานต่าง ๆ ดังนี้
  - รองประธานเจ้าหน้าที่บริหาร
  - ประธานเจ้าหน้าที่สายงานบริหารส่วนกลาง
  - ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
  - ผู้จัดการฝ่ายบัญชี
  - ผู้จัดการฝ่ายทรัพยากรบุคคล
- คณะทำงานความปลอดภัยสารสนเทศมีหน้าที่ดังนี้
  - ตรวจสอบ และอนุมัติ ปรับปรุงระเบียบปฏิบัติความปลอดภัยสารสนเทศ ตามกำหนด หรือตามสถานการณ์
  - วางแผนประชาสัมพันธ์ และอบรมบุคลากรทุกหน่วยงานเข้าใจถึงความปลอดภัยสารสนเทศ
  - ตรวจสอบ และให้ความเห็นชอบโครงการที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ
  - วางแผน ตรวจสอบ และบริหารจัดการความเสี่ยงต่าง ๆ ที่เกิดจากข้อจำกัดของระบบ
  - ตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องด้านความมั่นคงปลอดภัย กรณีฉุกเฉิน

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

จุดประสงค์และขอบเขต :

เพื่อรักษาความมั่นคงปลอดภัยสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานจากภายนอก และการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

2.2.1 ระเบียบปฏิบัติสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

ต้องมีการกำหนดและปฏิบัติตามระเบียบปฏิบัติ หรือมาตรการสนับสนุน สำหรับการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook, Tablet, Smartphone และอุปกรณ์สื่อสารเคลื่อนที่อื่นๆ) ที่มีการนำมาใช้งาน โดยให้พนักงาน/ผู้ขอใช้ แจ้งขอใช้งาน อุปกรณ์คอมพิวเตอร์แบบพกพา และมีหัวหน้าหน่วยงานที่เกี่ยวข้องรับทราบและอนุมัติเป็นหลักฐานจึงส่งให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาอนุมัติ และให้เจ้าหน้าที่ IT ดำเนินการ เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว และควรคำนึงถึงความเสี่ยงของการทำงานในสภาพแวดล้อมที่ไม่ได้รับการป้องกัน

โดยให้ปฏิบัติตามแนวปฏิบัติเพื่อการใช้อุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคล อย่างเคร่งครัดดังนี้

- ต้องเป็นอุปกรณ์ที่ปลอดภัย ไม่มีความเสี่ยงในการติด Virus / Malware / Ransomware
- ให้ใช้งานกับเครื่องคอมพิวเตอร์ที่มีความเชื่อถือได้ (ไม่ใช้งานกับคอมพิวเตอร์สาธารณะ) และเครื่องคอมพิวเตอร์นั้นต้องมีโปรแกรมป้องกันไวรัสและอัพเดตให้ทันสมัย
- ต้องมีระบบป้องกันข้อมูล เช่น ใช้รหัสผ่านก่อนใช้งานและมีการเข้ารหัสข้อมูลไว้ด้วย

- ห้ามนำอุปกรณ์ที่ไม่รู้จักแหล่งที่มา มาใช้งานกับเครื่องหรือระบบงานของบริษัท
- ผู้ครอบครองหรือผู้ใช้งานต้องรับผิดชอบหากข้อมูลสำคัญของบริษัทสูญหาย หรือติด Virus / Malware / Ransomware โดยสามารถพิสูจน์ได้ว่าต้นเหตุมาจากอุปกรณ์ที่นำมาใช้งาน
- ห้ามมีไฟล์ภาพหรือสื่อหรือข้อมูลต่างๆ ที่ผิดกฎหมาย เช่น ไฟล์ภาพลามก ไฟล์เกมส์พนัน อยู่ในอุปกรณ์คอมพิวเตอร์แบบพกพา
- ห้ามมีโปรแกรมละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา หรือมีการดัดแปลงระบบในอุปกรณ์แบบพกพา

2.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)

อนุญาตให้เจ้าหน้าที่ IT ดำเนินการติดตั้งโปรแกรมสำหรับการปฏิบัติงานจากระยะไกล โดยให้ปฏิบัติตามนโยบายเรื่องการ ปฏิบัติงานจากระยะไกล (Teleworking) อย่างเคร่งครัด ดังนี้

- เจ้าหน้าที่ IT จะดำเนินการติดตั้ง/ตั้งค่า Program Remote ให้ผู้ใช้งานระบบตามรายการ Software List เท่านั้น
- เจ้าหน้าที่ IT ต้องทำการแจ้งผู้ใช้งานและได้รับการอนุญาตจากผู้ใช้งานก่อนทำการเข้าถึงระบบผ่านการปฏิบัติงานจากระยะไกล
- ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม (Port List)
- การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อ ไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ เมื่อมีการร้องขอที่จำเป็นเท่านั้น

2.2.3 การใช้งานเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

อนุญาตให้บุคลากรของบริษัทและบุคคลภายนอกซึ่งเป็นคู่ค้า ที่จำเป็นต้องปฏิบัติงานจากภายนอก โดยให้พนักงาน/ผู้ขอใช้ แจ้งขอใช้งาน VPN และมีหัวหน้าหน่วยงานที่เกี่ยวข้องรับทราบและอนุมัติเป็นหลักฐานจึงส่งให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาอนุมัติ และให้เจ้าหน้าที่ IT ดำเนินการติดตั้งระบบและแจ้งผลการดำเนินการให้พนักงาน/ผู้ขอใช้ ให้รับทราบ

โดยให้ปฏิบัติตามนโยบายเรื่องการใช้งานเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) อย่างเคร่งครัด ดังนี้

- รายชื่อผู้ใช้งานระบบ VPN จะต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติไว้อย่างชัดเจน และฝ่ายเทคโนโลยีสารสนเทศจะยกเลิกสิทธิ์ในการใช้งานระบบทันทีในวันที่พนักงานพ้นสภาพ หรือตามระยะเวลาที่กำหนดตอนร้องขอ
- เจ้าหน้าที่ IT จะดำเนินการติดตั้ง/ตั้งค่า VPN ให้ผู้ใช้งานระบบ เฉพาะผู้ที่ได้รับการอนุมัติเท่านั้น
- การเข้าถึงระยะไกลที่ปลอดภัยต้องได้รับการควบคุมอย่างเข้มงวดด้วยการเข้ารหัส และรหัสผ่านที่ชัดเจน ซึ่งรหัสผ่านจะเป็นของแต่ละคนที่ใช้งาน โดยแบ่งแยกแต่ละผู้ใช้งานอย่างชัดเจน
- ผู้ใช้งานระบบที่ได้รับอนุญาตปกป้องการเข้าสู่ระบบและรหัสผ่านโดยไม่เปิดเผยรหัสผ่านกับผู้อื่นเด็ดขาด
- ในขณะที่ใช้คอมพิวเตอร์ของบริษัทเพื่อเชื่อมต่อกับเครือข่ายบริษัทของบริษัทจากระยะไกล และหลังจากใช้งานเสร็จสิ้นแล้วให้ยกเลิกการเชื่อมต่อ VPN ทุกครั้ง

- โฮสต์ทั้งหมดที่เชื่อมต่อกับเครือข่ายภายในของบริษัทผ่านเทคโนโลยีการเข้าถึงระยะไกลจะต้องมีซอฟต์แวร์ป้องกันไวรัสติดตั้งอยู่ในเครื่องนั้น ๆ ด้วย

หมวดที่ 3 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

3.1 ระเบียบปฏิบัติก่อนการจ้างงาน (Prior to Employment Policy)

จุดประสงค์และขอบเขต :

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเอง และมีความเหมาะสม ตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงานบริษัท

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

การคัดเลือกบุคลากร (Screening)

- เจ้าหน้าที่บุคคล ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นพนักงานประจำ พนักงานชั่วคราว หรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน
- เจ้าหน้าที่บุคคล ต้องจัดให้พนักงานมีการลงนาม การไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement : NDA) โดยมีการระบุข้อความการไม่เปิดเผยความลับของบริษัท ไว้ในเอกสารสัญญาจ้างงาน การลงนามในสัญญาจ้างงานให้ถือเป็นการลงนามการไม่เปิดเผยความลับของบริษัทด้วย
- ข้อตกลง และเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) ฝ่ายบุคคลและธุรการต้องกำหนดเงื่อนไขการจ้างงานในสัญญาจ้างกับพนักงาน รวมถึงมีการระบุหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ (Job Description) ที่ชัดเจน โดยเจ้าหน้าที่ทรัพยากรบุคคล ต้องแจ้งให้เจ้าหน้าที่ IT และหน่วยที่เกี่ยวข้องทราบทันทีเมื่อมีเหตุ ดังนี้
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงานและลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

3.2 ระเบียบปฏิบัติระหว่างการจ้างงาน (During Employment Policy)

จุดประสงค์และขอบเขต :

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนัก และปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท และเพื่อลดความเสี่ยงของสารสนเทศที่เกิดจากบุคลากร ทั้งที่เกิดจากการละเมิดความปลอดภัยสารสนเทศโดยเจตนาและไม่ได้เจตนา หรือจากการละเลยต่อการปฏิบัติหน้าที่ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

ฝ่ายบุคคลและธุรการ ต้องจัดให้พนักงานหรือตัวแทนจากแต่ละฝ่าย/แผนก เข้ารับฟังการอบรม อย่างน้อยปีละ 1 ครั้ง และให้มีการสื่อสารกับบุคลากรภายในแผนกภายหลังได้รับการอบรมแล้ว เพื่อเป็นการสร้างความตระหนัก และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ ดังนี้

- พนักงานของบริษัททุกคนต้องได้รับการอบรมให้ความรู้ โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล
- ต้องจัดอบรมให้ความรู้แก่พนักงานภายในบริษัท เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับระเบียบปฏิบัติความมั่นคงปลอดภัย การเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศ และการสื่อสารของบริษัทด้วย
- พนักงานที่เข้าใหม่ทุกคนจะต้องรับทราบเกี่ยวกับระเบียบปฏิบัติรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ภายใน 30 วันนับจากเข้าทำงานในหน่วยงาน เพื่อให้พนักงานหรือผู้ที่เกี่ยวข้องได้ศึกษา และถือปฏิบัติโดยอาจเป็นส่วนหนึ่งของการปฐมนิเทศ และ ต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย
- เจ้าหน้าที่ทรัพยากรบุคคล และเจ้าหน้าที่ IT มีหน้าที่ในการแจ้งให้ทราบ เกี่ยวกับระเบียบปฏิบัติความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทให้แก่บุคลากรด้วย

กระบวนการทางวินัย (Disciplinary Process)

ผู้บริหาร ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนระเบียบปฏิบัติ กฎ และ/หรือ ระเบียบปฏิบัติของบริษัท โดยพนักงานทุกคนต้องลงลายมือชื่อรับทราบในแบบฟอร์มการรับทราบเงื่อนไขการใช้งานระบบสารสนเทศ ซึ่งกระบวนการทางวินัยที่กำหนดขึ้นนี้เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศของบริษัท โดยการฝ่าฝืนหรือละเลยต่อหน้าที่และระเบียบปฏิบัติถือว่ามีความผิด ต้องพิจารณาตามบทลงโทษของบริษัท ซึ่งขึ้นอยู่กับความรุนแรงของผลกระทบที่เกิดขึ้นกับบริษัท

3.3 ระเบียบปฏิบัติหลังการสิ้นสุด หรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment Policy)

จุดประสงค์และขอบเขต :

เป็นการควบคุมความปลอดภัยของสารสนเทศให้ดียิ่งขึ้น และเพื่อป้องกันผลประโยชน์ของบริษัทซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

ฝ่ายบุคคลและธุรการและหน่วยงานต่าง ๆ ร่วมกันกำหนดขั้นตอนการปฏิบัติ ของพนักงานที่ออกจากบริษัท เมื่อสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อมีการเปลี่ยนการจ้างงาน ดังนี้

- หน่วยงานต้นสังกัดของพนักงานที่ลาออก มีหน้าที่แจ้งไปยังฝ่ายบุคคลและธุรการถึงเรื่องการลาออก หรือการปรับเปลี่ยนตำแหน่งของพนักงาน
- หน่วยงานต้นสังกัดของพนักงานที่ลาออก มีหน้าที่แจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานของบริษัทเพื่อทำการถอดถอนสิทธิการเข้าใช้ระบบงานต่าง ๆ และการเข้า-ออกพื้นที่ของบริษัท เพื่อดำเนินการเพิกถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ์
- ฝ่ายเทคโนโลยีสารสนเทศ ทำการสำรองข้อมูลที่จำเป็นของพนักงาน และแจ้งให้หน่วยงานที่เกี่ยวข้องทราบถึงวิธีเข้าถึงข้อมูลดังกล่าว

หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset Management)

4.1 ระเบียบปฏิบัติ และหน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets Policy)

จุดประสงค์และขอบเขต :

ทรัพย์สิน หมายถึง ทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ข้อมูล ซอฟต์แวร์ หรืออุปกรณ์ที่เกี่ยวข้องในการประมวลผล นอกจากนี้บริษัทควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน แต่อย่างไรก็ตามเจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว เพื่อให้มีการระบุทรัพย์สินของบริษัท และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

4.1.1 การจัดการบัญชีทรัพย์สิน (Inventory of Assets)

- ต้องจัดทำและเก็บทะเบียนทรัพย์สิน ซึ่งรวมถึงทรัพย์สินซอฟต์แวร์ (Software Asset) ทรัพย์สินอุปกรณ์ (Hardware Asset) ทรัพย์สินบริการ (Service Asset) ทรัพย์สินข้อมูล (Data Inventory) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อทรัพย์สินอย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการทรัพย์สินของบริษัท โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการควบคุมทรัพย์สินถาวร ของฝ่ายบัญชี รวมถึงกำหนดให้เจ้าหน้าที่ IT จัดทำทะเบียนคุมทรัพย์สินด้าน IT ไว้ด้วย
- ต้องมีการตรวจสอบทรัพย์สิน (Inventory Check) ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สินทุกประเภทตามระยะเวลาที่กำหนดไว้ ตรวจนับร่วมกับฝ่ายบัญชี ปีละ 1 ครั้ง และสุ่มตรวจนับโดยเจ้าหน้าที่เทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง

4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of Assets)

ผู้ใช้งาน มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น เจ้าของทรัพย์สิน ต้องสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สินตลอดจนการแจ้งถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับทรัพย์สินให้เจ้าหน้าที่ IT ทราบ

4.1.3 การอนุญาตให้ใช้ทรัพย์สิน (Acceptable Use for Assets)

- ต้องมีการกำหนดกฎเกณฑ์สำหรับการใช้งานสารสนเทศอย่างเหมาะสม และกฎการอนุญาตให้ใช้ข้อมูลและทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ โดยแสดงบันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูล ตามระเบียบบริษัทเรื่องการแจ้งจัดเตรียมอุปกรณ์คอมพิวเตอร์และระบบงานสำหรับพนักงานใหม่ และเรื่องการขอยืมใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ IT ชั่วคราว
- การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์ มีดังนี้
  - ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่บริษัทฯ เป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของบริษัทฯ การใช้งานระบบและอุปกรณ์

ต่างๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวน หรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่

- เจ้าหน้าที่ ตลอดจนหน่วยงานภายนอกที่ได้รับการว่าจ้างโดยบริษัทฯ จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัยและคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของบริษัทฯ
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ของบริษัท อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นทรัพย์สินของตน
- เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของบริษัทฯ ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้ง เมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของบริษัทฯ รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใดๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทฯ ก่อนได้รับอนุญาตจากผู้บริหาร/ผู้มีอำนาจ
- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัทฯ อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนำที่ระบุไว้ตามหัวข้อ 2.2.1 ระเบียบปฏิบัติสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)
- อุปกรณ์คอมพิวเตอร์ของบริษัทต้องไม่ถูกดัดแปลงหรือติดตั้งอุปกรณ์เพิ่มเติมใดๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้นๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์ หรือซอฟต์แวร์ใดๆ บนเครื่องคอมพิวเตอร์ของบริษัท อย่างเด็ดขาด

- การอนุญาตให้ใช้งานทรัพย์สินด้านซอฟต์แวร์มีดังนี้
  - ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท
  - ซอฟต์แวร์ที่นำมาใช้ ในการประมวลผล และจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อมาต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสม โดยเป็นไปตามกรอบอำนาจอนุมัติก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัทฯ

- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของบริษัทฯ มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้
- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศพื้นฐาน ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทฯ เท่านั้น

- การอนุญาตให้ใช้งานอินเทอร์เน็ต มีดังนี้
  - บริษัทฯ จัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอกเพื่อเพิ่มประสิทธิภาพในการทำงาน และการให้บริการของบริษัทฯ
  - ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทฯ และบุคคลผู้ที่เกี่ยวข้องกับบริษัทฯ เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
  - การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้บริษัทฯ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งาน ในลักษณะที่ไม่เหมาะสม
  - หลีกเลี่ยงการคลิ๊กหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต แต่หากดำเนินการโดยมิได้เจตนาให้แจ้งฝ่ายเทคโนโลยีสารสนเทศให้ทราบโดยทันที
  - ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
  - ห้ามใช้ทรัพย์สินของบริษัทแสดงความคิดเห็นส่วนตัวของพนักงาน ในรูปแบบอิเล็กทรอนิกส์ทุกรูปแบบโดยความเสียหายใด ๆ จากการแสดงความคิดเห็นดังกล่าวถือเป็นความรับผิดชอบของพนักงานผู้นั้น
- การอนุญาตให้ใช้งานอีเมล มีดังนี้
  - ผู้ใช้งานอีเมลทั้งหมดของบริษัท ควรมี E-mail Account เป็นของตนเอง

- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล ไปใช้ในทางที่ผิด
- E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น hr@kincorp.co.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของส่วนงาน
- E-mail Account ทั้งหมดและอีเมลทุกฉบับ (รวมถึงอีเมลส่วนตัว) ที่ถูกสร้างและเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นทรัพย์สินของบริษัทฯ
- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมลของบริษัทฯ
- ขนาดของอีเมลและไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมลและไฟล์แนบมีขนาดใหญ่ เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมลดังกล่าวได้
- ผู้ใช้งานต้องลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล ให้เป็นไปตามขนาดที่บริษัท กำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมลที่เกี่ยวข้องกับการทำงาน และอีเมลตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-mail Account ของบริษัทฯ เพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
- ห้ามใช้ E-mail Account ของบริษัทฯ ในการประกาศข้อมูลใดๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือ เป็นส่วนหนึ่งของการทำงานให้กับบริษัทฯ
- ซอฟต์แวร์สำหรับใช้งานอีเมลควรได้รับการตั้งค่าให้อีเมลส่งออกทุกฉบับ มีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงานบริษัท และเบอร์โทรศัพท์ติดต่อ
- ห้ามผู้ใช้งานทำสำเนาข้อความ หรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมลของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมลด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมลนั้นในนามตัวแทนของบริษัทฯ
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล หัวจดหมายอีเมล ลายเซ็นในอีเมล หรือ E-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ E-mail Account ของตน เว้นแต่เกิดจากกรณีจำเป็นและต้องให้ความยินยอมอย่างเป็นลายลักษณ์อักษร

- ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมลขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail) เป็นต้น
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใดๆ กับการส่งอีเมลหลอกลวง หรือการส่งอีเมลในลักษณะลูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้ายทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนา และอีเมลที่กระทบต่อความมั่นคงของชาติหรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมลที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงาน และส่งผลเสียต่อบริษัทฯ
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษ เมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมลบอมบ์ หรือโปรแกรมแฝง
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่าเครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมลโดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

- การอนุญาตให้ใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้
  - ผู้ใช้งานต้องปกป้องความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่เมื่อจำเป็นต้องส่งข้อมูลนั้นผ่านเครื่องโทรสาร
  - ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิด หมายเลขผิด ส่วนงาน เป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น
  - ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคล ที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น
  - ห้ามผู้ใช้งานบันทึกหรือฝากข้อความที่มีข้อมูลลับในเครื่องตอบรับโทรศัพท์อัตโนมัติ หรือระบบวอยซ์เมล์โดยเด็ดขาด
  - ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือ ผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่น Voice Over IP หรือในระหว่างการประชุมทางไกล เว้นแต่ ผู้เข้าร่วมการประชุมทุกหน่วยงานได้รับการพิสูจน์ตัวตนแล้วว่า เป็นผู้ที่เกี่ยวข้องและมีสิทธิ์รับทราบข้อมูล
  - ผู้ที่เกี่ยวข้องต้องตรวจสอบอย่างรอบคอบและระมัดระวัง เพื่อให้มั่นใจว่าไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลที่สนทนาอยู่

- การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสมสามารถป้องกันเสียงลอดออกมาได้ เป็นต้น
- ผู้ใช้งานต้องระมัดระวังการใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสารเพื่อป้องกันข้อมูลลับถูกเปิดเผย แก่บุคคลที่ไม่ได้รับอนุญาต
- ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใดๆ ทางโทรศัพท์ ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้น เป็นผู้ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าวก่อนที่จะเปิดเผยข้อมูล
- ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสาร ที่มีข้อมูลลับ โดยสำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับ

4.1.4 การคืนทรัพย์สิน (Return of Assets)

พนักงาน และลูกจ้างของหน่วยงานภายนอก ทั้งหมดต้องคืนทรัพย์สินของบริษัททั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง ในวันสุดท้ายของการทำงาน โดยทรัพย์สินที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจะต้องมีการตรวจสภาพทรัพย์สินจากฝ่ายเทคโนโลยีสารสนเทศเสียก่อน หากผลการตรวจสอบพบว่ามีความชำรุดเสียหาย หรือมีข้อมูลบางอย่างขาดหายไป ผู้รับผิดชอบจะต้องได้รับผิดชอบตามข้อกำหนดที่ได้ตกลงไว้ โดยปฏิบัติตามระเบียบบริษัท เรื่องการลาออก ของฝ่ายทรัพยากรบุคคล

4.2 ระเบียบปฏิบัติการจัดขั้นความลับของสารสนเทศ (Information Classification Policy)

ระเบียบปฏิบัติของบริษัทได้กำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้น และได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้ระเบียบปฏิบัติยังได้กำหนดถึงบทบาทของเจ้าของข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้องกับการจัดลำดับชั้นของข้อมูล เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อบริษัท

4.3 ระเบียบปฏิบัติการจัดการสื่อบันทึกข้อมูล (Media Handling Policy)

จุดประสงค์และขอบเขต :

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัทฯ โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทำขั้นตอนสำหรับการบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูล ต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาตการนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างนี้ที่นำส่ง หรือขนย้ายสื่อบันทึกข้อมูลนั้นต้องกำหนดวิธีปฏิบัติ และสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูล

อนึ่งบริษัทฯ ไม่มีนโยบายให้ผู้ใช้งานระบบ ใช้งานสื่อบันทึกข้อมูลสื่อบันทึกข้อมูล

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)

5.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

จุดประสงค์และขอบเขต :

เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย และเพื่อลดความเสี่ยงด้าน การเข้าใช้งานอย่างไม่เหมาะสม จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็น และความต้องการทางธุรกิจ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

5.1.1 การควบคุมการเข้าถึง (Access Control)

- มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดย ผู้ใช้งานต้องเขียนแบบฟอร์มขอเพิ่ม/เปลี่ยนแปลงบัญชีผู้ใช้งาน ส่งให้ผู้จัดการต้นสังกัด อนุมัติการขอเข้าใช้งาน จากนั้นส่งมาที่เจ้าหน้าที่ IT ดำเนินการสร้างบัญชีผู้ใช้งาน และกำหนดสิทธิการใช้งานระบบ เสร็จแล้วส่งผู้จัดการเจ้าหน้าที่ IT สอบทานและอนุมัติ
- การไม่แสดงค่าปกติ (Default) ให้ไม่แสดงรหัสผ่านบนหน้าจอ
- ผู้ใช้งานจะได้รหัสผ่านแบบสุ่มในครั้งแรกของการเข้าระบบและจะถูกบังคับให้ดำเนินการเปลี่ยน รหัสผ่านทันทีเพื่อใช้งานต่อไป
- ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน ก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมี การทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
- เปิดใช้งาน Multi Factor Authentication (MFA) หากระบบรองรับ
- ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้
- ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ
  - ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น
  - ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ
  - การเข้าถึงข้อมูลและระบบสารสนเทศของบริษัท จะกระทำได้ก็ต่อเมื่อ ได้รับการอนุมัติ โดยผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานใน

หน้าที่ของบุคคลนั้น ๆ เท่านั้น ความปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดระเบียบปฏิบัติ และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึง การให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูล หรือ ระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูล และการกู้ข้อมูลที่เสียหายกลับคืนมา

5.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services) ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึง เท่านั้น

- ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคง ปลอดภัยให้แก่ข้อมูล และระบบเทคโนโลยีสารสนเทศ อาทิ
- ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย อาทิ Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP)
- จำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ-ส่งไฟล์ขนาดใหญ่ ฟังเพลง ออนไลน์ ดูทีวีออนไลน์ หรือ เล่นเกมส์ออนไลน์ ในช่วงเวลาทำการ ยกเว้นกรณีที่ได้รับอนุญาต จากผู้บริหาร/ผู้มีอำนาจ
- ผู้ใช้งานจะต้องสามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัย ให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดต้องได้รับการตั้งค่าให้มีความปลอดภัย และการมีการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย
- ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรม และได้รับการติดตั้งโดยผู้ที่มีความชำนาญ ที่ผ่านการพิจารณาอนุมัติแล้ว
- อุปกรณ์เครือข่าย และ เซิฟเวอร์ รวมถึงซอฟต์แวร์ ต้องทำการสำรองข้อมูลค่า Configuration ก่อนและหลังดำเนินการใด ๆ กับตัวอุปกรณ์และระบบ รวมถึงมีการสำรองค่า Configuration ไว้อย่างน้อย 3 เวอร์ชั่นทั้งก่อนและหลังดำเนินการ
- อุปกรณ์เครือข่าย อาทิ Router, Firewall, Switch, Wireless Access Point ต้องได้รับการตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้น ๆ หรือตามคำแนะนำของสำนักงาน ด้านความมั่นคงปลอดภัยต่าง ๆ อาทิ NCSA หรือ ETDA
- IP Address ต้องได้รับการลงทะเบียน แจกจ่าย และบริหารจัดการโดยเจ้าหน้าที่ IT

- อุปกรณ์เครือข่ายที่สำคัญ เช่น Router, Core Switch ต้องมีอุปกรณ์สำรองไฟฟ้า (UPS) เสมอ
- ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)
- ข้อตกลงการให้บริการเครือข่ายต้องระบุถึงรายละเอียด และข้อกำหนดเกี่ยวกับการรักษาความ มั่นคงปลอดภัย ระดับการให้บริการ และการบริหารจัดการบริการเครือข่ายทั้งหมด หากบริการเครือข่ายนั้นได้รับการดำเนินการโดยหน่วยงานภายนอก ต้องมีการระบุถึงสิทธิของบริษัทฯ ในการติดตามตรวจสอบ และตรวจประเมินการทำงานของหน่วยงานภายนอกด้วย

5.2 ระเบียบปฏิบัติการควบคุมการเข้าถึงระบบ (System and Application Access Control Policy)

จุดประสงค์และขอบเขต :

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิเข้าใช้งานในระดับระบบปฏิบัติการ (Operating System) ฝ่ายเทคโนโลยีสารสนเทศ การตรวจสอบผู้ใช้และการบริหารรหัสผ่านสำหรับผู้ใช้งาน รวมถึงการควบคุมเวลาในการเชื่อมต่อสู่ระบบ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

5.2.1 การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึง ทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท

5.2.2 การบริหารจัดการสิทธิ์ตามระบบสิทธิ์การเข้าถึง (Management of Privileged Access Right)

- ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย
- ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ

5.2.3 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

- ต้องมีกระบวนการจัดการการส่งมอบข้อมูล เพื่อพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นความลับ และการเก็บรักษาข้อมูลความลับของตัวเอง การส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ

5.2.4 การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

- ทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง
- ขั้นตอนการทบทวนสิทธิ

1) เจ้าหน้าที่ IT ดึงข้อมูลตารางการตั้งค่าสิทธิการเข้าถึงระบบ (Permission Matrix) จากระบบงานหลักของบริษัท เสร็จแล้วแยกส่งอีเมลให้กับผู้จัดการของทุกฝ่ายเพื่อพิจารณาทบทวนสิทธิ
2) ผู้จัดการฝ่ายของผู้ใช้งานระบบ พิจารณาทบทวนสิทธิการเข้าถึง/เข้าใช้งานระบบ ของพนักงานภายในสังกัดตนเอง ว่ายังคงมีความเหมาะสมเพียงใด จากนั้นส่งอีเมลแจ้งเจ้าหน้าที่ IT
3) เจ้าหน้าที่ IT ติดตามและรวบรวมข้อมูลผลการทบทวนสิทธิของแต่ละฝ่ายงาน จากนั้นส่งอีเมลสรุปผลการทบทวน ให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และผู้บริหารรับทราบ

5.2.5 การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights)

- สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องได้รับการถอดถอน เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ
- ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

5.3 ระเบียบปฏิบัติบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

จุดประสงค์และขอบเขต :

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์ตัวตน

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

ใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

- การใช้งานและเก็บรักษาข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน ต้องดำเนินการตามระเบียบปฏิบัติหรือวิธีปฏิบัติของบริษัท สำหรับการใช้งานข้อมูลพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ เช่น
  - เก็บรักษา Username และ Password ต้องเป็นความลับห้ามเปิดเผยให้บุคคลอื่นทราบ
  - หลีกเลี่ยงการเก็บบันทึกข้อมูลการตรวจสอบความลับ เว้นแต่สามารถเก็บไว้อย่างปลอดภัยได้และเมื่อได้รับข้อมูล Password ซึ่งเป็นข้อมูล Default ควรมีการแก้ไขทันทีเมื่อเข้าใช้งานระบบครั้งแรก

5.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

จุดประสงค์และขอบเขต :

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อมุ่งเน้นให้ผู้ใช้งานระบบมีความตระหนักถึง ความปลอดภัยในการใช้งานระบบข้อมูล โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่าน และต้องทราบถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานคอมพิวเตอร์

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

5.4.1 ระเบียบปฏิบัติหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy)

- ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศ ที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน
- บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และมีการกำหนดระยะเวลา ในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น
- บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร (IT Security Policy) ของบริษัทฯ อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของสำบริษัทฯ

5.4.2 ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure)

- ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง

5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)

ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติของบริษัทสำหรับการใช้งานข้อมูล การพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังต่อไปนี้

- ผู้ใช้ต้องกำหนดและใช้รหัสผ่านที่มีประกอบด้วย ตัวเลข สัญลักษณ์ และตัวอักษร รวมกัน อย่างน้อย 8 ตัวอักษร กรณีโปรแกรมหรือระบบใด มีข้อจำกัดในการตั้งค่า ให้แจ้งไว้ในคู่มือการบริหารงานด้านสารสนเทศด้วย
- ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ ทุก ๆ 90 วัน ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตาม และผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำกับของเดิมอย่างน้อย 5 ครั้งที่ผ่านมา
- จำนวนครั้งที่ระบบยอมให้ผู้ใช้งานใส่รหัสผ่านผิดสูงสุด คือ 3 ครั้งหากใส่รหัสผ่านผิดระบบ จะล๊อคการใช้งานชั่วคราว ระยะเวลา 30 นาที และระบบจะทำการยกเลิกการล๊อคใช้งาน ชั่วคราว หลังจาก 30 นาที

5.4.4 การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

- โปรแกรมที่ใช้งานต้องอยู่ภายใต้การควบคุมพื้นฐานจากรายการ Software List หรือหากมีโปรแกรมใช้งานเพิ่มเติมต้องให้พนักงาน/ผู้ขอใช้ แจ้งขอใช้งาน โปรแกรม และมีหัวหน้าหน่วยงานที่เกี่ยวข้องรับทราบและอนุมัติเป็นหลักฐานจึงส่งให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาอนุมัติ และให้เจ้าหน้าที่ IT ดำเนินการ
- การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

- ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่
  - ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
  - ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
  - จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
  - ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

5.4.5 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)

- ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง หรือให้บริการ เช่น
  - ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
  - ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

จุดประสงค์และขอบเขต :

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องการความลับ การปลอมแปลง หรือ ความถูกต้องของสารสนเทศ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

การใช้มาตรการเข้ารหัสข้อมูล (Use of Cryptographic Controls)

- บริษัทฯ ต้องมีระเบียบปฏิบัติการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง
- กำหนดให้มีการเข้ารหัสสำหรับข้อมูลสำคัญหรือข้อมูลลับแต่ละประเภท โดยข้อมูลที่มีระดับชั้นความลับต้องมีการเข้ารหัสในการ จัดเก็บ และต้องส่งผ่านช่องทางที่มีการเข้ารหัส เช่น SSL เป็นต้น
- การรับส่ง Email ได้ทำการเปิดใช้งานการเข้ารหัส (Encryption) โดยทำการเข้ารหัสในระดับของ Data File ที่แนบมากับอีเมล
- ปฏิบัติตามเอกสารชั้นความลับของบริษัท

หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

7.1 ระเบียบปฏิบัติเกี่ยวกับบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

จุดประสงค์และขอบเขต :

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพ ที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สิน ของบริษัทฯ และเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

7.1.1 การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

- หน่วยงานได้กำหนดพื้นที่ตั้ง ห้อง Server ที่มีสภาพแวดล้อมภายนอกปลอดภัยจากภัยคุกคามภายนอก คือ อยู่ในสถานที่ ๆ เข้าถึงได้โดยยากจากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้
- หน่วยงานได้จำแนก กำหนด และแบ่งบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspaces)” รวมทั้งจัดทำแผนผังแสดงตำแหน่ง และชนิดของพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ และแจ้งให้ทราบ

7.1.2 การควบคุมการเข้าออก (Physical Entry Controls)

บริษัทฯ จัดให้มีการควบคุมการเข้าออกในบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะ “เจ้าหน้าที่ฝ่าย IT” ที่มีสิทธิ์เท่านั้น และหรือผู้ที่ได้รับสิทธิ์จากผู้บริหาร/ผู้มีอำนาจ และมีแนวทางปฏิบัติ ดังนี้

- ต้องกำหนด “เจ้าหน้าที่ฝ่าย IT” และหรือผู้ที่ได้รับสิทธิ์จากผู้บริหาร/ผู้มีอำนาจ ที่มีสิทธิ์ผ่าน เข้าออก ช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน
- หากมีบุคคลอื่นใดที่ไม่ใช่ “เจ้าหน้าที่ฝ่าย IT” ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคล และการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และ ไม่อนุญาตให้เข้าพื้นที่) และต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Data Center) ของบุคคลภายนอกทุกครั้ง จัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี
- เจ้าหน้าที่ของบริษัทฯ ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคล ที่ไม่ได้รับอนุญาต

7.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing Offices, Room and Facilities)

- จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับบริษัทฯ ห้องทำงานและ เครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์ หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า ออกของบุคคลเป็นจำนวนมาก สำนักงานหรือห้องจะต้องไม่มีป้าย หรือ สัญลักษณ์ ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตู หน้าต่างของสำนักงาน หรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่ ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น
- ผู้ใช้งานพื้นที่เทคโนโลยีสารสนเทศหรือห้อง server ต้องทำการปิดประตูทันทีหลังจากเปิดประตู และต้องระวังไม่ให้มีการเปิดประตูทิ้งไว้ในขณะใช้งาน
- มีการติดตั้งกล้องวงจรปิด และบันทึกภาพตลอดเวลา โดยสามารดูย้อนหลังได้อย่างน้อย 30 วัน
- ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงานในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด
- ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะ โดยไม่ได้รับการทำลายอย่างเหมาะสม วิธีการทำลายข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์เหล่านี้
- เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

7.1.4 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environmental Threats)

- หน่วยงานต้องมีการป้องกันจากการทำลายของธรรมชาติ หรือคนที่อาจจะเกิดขึ้น ซึ่งเป็นภัยคุกคามจากภายนอก ต้องมีการเตรียมการป้องกันเหตุที่อาจเกิดขึ้น
- ศูนย์คอมพิวเตอร์ ต้องมีระบบป้องกันอัคคีภัย ระบบปรับอากาศและความชื้น ระบบกระแสไฟฟ้า
- เครื่องปรับอากาศ มี 2 ชุดทำงานสลับกัน โดยตั้งความเย็นอยู่ที่ 20-22 องศา และมีความชื้นอยู่ที่ 45-50%

7.1.5 การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

- หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน
- หัวหน้าของแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น

7.2 ระเบียบปฏิบัติเกี่ยวกับการจัดการอุปกรณ์ (Equipment Management Policy)

จุดประสงค์และขอบเขต :

เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์ คอมพิวเตอร์ ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

7.2.1 การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

จัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัย รวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับ อุปกรณ์เหล่านั้น

7.2.2 การติดตามการทำงานของเครื่องแม่ข่าย (Server Monitor)

มีการจัดทำรายงานสถานการณ์ทำงานของเครื่องแม่ข่ายต่าง ๆ รวมถึงอุปกรณ์รอบข้างที่จำเป็น เป็นประจำทุกวัน โดยผู้ปฏิบัติจะทำการบันทึกสถานการณ์การทำงานต่าง ๆ ทางกายภาพ และมีการจัดทำรายงานสรุปสถานการณ์ทำงานภายในห้อง Server ให้กับทางผู้บริหารให้ทราบเป็นประจำทุกเดือน

7.2.3 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้อง5ได้รับการป้องกันการล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุ มาจากการล้มเหลวของระบบ และอุปกรณ์สนับสนุนการทำงานต่าง ๆ

- กำหนดให้มีระบบกระแสไฟฟ้าสำรอง เช่น ใช้ Uninterruptible Power Supply (UPS) เป็นต้น
- ทดสอบและตรวจสอบความพร้อมของเครื่องกำเนิดไฟฟ้าสำรอง ระบบไฟฟ้าสำรอง รวมทั้งแหล่งพลังงานสำรองอย่างน้อยทุกเดือน อย่างน้อยปีละ 1 ครั้ง
- การเดินสายไฟและสายเคเบิล (Cabling Security) ต้องกำหนดให้มีการป้องกันการเดินสายไฟฟ้า หรือสายเคเบิ้ลเข้ามาภายในอาคารสำนักงาน
- บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน และมีการติดตั้งตู้พักสาย ต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิ์เท่านั้น
- กำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ 1 ครั้ง เป็นต้น

หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

8.1 ระเบียบปฏิบัติการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities Policy)

จุดประสงค์และขอบเขต :

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

8.1.1 กำหนดมาตรการควบคุมด้าน Security Baseline เพื่อใช้ในการตั้งค่าระบบปฏิบัติการ

- อ้างอิงมาตรฐานการตรวจสอบตาม CIS Center for Internet Security (cisecurity.org) และนำมาปรับใช้พื้นฐานเท่าที่จำเป็นสำหรับองค์กร
- อ้างอิงตาม Owasp OWASP Foundation, the Open Source Foundation for Application Security และนำมาปรับใช้พื้นฐานเท่าที่จำเป็นสำหรับองค์กร

8.1.2 กำหนดเรื่องการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต เช่น Intrusion Prevention System (IPS) เป็นต้น

8.1.3 กำหนดเรื่องการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (Patch Management)

8.1.4 การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

- ต้องจัดทำคู่มือ และ/หรือ ขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียด ขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ
- มีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

8.1.5 การจัดการการเปลี่ยนแปลง (Change Management)

- มีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ทุกครั้ง โดยปฏิบัติตามระเบียบปฏิบัติงานเรื่องการขอใช้บริการเจ้าหน้าที่ IT
- เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ เช่น ระบบปรับอากาศ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ ฯลฯ เจ้าหน้าที่ต้องประสานงานหรือรายงานกับ คณะกรรมการ
- เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการ ในการร้องขอการเปลี่ยนแปลงทุกครั้ง
- มีการประชุมเป็นประจำเพื่อตรวจสอบ คำร้องขอการเปลี่ยนแปลง (Change Request) และพิจารณาตรวจสอบการเปลี่ยนแปลงต่าง ๆ ให้เป็นที่พอใจและยอมรับได้

- ตาราง และ/หรือ แผนการเปลี่ยนแปลงทุกครั้งต้องได้รับความเห็นชอบจากผู้บริหาร/ผู้มีอำนาจอนุมัติก่อนจะทำการเปลี่ยนแปลง
- บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบโดยบันทึกฯ ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
  - วันที่รับเรื่อง และวันที่ทำการเปลี่ยนแปลง
  - เจ้าของข้อมูล และผู้ดูแลระบบ
  - วิธีการเปลี่ยนแปลง
  - ผลของการเปลี่ยนแปลง (สำเร็จ หรือล้มเหลว)

8.1.6 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

- มีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศ และการสื่อสารปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมของทรัพยากรชนิดต่าง ๆ
- มีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต (อาทิ ความต้องการใน 1 ปีที่จะถึง เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น) สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี
- แผนการจัดการขีดความสามารถของระบบต้องประกอบด้วยวิธีการจัดการขีดความสามารถ อาทิ การ Tuning การจัดหาเพิ่มเติม

8.1.7 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบและสภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment)

- ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบออกจากกับเครื่องที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบ ที่ใช้งานจริงด้วย

8.2 ระเบียบปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware Policy)

จุดประสงค์และขอบเขต :

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย และได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี เพื่อควบคุม และป้องกันซอฟต์แวร์ และข้อมูลจากโปรแกรมที่ไม่ประสงค์ดีและซอฟต์แวร์อันตราย

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against Malware) มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

- ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกัน Virus Version ล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่อง Server โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา
- ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้โปรแกรมค้นหา Virus ทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย การติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก 6 เดือน และ ต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย
- ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดหาโปรแกรมหรือเครื่องมือสำหรับตรวจสอบระบบที่ใช้งานอยู่ปัจจุบันเพื่อนำไปประเมินความเสี่ยง
- ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตควรมีการตรวจหา Virus ก่อนนำไปใช้งาน โดยมีการติดตั้งระบบตรวจจับ virus ที่ใช้ร่วมกันในบริษัท
- ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใดๆ ตัวอย่างเช่น ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง อีเมลบอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ของบริษัทฯ
- ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้นต้องตรวจสอบ Virus คอมพิวเตอร์ก่อนใช้งานทุกครั้ง
- เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชั่นการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้น ในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

8.3 ระเบียบปฏิบัติการสำรองข้อมูล (Backup Policy)

จุดประสงค์และขอบเขต :

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย และเพื่อป้องกันการสูญหายของข้อมูล

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

การสำรองข้อมูล (Information Backup)

ข้อมูลสำหรับสารสนเทศ ซอฟต์แวร์และอิมเมจของระบบ ต้องมีการดำเนินการสำรองไว้ และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอ ตามระเบียบปฏิบัติการสำรองข้อมูลที่ได้ตกลงไว้

- ต้องกำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบโดยปฏิบัติคู่มือการบริหารสารสนเทศ หัวข้อเรื่องการสำรองข้อมูลและการกู้คืน (Backup & Restore)

- จัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา
- มีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ
- กำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง
- ต้องมีกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบเป็นระยะ ๆ
- ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง
- ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์
- ต้องลงบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูล ต้องได้รับการตรวจสอบเป็นประจำทุกปี
- กระบวนการในการเก็บข้อมูลระหว่างสถานที่ระบบคอมพิวเตอร์และสถานที่เก็บข้อมูลต้องได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง
- สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
  - ชื่อระบบ
  - วันสร้าง
  - ระดับความสำคัญของข้อมูล
  - รายละเอียดติดต่อผู้ดูแลข้อมูล

8.4 ระเบียบปฏิบัติการบันทึกข้อมูลล็อก และการเฝ้าระวัง (Logging and Monitoring Policy)

จุดประสงค์และขอบเขต :

เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

8.4.1 การบันทึกข้อมูลล็อก แสดงเหตุการณ์ (Event Logging)

- ข้อมูล Log แสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้จัดเก็บ และทบทวนอย่างสม่ำเสมอ อุปกรณ์บันทึกข้อมูล Log จะได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไข และการเข้าถึงโดยไม่ได้รับอนุญาต

8.4.2 การป้องกันข้อมูลล็อก (Protection of Log Information)

- ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศเพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

8.4.3 ข้อมูลล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ (Administrator and Operator Logs)

- ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น ๆ รวมถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย

8.4.4 การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

- ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในหน่วยงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ถูกบุกรุกตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

8.5 ระเบียบปฏิบัติการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software Policy)

จุดประสงค์และขอบเขต :

เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

- ซอฟต์แวร์คอมพิวเตอร์ทุกเครื่อง จะถูกต้องตั้งโดย หน่วยงานเทคโนโลยีสารสนเทศ เท่านั้น โดยมีการตรวจสอบตามข้อกำหนด เรื่อง การบริหารจัดการทรัพย์สิน (Asset Management)
- ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบ การใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

8.6 ระเบียบปฏิบัติการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management Policy)

จุดประสงค์และขอบเขต :

เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ และเพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

- ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับ เพื่อลดความเสี่ยงดังกล่าว

8.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

- บริษัทฯ ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญา ที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด
- บริษัทฯ ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่ โดยฝ่ายเทคโนโลยีสารสนเทศ ทำการตรวจสอบการติดตั้งซอฟต์แวร์ของพนักงานทุกคน อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่า ไม่มีการใช้ซอฟต์แวร์ที่ละเมิดทรัพย์สินทางปัญญา
- ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ บนระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยเด็ดขาด
- เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่บริษัท มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของสำนักงาน เพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตจากผู้บริหาร/ผู้มีอำนาจ และในขณะเดียวกัน พนักงานของบริษัทฯ ไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทฯ โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

บริษัทฯ กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าสำนักงานมีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์ เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น บริษัทอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มี ใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

9.1 ระเบียบปฏิบัติการจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

จุดประสงค์และขอบเขต :

เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัทฯ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

9.1.1 การควบคุมการเข้าถึงเครือข่าย (Network Control)

เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่าง ๆ หัวหน้าหน่วยงานควบคุมระบบเครือข่าย ต้องรับผิดชอบในการจัดให้มีการควบคุมการปฏิบัติการด้านเครือข่าย ดังต่อไปนี้

- กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร (Network Configuration) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สายที่ใช้ในการสื่อสารของเครือข่ายทั้งหมดอย่างชัดเจน โดยจัดทำและปรับปรุง แผนภาพเครือข่ายให้ทันสมัยอยู่เสมอ
- ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด
- การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย
- ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่หน่วยงานนั้นรับผิดชอบ
- ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย
- บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่าย ตลอดจนโครงสร้างพื้นฐานของบริษัทฯ ด้วย
- จัดให้มีการควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่จัดไว้
- มีมาตรการในการควบคุมดูแลสภาพและประเมินประสิทธิภาพการใช้งานของคู่สาย สายสื่อสารและอุปกรณ์ในเครือข่ายสื่อสาร เพื่อให้พร้อมใช้งานตลอดเวลา
- บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ ประเมินประสิทธิภาพของระบบเครือข่ายอย่างน้อย ปีละ 1 ครั้ง และวางแผนในการปรับปรุงระบบเครือข่ายให้สามารถรองรับปริมาณงานที่จะขยายตัวในอนาคต

9.1.2 ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

- ระบบเครือข่ายทั้งหมดของบริษัท ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

- ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะ และติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของบริษัท ทั้งทางด้านกายภาพและทางด้าน Logical และต้อง ไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายของบริษัทฯได้
- ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัทฯ โดยไม่ได้รับอนุญาตจากเจ้าหน้าที่ IT
- ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัท โดยเด็ดขาด หากมีความจำเป็นต้องใช้งาน ต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง
- ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด
- ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัท ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัท โดยเด็ดขาด
- การกำหนดเรื่องการป้องกันการบุกรุก
- การระบุเรื่องการเปิดใช้งาน Port ที่จำเป็นเท่านั้น

9.1.3 การจัดแบ่งเครือข่ายภายในบริษัท (Segregation in Network)

- ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และโซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการ บุกรุกได้อย่างเป็นระบบ
- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

9.2 ระเบียบปฏิบัติการถ่ายโอนข้อมูล (Information Transfer)

9.2.1 การถ่ายโอนข้อมูล ต้องกระทำภายใต้การปฏิบัติงานของบริษัทและเป็นไปตามขั้นตอนของการจัดลำดับชั้นความลับของบริษัทเท่านั้น

9.2.2 ห้ามถ่ายโอนข้อมูลไปภายนอกโดยไม่ได้รับอนุญาตอย่างเด็ดขาด หรือโอนโดยไม่ใช่เป็นการปฏิบัติหน้าที่ปกติในการปฏิบัติงานตามตำแหน่งงาน

9.2.3 การถ่ายโอนข้อมูลส่วนบุคคล ต้องปฏิบัติตามนโยบายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด

หมวดที่ 10 การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

10.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

จุดประสงค์และขอบเขต :

เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

10.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification

- ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจน ในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน หรือการปรับปรุงระบบที่มีอยู่แล้ว หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้
  - มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น
  - มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล เป็นต้น

10.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

- สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับ การป้องกันและการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

10.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

- สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

10.2 ระเบียบปฏิบัติสำหรับกระบวนการในการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes)

จุดประสงค์และขอบเขต :

เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบ สารสนเทศ (development lifecycle)

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

10.2.1 ระเบียบปฏิบัติการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

- ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามระเบียบปฏิบัติหรือข้อกำหนดที่บริษัทกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้อง สามารถแก้ไขช่องโหว่ที่ตรวจพบได้

10.2.2 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

- ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการ เพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น
  - คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
  - ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
  - ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
  - เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ

10.2.3 การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)

- เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบ และทดสอบซอฟต์แวร์ต่างๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

10.2.4 การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

- เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบ และจัดทำเป็นเอกสาร เพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

10.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

- เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรม ระบบต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ โดยให้คณะทำงานความปลอดภัยฯ มีหน้าที่ดูแล ระบบด้านความมั่นคงปลอดภัยด้านโครงสร้างบริษัท

10.2.6 การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development)

- ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทฯ ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

10.2.7 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

- โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา

10.2.8 การทดสอบเพื่อรับรองระบบ (System/User acceptance testing)

- มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่และระบบที่ปรับปรุง

10.3 ระเบียบปฏิบัติข้อมูลสำหรับการทดสอบ (Test data)

จุดประสงค์และขอบเขต :

เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

10.3.1 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกัน เพื่อลดความเสี่ยงของการเข้าถึง หรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

- ในการพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) และระบบที่ใช้งานจริง (Production System)
- ต้องจัดให้มีระเบียบปฏิบัติที่ชัดเจนในการโอนย้ายโปรแกรมที่พัฒนาเสร็จแล้ว ไปยังระบบที่ใช้งานจริง
- ต้องไม่มีการติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาโปรแกรมอื่น ๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง

10.3.2 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

- ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวดที่ 11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

11.1 ระเบียบปฏิบัติเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

จุดประสงค์และขอบเขต :

เพื่อให้มีการป้องกันทรัพย์สินของบริษัท ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

11.1.1 ระเบียบปฏิบัติความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

- หน่วยงานจะต้องกำหนดให้มีการจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างหน่วยงานกับผู้ให้บริการภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร โดยเจ้าหน้าที่ IT จัดทำแบบฟอร์ม แบบประเมินผู้ให้บริการ และรวบรวมจัดทำเป็นรายงานการประเมินผู้ให้บริการภายนอก ซึ่งจะทำการประเมินในช่วง 1-2 เดือนก่อนสัญญาว่าจ้างจะหมดอายุ และกำหนดให้ส่งผลการประเมินฯ แนบไปกับใบขออนุมัติต่อสัญญาว่าจ้างในรอบถัดไป

11.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)

- เจ้าหน้าที่ IT ต้องมีส่วนร่วมกับฝ่ายจัดซื้อจัดจ้าง ในการระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่างบริษัทกับผู้ให้บริการภายนอก ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ต้องปฏิบัติตามระเบียบปฏิบัติเรื่องการจัดซื้อจัดจ้าง ของบริษัท และเมื่อมีความจำเป็นต้องให้ผู้ให้บริการภายนอกนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ และก่อนที่จะอนุญาตให้สามารถเข้าถึงได้ ผู้ให้บริการภายนอกต้องมีการลงทะเบียนใช้งานระบบสารสนเทศ ไว้กับฝ่ายเทคโนโลยีสารสนเทศ

11.2 ระเบียบปฏิบัติการบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

จุดประสงค์และขอบเขต :

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ใน ข้อตกลงการให้บริการของผู้ให้บริการภายนอก

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

11.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

- บริษัทฯ ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับบริษัท ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก
- ต้องมีการตรวจสอบการให้บริการจากหน่วยงานภายนอกผู้ทำหน้าที่ตรวจสอบจำเป็นต้องมีความรู้ ความเข้าใจในเรื่องความปลอดภัยสารสนเทศ ตลอดจนเงื่อนไขและข้อตกลงต่าง ๆ

- ในกรณีที่มีเหตุการณ์ที่กระทบต่อความปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการเพื่อรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมายในกรณีที่จำเป็น
- ต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ โดยมีการตรวจประเมินผู้ให้บริการจากภายนอกทุกปี
- ทุกขั้นตอนการดำเนินการใดจากผู้ให้บริการภายนอกทั้งที่ทำผ่านระบบหรือเข้าพื้นที่เพื่อดำเนินการจะต้องมีเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศติดตามตั้งแต่ต้นจนเสร็จสิ้นกระบวนการ

11.2.2 การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

- การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของบริษัท ทุกครั้ง ต้องเป็นไปตามกระบวนการเรื่องการคัดเลือกและประเมินผู้ขาย / ผู้ให้บริการ ของบริษัทฯ
- การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงระเบียบปฏิบัติ ขั้นตอนการปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบัน ต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจ ที่เกี่ยวข้องมาพิจารณาด้วย และต้องมี การทบทวนการประเมินความเสี่ยงใหม่

หมวดที่ 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1 ระเบียบปฏิบัติการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

จุดประสงค์และขอบเขต :

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทฯ ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และเพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

12.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

- ต้องกำหนดหน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยของหน่วยงาน และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี เพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ ความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำเอกสารสำหรับการรับแจ้งปัญหาในแบบฟอร์มการแจ้งและแก้ปัญหาทางด้าน IT หรือให้แจ้งปัญหาทางอีเมล ส่งให้ผู้จัดการฝ่ายต้นสังกัดอนุมัติทางอีเมล และส่งให้เจ้าหน้าที่ IT ดำเนินการ
- กำหนดเรื่องบันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าว เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่เกิดเหตุการณ์
- กำหนดให้ทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างน้อยปีละ 1 ครั้ง
- ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท โดยผ่านช่องทางรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้
- ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในบริษัท ต่อผู้บังคับบัญชา หรือหน่วยงานจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที
- ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อผู้บริหารหรือคณะกรรมการทันที
- ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อผู้บริหารหรือคณะกรรมการทันที

- ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในบริษัท ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย (Security Management) และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง
- การกระทำอื่นๆ ที่ถือเป็นข้อห้ามของบริษัทฯ มีดังนี้
    - การกระทำใดๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่นๆ ที่กล่าวถึงด้านล่างนี้ ถือเป็นข้อห้ามของบริษัท ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาด ทั้งนี้บริษัทฯ มิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น หมายเหตุ : เจ้าหน้าที่บางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงระบบเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ
    - การใช้งานทรัพยากรของสำนักงาน ฯ เพื่อการจัดหาหรือส่งต่อวัสดุ เอกสาร หรือรูปภาพ ลามกอนาจาร หรือที่ขัดต่อกฎหมาย
    - การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่บริษัทฯ กำหนดให้ เพื่อเสนอขายสินค้าหรือบริการใด ๆ
    - การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่าย ตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์ แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย
    - การใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing
    - การทำ Port Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ ที่ได้รับมอบหมาย
    - การดักฟังหรือดักจับข้อมูลที่พนักงานไม่ได้รับอนุญาต ให้รับรู้ด้วยวิธีการใด ๆ เว้นแต่ เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
    - การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
    - การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ระบบเครือข่ายใด ๆ
    - การใช้โปรแกรม/สคริปต์/คำสั่ง หรือการส่งข้อความใด ๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่าง ๆ

- การให้ข้อมูลลับเกี่ยวกับรายชื่อพนักงาน รายชื่อลูกค้า ความลับของบริษัท และข้อมูลลับอื่น ๆ แก่บุคคลภายนอก
- การข่มขู่คุกคามทุกรูปแบบผ่านอีเมล โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษา ความถี่ หรือขนาดของข้อความการแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)
- การละเมิดสิทธิ์ส่วนบุคคล ลิขสิทธิ์ของบริษัท ความลับของบริษัท สิทธิบัตร ทรัพย์สิน ทางปัญญา หรือกฎหมายอื่นใด

การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events) ประเด็นปัญหาต่าง ๆ ที่ได้รับแจ้ง และได้ดำเนินการแก้ไขเสร็จแล้วตามกำหนดระยะเวลา จะถูกนำข้อมูลดังกล่าวมาประมวลผล เพื่อสรุปออกมาเป็นรายงาน เพื่อแสดงให้เห็นว่าในช่วงเวลาที่ผ่านมานั้น มีปัญหาเรื่องอะไรมากที่สุด สาเหตุของปัญหาดังกล่าวเกิดจากอะไร และจะมีวีการป้องกันไม่ให้ปัญหานั้นเกิดขึ้นมาได้อย่างไร โดยหน่วยงานเทคโนโลยีสารสนเทศ จะทำรายงานสรุปดังกล่าว เพื่อนำเสนอคณะทำงานความมั่นคงปลอดภัยสารสนเทศ เป็นประจำทุก 1 ปี เพื่อร่วมพิจารณาปัญหาและวางแนวทางป้องกันปัญหาที่เกิดขึ้นในอนาคต

หมวดที่ 13 การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

13.1 ระเบียบปฏิบัติความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity Policy)

จุดประสงค์และขอบเขต :

เพื่อป้องกันการหยุดชะงักในการดำเนินงานของบริษัท ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบไม่ว่าจะด้วยอุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหาย ต่อบริษัทไม่มากก็น้อย ดังนั้นจึงควรจัดทำแผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ เพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักของบริษัทต่อไปได้

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

- บริษัทต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่อง ในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ
- ต้องจัดทำแนวทางปฏิบัติ ในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ควรพิจารณา ดังนี้
  - การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิด ความเสียหายและมีผลกระทบต่อการดำเนินงานของบริษัทฯ และการให้บริการ ด้านเทคโนโลยีสารสนเทศบริษัท
  - การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของ ความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
  - การดำเนินการเพื่อให้บริษัท สามารถดำเนินงานเป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
  - การกลับคืนสู่การทำงานปกติ เพื่อให้การดำเนินงานของบริษัทฯ กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

13.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement information security continuity)

- ต้องจัดตั้งแผนสร้างความต่อเนื่องให้กับธุรกิจของระบบเทคโนโลยีสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงาน เจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลข้อมูล เป็นต้น
- ต้องจัดทำแผนรองรับ เหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ 1 ครั้ง โดยปฏิบัติตามเอกสารนโยบาย เรื่องแผนความต่อเนื่องของธุรกิจ (BCP) และแผนการฟื้นฟูระบบงาน (DRP)

13.1.3 การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

- ต้องกำหนดเวลาการ ทดสอบแผน กำหนดการทดสอบแผนฉุกเฉินที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ
- ต้องกำหนดเหตุการณ์ จำลองที่จะใช้ทดสอบและรายละเอียด ในการกำหนดรายละเอียดของเหตุการณ์จำลอง ควรระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่ เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน ฉุกเฉิน
- ต้องกำหนดทรัพยากรต่างๆ ที่ใช้ในการทดสอบแผนฉุกเฉิน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุมประสานงาน และรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่และอุปกรณ์เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย
- ต้องกำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

13.2 ระเบียบปฏิบัติการเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)

จุดประสงค์และขอบเขต :

เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

13.2.1 สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

- อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนด

หมวดที่ 14 ความสอดคล้อง (Compliance)

14.1 ระเบียบปฏิบัติปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

จุดประสงค์และขอบเขต :

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญา/ทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

14.1.1 การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

- บริษัทฯ ต้องมีการศึกษาและกำหนดรายการของระเบียบปฏิบัติ กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน
- เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของระเบียบปฏิบัติกฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ และ การสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด และมีรายการดังต่อไปนี้เป็นอย่างน้อย
  - ระเบียบปฏิบัติการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
  - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
  - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
  - พ.ร.บ. กำหนดหลักเกณฑ์และวิธีการในการกระทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
  - พ.ร.บ. ลิขสิทธิ์
  - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัท สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
- เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งาน เพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่ระเบียบปฏิบัติต่าง ๆ ของบริษัทฯ กำหนดไว้
- บริษัทฯ ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้อง แจ้งให้ทราบล่วงหน้า อย่างไรก็ตามบริษัท จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใดๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

- ห้ามพนักงานบริษัทฯ ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัทฯ กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม
- การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใดๆ ออกนอกประเทศไม่ขัดต่อข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

14.1.2 สินทรัพย์ทางปัญญา (Intellectual Property Rights)

- ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด
- ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่าง เคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตาม ลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่ โดยให้เจ้าหน้าที่ IT ทำการตรวจสอบการติดตั้ง/การใช้งานซอฟต์แวร์ของพนักงานอย่างน้อยปีละ 1 ครั้ง หากพบการใช้งานที่ไม่ถูกต้อง ต้องดำเนินการลบการติดตั้งทันที และพิจารณาโทษตามกระบวนการพิจารณาของ ฝ่ายทรัพยากรบุคคล และถ้าหากมีความจำเป็น บริษัท อาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้
- ห้ามผู้ใช้งานดำเนินการทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบ เทคโนโลยีสารสนเทศ ของบริษัท โดยเด็ดขาด
- เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่บริษัท มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ ตั้งใจหรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใดๆ ที่ติดตั้งอยู่ในเครื่อง คอมพิวเตอร์ของบริษัท เพื่อจุดประสงค์ใดๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตจาก ISMR และในขณะเดียวกันเจ้าหน้าที่บริษัท ไม่ควรจะติดตั้งโปรแกรมใดๆ ลงในเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

14.1.3 การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

- ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล

14.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

- ต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญาที่เกี่ยวกับบริษัทฯ

14.1.5 การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

- ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

14.2 ระเบียบปฏิบัติการทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

จุดประสงค์และขอบเขต :

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับระเบียบปฏิบัติ และขั้นตอนปฏิบัติงานของบริษัท

เนื้อหาระเบียบปฏิบัติ และการดำเนินการ :

14.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

- ต้องมีการทบทวน วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติของบริษัท เช่น ทบทวนวัตถุประสงค์ มาตรการ ระเบียบปฏิบัติ วิธีปฏิบัติงานต่างๆ ให้ถูกต้องและเป็นปัจจุบัน ตามรอบระยะเวลาที่กำหนด เช่น ปีละ 1 ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

14.2.2 ทบทวนความสอดคล้องกับระเบียบปฏิบัติความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

- ต้องจัดให้มีการทบทวนระบบทั้งหมดของหน่วยงานตามระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้
- ต้องมีการตรวจสอบและทบทวนเอกสารระเบียบปฏิบัติ มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

14.2.3 ทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

- ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และ ทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

นโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ อนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2568 เมื่อวันที่ 31 มกราคม 2568 และให้มีผลใช้บังคับตั้งแต่วันที่ 1 กุมภาพันธ์ 2568 เป็นต้นไป

ทะเบียนควบคุมเอกสาร

ลำดับ	วันที่จัดทำ	รายละเอียดการดำเนินการ	วันที่บังคับใช้	ผู้ดำเนินการ
01	23 ธ.ค. 67	จัดทำเล่มนโยบาย	01 ก.พ. 68	ฝ่ายเทคโนโลยีสารสนเทศ