สารบัญ

เนื้อหา	หน้า
1. นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)	1
2. การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)	6
3. การรักษาความปลอดภัยด้านข้อมูล (Data Security)	8
4. การควบคุมการเข้าถึง (Access Control)	12
5. การบริหารจัดการสินทรัพย์เทคโนโลยีสารสนเทศ	18
6. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)	22
7. ความมั่นคงปลอดภัยด้านการดำเนินงาน (Operation Security)	24
8. ความมั่นคงปลอดภัยในการบริหารจัดการผู้ให้บริการ (Supplier Security Management)	28
9. ความมั่นคงปลอดภัยสาหรับการสื่อสารข้อมูล (Communications Security)	29
10. การจัดหา พัฒนา และดูแลรักษาระบบเทคโนโลยีสารสนเทศ (IT System Acquisition, Development, and Maintenance)	30
11. การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan)37	34
12. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Incident Management)	35
13. การบริหารจัดการข้อมูลส่วนบุคคล	36
15. การตรวจสอบนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ	38

บทนำ

1.1 บทนำ

ในปัจจุบัน เทคโนโลยีสารสนเทศมีบทบาทและเป็นกลไกที่สำคัญอย่างยิ่งในการขับเคลื่อนธุรกิจ ตั้งแต่การบริหารจัดการร้านสาขา การขาย จัดซื้อ บัญชีและการเงิน การบริหารจัดการทรัพยากรบุคคล และอื่นๆ ทำให้บริษัทเผชิญความเสี่ยงที่มาพร้อมกับเทคโนโลยีสารสนเทศเหล่านี้อย่างหลีกเลี่ยงไม่ได้ เช่น ภัยคุกคามทางไซเบอร์ (Cyber Attack) ข้อมูลสูญหายจากอุบัติเหตุต่างๆ การดำเนินงานหยุดชะงักเนื่องจากระบบเทคโนโลยีสารสนเทศไม่สามารถใช้งานได้ เป็นต้น สิ่งเหล่านี้ล้วนส่งผลกระทบต่อการดำเนินงานของบริษัทอย่างมีนัยสำคัญ ฝ่ายเทคโนโลยีสารสนเทศได้ศึกษาปัจจัยต่างๆ ที่อาจส่งผลกระทบต่อธุรกิจ และหาแนวทางในการแก้ปัญหาที่เหมาะสมกับแต่ละความเสี่ยงและเหตุการณ์ เพื่อรองรับและสามารถแก้ปัญหาได้อย่างทันเวลาเมื่อเกิดเหตุการณ์ฉุกเฉินขึ้น โดยมุ่งหวังที่จะให้ส่งผลกระทบต่อธุรกิจน้อยที่สุด อย่างไรก็ตาม ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศจะมีประสิทธิ์ภาพสูงสุดได้ก็ต่อเมื่อพนักงานทุกคนทั่วทั้งบริษัทให้ความสำคัญและปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) และแนวปฏิบัติต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด

1.2 วัตถุประสงค์

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) (“นโยบายฉบับนี้”) จัดทำขึ้นโดยมีวัตถุประสงค์ ดังนี้

- เพื่อกำหนดแนวปฏิบัติ ทิศทาง และให้การสนับสนุนแก่พนักงานทั่วทั้งบริษัทในการดำเนินงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และสามารถนำไปปฏิบัติอย่างเป็นมาตรฐานเดียวกันและต่อเนื่อง
- เพื่อให้บริษัทมีมาตรฐานการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ โดยการกำหนดนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ แนวทางการปฏิบัติ และมีบทลงโทษหากมีการละเมิดหรือฝ่าฝืน
- เพื่อให้พนักงานทั่วทั้งบริษัทตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศรวมถึงการส่งเสริมให้มีการฝึกอบรมที่เกี่ยวข้องอย่างต่อเนื่อง
- เพื่อให้บริษัทมีการบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้อง ความสมบูรณ์ และพร้อมใช้งานอยู่เสมอ จากการมีแผนบริหารจัดการความต่อเนื่องทางธุรกิจ เมื่อเกิดเหตุการณ์ฉุกเฉินไม่คาดคิด ตลอดจนมีแผนการสำรองและกู้คืนระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศอย่างรวดเร็วและทันเวลา
- เพื่อป้องกันการละเมิดทางกฎหมาย สังคม ศีลธรรม จากการเข้าถึงข้อมูล/สารสนเทศขององค์กร โดยกำหนด กฎระเบียบข้อบังคับให้ผู้ใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรมีแนวทางปฏิบัติงานที่เป็นมาตรฐานสากล โดยอ้างอิงมาตรฐานของ ISOIEC 27001 (Information Security Standard) และ ITIL (Information Technology Infrastructure Library)

นโยบายฉบับนี้ให้มีผลบังคับใช้กับกรรมการ ผู้บริหาร และพนักงานทุกท่านในบริษัท รวมถึงบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลเทคโนโลยีสารสนเทศของบริษัท หากผู้ใดฝ่าฝืนนโยบายฉบับนี้ถือเป็นความผิดและต้องได้รับพิจารณาลงโทษตามระเบียบของบริษัท

บริษัทกำหนดให้มีการสื่อสารนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) แก่พนักงาน ผู้ปฏิบัติงาน และผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบ เพื่อให้เกิดความเข้าใจในความเสี่ยง และปฏิบัติตามนโยบายฉบับนี้ เพื่อลดและควบคุมความเสี่ยงดังกล่าว และบริษัทต้องมีการจัดอบรมประจำปีเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) เพื่อให้พนักงานทุกคนเข้าใจ และรับทราบถึงการเปลี่ยนแปลงที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

1.3 คำจำกัดความ

นิยาม/ศัพท์/อักษรย่อ	คำอธิบาย
Hardware	เครื่องคอมพิวเตอร์และอุปกรณ์ต่อเชื่อม หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ
Software	โปรแกรม/แอปพลิเคชัน/ระบบที่ใช้งานภายในองค์กร ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
Server	คอมพิวเตอร์แม่ข่าย
Cloud	ระบบคอมพิวเตอร์ที่เกิดขึ้นเพื่อรองรับการทำงานของผู้ใช้งานในทุกๆด้าน ทางด้านระบบเครือข่าย การการจัดเก็บข้อมูล ด้านการติดตั้งข้อมูล เป็นต้น
Username	ชื่อผู้ใช้งาน
Password	รหัสผ่าน
Anti-virus	โปรแกรมที่สร้างขึ้นเพื่อคอยตรวจจับ ป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์
Firewall	เครื่องมือที่ใช้สำหรับป้องกันระบบ Network (เครือข่าย) จากการสื่อสารทั่วไปที่ถูกบุกรุก จากผู้ที่ไม่ได้รับอนุญาติ
Malware	โปรแกรมชนิดหนึ่งที่ถูกสร้างมาเพื่อประสงค์ร้ายต่อคอมพิวเตอร์
Domain	ชื่อที่ใช้ระบบลงในคอมพิวเตอร์ เพื่อไปค้นหาในระบบ
การสำรองข้อมูล	การทำสำเนาข้อมูลเก็บแยกเอาไว้เพื่อนำมาเรียกคืนเมื่อเกิดการสูญหายของข้อมูล
MS Dynamics	Microsoft Dynamics
SSL	Secure Socket Layer
SSID	Service Set Identifier
WPA2	Wi-Fi Protected Access
PM	Preventive Maintenance
MA	Maintenance Service Agreement
POS	Point of Sale ระบบขายหน้าร้าน

1.4 ภาพรวมบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1.4.1 บทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศบริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้มีหน้าที่และความรับผิดชอบหลักในการกำกับดูแลและบริหารจัดการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท โดยการปฏิบัติงานต้องมีการแบ่งแยกหน้าที่และกำหนดความรับผิดชอบ (Segregation of Duties) เพื่อลดโอกาสที่จะมีการใช้สินทรัพย์ที่เกี่ยวข้องกับระบบสารสนเทศผิดวัตถุประสงค์โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาเพื่อเป็นการตรวจสอบซึ่งกันและกัน และเพื่อป้องกันการแก้ไข

หรือเปลี่ยนแปลงระบบโดยไม่ได้รับการอนุมัติหรือตรวจสอบอย่างเหมาะสม การแบ่งแยกหน้าที่และกำหนดความรับผิดชอบ (Segregation of Duties) ถือเป็นพื้นฐานที่สำคัญของการควบคุมภายในที่ดี โดยบริษัทแบ่งแยกหน้าที่โดยทั่วไปของบุคลากรด้านเทคโนโลยีสารสนเทศ ตามตัวอย่างดังนี้

- การบริหารจัดการระบบปฏิบัติการคอมพิวเตอร์ (Computer Operations Management)
- การบริหารจัดการระบบเครือข่าย (Network Management)
- การควบคุมดูแลระบบเทคโนโลยีสารสนเทศ (System Administration)
- การพัฒนาและดูแลรักษาระบบเทคโนโลยีสารสนเทศ (System Development and Maintenance)
- การบันทึกข้อมูลในระบบเทคโนโลยีสารสนเทศ (Data Entry)
- การควบคุมดูแลความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Security Administration)
- การตรวจสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (Security Audit)

ทั้งนี้ หากบริษัทมีข้อจำกัดในการแบ่งแยกหน้าที่ของบุคลากรด้านเทคโนโลยีสารสนเทศตามที่กำหนด บริษัทพิจารณาการควบคุมอื่นๆ ทดแทน (Compensating Controls) เช่น การตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) อย่างสม่ำเสมอการสอบทานและกำกับดูแลโดยหัวหน้างานอย่างเคร่งครัด (Close Supervision and Review) เป็นต้น

1.4.2 การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security)

ก่อนการจ้างงาน (Prior employment) พนักงานทุกคนต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) อย่างเคร่งครัด และมีหน้าที่ต้องปกป้อง ดูแล และรักษาข้อมูลและทรัพย์สินของบริษัทอย่างเหมาะสม

บริษัทกำหนดเกณฑ์ในการตรวจสอบและคัดเลือกพนักงานใหม่อย่างชัดเจน โดยพิจารณาถึงประวัติส่วนตัว ประวัติอาชญากรรม ประวัติการศึกษา ประวัติการทำงาน เป็นต้น เพื่อให้มั่นใจว่าบริษัทได้รับพนักงานที่มีคุณภาพ และลดความเสี่ยงด้านการละเมิดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อ้างอิงนโยบาย OKJ-HRM-REC การสรรหาพนักงาน

บริษัทกำหนดข้อตกลงและเงื่อนไข รวมถึงความรับผิดชอบในการรักษาความปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศในสัญญาจ้างอย่างชัดเจนและเป็นลายลักษณ์อักษร และให้ผู้รับจ้างหรือพนักงานลงนามรับทราบและถือปฏิบัติตามอย่างเคร่งครัด นอกจากนี้ บริษัทอาจพิจารณาเพิ่มเงื่อนไขกำหนดให้ผู้รับจ้างหรือพนักงานลงนามในสัญญาการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) กับบริษัทก่อนเริ่มทำงาน โดยข้อกำหนดและเงื่อนไขในสัญญาจ้าง และสัญญาการไม่เปิดข้อมูล (Non-disclosure Agreement) ให้มีผลบังคับตามกฎหมายอีกเป็นเวลา 1 ปี ภายหลังสิ้นสุดสภาพการเป็นผู้รับจ้างหรือพนักงานของบริษัทระหว่างจ้างงาน (During Employment)

ผู้บริหารให้การสนับสนุนและกำกับดูแลให้พนักงานทุกคน รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท ปฏิบัติตามนโยบายฉบับนี้ และแนวปฏิบัติอื่นๆ ที่เกี่ยวข้องอย่างเคร่งครัด

- บริษัทกำหนดให้พนักงานลงนามยืนยันการปฏิบัติตามนโยบายฉบับนี้เป็นประจำอย่างน้อยปีละ 1 ครั้ง (Annual IT Security Confirmation)
- บริษัทกำหนดให้มีการตรวจสอบการปฏิบัติงานของพนักงานทั้งองค์กรอย่างเหมาะสม เพื่อให้มั่นใจว่าพนักงานได้ปฏิบัติตามนโยบายฉบับนี้อย่างมีประสิทธิ์ภาพ
- บริษัทจัดให้มีการฝึกอบรมแก่พนักงานหรือบุคคลภายนอกที่เกี่ยวข้องกับข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท (ตามความเหมาะสม) ในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทเป็นประจำอย่างน้อยปีละ 1 ครั้ง รวมถึงการจัดฝึกอบรมเพื่อให้ทราบถึงการเปลี่ยนแปลงข้อมูลอย่างสม่ำเสมอ ทั้งนี้ บริษัทกำหนดให้มีการทดสอบเพื่อประเมินผลความรู้และความเข้าใจทุกครั้งภายหลังการฝึกอบรม หากไม่ผ่านการทดสอบหรือประเมินผลบริษัทกำหนดให้มีการฝึกอบรมเพิ่มเติมหรือพิจารณาแนวทางอื่นๆ ตามความเหมาะสม

- บริษัทกำหนดให้พนักงานฝ่ายเทคโนโลยีสารสนเทศได้รับการฝึกอบรมในเรื่องที่เกี่ยวข้องกับการปฏิบัติงานอย่างเหมาะสมและเพียงพอ
- บริษัทกำหนดบทลงโทษ (Disciplinary Action) สำหรับการละเมิดหรือไม่ปฏิบัติตามนโยบายฉบับนี้ โดยกำหนดแนวทางการสอบสวน และพิจารณาบทลงโทษอย่างเหมาะสมตามแต่ละเหตุการณ์สิ้นสุดการจ้างงานหรือการเปลี่ยนแปลงงาน (Termination or Change of employment)
- บริษัทกำหนดแนวปฏิบัติที่เกี่ยวข้องการสิ้นสุดการจ้างงานอย่างชัดเจน อ้างอิงนโยบาย OKJHRM-RES การจัดการ การลาออกและการเลิกจ้าง
- บริษัทเรียกคืนทรัพย์สิน อุปกรณ์ต่างๆ และเพิกสิทธิ์การใช้งานระบบต่างๆ ของบริษัท
- บริษัทสื่อสารให้พนักงานที่สิ้นสุดการจ้างงานทราบถึงข้อกำหนดและเงื่อนไขในการรักษาความลับ และข้อมูลต่างๆ ขององค์กรตามที่ได้ลงนามในสัญญาจ้าง หรือสัญญาการไม่เปิดเผยข้อมูล (Non-disclosure agreement)
- บริษัทกำหนดให้แก้ไข เปลี่ยนแปลง หรือยกเลิกสิทธิ์เดิมของพนักงานที่ได้เปลี่ยนแปลงงาน และขอเพิ่มสิทธิ์การทำงานในแผนกงานอื่นๆ
- บริษัทกำหนดให้มีการถ่ายทอดงานสำหรับตำแหน่งงานที่สำคัญ (Transition) ก่อนสิ้นสุดการทำงาน

1.5 โครงสร้างคณะทำงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

เพื่อเป็นการติดตามการทำงาน และกำกับดูแลความปลอดภัยสารสนเทศ บริษัทจึงได้กำหนดคณะทำงานจำนวน 2 กลุ่ม ได้แก่ คณะกรรมการความปลอดภัยสารสนเทศ และหน่วยงานความมั่นคงปลอดภัยสารสนเทศ โดยมีหน้าที่ดังนี้

- คณะกรรมการความปลอดภัยสารสนเทศ เป็นเจ้าของนโยบายนี้ มีหน้าที่ต้องรับผิดชอบในการดูแลและสอบทานเนื้อหาของนโยบายอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การเปลี่ยนแปลงกลยุทธ์หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างเทคโนโลยี เป็นต้น
- หน่วยงานความมั่นคงสารสนเทศ มีหน้าที่ในการติดตามการทำงานของฝ่ายเทคโนโลยีสารสนเทศ อนุมัติแผน IT Master Plan และทบทวนความสอดคล้องของขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง เป็นต้น

บริษัทได้กำหนดหัวข้อการประชุม และกำหนดระยะเวลาในการทบทวน เป็นตัวกลางในการตรวจสอบการทวนสอบขั้นตอนต่างๆ ว่าได้ปฏิบัติตามครบถ้วนหรือไม่ ดังนี้

ขั้นตอนการดำเนินการ	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
ทบทวนนโยบาย กฎระเบียบความมั่นคงปลอดภัยสารสนเทศ	ปีละ 1 ครั้ง	คณะกรรมการความมั่นคงฯ
ทบทวนรายการเอกสารสัญญา และลิขสิทธิ์ต่าง ๆ	ปีละ 1 ครั้ง	คณะกรรมการความมั่นคงฯ
ทบทวนแผน และรับรองผลการทดลองใช้แผนสำรองกรณีฉุกเฉิน	ปีละ 1 ครั้ง	คณะกรรมการความมั่นคงฯ
นำเสนอ IT Master Plan พร้อมงบประมาณ	ปีละ 1 ครั้ง	หน่วยงานความปลอดภัยสารสนเทศ
ทวนสอบสิทธิ์การเข้าถึงระบบสารสนเทศกับหน่วยงานและพนักงาน	รายไตรมาส	หน่วยงานความปลอดภัยสารสนเทศ
รายงานสรุปผลการตรวจสอบบำรุงรักษาอุปกรณ์ และทรัพย์สิน	ปีละ 1 ครั้ง	หน่วยงานความปลอดภัยสารสนเทศ

ขั้นตอนการดำเนินการ	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
ทวนสอบอุปกรณ์คอมพิวเตอร์ และทรัพย์สิน	ปีละ 1 ครั้ง	หน่วยงานความปลอดภัยสารสนเทศ
รายงานสถานะการทำงานของ Server และระบบสำรองข้อมูล	ปีละ 4 ครั้ง	หน่วยงานความปลอดภัยสารสนเทศ
รายงานสรุปผลการแก้ไขปัญหาในระบบสารสนเทศ	ปีละ 4 ครั้ง	หน่วยงานความปลอดภัยสารสนเทศ
รายงานการใช้เครือข่ายของแต่ละหน่วยงาน	ปีละ 4 ครั้ง	หน่วยงานความปลอดภัยสารสนเทศ

รายชื่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ

ชื่อ – นามสกุล	ตำแหน่ง	หน้าที่
นาย จิรายุทธ ภูวพูนผล	ประธานเจ้าหน้าที่เกษตรอัจฉริยะ	ประธาน
นายชลากร เอกชัยพัฒนกุล	ประธานเจ้าหน้าที่บริหาร	รองประธาน
นายวรเดช สุชัยบุญศิริ	ประธานเจ้าหน้าที่ซัพพลายเชน	
นาย รุ่งโรจน์ ไชยวุฒิ	ผู้อำนวยการซัพพลายเชน	
นางสาว นภัสร์ฌาน์ ศรีอารย์ทาส	ผู้จัดการแผนกบริหารงานบุคคล	
นาย จุพชาติ วรสาร	IT Project & Application Manager	
นาย สุทัศ วีสี	IT Network & Infrastructure Manager	
นาย จิรายุทธ สุธีรัตนา	Business Analyst	
นางสาว อรอุมา ไม้สันเทียะ	พนักงานเทคโนโลยีสารสนเทศ	

รายชื่อหน่วยงานความปลอดภัยสารสนเทศ

ชื่อ – นามสกุล	ตำแหน่ง	หน้าที่
นาย จิรายุทธ ภูวพูนผล	ประธานเจ้าหน้าที่เกษตรอัจฉริยะ	ประธาน
นางสาว เบญญาภา เตชะมณีสถิตย์	ประธานเจ้าหน้าที่ปฏิบัติการ	รองประธาน
นางสาว ภวิษย์เพ็ญ เหล่ารัตนไพบูลย์	ประธานเจ้าหน้าที่บัญชีและการเงิน	
นางสาว นิธิพร สีตะระโส	ผู้อำนวยการบัญชีและการเงิน	
นาย อรุณ บิลหลี	ผู้จัดการบริหารภาคการขาย	
นาย จุพชาติ วรสาร	IT Project & Application Manager	
นาย สุทัศ วีสี	IT Network & Infrastructure Manager	
นาย อรรถวุฒิ เขตนอก	Head OF IT System & Network	
นาย ธรรธนวรรธ นิลพยัคฆ์	พนักงานเทคโนโลยีสารสนเทศ	
นาย จักรพันธ์ พิมพ์แพง	พนักงานเทคโนโลยีสารสนเทศ	
นาย ธีรพงษ์ ชะดุงรัมย์	พนักงานเทคโนโลยีสารสนเทศ	

2. การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)

2.1 การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงานจากองค์กร

นโยบาย

2.1.1 การสรรหาบุคลากร (Screening)

1) พนักงานแผนกบริหารทรัพยากรบุคคล ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคน ก่อนที่จะบรรจุเป็นผู้บริหาร พนักงานชั่วคราวหรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน
2) พนักงานแผนกบริหารทรัพยากรบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง “พนักงาน” และองค์กร ว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้นๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
3) ปฏิบัติตามวิธีปฏิบัติงานเรื่อง: การบริหารจัดการทรัพยากรบุคคลด้านการรักษาความมั่นคง ปลอดภัยสารสนเทศ (Human resources security)

2.1.2 ข้อกำหนดและเงื่อนไขของการจ้างงาน (Terms and conditions of employment)

1) พนักงานแผนกบริหารทรัพยากรบุคคล ต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึง หน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ โดยพนักงานแผนกกลุ่มบริหารทรัพยากรบุคคล ต้องแจ้งให้องค์กร ทราบทันทีเมื่อมีเหตุดังนี้
   - การว่าจ้างงาน
   - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
   - การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงานและลูกจ้าง หรือการถึงแก่กรรม
   - การโยกย้ายหน่วยงาน
   - การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

2.2 การสร้างความความมั่นคงปลอดภัยขณะเป็นพนักงาน (During employment)

วัตถุประสงค์

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความ มั่นคงปลอดภัยสารสนเทศขององค์กร

นโยบาย

2.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

1) ต้องกำหนดให้พนักงาน พนักงานข้าราชการ และพนักงานหน่วยงานภายนอกที่ว่าจ้างมา ปฏิบัติงานรับทราบและปฏิบัติตามนโยบาย กฎ ระเบียบและขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษา ความมั่นคงปลอดภัยสารสนเทศขององค์กร ด้วย

2.2.2 การสร้างความตระหนัก การให้ความรู้และการอบรมให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

1) พนักงานขององค์กร หรือผู้รับจ้างขององค์กรทุกคนต้องได้รับการอบรมให้ความรู้ โดยเนื้อหาที่แต่ละ บุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล เพื่อเป็นการ สร้างความตระหนักและฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
2) ต้องจัดอบรมให้ความรู้แก่พนักงานในองค์กร เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้าง ความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับ นโยบายความมั่นคงปลอดภัยและการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสาร ขององค์กร ด้วย
3) พนักงานใหม่ขององค์กรทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคง ปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือได้รับเอกสารนโยบายการรักษาความมั่นคง ปลอดภัยสารสนเทศฯ ฉบับย่อ และระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานภายใน 30 วันนับจากเข้า ทำงานในหน่วยงาน เพื่อให้ข้าราชการพนักงาน หรือผู้ที่เกี่ยวข้องได้ศึกษาและถือปฏิบัติ โดยอาจเป็น ส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย
4) พนักงานแผนกการบริหารทรัพยากรบุคคล มีหน้าที่ในการแจ้งให้ทราบ เกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้าน ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้แก่พนักงานด้วย

2.2.3 กระบวนการทางวินัย (Disciplinary Process)

1) ผู้บริหาร ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือ ระเบียบปฏิบัติขององค์กร แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตาม ฐานความผิดที่ได้กระทำ ตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

2.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์

เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

นโยบาย

2.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

1) ต้องมีการกำหนดและสื่อสารให้พนักงานหรือผู้ทำสัญญาได้รับทราบ รวมทั้งมีการควบคุมให้ ปฏิบัติตามข้อกำหนดในสัญญา
2) พนักงานแผนกการบริหารทรัพยากรบุคคล มีหน้าที่ดูแลหากมีการแต่งตั้งโยกย้าย ปลดหรือ เปลี่ยนแปลงตำแหน่งใดๆ ที่เกี่ยวข้องกับความรับผิดชอบในองค์กร
3) พนักงานผู้เกี่ยวข้องเมื่อได้รับเรื่องของผู้ใช้งานที่สิ้นสุดสภาพการจ้างงานหรือเปลี่ยนหน้าที่ความรับผิดชอบจากฝ่ายบุคคล ให้ปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศ เพื่อดำเนินการเพิกถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ์

3. การรักษาความปลอดภัยด้านข้อมูล (Data Security)

3.1 การกำหนด/แก้ไข/เปลี่ยนแปลงยกเลิกสิทธิ์

บริษัทกำหนดตารางควบคุมสิทธิ์ (Access Authorization Matrix) ในการเข้าถึงข้อมูลในระบบต่างๆ ของบริษัท เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลสำคัญอย่างไม่เหมาะสม โดยบริษัทต้องพิจารณากำหนดสิทธิ์การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศตามความเหมาะสมของบทบาทและหน้าที่ อีกทั้งกำหนดอำนาจในการดำเนินรายการต่างๆ ให้มีการตรวจสอบการปฏิบัติงานเป็นลำดับชั้น หรือตรวจสอบไขว้กัน (Cross Check) อย่างเหมาะสม

การเข้าถึงข้อมูล ระบบสารสนเทศและการลงทะเบียนผู้ใช้งานจะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชาสูงสุดของฝ่ายงานของบุคคลที่ต้องการเข้าถึง และบุคคลนั้นสามารถเข้าใช้ข้อมูลและระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของตนเองเท่านั้น โดยฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยปฏิบัติตามกระบวนการบริหารจัดการการเข้าถึงของผู้ใช้งานทั่วไป การสร้างหรือแก้ไขบัญชีสิทธิ์ผู้ใช้งาน และการทบทวนสิทธิ์ผู้ใช้งานตามนโยบาย OKJ-GITC-DTS-01 การกำหนด/แก้ไข/เปลี่ยนแปลง ยกเลิกสิทธิ์ และนโยบาย GITC-DTS-02 การสอบทานสิทธิ์ผู้ใช้งานประจำปี

บริษัทกำหนดให้ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไข หรือเปลี่ยนแปลงสิทธิ์โดยต้องได้รับการอนุมัติโดยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อนเท่านั้น และต้องมีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบในกรณีที่มีปัญหาเกิดขึ้น

3.2 การกำหนดรหัสในการเข้าถึงข้อมูล (Cryptography)

3.2.1. การเข้ารหัสข้อมูล บริษัทกำหนดลำดับชั้นความลับของข้อมูล (Information Class cation) และกำหนดมาตรฐานการเข้ารหัสข้อมูล

- บริษัทกำหนดให้มีการทบทวนการเข้าถึงข้อมูลตามลำดับชั้นความลับของข้อมูล (Information Classification) เป็นประจำอย่างน้อยปีละ 1 ครั้ง
- บริษัทกำหนดค่าให้ระบบปฏิเสธการเข้าถึงหากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง และต้องได้รับการพิจารณาจากฝ่ายเทคโนโลยีสารสนเทศในการปลดล็อคในการเข้าใช้งาน และเพื่อตรวจสอบและหาสาเหตุที่แท้จริง
- บริษัทกำหนดมาตรฐานในการบริหารจัดการและการกำหนดรหัสผ่านการใช้งานสำหรับผู้ใช้งานอย่างชัดเจน โดยมีมาตรฐานการกำหนดรหัสผ่าน ดังนี้
  - ความยาวของรหัสต้องไม่น้อยกว่า 9 ตัวอักษร
  - ประกอบด้วยอักษรภาษาอังกฤษพิมพ์ใหญ่
  - ประกอบด้วยอักษรภาษาอังกฤษพิมพ์เล็ก
  - ประกอบด้วยตัวเลข
  - ประกอบด้วยเครื่องหมายหรืออักขระพิเศษ เช่น !@#$%^&*()_+ เป็นต้น
  - ไม่สามารถกำหนดรหัสผ่านซ้ำเดิมที่เคยใช้ในระยะเวลา 1 ปี
- บริษัทกำหนดให้รหัสผ่านมีอายุการใช้งาน 90 วัน โดยผู้ใช้งานจะได้รับอีเมลแจ้งเตือนรหัสผ่านหมดอายุและการเปลี่ยนรหัสผ่านล่วงหน้า 7 วัน และ จะได้รับอีเมลแจ้งเตือนเป็นประจำทุกวันจนกว่าจะเปลี่ยนรหัสผ่านใหม่ (โดยจะมีการแจ้งเตือนให้เปลี่ยนรหัสผ่านก่อนทำการ login เข้าใช้งาน) หากผู้ใช้งานไม่เปลี่ยนรหัสผ่าน บัญชีผู้ใช้งานจะถูกจำกัดการเข้าถึง (Lock) โดยอัตโนมัติ และต้องแจ้งผู้ดูแลระบบเพื่อดำเนินการแก้ไขหรือปลด Lock และเปลี่ยนรหัสผ่านเพื่อใช้งาน
- บริษัทกำหนดให้ผู้ใช้งานต้องใส่รายละเอียดชื่อผู้ใช้งานและรหัสผ่าน (Username and Password) ทุกครั้งที่ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท และผู้ใช้งานต้องออกจากระบบ (Log out) ทุกครั้งหลังจากการใช้งาน และไม่อนุญาตให้เลือกใช้งานประเภทการจำรหัสผ่าน (Remember password) เพื่อป้องกันการนำชื่อผู้ใช้งานและรหัสผ่านไปใช้ในทางที่ไม่เหมาะสม

พนักงานฝ่ายเทคโนโลยีสารสนเทศบันทึกการเข้าสู่ระบบทุกครั้งที่มีการ Log in ทั้งที่ประสบความสำเร็จและล้มเหลว เพื่อเป็นข้อมูลสำหรับการตรวจสอบหากจำเป็น

3.2.2. การเข้ารหัสข้อมูล บนระบบ POS (ระบบขายหน้าร้าน)

- บริษัทกำหนดให้สามารถทำการแก้ไข รหัสด้วยตัวเองผ่านระบบ POS (ระบบขายหน้าร้าน)
- บริษัทกำหนดให้สามารถทำการแก้ไข รหัสด้วยตัวเองผ่านหน้าเว็บไซต์ BackOffice POS
- บริษัทกำหนดค่าให้ระบบปฏิเสธการเข้าถึงหากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 5 ครั้งและต้องได้รับการพิจารณาจากฝ่ายเทคโนโลยีสารสนเทศในการปลดล็อคในการเข้าใช้งานและเพื่อตรวจสอบและหาสาเหตุที่แท้จริง
- บริษัทกำหนดค่ามาตรฐานในการบริหารจัดการและการกำหนดค่ารหัสผ่านการใช้งานสำหรับ ผู้ใช้งานอย่างชัดเจน โดยมีมาตรฐานการกำหนดค่ารหัสผ่าน ดังนี้
  - ความยาวของรหัสต้องมี 6 ตัวเลข
  - ประกอบด้วยตัวเลข
  - ไม่สามารถกำหนดค่ารหัสผ่านซ้ำเดิมที่เคยใช้ในระยะเวลา 1 เดือน
- บริษัทกำหนดให้รหัสผ่านมีอายุการใช้งาน 60 วัน โดยผู้ใช้งานจะได้รับการแจ้งเตือนรหัสผ่านหมดอายุและการเปลี่ยนรหัสผ่านล่วงหน้า 7 วัน และ จะได้รับการแจ้งเตือนเป็นประจำทุกวันจนกว่าจะเปลี่ยนรหัสผ่านใหม่บนหน้าระบบ POS หากผู้ใช้งานไม่เปลี่ยนรหัสผ่านบัญชี ผู้ใช้งานจะถูกจำกัดการเข้าถึง (Lock) โดยอัตโนมัติ และต้องแจ้งผู้ดูแลระบบเพื่อดำเนินการแก้ไขหรือปลด Lock และเปลี่ยนรหัสผ่านเพื่อใช้งาน
- บริษัทกำหนดให้ผู้ใช้งานต้องใส่รายละเอียดชื่อผู้ใช้งานและรหัสผ่าน (Username and Password) ทุกครั้งที่ใช้งานระบบ POS และผู้ใช้งานต้องออกจากระบบ (Log out) ทุกครั้งหลังจากการใช้งาน และไม่อนุญาตให้เลือกใช้งานประเภทการจำรหัสผ่าน (Remember password) เพื่อป้องกันการนำชื่อผู้ใช้งานและรหัสผ่านไปใช้ในทางที่ไม่เหมาะสม

พนักงานฝ่ายเทคโนโลยีสารสนเทศบันทึกการเข้าสู่ระบบทุกครั้งที่มีการ Log in ทั้งที่ประสบความสำเร็จและล้มเหลว เพื่อเป็นข้อมูลสำหรับการตรวจสอบหากจำเป็น

3.3 การเข้าถึงข้อมูลระยะไกล

3.3.1 บริษัทอนุญาตให้พนักงานในองค์กร ที่จำเป็นต้องปฏิบัติงานจากภายนอกองค์กรในกรณีที่จำเป็น โดยปฏิบัติตามวิธีปฏิบัติงานเรื่อง การรักษาความปลอดภัยด้านข้อมูล (GITC-DTS-04) และวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (GITC-ASC-01) เพื่อให้มีการตรวจพิสูจน์ตัวตนและควบคุมการทำงาน จากระยะไกลโดยการแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในองค์กร และใช้งานเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) โดยมีขั้นตอน ดังนี้

พนักงานบริษัทต้องบันทึกแบบฟอร์มการขอเข้าถึงข้อมูลระยะไกล (VPN Request Form) ผ่านระบบ F1 ผู้บังคับบัญชาแต่ละสายงานพิจารณาตรวจสอบและอนุมัติการขอเข้าถึงข้อมูลระยะไกล และลงนามอนุมัติในแบบฟอร์มการขอเข้าถึงข้อมูลระยะไกล (VPN Request Form) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาตรวจสอบและอนุมัติการขอเข้าถึงข้อมูลระยะไกล และลงนามอนุมัติในแบบฟอร์มการขอเข้าถึงข้อมูลระยะไกล (VPN Request Form) และเปิดสิทธิ์ในการเข้าถึงข้อมูลระยะไกล และพนักงานฝ่ายเทคโนโลยีสารสนเทศบันทึกรายการใช้งานการเข้าถึงข้อมูลระยะไกล (VPN Usage Log)

กรณีที่ไม่ใช่พนักงานในองค์กร จะต้องปฏิบัติตามขั้นตอน ดังนี้

- ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอ เพื่อขอใช้สิทธิ์ในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ
- แผนกเทคโนโลยีสารสนเทศ เป็นผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote access)
- ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากหัวหน้าแผนกเทคโนโลยีสารสนเทศ และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบ และข้อมูลอย่างเคร่งครัด

- ผู้ดูแลระบบต้องควบคุมพอร์ต (Port) ที่ระบบเทคโนโลยีสารสนเทศเทศให้บริการ ใช้ในการเข้าสู่ระบบ อย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการ อนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น
- การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของ ความจำเป็นเท่านั้น และให้ปิด Port และ Modem เมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

โดยผู้ใช้งานภายนอกองค์กร ต้องทำการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก โดยมีแนวทางปฏิบัติดังนี้

- การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)
- การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)
- การเข้าสู่ระบบสารสนเทศของนั้น จะต้องมีการตรวจสอบผู้ใช้งาน
- การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการ ตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส

3.3.2 บริษัทอนุญาตให้เจ้าหน้าที่ IT ทำการ Remote Support โดยใช้ Program Anydesk ที่ทางบริษัท ทำการจัดซื้อลิขสิทธิ์ไว้ เพื่อความรวดเร็วในการให้บริการ โดยมีขั้นตอนดังนี้

- เจ้าหน้าที่ IT ทำการ Install Anydesk ที่เครื่อง Client ทุกสาขา โดยกำหนดรหัสผ่านตามมาตรฐาน SP800-63-3 ให้มีความยาวตั้งแต่ 8 ตัวอักษรขึ้นไป มีส่วนประกอบของอักขระภาษาอังกฤษตัวพิมใหญ่ ตัวพิมเล็ก ตัวเลข และอักขระพิเศษ
- เจ้าหน้าที่ IT ทำการบันทึก Host และรหัสผ่านใน Program Anydesk
- เจ้าหน้าที่ IT จะ Remote ผ่าน Program Anydesk หลังจากได้รับการแจ้งปัญหาทาง Ticket ในระบบ F1 เท่านั้น

3.4 การใช้งานอุปกรณ์คอมพิวเตอร์ส่วนตัว, อุปกรณ์พกพา และอุปกรณ์ส่วนตัวในสำนักงาน

3.4.1 การใช้งานอุปกรณ์พกพา

- ผู้ใช้งานต้องปฏิบัติตาม ประกาศบันทึกข้อความ (MEMO) ฉบับที่ IT-20231010001/2566 “ประกาศห้ามใช้งานอุปกรณ์ , Email ส่วนตัว และ การกำหนดรหัสในการเข้าถึงข้อมูล” ว่าด้วยเรื่องของการห้ามใช้งานอุปกรณ์พกพาและอุปกรณ์ส่วนตัวในสำนักงาน,เรื่องของการกำหนดรหัสในการเข้าถึงข้อมูล ขององค์กรอย่างเคร่งครัด ซึ่งหมายรวมถึงอุปกรณ์คอมพิวเตอร์พกพาใดๆ ที่ใช้ในการ เชื่อมต่อเข้าสู่ระบบเครือข่าย และ/หรือ ที่ใช้ในการเก็บรักษาข้อมูลขององค์กร อันได้แก่
  - อุปกรณ์มือถือ (ออแกไนเซอร์ส่วนตัว พีดีเอ พ๊อคเก็ตพีซี เป็นต้น)
  - สมาร์ทโฟน โทรศัพท์เคลื่อนที่ และ แท็บเล็ตพีซี

3.4.2 การปฏิบัติงานจากภายนอกองค์กร

- พนักงานต้องหลีกเลี่ยงการปฏิบัติงานจากภายนอกองค์กร (Teleworking หรือ Telecommuting) ไม่ว่าการปฏิบัติงานนั้นจะกระทำโดยใช้อุปกรณ์คอมพิวเตอร์ขององค์กร หรืออุปกรณ์คอมพิวเตอร์ ส่วนตัว เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้น
- เข้ารหัสข้อมูลที่ถูกนำไปใช้ในการปฏิบัติงานนอกสถานที่ หรือการปฏิบัติงานจากภายนอกองค์กร ตาม Encryption Standard ขององค์กร
- พนักงานที่ได้รับอนุญาตให้ปฏิบัติงานจากภายนอกองค์กร ต้องใช้ความระมัดระวังมากเป็นพิเศษ เพื่อ ปกป้องอุปกรณ์คอมพิวเตอร์พกพา รวมถึงข้อมูลที่อยู่ในอุปกรณ์เหล่านั้นมิให้ถูกล่วงละเมิดโดยบุคคล ที่ไม่ได้รับอนุญาต ซึ่งรวมถึงสมาชิกในครอบครัวของพนักงานด้วย
- พนักงานต้องได้รับการฝึกอบรม หรือได้รับคำแนะนำอย่างเหมาะสมเกี่ยวกับการเข้าถึงระบบจากระยะไกล และการปกป้องข้อมูลที่ถูกใช้งาน หรือถูกเก็บรักษาอยู่ภายนอกสถานที่อันเนื่องมาจากการ ปฏิบัติงานจากภายนอกองค์กร
- สถานที่ปฏิบัติงานจากภายนอกองค์กรต้องมีความปลอดภัยทางด้านกายภาพทั้งในส่วนของตัวอาคาร และสภาพแวดล้อม

- การสื่อสารระหว่างสถานที่ในการปฏิบัติงานจากภายนอกองค์กร กับองค์กรอื่นๆ ต้องเป็นไปอย่างมั่นคง ปลอดภัย
- เปิดการใช้งาน Virtual Desktop ในการปฏิบัติงานจากภายนอกองค์กร เพื่อป้องกันข้อมูลที่ถูกเก็บบน เครื่องรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต
- การปฏิบัติงานจากภายนอกองค์กร พนักงานต้องป้องกันการเข้าถึงข้อมูลของทางองค์กรจากบุคคลที่ไม่เกี่ยวข้อง เช่น เพื่อน หรือ บุคคลในครอบครัว
- การใช้งานเครือข่ายไร้สายที่บ้านของพนักงาน ต้องเป็นไปอย่างมั่นคงปลอดภัย โดยต้องมีการเข้ารหัส สัญญาณ และป้องกันการเข้าถึงจากบุคคลที่ไม่เกี่ยวข้อง (การเข้ารหัสของ Wi-fi ขั้นต่ำเป็น WPA2)
- งานที่พนักงานทำให้องค์กร จากระยะไกลในอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานจะถือว่าเป็น ทรัพย์สินทางปัญญาขององค์กร
- อุปกรณ์คอมพิวเตอร์ที่นำออกไปใช้งานนอกองค์กร จำเป็นที่จะต้องมีการระบุสถานที่ Geolocation เพื่อการระบุพิกัด สถานที่ ประเทศที่ไม่เป็นสถานที่ต้องสงสัยว่าจะมีการโจมตีทางไซเบอร์มายังองค์กร และเป็นการระบุสถานที่ที่ใช้งานอุปกรณ์นั้นๆ

3.4.3 การใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน

- เทคโนโลยีสารสนเทศมีสิทธิ์ในการปฏิเสธการเข้าใช้งานจากอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในการเข้าถึงข้อมูลและระบบของทางองค์กร หากองค์กร พบว่าอุปกรณ์ดังกล่าวอาจก่อให้เกิด ความเสี่ยงต่อข้อมูล, ระบบ, พนักงาน และองค์กร
- เทคโนโลยีสารสนเทศมีสิทธิ์ในการติดตั้งโปรแกรมทำลายข้อมูล (Self-Destruct) บนอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานที่นำมาใช้ปฏิบัติงาน โดยองค์กร อาจจะมีการสั่งลบข้อมูลบนอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในกรณีที่เกิดเหตุการณ์ที่ทำให้เกิดการรั่วไหลหรือความไม่ปลอดภัยของข้อมูล
- องค์กรมีสิทธิ์ที่จะตรวจสอบอุปกรณ์คอมพิวเตอร์ส่วนตัวที่มีการใช้งานกับ Infrastructure ของทางองค์กร หากพนักงานปฏิเสธการตรวจสอบ ทางองค์กรจะทำการยกเลิกสิทธิ์ในการเข้าถึง รวมทั้ง User ID และ Password ของพนักงาน
- อุปกรณ์คอมพิวเตอร์ส่วนตัวทั้งหมดที่เข้าถึงเครือข่ายขององค์กรจะสามารถถูกตรวจสอบโดยองค์กรได้ ว่าได้รับอนุญาตจากทางองค์กร แล้วหรือไม่ หากองค์กรพบว่าเป็นอุปกรณ์คอมพิวเตอร์ส่วนตัวที่ไม่ได้ รับอนุญาตและพยายามที่จะเข้าถึงเครือข่ายของทางองค์กรจะถูกปฏิเสธการเข้าถึงทันที
- อุปกรณ์คอมพิวเตอร์ส่วนตัวจะสามารถเข้าถึงเครือข่ายและข้อมูลของทางองค์กร โดยการใช้งานผ่าน SSL/TLS VPN โดยข้อมูลการเข้าถึง SSL/TLS VPN Portal ขององค์กรจะถูกส่งให้พนักงานเมื่อได้รับ อนุญาตจากแผนกเทคโนโลยีสารสนเทศ
- พนักงานที่ใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงานต้องปฏิบัติตาม ประกาศบันทึกข้อความ (MEMO) ฉบับที่ IT-20231010001/2566 ขององค์กร อย่างเคร่งครัด
- ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบายเงื่อนไขข้อตกลงตามเอกสารฉบับนี้ แม้ว่าการฝ่าฝืนนั้นจะกระทำ ไม่เสร็จโดยสมบูรณ์ก็ให้ถือว่ามีความผิดโดยสมบูรณ์
- ผู้กระทำความผิดเกี่ยวกับ กฎ ระเบียบ เงื่อนไข หรือนโยบายขององค์กร ครั้งที่ 1 ให้ลงโทษ ผู้กระทำผิดตามระเบียบของบริษัท โดยการว่ากล่าวตักเตือนด้วยวาจา
- ผู้กระทำความผิดเกี่ยวกับ กฎ ระเบียบ เงื่อนไข หรือนโยบายขององค์กร ครั้งที่ 3 ให้ลงโทษ ผู้กระทำผิดตามระเบียบของบริษัท โดยตักเตือนเป็นลายลักษณ์อักษร
- ผู้กระทำความผิดเกี่ยวกับ กฎ ระเบียบ เงื่อนไข หรือนโยบายขององค์กร ครั้งที่ 2 ให้ลงโทษ ผู้กระทำผิดตามระเบียบของบริษัท โดยอาจจะทำการ Block อุปกรณ์ Computer ออกจากระบบ

4. การควบคุมการเข้าถึง (Access Control)

4.1 การควบคุมการเข้าถึงระบบงานของบริษัท

บริษัทกำหนดการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาตในระบบต่างๆ ของบริษัท โดยพนักงานที่ต้องการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ เพิ่มเติม ให้ดำเนินการอ้างอิงนโยบาย GITC-ACS-01 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทจากบุคคลภายนอก

บริษัทกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศต่างๆ ตามความเหมาะสมของบทบาท หน้าที่ และความรับผิดชอบในการปฏิบัติงาน (Privilege access level) และมีการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) อย่างเหมาะสม เพื่อป้องกันไม่ให้พนักงานคนใดคนหนึ่งได้รับสิทธิ์เกินกว่าบทบาท หน้าที่ และความรับผิดชอบอย่างไม่เหมาะสมบริษัทกำหนดตารางควบคุมสิทธิ์ (Access Authorization Matrix) เพื่อจำกัดให้พนักงานได้เข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศสอบทานและทบทวนตารางควบคุมสิทธิ์ (Access Authorization Matrix) เป็นประจำอย่างน้อยปีละ 1 ครั้ง

พนักงานฝ่ายเทคโนโลยีสารสนเทศบันทึกรายการ (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศทุกครั้งที่มีการใช้งาน

บริษัทจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจสอบการละเมิดความปลอดภัยที่มีต่อข้อมูล/สารสนเทศ

บริษัทจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ รวมถึงการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

4.2 การบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน

- พนักงานแต่ละคนมีชื่อผู้ใช้งานและรหัสผ่าน (Username and Password) ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัทเป็นของตนเอง และมีความรับผิดชอบในการป้องกันและเก็บรักษาชื่อผู้ใช้งานและรหัสผ่าน(Username and Password) ไว้เป็นความลับ โดยผู้ใช้งานควรออกจากระบบ (Log out) ทันทีเมื่อใช้งานเสร็จหรือไม่มีความจำเป็นที่ต้องใช้งานอีก โดยถ้าไม่ได้ใช้งานระบบจะ Log out โดยอัตโนมัติภายในเวลา 15 นาที
- พนักงานต้องปฏิบัติตามนโยบายการกำหนดรหัสในการเข้าถึงข้อมูล (Cryptography) ในข้อ 2.2
- พนักงานฝ่ายเทคโนโลยีสารสนเทศต้องบริหารจัดการและกำกับดูแลการเพิ่ม แก้ไข เปลี่ยนแปลง เพิกถอน หรือยกเลิกสิทธิ์การใช้งานของพนักงานอย่างเหมาะสมเมื่อมีการเปลี่ยนแปลง และพนักงานฝ่ายเทคโนโลยีสารสนเทศต้องเก็บบันทึกรายละเอียดผู้ใช้งานทั้งหมดในระบบเทคโนโลยีสารสนเทศของบริษัท และทบทวนหรือปรับปรุงให้ทันสมัยอยู่ตลอดเวลา
- บริษัทไม่อนุญาตให้ใช้ชื่อผู้ใช้งานและรหัสผ่าน (Username and Password) ลักษณะร่วมกัน (Shared Username and Password) ยกเว้น ผู้ใช้งานและรหัสผ่าน ที่บริษัทกำหนดไว้สำหรับการใช้งานร่วมกันเพื่อความสะดวกในการทำงาน เช่น ผู้ใช้งานและรหัสผ่าน ในการสร้างใบสั่งซื้อ ซึ่งจะมอบให้กับแต่ละแผนก (แตกต่างกัน) เพื่อให้พนักงานในแผนกสามารถที่จะใช้ในการสร้างใบสั่งซื้อ ผู้ใช้งานและรหัสผ่านที่ใช้ร่วมกันนี้ จะถูกตรวจสอบการทำรายการจากผู้จัดการ และหากมีความเสียหายเกิดขึ้นผู้จัดการแผนก และพนักงานในแผนกนั้นจะต้องรับผิดชอบความเสียหายร่วมกัน

  4.2.1 ผู้ใช้งานและรหัสผ่าน ที่มีลักษณะการใช้งานร่วมกัน (Shared Username and Password) แบ่งออกเป็น 2 ประเภท คือ Application Shared และ Active Directory Shared ซึ่งทั้ง 2 ประเภทนี้จัดทำขึ้นเพื่ออำนวยความสะดวกให้กับกลุ่มพนักงาน เช่น พนักงานของแต่ละแผนก พนักงานของแต่ละฝ่าย หรือพนักงานของแต่ละสาขา ให้สามารถเข้าถึงและใช้งานระบบในฐานะตัวแทนของแต่ละกลุ่มพนักงาน ในระดับ Application Shared จะเป็นการทำรายการ Request ต่าง ๆ เช่น การสั่งซื้อ, การแจ้งเรื่อง ซึ่งจะต้องมีผู้บริหารระดับสูงขึ้นไปอนุมัติ ในระดับ Active Directory Shared จะมีไว้เพื่อการ Login เข้าใช้งานโปรแกรมต่าง ๆ ภายในเครื่อง ซึ่งโปรแกรมเหล่านั้นจะมีการควบคุมการเข้าถึงด้วย User และ Password เฉพาะอีกชั้นเพื่อเป็นการยืนยันตัวตน

4.2.2 ขั้นตอนปฏิบัติ (Work instruction for Shared Username and Password) ในการควบคุมผู้ใช้งานและรหัสผ่าน ที่มีลักษณะการใช้งานร่วมกัน เป็นดังนี้

- ผู้จัดการแผนก สื่อสารกับพนักงานที่ใช้งาน Shared Username และ Password ให้ทราบว่า จะมีการเปลี่ยนรหัสผ่านเป็นประจำทุก ๆ 90 วัน และให้พนักงานจดจำรหัสผ่านใหม่ พร้อมทั้งห้ามแสดงรหัสผ่านใหม่ให้ผู้อื่นทราบ และถือเป็นความลับของแผนก
- กรณีที่พนักงานในแผนกลาออก ให้ผู้จัดการแผนกพิจารณาตามความเหมาะสมว่าจะให้คงรหัสผ่านจนกว่าจะถึงรอบการเปลี่ยนรหัสผ่าน หรือจะขอเปลี่ยนรหัสผ่านเลยเพื่อความปลอดภัย หากต้องการเปลี่ยนรหัสผ่านให้ติดต่อฝ่ายเทคโนโลยีสารสนเทศ เพื่อทำการขอรหัสผ่านใหม่

4.3 การควบคุมการเข้าถึงระบบของผู้ดูแลระบบหรือผู้ใช้งานที่มีสิทธิ์พิเศษ

ผู้ใช้งานที่เป็นผู้ดูแลระบบ (System Administrator) หรือผู้ใช้งานที่มีสิทธิ์พิเศษ (Super User or Privileged Access) ต้องได้รับการอนุมัติให้ใช้งานตามความจำเป็นเท่านั้น และให้มีจำนวนน้อยที่สุด

ผู้ใช้งานที่มีสิทธิ์ (Super User or Privileged Access) ในการเข้าสู่ระบบ Active Directory ของระบบเครื่องคิดเงินสำหรับสาขา จะมีสิทธิ์ในการ Login เข้าสู่ระบบได้ไม่เกิน 20 เครื่องต่อ 1 user

การขอสร้าง เปลี่ยนแปลง แก้ไข หรือยกเลิกสิทธิ์ที่เป็นผู้ดูแลระบบ (System Administrator) หรือผู้ใช้งานที่มีสิทธิ์พิเศษ (Super User or Privileged Access) ต้องได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และผู้บริหารที่กำกับดูแลฝ่ายงานเทคโนโลยีสารสนเทศเท่านั้น

การขอเปลี่ยนแปลงระบบ (Change Request) ที่จะต้องใช้สิทธิ์สูงสุด (Super Admin) ในการจัดการระบบต่างๆ ทุกระบบจะต้องมีเอกสารสรุปเนื้อหาความต้องการการเปลี่ยนแปลงระบบ รวมถึงผู้จัดการแผนกเทคโนโลยีสารสนเทศจะต้องทำการขออนุมัติ และ ได้รับการอนุมัติจากผู้บริหารที่กำกับดูแลฝ่ายงานเทคโนโลยีสารสนเทศเท่านั้น

เมื่อดำเนินการปรับปรุงระบบตามความต้องการแล้ว จะต้องทำการเปลี่ยนรหัสผ่านโดยใช้มารตฐานรหัสที่ได้ประกาศไว้ในเอกสาร โดยผู้ที่เปลี่ยนรหัสผ่านจะต้องเป็นผู้บริหารที่กำกับดูแลฝ่ายงานเทคโนโลยีสารสนเทศเท่านั้น และทำการจัดเก็บเป็นความลับในสถานที่ปิดเช่นเดิม

ผู้จัดการแผนกเทคโนโลยีสารสนเทศบันทึกรายการ (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศทุกครั้งที่มีการใช้งาน

ผู้ดูแลระบบกำหนดการควบคุมการเข้าถึง Source Code ของระบบเทคโนโลยีสารสนเทศที่ใช้ปฏิบัติงานจริง เช่น ไม่จัดเก็บ Source Code ไว้ในเครื่องที่ใช้งาน และจัดเก็บไว้ในสถานที่ที่ปลอดภัย หรือไม่นำข้อมูล Source Code ที่ใช้ปฏิบัติงานจริงปะปนกับข้อมูล Source Code ที่อยู่ระหว่างการทดสอบ เป็นต้น

4.4 การควบคุมการเข้าถึงระบบของบุคคลภายนอก

บุคคลภายนอกที่ประสงค์จะเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทต้องเข้าใจและปฏิบัติตามนโยบายฉบับนี้และมาตรการอื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งครัด

- บุคคลภายนอกบันทึกแบบฟอร์มการขอเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท (System Access Request Form) พร้อมระบุเหตุผลและขอบเขตของการเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลที่ต้องการ และจัดส่งให้ผู้บังคับบัญชาของฝ่ายงานที่เกี่ยวข้อง
- ผู้บังคับบัญชาฝ่ายงานพิจารณาตรวจสอบและอนุมัติการขอเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท (System Access Request Form) และลงนามอนุมัติในแบบฟอร์มการขอเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท(System Access Request Form)

- ผู้บังคับบัญชาฝ่ายงานแจ้งบุคคลภายนอกถึงนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและมาตรการอื่นๆ ที่เกี่ยวข้อง และให้บุคคลภายนอกลงนามรับทราบและถือปฏิบัติตามนโยบายดังกล่าวอย่างเป็นลายลักษณ์อักษร
- ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาตรวจสอบและอนุมัติการขอเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท (System Access Request Form) และลงนามอนุมัติในแบบฟอร์มการขอเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท (System Access Request Form)
- ผู้ดูแลระบบสร้างชื่อผู้ใช้และรหัสผ่าน (Username and Password) สำหรับบุคคลภายนอก โดยจำกัดการเข้าถึงระบบเทคโนโลยีสารสนเทศตามความจำเป็นในการปฏิบัติงานและความเหมาะสมเท่านั้น โดยกำหนดอายุการใช้งานตามกรอบเวลาในสัญญาจ้าง หรือเมื่อสิ้นสุดการปฏิบัติงาน โดยหน่วยงานที่เกี่ยวข้องมีหน้าที่และความรับผิดชอบในการแจ้งผู้ดูแลระบบเพื่อยกเลิกสิทธิ์ของบุคคลภายนอกทันทีเมื่อสิ้นสุดการปฏิบัติงานหรือไม่มีความจำเป็นในการใช้งาน

4.5 การควบคุมการเข้าถึงเครือข่าย

บริษัทควบคุมการเข้าถึงเครือข่าย โดยอุปกรณ์หรืออุปกรณ์เครือข่ายต่างๆ ต้องได้รับการตั้งค่าความปลอดภัยตามมาตรฐานก่อนที่จะเชื่อมต่อกับระบบเครือข่ายของบริษัท เพื่อรักษาความปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ ดังนี้

4.5.1 การเข้าถึงเครือข่าย

บริษัทกำหนดสิทธิ์การเข้าถึงเครือข่ายโดยผู้ใช้งานต้องมีชื่อผู้ใช้งานและรหัสผ่านตามที่กำหนด หากไม่มี ผู้ใช้งานจะไม่สามารถเข้าถึงเครือข่ายของบริษัทได้

บริษัทจัดให้มีระบบเครือข่ายที่มีความปลอดภัย มั่นคง และสามารถบริหารจัดการได้อย่างมีประสิทธิ์ภาพ

พนักงานฝ่ายเทคโนโลยีสารสนเทศตรวจสอบการเข้าถึงเครือข่ายของบริษัทโดยไม่ได้รับอนุญาตอย่างสม่ำเสมอ เพื่อตรวจสอบและป้องกันความปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้มีระบบตรวจสอบและป้องกันการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย

บริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัยเป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (physical disconnect) และจุดเชื่อมต่อ (disable port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่ายออกจากระบบเครือข่ายโดยสิ้นเชิง

4.5.2 การใช้เครือข่ายอินเทอร์เน็ต

การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตของบริษัท ผู้ขอใช้งานต้องกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับฝ่ายเทคโนโลยีสารสนเทศ โดยผู้ใช้งานต้องเป็นพนักงานของบริษัทเท่านั้น

ทางบริษัท ปลูกผักเพราะรักแม่ จำกัด (มหาชน) (องค์กร) ไม่อนุญาตให้บุคคลภายนอก ลงทะเบียนใช้เครือข่ายอินเทอร์เน็ตของภายในองค์กร หากต้องการที่จะใช้เครือข่ายอินเทอร์เน็ตของบริษัทสำหรับบุคคลภายนอก จะต้องได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

ไม่อนุญาตให้ใช้ระบบเครือข่ายอินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงพาณิชย์ส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน เป็นต้น

ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้นทั้งหมด

ไม่อนุญาตให้พนักงานเปิดเผยข้อมูลที่สำคัญและเป็นความลับของบริษัท ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัท หรือการทำลายความสัมพันธ์กับบุคลากรของฝ่ายงานอื่นๆ

ไม่อนุญาตให้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทหรือฝ่ายงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

ไม่อนุญาตให้พนักงาน Download หรือ Update ซอฟต์แวร์จากระบบอินเทอร์เน็ต ไม่ว่ากรณีใดก็ตาม รวมถึงไม่อนุญาตให้พนักงาน Download รูปภาพ หรือข้อมูลใดๆ ที่จะนำไปสู่ความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

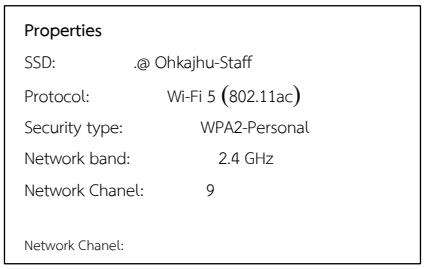
ความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ความเสี่ยงต่อการนำเข้า Malware หรือชุดคำสั่งไม่พึงประสงค์ ข้อมูล รูปภาพ ที่ไม่เกี่ยวข้องกับกิจการขององค์กร

ไม่อนุญาตให้พนักงาน Upload รูปภาพ ข้อมูลใดๆ บน Portal ขององค์กร หรือการตั้งกระทู้ส่งต่อรูปภาพ/ข้อความบนPortal ภายนอกองค์กรที่จะนำไปสู่ความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562ความเสี่ยงต่อการนำเข้า Malware หรือชุดคำสั่งไม่พึงประสงค์ ข้อมูล รูปภาพ ที่ไม่เกี่ยวข้องกับกิจการขององค์กร

4.5.3 การบริหารจัดการข้อมูลผ่านเครือข่ายอินเทอร์เน็ตการรับส่งข้อมูลสำคัญของบริษัทผ่านอีเมลต้องมีการกำหนดรหัสเสมอ

การรับส่งข้อมูลสำคัญหรือไฟล์ข้อมูลผ่านเครือข่ายอินเทอร์เน็ต ข้อมูลจะต้องได้รับการเข้ารหัสเสมอ เช่น Secure FTP, VPN หรือ SSL เป็นต้น

- การรับส่งข้อมูลแบบไร้สาย (W-Fi) จากอุปกรณ์พกพาหรือเครือข่ายภายในองค์กรต้องมีการเข้ารหัสเสมอ โดยใช้การเข้ารหัสแบบ WPA2 หรือแบบที่มีความปลอดภัยสูงสุด



การเข้าถึงข้อมูลของบริษัทผ่านเครือข่ายสาธารณะ (Public Network) จากอุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการเข้ารหัสเสมอ

4.5.4 การดูแลระบบเครือข่ายและคอมพิวเตอร์

บริษัทวางแผนและจัดระบบความปลอดภัยในระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายและอุปกรณ์ต่อพ่วงกับระบบเครือข่าย ได้แก่ Firewall, Anti-Virus, Ani- Spam, Virtual Private Network (VPN) ฝ่ายเทคโนโลยีสารสนเทศควบคุม ดูแลบำรุงรักษาปฏิบัติงานเกี่ยวกับการรักษาความปลอดภัยทางข้อมูล(Information Security) ซึ่งจะต้องทำการศึกษาถึงความไม่ปลอดภัยในการใช้งานสารสนเทศที่เกี่ยวข้องกับคอมพิวเตอร์และปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอฝ่ายเทคโนโลยีสารสนเทศควบคุม ดูแล ความมั่นคงปลอดภัยทางด้านระบบโปรแกรมประยุกต์ รวมถึงระบบอื่นๆ ขององค์กร และสิทธิ์การเข้าใช้งานระบบฝ่ายเทคโนโลยีสารสนเทศควบคุม ดูแล ความมั่นคงปลอดภัยทางด้านระบบจดหมายอิเล็กทรอนิกส์ (อีเมล) และสิทธิ์การเข้าใช้งานระบบ

กรณีพบความผิดปกติเกิดขึ้นในระบบ ผู้ดูแลระบบเครือข่ายและระบบคอมพิวเตอร์มีอำนาจระงับการใช้เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเพื่อป้องกันความเสียหายได้ ตามอำนาจที่กำหนดไว้

พนักงานฝ่ายเทคโนโลยีสารสนเทศไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิ์ในการเข้าถึงข้อมูลนั้น และต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

ฝ่ายเทคโนโลยีสารสนเทศจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) โดยถือปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ควบคุมดูแลซอฟต์แวร์ และโปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนของพนักงานให้ถูกต้องตามลิขสิทธิ์ของซอฟต์แวร์หรือโปรแกรมที่ติดตั้งอยู่ฝ่ายเทคโนโลยีสารสนเทศวิเคราะห์ความเสี่ยง ประเด็นในแง่กฎหมาย จรรยาบรรณในเรื่อง “ความปลอดภัยในระบบคอมพิวเตอร์” ซึ่งเกี่ยวข้องกับบรรดาผู้ใช้งานคอมพิวเตอร์เพื่อวัตถุประสงค์ต่างๆ เช่น แฮกเกอร์ (Hacker) เป็นต้น

ฝ่ายเทคโนโลยีสารสนเทศจัดทำคู่มือการใช้งานระบบเครือข่ายและคอมพิวเตอร์ เพื่อเป็นแนวทางและวิธีปฏิบัติแก่ผู้ใช้งานระบบปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายตามที่ผู้บังคับบัญชามอบหมาย รักษาความปลอดภัยในคอมพิวเตอร์ส่วนบุคคล รักษาความปลอดภัยในระบบฐานข้อมูล รักษาความปลอดภัยในเครือข่ายการสื่อสารข้อมูลและการป้องกันทางกายภาพ และปิดโอกาสที่ระบบหรือโปรแกรมที่ใช้งานอาจเกิดจากความผิดพลาดหรือข้อบกพร่องจากการออกแบบระบบรวมถึงสาเหตุอื่นๆ ที่ทำให้เกิดการโจมตีระบบเทคโนโลยีสารสนเทศจากบุคคลภายนอกได้

4.5.5 การบริหารจัดการการใช้งานอีเมล

ผู้ใช้งานอีเมลของบริษัททุกคนต้องมีบัญชีอีเมล (Email Account) เป็นของตนเอง โดยใช้ Domain ของบริษัท เช่น xxx@ohkhajhu.com เป็นต้น บัญชีอีเมล (Email Account) ของทุกคนต้องได้รับการป้องกันด้วยรหัสผ่านตามข้อกำหนดรหัสผ่านที่บริษัทกำหนด

บัญชีอีเมล (Email Account) ที่มีวัตถุประสงค์พิเศษ เช่น บัญชีอีเมล- (Email Account) ส่วนกลางของฝ่ายงาน เป็นต้น อาจได้รับการสร้างขึ้น และต้องกำหนดพนักงานผู้รับผิดชอบเป็นเจ้าของบัญชีอีเมล (Email Account) นั้นๆ

บัญชีอีเมล (Email Account) รวมถึงอีเมลทุกฉบับ ที่ถูกสร้าง และเก็บรักษาอยู่ในอุปกรณ์คอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นสินทรัพย์ของบริษัท

ห้ามใช้บัญชีอีเมล (Email Account) ของบริษัท กระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือการกระทำการใดๆ ที่ส่งผลกระทบในทางลบต่อบริษัท เว้นแต่การดำเนินการดังกล่าวเกี่ยวข้องหรือเป็นส่วนหนึ่งของการดำเนินงานของบริษัท

ห้ามผู้ใช้งานบัญชีอีเมล (Email Account) ของบริษัทปลอมแปลงข้อความในอีเมล ลายเซ็น หรือข้อมูลอื่นๆ ของบัญชีอีเมล (Email Account) บุคคลอื่น

ผู้ใช้งานบัญชีอีเมล (Email Account) ต้องมิยอมให้บุคคลอื่นใช้งานบัญชีอีเมล (Email Account) ของตน โดยเด็ดขาด

ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากบุคคลที่ไม่รู้จัก

ผู้ใช้งานต้องแจ้งพนักงานฝ่ายเทคโนโลยีสารสนเทศโดยทันที หากได้รับข้อความเตือนจากโปรแกรม Ani-virus ว่าอุปกรณ์คอมพิวเตอร์มี Virus หรือ Malware ข้อกำหนดอื่นๆ ตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด

4.6 การจัดชั้นความลับ และการจัดการข้อมูล

บริษัทพิจารณากำหนดหลักเกณฑ์ในการจัดชั้นข้อมูล เนื่องจากข้อมูลของบริษัทมีความหลากหลายและมีความสำคัญและผลกระทบไม่เท่ากัน ทำให้บริษัทไม่สามารถกำหนดมาตรการหรือแนวทางรักษาความปลอดภัยได้เหมือนกันสำหรับข้อมูลทุกระดับชั้นข้อมูล และอาจทำให้การบริหารจัดการข้อมูลไม่มีประสิทธิภาพ บริษัทจึงมีความจำเป็นที่ต้องกำหนดมาตรการในการป้องกันข้อมูลที่มีความแตกต่างกันตามแต่ระดับชั้นข้อมูล ด้วยเหตุนี้ บริษัทจึงกำหนดชั้นข้อมูลของบริษัทเป็น 4 ระดับชั้นข้อมูล ดังนี้

ชั้นที่ 1 ข้อมูลที่สามารถเปิดเผยต่อสาธารณชนได้ (Public) หมายถึงข้อมูลที่สามารถเปิดเผยและเผยแพร่สู่สาธารณชนได้ผ่านช่องทางของบริษัท เช่น เว็บไซต์ของบริษัท รายงานประจำปี งบการเงิน เป็นต้น โดยเป็นการเปิดเผยเพื่อประโยชน์ของบริษัทหรือตามที่กำหนดโดยกฎหมาย กฎระเบียบ หรือข้อบังคับจากหน่วยงานกำกับดูแล

ชั้นที่ 2 ข้อมูลที่ใช้ภายในบริษัทเท่านั้น (Private or Internal Use) หมายถึงข้อมูลที่ใช้ภายในบริษัทเท่านั้น ซึ่งข้อมูลเหล่านี้ส่งผลกระทบต่อการปฏิบัติงานของบริษัท และอาจทำให้เกิดความเสียหายแก่บริษัทได้หากเปิดเผยออกสู่สาธารณชน เช่น ระเบียบนโยบาย คู่มือปฏิบัติงาน ประกาศต่างๆ เป็นต้น ข้อมูลเหล่านี้ต้องได้รับการป้องกันการเข้าถึงจากบุคคลภายนอก

ชั้นที่ 3 ข้อมูลที่เป็นความลับ (Confidential) หมายถึงข้อมูลที่เป็นความลับและเปิดเผยสำหรับกลุ่มคนเฉพาะกลุ่มเท่านั้นซึ่งกำหนดโดยฝ่ายงานเจ้าของข้อมูลและต้องได้รับการอนุญาตและอนุมัติโดยผู้บังคับบัญชาสูงสุดของฝ่ายงานเจ้าของข้อมูลอย่างเป็นลายลักษณ์อักษร ซึ่งข้อมูลเหล่านี้ส่งผลกระทบต่อธุรกิจอย่างมีนัยสำคัญ และหากเกิดการรั่วไหลของข้อมูลอาจนำไปสู่ความเสียหายที่มีนัยสำคัญต่อองค์กร เช่น ข้อมูลส่วนบุคคลของลูกค้า ข้อมูลส่วนบุคคลของพนักงานและผู้มีส่วนได้เสียขององค์กร แผนดำเนินธุรกิจ แผนการตลาด รายการอาหารใหม่ รายการโปรโมชั่นต่างๆ เป็นต้น ข้อมูลเหล่านี้ต้องได้รับการป้องกันการเข้าถึงจากบุคคลภายนอกและบุคคลภายในที่ไม่ได้รับอนุญาต หากต้องเปิดเผยข้อมูลเนื่องจากข้อกำหนดทางกฎหมาย ประธานพนักงานบริหาร (CEO) ลงนามอนุญาตอย่างเป็นลายลักษณ์อักษร เพื่อให้เปิดเผยข้อมูลชั้นที่ 3

ชั้นที่ 4 ข้อมูลที่เป็นความลับพิเศษ (Top Secret) หมายถึงข้อมูลที่เป็นความลับสูงสุดของกิจการ ซึ่งข้อมูลเหล่านี้จะถูกจำกัดการเข้าถึงเพียงแค่ผู้บริหารระดับสูงเท่านั้น เนื่องจากเป็นข้อมูลที่มีความสำคัญต่อการดำเนินธุรกิจ การตัดสินใจ หรือการกำหนดทิศทางของบริษัทในอนาคต ซึ่งข้อมูลเหล่านี้ถ้วนส่งผลต่อการดำเนินธุรกิจ และหากเกิดการรั่วไหลของข้อมูลอาจทำไปสู่การสูญเสียการแข่งขันทางธุรกิจหรือสูญเสียรายได้อย่างร้ายแรง เช่น แผนการขยายธุรกิจและแผนการลงทุนสูตรอาหาร ข้อมูลความลับทางการค้า แผนกลยุทธ์ เป็นต้น ข้อมูลเหล่านี้ต้องได้รับการป้องกันการเข้าถึงบุคคลต่างๆ อย่างสูงสุดทั้งบุคคลภายนอกและบุคคลภายในที่ไม่ได้รับอนุญาต หากต้องเปิดเผยข้อมูลเนื่องจากข้อกำหนดทางกฎหมายประธานกรรมการบริษัทต้องลงนามอย่างเป็นลายลักษณ์อักษร เพื่ออนุญาตให้เปิดเผยข้อมูลชั้นที่ 4 ทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศต้องสอบทาน ทบทวน และปรับปรุงความเหมาะสมของการกำหนดระดับชั้นความลับของข้อมูลอย่างน้อยปีละ 1 ครั้ง ในกรณีเกิดการรั่วไหลของข้อมูลสารสนเทศที่อยู่ในระดับความลับชั้นที่ 3 และ 4 ผู้บริหารกำหนดให้มีการแต่งตั้งคณะกรรมการสอบสวนเพื่อสอบสวนหาสาเหตุข้อผิดพลาด และแนวทางแก้ไขอย่างเหมาะสมนอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีแนวทางป้องกันการรั่วไหลของข้อมูลสารสนเทศอย่างเหมาะสม และรายงานให้ผู้บริหารทราบเป็นประจำบริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการจัดเก็บข้อมูลสารสนเทศตามระดับชั้นความลับที่กำหนดเพื่อความปลอดภัยของข้อมูล รวมถึงการจัดเก็บข้อมูลต่างๆ ในระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม ดังนี้

- กำหนดแนวปฏิบัติในการจัดเก็บข้อมูลตามระดับชั้นความลับ
- จัดเก็บข้อมูลสำรองในสื่อบันทึกข้อมูลและจัดทำรายงานการสำรองข้อมูลอย่างชัดเจน และจัดเก็บในที่ที่ปลอดภัยพร้อมกำหนดรหัสในการเข้าถึงข้อมูล
- กำหนดมาตรการรักษาความปลอดภัยทางกายภาพของระบบเทคโนโลยีสารสนเทศ และอุปกรณ์ในการบันทึกข้อมูลสำรองตรวจสอบข้อมูลที่จัดเก็บ รวมถึงข้อมูลสำรองเป็นประจำ
- ทบทวนสิทธิ์การเข้าถึงข้อมูลของแต่หละระบบเป็นประจำหรืออย่างน้อย ปี หละ 1 ครั้ง

4.7 การเข้าถึง Website ผ่าน Secure Socket Layer

องค์กรตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของเว็บไซต์ เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยของเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้นสูงด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัส ที่ระดับ 128 bits (128-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง ที่มีการใช้งานผ่านเครือข่ายอินเทอร์เน็ตขององค์กรทำให้ผู้ที่ดักจับข้อมูลระหว่างทาง ไม่สามารถนำข้อมูล

ไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล โดยผู้ใช้บริการสามารถสังเกตได้จากชื่อโปรโตคอลที่เป็น

1. https://www.ohkajhu.com

เทคโนโลยีเสริมที่นำมาใช้ในการรักษาความมั่นคงปลอดภัย องค์กรได้นำเทคโนโลยีระดับสูงดังต่อไปนี้ เพื่อปกป้องข้อมูลส่วนตัวของผู้ใช้งาน

- Firewall เป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ์หรือ ผู้ที่องค์กร อนุมัติเท่านั้นจึงจะผ่าน Firewall เพื่อเข้าถึงข้อมูลได้
- Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมี การติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิ์ภาพสูง และ Update อย่างสม่ำเสมอ
- Cookies เป็นไฟล์คอมพิวเตอร์เล็กๆ ที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็น ลงในเครื่องคอมพิวเตอร์ของผู้ใช้บริการ เพื่อความสะดวกและรวดเร็วใน การติดต่อสื่อสาร อย่างไรก็ตามองค์กร ตระหนักถึงความเป็นส่วนตัวของ ผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ถ้าหากมีความจำเป็น ต้องใช้ Cookies องค์กรจะพิจารณาอย่างรอบคอบ และตระหนักถึงความปลอดภัย และความเป็นส่วนตัวของผู้ใช้บริการเป็นหลัก

4.8 การใช้งานจดหมายอิเล็กทรอนิกส์

องค์กรตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของการใช้งานจดหมายอิเล็กทรอนิกส์ โดยใช้การเข้ารหัสที่เรียกว่า PGP หรือ Pretty Good Privacy เป็นวิธีการเข้ารหัสลับและถอดรหัสลับข้อมูล ซึ่งทำให้เกิดการรักษาความลับและความเป็นต้นฉบับของเอกสารเอาไว้ได้ในการติดต่อสื่อสารกัน ซึ่ง PGP ใช้หลักการ Public key และ Private key ในการเข้าและถอดรหัสเช่นเดียวกับ PKI แต่แตกต่างจาก PKI ที่ปล่อยหน้าที่การพิสูจน์ความน่าเชื่อถือ public key ไว้กับ user โดยการแลกเปลี่ยนระหว่างกัน ภายใน Web of Trust ในขณะที่ PKI จะใช้ CA เป็นบุคคลที่สามในการยืนยันความน่าเชื่อถือของ Public Key โดยในส่วนของ Email จะแสดงในรูปแบบของ xxx@ohkhajhu.com

5. การบริหารจัดการสินทรัพย์เทคโนโลยีสารสนเทศ

5.1 การบริหารจัดการบัญชีสินทรัพย์

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำและบันทึกข้อมูลสินทรัพย์ที่เกี่ยวข้องเทคโนโลยีสารสนเทศ และจัดทำทะเบียนสินทรัพย์เทคโนโลยีสารสนเทศ (Information Technology Asset Register) เช่น อุปกรณ์ Hardware, Software, CPU เป็นต้น นอกจากนี้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ควบคุมและจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศทั้งหมดของบริษัท เพื่อสนับสนุนการปฏิบัติงานของพนักงานหรือผู้ใช้งานตามที่ได้รับมอบหมาย

ฝ่ายเทคโนโลยีสารสนเทศต้องตรวจสอบสินทรัพย์ที่เกี่ยวข้องเทคโนโลยีสารสนเทศ (Asset Check) และการตรวจสอบการใช้งานอุปกรณ์คอมพิวเตอร์ (Preventive Maintenance: PM) เป็นประจำอย่างน้อยปีละ 1 ครั้ง และเปรียบเทียบกับข้อมูลสินทรัพย์ที่บันทึกในระบบ และปรับปรุงข้อมูลสินทรัพย์ในระบบและทะเบียนสินทรัพย์เทคโนโลยีสารสนเทศ (Information Technology Asset Register) ให้มีความเหมาะสม ทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่และความรับผิดชอบในการตรวจสอบสินทรัพย์ที่เกี่ยวข้องเทคโนโลยีสารสนเทศให้อยู่ในสภาพที่เรียบร้อยและพร้อมใช้งานอยู่เสมอตามที่กำหนดในมาตรฐานการใช้เครื่องคอมพิวเตอร์และซอฟต์แวร์

5.2 การถือครองสินทรัพย์

บริษัทกำหนดผู้มีหน้าที่รับผิดชอบในการรักษาข้อมูลและสินทรัพย์ ที่เกี่ยวข้อง เทคโนโลยีสารสนเทศของบริษัทอย่างชัดเจน หากมีการเปลี่ยนแปลงในสินทรัพย์ดังกล่าว ผู้รับผิดชอบต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศในฐานะผู้ควบคุมดูแลสินทรัพย์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของบริษัทเพื่อรับทราบและหาแนวทางแก้ไขทันที

5.3 การอนุญาตใช้สินทรัพย์

ฝ่ายเทคโนโลยีสารสนเทศจะจัดเตรียมอุปกรณ์คอมพิวเตอร์ รวมถึงซอฟต์แวร์ที่เกี่ยวข้อง เพื่อสนับสนุนการปฏิบัติงานให้แก่พนักงานแต่ละคนตามตำแหน่งงาน หน้าที่ ฝ่ายงาน และความเหมาะสมตามลักษณะการใช้งาน ซึ่งคุณสมบัติของสินทรัพย์อาจมีความแตกต่างกันไป

5.3.1 การขออนุญาตใช้สินทรัพย์ด้านเทคโนโลยีสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศ เตรียมอุปกรณ์คอมพิวเตอร์สำหรับพนักงานที่ได้รับสิทธิ์ให้ใช้งานโดยต้องผ่านการอนุมัติโดยผู้บังคับบัญชาสูงสุดของฝ่ายงานและเห็นชอบจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ซึ่งประเภทและรุ่นของอุปกรณ์คอมพิวเตอร์จะแตกต่างและจำแนกตามลักษณะการใช้งานตามเอกสารแนบ 1 ตารางสรุปประเภทและรุ่นอุปกรณ์คอมพิวเตอร์ตามลักษณะการใช้งาน หากกรณีพนักงานใหม่ที่ได้รับสิทธิ์ให้ใช้งาน พนักงานใหม่จัดทำแบบฟอร์มการขออนุญาตใช้อุปกรณ์ด้านเทคโนโลยีสารสนเทศ (IT Equipment Request Form (F1)) โดยต้องผ่านการอนุมัติโดยผู้บังคับบัญชาสูงสุดของฝ่ายงานและเห็นชอบจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

ในกรณีที่พนักงานซึ่งไม่ได้สิทธิ์การใช้งานอุปกรณ์คอมพิวเตอร์มีความจำเป็นที่จะต้องใช้งาน พนักงานบันทึกแบบฟอร์มการขออนุญาตใช้อุปกรณ์ด้านเทคโนโลยีสารสนเทศ (IT Equipment Request Form (F1)) และต้องได้รับการอนุมัติจากผู้บังคับบัญชาสูงสุดของสายงาน และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

ในกรณีที่พนักงานต้องการใช้อุปกรณ์คอมพิวเตอร์ที่มีคุณสมบัตินอกเหนือจากที่กำหนดในตารางสรุปประเภทและรุ่นอุปกรณ์คอมพิวเตอร์ตามลักษณะการใช้งาน พนักงานต้องจัดทำบันทึกข้อความ (Memo) พร้อมระบุเหตุผลและความจำเป็นและต้องได้รับการอนุมัติจากผู้บังคับบัญชาสูงสุดของสายงาน และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ทั้งนี้ การจัดซื้ออุปกรณ์คอมพิวเตอร์เพิ่มเติมต้องเป็นไปตามขั้นตอนที่กำหนดในนโยบาย OKJ-P2P-PUR การจัดการใบขอซื้อ

พนักงานที่ประสงค์จะขอยืมอุปกรณ์ด้านเทคโนโลยีสารสนเทศ จัดทำแบบฟอร์มการขอยืมอุปกรณ์ด้านเทคโนโลยีสารสนเทศ (IT Equipment Borrow Form (F1)) และจัดส่งให้ผู้บังคับบัญชาสูงสุดของฝ่ายงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาอนุมัติ

สำหรับอุปกรณ์คอมพิวเตอร์ Apple ฝ่ายงานที่รับผิดชอบสินทรัพย์ต้องจัดให้มีผลิตภัณฑ์ประกัน Apple Care ทุกครั้ง เนื่องจากค่าซ่อมแซมสินทรัพย์อาจมีมูลค่าสูง และเพื่อให้ได้รับความคุ้มครองการซ่อมและบริการช่วยเหลือจากศูนย์บริการทั้งทางซอฟต์แวร์และฮาร์ดแวร์ เนื่องจากเป็นอุปกรณ์เฉพาะทาง โดยพนักงานฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้ประสานงานส่งซ่อมและติดตามกรณีที่อุปกรณ์มีปัญหาเท่านั้น

อุปกรณ์คอมพิวเตอร์ของบริษัทต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์ใดๆ ทั้ง Hardware และ Software เพิ่มเติมก่อนได้รับการอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

บริษัทสามารถปรับปรุง เปลี่ยนแปลง หรือแก้ไขคุณสมบัติหรือรุ่นของอุปกรณ์คอมพิวเตอร์ต่างๆ ตามความเหมาะสมเพื่อให้รองรับการเปลี่ยนแปลง เทคโนโลยีแบบใหม่ หรือป้องกันความปลอดภัยทางเทคโนโลยีสารสนเทศ โดยต้องได้รับการอนุมัติจากผู้บริหารสูงสุดในสายงานเทคโนโลยีสารสนเทศ

5.3.2 การอนุญาตใช้สินทรัพย์ด้านซอฟต์แวร์ บริษัทกำหนดการควบคุมการใช้งานซอฟต์แวร์ต่างๆ เช่น โปรแกรม แอปพลิเคชัน ระบบต่างๆ เป็นต้น ที่ติดตั้งในอุปกรณ์คอมพิวเตอร์ของบริษัท ให้ถูกลิขสิทธิ์และจำเป็นต่อการปฏิบัติงานตามลักษณะงานแต่ละบุคคล

ซอฟต์แวร์ทั้งหมดที่ติดตั้งในอุปกรณ์คอมพิวเตอร์ของบริษัทหมายถึง ซอฟต์แวร์สำเร็จรูป (Package Software) ทั้งที่เป็นการซื้อและเช่าซื้อโปรแกรมแอปพลิเคชันระบบต่างๆ ที่บริษัทว่าจ้างให้บริษัทภายนอกจัดทำขึ้นเพื่อใช้งานเฉพาะด้าน หรือใช้งานร่วมกับโปรแกรม/แอปพลิเคชันระบบที่มีอยู่แล้ว เพื่อให้สนับสนุนการทำงานให้มีประสิทธิภาพมากยิ่งขึ้น

บริษัทมีสิทธิ์เต็มที่ในการพัฒนาซอฟต์แวร์สำหรับคอมพิวเตอร์ ไม่ว่าจะเป็นการพัฒนาด้วยตนเอง หรือว่าจ้างบริษัทภายนอกในการพัฒนาและการจัดซื้อซอฟต์แวร์ ซึ่งจะต้องดำเนินการตามขั้นตอนที่กำหนดไว้ในนโยบายการ

จัดซื้อของฝ่ายจัดซื้อ ทั้งนี้เอกสารที่เกี่ยวข้องกับการพัฒนาระบบทั้งหมด รวมถึงเอกสารการจัดซื้อจัดจ้าง ถือเป็นทรัพย์สินของบริษัท

บริษัทห้ามมิให้พนักงานคัดลอกซอฟต์แวร์ที่มีลิขสิทธิ์คุ้มครอง คัดลอกเนื้อหาที่มีลิขสิทธิ์คุ้มครอง เช่น ภาพยนตร์และเพลงที่มีลิขสิทธิ์ เป็นต้น เก็บไว้ในเครื่องคอมพิวเตอร์ในทุกกรณี

บริษัทห้ามมิให้พนักงานทำการติดตั้งหรือใช้ซอฟต์แวร์ที่มีลิขสิทธิ์คุ้มครอง โดยที่ทางบริษัทหรือพนักงานไม่ได้ดำเนินการจัดซื้ออย่างถูกกฎหมายและตามนโยบาย OKJ-P2P-PUR01 การจัดการใบขอซื้อ และ OKJ-P2P-PUOการจัดการใบสั่งซื้อ ของฝ่ายจัดซื้อที่กำหนดไว้

การติดตั้งซอฟต์แวร์พื้นฐาน ฟรีแวร์ หรือซอฟต์แวร์ที่จัดซื้อมาอย่างถูกต้องโดยบริษัท ต้องดำเนินการติดตั้งโดยพนักงานฝ่ายเทคโนโลยีสารสนเทศเท่านั้น รายละเอียดซอฟต์แวร์ตามเอกสารแนบ 2 ตารางสรุปรายชื่อและคุณสมบัติซอฟต์แวร์ สำหรับซอฟต์แวร์เสรีหรือฟรีแวร์ที่ได้รับอนุญาตใช้งาน ต้องเป็นซอฟต์แวร์ที่สามารถใช้งานได้ในระดับองค์กร และตรงตามมาตรฐาน GNU Privacy Guard ซึ่งเป็นสัญญาอนุญาตสำหรับซอฟต์แวร์เสรีหรือฟรีแวร์ที่ได้รับความนิยมสูงที่สุดในปัจจุบัน สำหรับผู้ใช้ซอฟต์แวร์ 4 ประการ ดังนี้

- เสรีภาพในการใช้งานซอฟต์แวร์ไม่ว่าใช้สำหรับจุดประสงค์ใด
- เสรีภาพในการศึกษาการทำงานของซอฟต์แวร์ และแก้ไขโค้ด การเข้าถึง Source Code
- เสรีภาพในการจำหน่ายแจกจ่ายซอฟต์แวร์
- เสรีภาพในการปรับปรุงและเปิดให้บุคคลทั่วไปใช้และพัฒนาต่อไป โดยมีเพียงเงื่อนไขว่า การนำไปใช้หรือนำไปพัฒนาต่อ จำเป็นต้องใช้สัญญาอนุญาตเดียวกัน

ในกรณีที่ฝ่ายงานใดสั่งซื้อซอฟต์แวร์อื่นๆเพิ่มเติม ฝ่ายงานนั้นต้องรับผิดชอบต่อการสั่งซื้อและงบประมาณในการสั่งซื้อตามนโยบายการจัดซื้อของฝ่ายจัดซื้อที่กำหนดไว้ และผู้รับผิดชอบสินทรัพย์หรือฝ่ายงานนั้นต้องรักษาไว้ซึ่งข้อมูลที่เกี่ยวกับการอนุญาตให้ใช้ซอฟต์แวร์ดังกล่าว หากมีการโอนสิทธิ์การใช้ซอฟต์แวร์ดังกล่าวให้บุคคลหรือฝ่ายงานอื่น บุคคลหรือฝ่ายงานผู้รับโอนต้องเป็นผู้รับผิดชอบแทน และต้องแจ้งข้อมูลในการโอนย้ายทุกครั้งให้แก่ฝ่ายเทคโนโลยีสารสนเทศ

ในกรณีที่พนักงานหรือฝ่ายงานใดไม่ปฏิบัติตามข้อกำหนดหรือนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พนักงานหรือฝ่ายงานอาจได้รับโทษทางวินัยตามที่ระบุในระเบียบหรือข้อบังคับของบริษัท รวมถึงการดำเนินการทางกฎหมายที่เกี่ยวข้อง (หากมี)

บริษัทสามารถปรับปรุง เปลี่ยนแปลง หรือแก้ไขคุณสมบัติหรือรุ่นของซอฟต์แวร์ต่างๆตามความเหมาะสม เพื่อให้รองรับการเปลี่ยนแปลง เทคโนโลยีแบบใหม่ หรือป้องกันความปลอดภัยทางเทคโนโลยีสารสนเทศ โดยต้องได้รับการอนุมัติจากผู้บริหารสูงสุดในสายงานเทคโนโลยีสารสนเทศ

การขอใช้ซอฟต์แวร์ลิขสิทธิ์ต่างๆ ต้องได้รับการพิจารณาและอนุมัติจากผู้บังคับบัญชาสูงสุดของแต่ละฝ่ายงาน และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ โดยฝ่ายงานต่างๆจะต้องเตรียมงบประมาณสำหรับค่าลิขสิทธิ์ในการใช้ซอฟต์แวร์นั้นๆ

5.4 การคืนสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

พนักงานของบริษัทต้องคืนสินทรัพย์ของบริษัททั้งหมดที่ตนเองถือครองเมื่อสิ้นสุดการเป็นพนักงาน หรือสิ้นสุดสัญญาจ้างตามขั้นตอนที่กำหนดในนโยบาย HRM-RES-01 การจัดการลาออกของพนักงาน เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ต่อพ่วงต่างๆ โทรศัพท์ กุญแจ บัตรผ่านเข้า - ออกสำนักงาน เป็นต้น โดยจัดทำแบบฟอร์มการคืนสินทรัพย์

ด้านเทคโนโลยีสารสนเทศ (IT Equipment Return Form) สำหรับอุปกรณ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศพนักงานฝ่ายเทคโนโลยีสารสนเทศต้องตรวจสอบสภาพสินทรัพย์ดังกล่าว หากพบความชำรุดหรือเสียหายหรือข้อมูลที่ขาดหายไป พนักงานหรือผู้รับผิดชอบสินทรัพย์นั้นต้องรับผิดชอบค่าเสียหายตามมูลค่าของสินทรัพย์และข้อมูลนั้นๆ

อุปกรณ์คอมพิวเตอร์ของพนักงานที่ลาออก เครื่องคอมพิวเตอร์จะถูกจัดเก็บไว้ที่ฝ่ายเทคโนโลยีสารสนเทศ เพื่อเตรียมความพร้อมสำหรับพนักงานใหม่ โดยพนักงานที่ลาออกจะต้องส่งคืนทรัพย์สินเทคโนโลยีสารสนเทศขององค์กรที่ถือครองไว้ทั้งหมดให้กับทางฝ่ายเทคโนโลยีสารสนเทศตรวจสอบและเก็บรักษาไว้ ในวันทำงานวันสุดท้าย

หากฝ่ายงานต้นสังกัดของพนักงานที่ลาออกต้องการสำรองข้อมูล (Backup) ในอุปกรณ์คอมพิวเตอร์ของพนักงานที่ลาออกไว้ ฝ่ายงานต้นสังกัดต้องแจ้งให้พนักงานเทคโนโลยีสารสนเทศทราบว่าต้องการสำรองข้อมูล (Back-up) ไปเก็บไว้ที่ใด โดยพนักงานจะดำเนินการสำรองข้อมูล (Back-up) ให้ภายใน 7 วัน หลังจากที่พนักงานลาออก

อุปกรณ์คอมพิวเตอร์จะถูกจัดเก็บไว้ที่คลังทรัพย์สินส่วนกลางของฝ่ายเทคโนโลยีสารสนเทศ โดยจะมีการทำบันทึกจัดเก็บไว้เป็นสินทรัพย์ของบริษัท กรณีที่ต้นสังกัดไม่รับพนักงานทดแทนและฝ่ายเทคโนโลยีสารสนเทศต้องการจะนำ ไปบริหารจัดการทรัพยากรให้เหมาะสมสำหรับฝ่ายงานอื่นหรือการใช้งานอื่นๆ ฝ่ายเทคโนโลยีสารสนเทศจะต้องขอความเห็นชอบและได้รับการอนุมัติจากผู้บังคับบัญชาสูงสุดของฝ่ายงานต้นสังกัดที่เป็นเจ้าของสินทรัพย์ก่อน และให้ดำเนินการตามขั้นตอนการโอนย้ายอุปกรณ์คอมพิวเตอร์

เมื่อฝ่ายงานต้นสังกัดรับพนักงานใหม่มาทดแทนพนักงานที่ลาออกไป หัวหน้าฝ่ายงานต้นสังกัดจะต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศ จัดเตรียมอุปกรณ์คอมพิวเตอร์ก่อนการใช้งาน และเปลี่ยนชื่ออุปกรณ์คอมพิวเตอร์สำหรับพนักงานใหม่ และส่งมอบก่อนวันเริ่มงานของพนักงานใหม่ ล่วงหน้า 3 วันทำการ พร้อมลงนามตรวจรับอุปกรณ์คอมพิวเตอร์ และข้อกำหนดในการใช้งาน รวมถึงค่าเสียหายที่ต้องรับผิดชอบหากอุปกรณ์คอมพิวเตอร์และข้อมูลของบริษัทเสียหาย

ซอฟต์แวร์ลิขสิทธิ์ของพนักงานที่ลาออก จะต้องทำการโอนย้ายซอฟต์แวร์ลิขสิทธิ์ไปยังหัวหน้าฝ่ายงานต้นสังกัด ก่อนวันทำงานวันสุดท้าย หากพนักงานที่ลาออกไม่ได้ทำการโอนย้ายซอฟต์แวร์ โดยแจ้งฝ่ายเทคโนโลยีสารสนเทศ เพื่อทำการโอนย้ายซอฟต์แวร์ลิขสิทธิ์ของพนักงานท่านนั้นไปยังหัวหน้าฝ่ายงานต้นสังกัดอัตโนมัติ หลังจากพนักงานท่านนั้นสิ้นสุดการทำงานแล้ว

เมื่อฝ่ายงานต้นสังกัดรับพนักงานใหม่มาทดแทนพนักงานที่ลาออกไป หัวหน้าฝ่ายงานต้นสังกัดหรือพนักงานที่ถือครองซอฟต์แวร์แทน จะต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศทำการโอนย้ายซอฟต์แวร์ลิขสิทธิ์ไปยังพนักงานใหม่

ฝ่ายเทคโนโลยีสารสนเทศจะต้องตรวจสอบความพร้อมใช้งานของซอฟต์แวร์มาตรฐาน รวมถึงลิขสิทธิ์ซอฟต์แวร์ก่อนพนักงานใหม่ใช้งานทุกครั้ง หากพนักงานใหม่มีความจำเป็นต้องใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ให้ตรวจสอบสิทธิ์การใช้งานรวมถึงลิขสิทธิ์ของซอฟต์แวร์ก่อนทุกครั้งว่ามีลิขสิทธิ์ถูกต้องหรือหมดอายุหรือไม่ พร้อมลงนามในเอกสารรับเครื่อง

กรณีที่ลิขสิทธิ์ซอฟต์แวร์ไม่ถูกต้องหรือหมดอายุ พนักงานฝ่ายเทคโนโลยีสารสนเทศจะต้องแจ้งให้พนักงานดำเนินการขออนุมัติจัดซื้อจากผู้บังคับบัญชาสูงสุดของฝ่ายงาน ตามนโยบายการจัดซื้อของฝ่ายจัดซื้อที่กำหนดไว้ จากนั้นจึงติดตั้งเมื่อการสั่งซื้อเสร็จสิ้นตามกระบวนการแล้วเท่านั้น

กรณีที่ไม่มีสิทธิ์ใช้ แต่พนักงานจำเป็นต้องใช้สำหรับการทำงาน พนักงานจะต้องขออนุมัติจากผู้บังคับบัญชาสูงสุดของฝ่ายงาน และผู้บริหารสูงสุดของสายงานเทคโนโลยีสารสนเทศ โดยฝ่ายงานต้นสังกัดจะต้องมีการจัดเตรียมงบประมาณในการจัดซื้อตามนโยบายการจัดซื้อของฝ่ายจัดซื้อที่กำหนดไว้

5.5 การใช้งานสินทรัพย์อย่างเหมาะสม

บริษัทกำหนดมาตรฐานและแนวปฏิบัติในการใช้งานสินทรัพย์ที่เกี่ยวกับเทคโนโลยีสารสนเทศ รวมถึงอุปกรณ์ ระบบเครือข่าย หรือระบบการประมวลผลต่างๆ โดยฝ่ายเทคโนโลยีสารสนเทศสื่อสารให้พนักงานทั่วทั้งองค์กรรับทราบและนำ ไปปฏิบัติตามมาตรฐานเดียวกัน

5.6 การจัดการสื่อบันทึกข้อมูล (Media Handling)

เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล เพื่อป้องกันความเสียหายต่อการดำเนินธุรกิจ อันเนื่องมาจากความเสียหายของสื่อบันทึกข้อมูลต่างๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์การกำหนดไว้

1) บริษัทไม่อนุญาตให้ใช้สื่อบันทึกข้อมูล เช่น ผ่านช่อง USB, ผ่านทาง CD/DVD หรือ External Drive เป็นต้น
2) หากฝ่ายใดต้องการใช้งานสื่อบันทึกข้อมูลภายนอก จะต้องได้รับการอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ โดยใช้แบบฟอร์มขอใช้ USB ที่มีผู้บังคับบัญชาอนุมัติ และฝ่ายเทคโนโลยีสารสนเทศ
3) จะต้องมีการลงทะเบียนสิทธิ์ให้กับผู้ที่ต้องการใช้สื่อบันทึกข้อมูล USB และรายงานหน่วยงานความมั่นคงสารสนเทศเพื่อทบทวนสิทธิ์ตามระยะเวลาที่กำหนด

6. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

6.1 บริเวณหรือพื้นที่ที่ต้องมีการรักษาความปลอดภัย

บริษัทกำหนดบริเวณหรือพื้นที่ที่จัดเก็บระบบเทคโนโลยีสารสนเทศหรืออุปกรณ์ต่างๆ ที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัทอย่างเหมาะสม เช่น ห้อง Server ศูนย์ข้อมูล (Data Center) เป็นต้น เพื่อป้องกัน ควบคุม และลดโอกาสที่จะเกิดความเสี่ยงต่างๆ ที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของบริษัท และเพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าถึงล่วงรู้ (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีสารสนเทศ (Availability Risk)

6.2 การควบคุมการเข้า- ออก

บริษัทกำหนดการควบคุมสำหรับบริเวณหรือพื้นที่ที่ต้องมีการรักษาความปลอดภัยดังกล่าว ดังนี้

- การระบุและจำกัดสิทธิ์และเวลาการเข้า - ออกบริเวณและพื้นที่ดังกล่าว โดยจำกัดเฉพาะพนักงานที่ได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศและเกี่ยวข้องกับการปฏิบัติงานเท่านั้น ข้อมูลและเวลาการเข้า - ออกบริเวณดังกล่าวได้รับการบันทึกอย่างเป็นลายลักษณ์อักษร พนักงานที่ได้รับสิทธิ์และพนักงานที่ปฏิบัติงานประจำในบริเวณและพื้นที่ดังกล่าวต้องติดบัตรประจำตัวพนักงานเพื่อยืนยันตัวตนตลอดเวลา
- บริษัทติดตั้งกล้องวงจรปิดในบริเวณและพื้นที่ดังกล่าว การตรวจสอบประวัติการเข้า - ออกบริเวณและพื้นที่ดังกล่าวเป็นประจำ และกำหนดให้มีการสอบทาน ทบทวน และปรับปรุงรายชื่อผู้มีสิทธิ์ในการเข้า - ออกบริเวณและพื้นที่ดังกล่าวอย่างน้อยปีละ 1 ครั้ง
- การจำกัดไม่ให้บุคคลภายนอกเข้าถึงบริเวณและพื้นที่ดังกล่าว หากพบเห็นบุคคลภายนอกเข้าถึงบริเวณหรือพื้นที่ดังกล่าวโดยไม่ได้รับอนุญาต ให้แจ้งพนักงานรักษาความปลอดภัยทันที
- หากพนักงานที่ได้รับสิทธิ์ในการเข้า - ออกบริเวณและพื้นที่ดังกล่าวลาออกหรือสิ้นสุดสัญญาจ้าง สิทธิ์ดังกล่าวต้องถูกเพิกถอนโดยทันทีก่อนวันสุดท้ายของการปฏิบัติงาน
- พนักงานที่ประสงค์จะขอสิทธิ์ในการเข้า - ออกบริเวณหรือพื้นที่ที่ต้องมีการรักษาความปลอดภัย ต้องบันทึกแบบฟอร์มการขอสิทธิ์ในการเข้า - ออกบริเวณหรือพื้นที่ที่ต้องมีการรักษาความปลอดภัย (Security Areas Access Request) และต้องได้รับการพิจารณาและอนุมัติโดยผู้บังคับบัญชาสูงสุดของฝ่ายงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

6.3 การรักษาความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์อื่น ๆ

บริษัทต้องจัดเก็บระบบเทคโนโลยีสารสนเทศและอุปกรณ์ที่สำคัญไว้ในบริเวณหรือพื้นที่ที่ต้องมีการรักษาความปลอดภัยและกำหนดมาตรการในการรักษาความมั่นคงปลดภัยอุปกรณ์และสินทรัพย์อื่นๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ ดังนี้

- การจัดให้บริเวณหรือพื้นที่ดังกล่าวไม่รวมอยู่กับการดำเนินงานส่วนงานอื่นๆ ที่ปะปนกับบุคคลภายนอก เช่น ร้านสาขา บริเวณคลังที่มีบุคคลภายนอกเข้า - ออกเป็นประจำ เป็นต้น
- กำหนดการป้องกันบริเวณหรือพื้นที่ดังกล่าวอย่างเหมาะสม เช่น ประตูปิดอย่างแน่นหนา พนักงานประจำหรือพนักงานรักษาความปลอดภัยในบริเวณหรือพื้นที่ดังกล่าว เป็นต้น
- บริเวณและพื้นที่ดังกล่าวต้องได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น ล็อคด้วยกุญแจ กำหนดรหัสผ่านใช้บัตรผ่านพื้นที่ (Access Card) เป็นต้น รวมถึงตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดล็อคอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย
- ข้อมูลที่เป็นความลับต่างๆต้องไม่ถูกวางไว้อย่างเปิดเผย หรือไม่ระมัดระวัง และการทำลายข้อมูลหรือเอกสารที่เป็นความลับต้องได้รับการดำเนินการตามมาตรฐานการทำลายเอกสารอย่างเหมาะสม รวมถึงไม่เปิดข้อมูลในหน้าจออุปกรณ์คอมพิวเตอร์โดยไม่ได้ใช้งาน และต้องออกจากชื่อผู้ใช้งาน หรือ Lock Screen ทุกครั้งที่ไม่ได้อยู่กับอุปกรณ์คอมพิวเตอร์ (Clear Desk and Clear Screen)

ฝ่ายเทคโนโลยีสารสนเทศกำหนดข้อปฏิบัติสำหรับการทำลายสื่อที่ใช้บันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร (Disposal of media procedures) และการทำเอกสารหรือข้อมูลต่างๆ ต้องได้รับการอนุมัติจากเจ้าของข้อมูล และกำหนดให้มีการบันทึกรายละเอียดการทำลายข้อมูลอย่างเป็นลายลักษณ์อักษร

- พนักงานผู้รับผิดชอบในสินทรัพย์ต้องปกป้องและดูแลสินทรัพย์ในความครอบครองอย่างเคร่งครัด ทั้งการปฏิบัติงานภายในบริษัท หรือการปฏิบัติงานภายนอกบริษัท
- พนักงานห้ามโอนย้ายสินทรัพย์ออก จากบริเวณหรือพื้นที่ดังกล่าวโดยไม่ได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร หากมีความประสงค์จะนำออกจากบริษัท ต้องปฏิบัติตามข้อปฏิบัติการโอนย้ายอุปกรณ์คอมพิวเตอร์ ดังนี้
    - การโอนย้ายอุปกรณ์คอมพิวเตอร์ และ/หรือซอฟต์แวร์ลิขสิทธิ์ประเภทซื้อขาด ให้เป็นไปตามขั้นตอนการโอนย้ายของทรัพย์สินของบริษัท อ้างอิงนโยบาย OKJ-A2R-TRF-01 การโอนย้ายสินทรัพย์
    - การโอนย้ายซอฟต์แวร์ลิขสิทธิ์ประเภทเช่าใช้งาน ฝ่ายงานต้นเรื่องจะต้องแจ้งผ่านฝ่ายเทคโนโลยีสารสนเทศ เพื่อแจ้งให้พนักงานฝ่ายเทคโนโลยีสารสนเทศที่ควบคุมดูแล ดำเนินการปรับเปลี่ยนสิทธิ์การใช้งานให้เป็นไปตามร้องขอ
- กรณีการโอนย้ายทรัพย์สินเนื่องจากพนักงานลาออก พนักงานฝ่ายเทคโนโลยีสารสนเทศที่ควบคุมดูแลจะต้องตรวจสอบข้อมูลและสภาพของอุปกรณ์ของพนักงานก่อนดำเนินโอนย้ายทุกครั้ง

บริษัทต้องจัดบริเวณหรือพื้นที่ดังกล่าวอย่างเป็นสัดส่วน เพื่อความสะดวกในการปฏิบัติงานและยังช่วยให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น นอกจากนี้ ควรแยกส่วนที่ต้องมีการเข้าถึงโดยพนักงานหลายฝ่ายออกจากบริเวณหรือพื้นที่ดังกล่าวอย่างชัดเจน

6.4 การป้องกันความเสียหายจากภัยพิบัติหรืออุบัติเหตุต่าง ๆ

บริษัทจัดให้ระบบเทคโนโลยีสารสนเทศและอุปกรณ์คอมพิวเตอร์ที่สำคัญอยู่ในบริเวณหรือพื้นที่ที่ต้องมีการรักษาความปลอดภัย รวมทั้งมีการกำหนดการควบคุมต่างๆ เพื่อป้องกันความเสียหายจากภัยพิบัติหรืออุบัติเหตุต่างๆ ดังนี้

ระบบการป้องกันไฟไหม้ บริษัทติดตั้งอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน กล้องวงจรปิด เป็นต้น เพื่อเตือนเหตุ ป้องกัน หรือระงับเหตุได้ทันเวลา นอกจากนี้ บริษัทจัดให้มีระบบดับเพลิงอัตโนมัติและถังดับเพลิงเพื่อ

ใช้สำหรับการดับเพลิงในเบื้องต้น นอกจากนี้ บริษัทกำหนดให้มีการทดสอบจากผู้ให้บริการสถานที่ในการส่งรายงานระบบแจ้งเตือนไฟไหม้และระบบดับเพลิงอัตโนมัติ รวมถึงการใช้งานถังดับเพลิง อย่างน้อยปีละ 1 ครั้ง

ระบบการป้องกันไฟฟ้าขัดข้อง บริษัทติดตั้งระบบป้องกันมิให้อุปกรณ์คอมพิวเตอร์ที่สำคัญได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า เช่น ระบบ Generators or Backup Electricity Feed, Uninterruptible Power Supply (UPS) Units, Multiple Power Feeds เป็นต้น เพื่อให้บริษัทสามารถดำเนินงานต่อเนื่องได้ และบริษัทกำหนดให้มีการตรวจสอบระบบไฟฟ้าอย่างน้อยไตรมาสละ 1 ครั้ง

ระบบควบคุมอุณหภูมิและความชื้น บริษัทต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรกำหนดอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (specification) ของระบบเทคโนโลยีสารสนเทศ เนื่องจากระบบเทคโนโลยีสารสนเทศอาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

ระบบเตือนภัยน้ำรั่ว บริษัทติดตั้งระบบเตือนภัยน้ำรั่ว ในบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา นอกจากนี้ หากบริเวณหรือพื้นที่ดังกล่าวตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ก็ควรหมั่นสังเกตว่า มีน้ำรั่วหรือไม่ อย่างสม่ำเสมอ

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศวิเคราะห์ และระบุปัจจัยเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ เช่น เหตุการณ์ภัยธรรมชาติ อุบัติเหตุต่างๆ เป็นต้น ประกอบกับข้อมูลหรือเหตุการณ์ในอดีต (Past Incidents) เพื่อกำหนดแนวทาง ในการควบคุม ป้องกัน และแก้ไข ความเสี่ยงจากภัยพิบัติหรืออุบัติเหตุต่างๆ ได้อย่างมีประสิทธิภาพและเหมาะสมยิ่งขึ้น และเสนอแนวทางดังกล่าวแก่ผู้บริหารสูงสุดสายงานเทคโนโลยีสารสนเทศเพื่อพิจารณาและอนุมัติต่อไป

7. ความมั่นคงปลอดภัยด้านการดำเนินงาน (Operation Security)

7.1 ขั้นตอนการปฏิบัติงาน หน้าที่ และความรับผิดชอบ

บริษัทกำหนดขั้นตอนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติงานและพนักงานผู้รับผิดชอบ ขั้นตอนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศครอบคลุมหัวข้อ ดังต่อไปนี้เป็นอย่างน้อย

- ขั้นตอนการเปิด – ปิดระบบเทคโนโลยีสารสนเทศ
- ขั้นตอนการลงทะเบียนหรือ Setup อุปกรณ์ Hardware หรือ Software
- ขั้นตอนการประมวลผลข้อมูลสารสนเทศ
- ขั้นตอนการติดตามการปฏิบัติงานของระบบเทคโนโลยีสารสนเทศ
- ขั้นตอนการดูแล และบำรุงรักษาระบบเทคโนโลยีสารสนเทศ
- ขั้นตอนการจัดการหรือแก้ไขปัญหาต่างๆ รวมถึงเหตุการณ์ฉุกเฉิน
- ขั้นตอนการสำรองและการกู้คืนข้อมูล

ฝ่ายเทคโนโลยีสารสนเทศสื่อสารขั้นตอนการปฏิบัติงานดังกล่าวแก่พนักงานทั่วทั้งองค์กรให้ถือปฏิบัติ โดยฝ่ายเทคโนโลยีสารสนเทศต้องทบทวนและปรับปรุงขั้นตอนการปฏิบัติงานดังกล่าวเป็นประจำอย่างน้อยปีละ 1 ครั้ง

7.2 การจัดการการเปลี่ยนแปลงระบบงาน

บริษัทกำหนดขั้นตอนการปฏิบัติงานในการเปลี่ยนแปลงระบบงานอย่างชัดเจนและเป็นลายลักษณ์อักษร รวมถึงขั้นตอน การปฏิบัติงานในการเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศในกรณีฉุกเฉิน (Emergency Change) โดยพนักงาน ฝ่ายเทคโนโลยีสารสนเทศสื่อสารขั้นตอนการปฏิบัติงานดังกล่าวให้พนักงานทราบและถือปฏิบัติทั่วทั้งบริษัท โดยมีขั้นตอนดังนี้

พนักงานบันทึกการร้องขอการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ (IT System/Change Request Form) โดยต้องจัดทำบันทึกเป็นลายลักษณ์อักษร

ผู้บังคับบัญชาสูงสุดของแต่ละฝ่ายงานพิจารณาตรวจสอบและอนุมัติการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ และลงนามอนุมัติในบันทึกการการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ (IT System/Change Request Form)

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศตรวจสอบ พิจารณาตรวจสอบและอนุมัติการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ และลงนามอนุมัติในบันทึกการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ (IT System/Change Request Form)

ฝ่ายเทคโนโลยีสารสนเทศประมินผลกระทบของการเปลี่ยนแปลงของระบบงานเทคโนโลยีสารสนเทศ ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการปฏิบัติงาน (Functionality) รวมถึงกฎเกณฑ์และข้อบังคับของหน่วยงานกำกับดูแล ที่เกี่ยวข้องกับระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร พร้อมสรุปอุปสรรคปัญหา และขั้นตอนในการปรับปรุงและแก้ไข และรายงานให้รองประธานพนักงานบริหารที่กำกับดูแลฝ่ายงานเทคโนโลยีสารสนเทศทราบ

การเปลี่ยนแปลงทุกครั้งต้องได้รับการบันทึกรายการเปลี่ยนแปลงอย่างครบถ้วน โดยประกอบไปด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย

- ชื่อโครงการ หรือระบบเทคโนโลยีสารสนเทศที่ต้องการเปลี่ยนแปลง
- วันที่ร้องขอ และวันที่เปลี่ยนแปลง
- ผู้รับผิดชอบ
- เป้าหมาย และเหตุผลของการเปลี่ยนแปลง
- ขั้นตอนและระยะเวลาในการดำเนินการ
- รายการแก้ไขเปลี่ยนแปลง
- ผลของการเปลี่ยนแปลง
- ข้อมูลอื่นๆ ตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด

การเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศในกรณีฉุกเฉิน (Emergency Change) พนักงานผู้ร้องขอสามารถร้องขอการเปลี่ยนแปลงผ่านทางอีเมลพร้อมระบุเหตุผลและความจำเป็น ให้แก่ผู้บังคับบัญชาสูงสุดของฝ่ายงานและผู้จัดการเทคโนโลยีหรือผู้บริหารสูงสุดของสายงานเทคโนโลยีสารสนเทศเพื่อพิจารณาตรวจสอบและอนุมัติ จากนั้น ให้พนักงานผู้ร้องขอดำเนินการจัดบันทึกการร้องขอการเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ (Change Request Form) และขออนุมัติตามกระบวนการให้แล้วเสร็จภายใน 5 วันนับจากวันที่มีการเปลี่ยนแปลง ทั้งนี้ การเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศในกรณีฉุกเฉิน (Emergency Change) กำหนดไว้สำหรับการตอบสนองต่อเหตุการณ์ฉุกเฉินหรือปัญหาด้านระบบเทคโนโลยีสารสนเทศเท่านั้น

นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีการแยกระบบสำหรับการพัฒนา ทดสอบ และการใช้งานจริงออกจากกัน (Separation of development, testing, and operational environments) เพื่อลดและป้องกันความเสี่ยงจากการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต หรือข้อมูลที่เสียหายได้

7.3 การจัดการและป้องกัน Virus หรือ Malware

บริษัทกำหนดมาตรการในการป้องกัน Virus หรือ Malware ต่างๆ อย่างชัดเจน โดยสื่อสารแนวปฏิบัติให้พนักงานทราบทั่วทั้งองค์กรเพื่อถือปฏิบัติเป็นมาตรฐานเดียวกัน ดังนี้

- บริษัทติดตั้งโปรแกรม Ani-Virus ที่ได้รับการประเมินและอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าอุปกรณ์คอมพิวเตอร์ รวมถึงคอมพิวเตอร์แม่ข่าย (Server) จะได้รับการปกป้องจาก Virus หรือ Malware อย่างเหมาะสมและมีประสิทธิ์ภาพ
- ฝ่ายเทคโนโลยีสารสนเทศติดตามและอัพเดท (Update) โปรแกรม Ani-Virus อย่างสม่ำเสมอ
- พนักงานทุกคนที่เป็นเจ้าของสินทรัพย์ต้องเปิดการใช้งานโปรแกรม Anti-Virus ตลอดเวลาที่ใช้งาน และพนักงานฝ่ายเทคโนโลยีสารสนเทศควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (Disable) ระบบป้องกัน Virus ที่ได้ติดตั้งไว้

- พนักงานทุกคนที่เป็นเจ้าของสินทรัพย์ต้องปฏิบัติตามข้อกำหนดการอนุญาตใช้สินทรัพย์อย่างเคร่งครัด และไม่ดำเนินการอันเป็นการละเมิดข้อปฏิบัติ และนำไปสู่ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- พนักงานทุกคนที่เป็นเจ้าของสินทรัพย์ต้องมีความระมัดระวังในการส่งข้อมูลผ่านระบบเครือข่ายของบริษัท ทั้งนี้ ผู้ใช้งานควรเปิดเฉพาะไฟล์ที่ได้รับจากบุคคลที่รู้จักและช่องทางการสื่อสารที่น่าเชื่อถือเท่านั้น และต้องทำการสแกน Virus ในไฟล์นั้นๆเสมอ และต้องระมัดระวังในการเปิดลิงค์ต่างๆ ซึ่งอาจพบ Virus หรือ Malware ได้
- อีเมลที่ส่งเข้าสู่ระบบเครือข่ายของบริษัทต้องได้รับการตรวจสอบ Virus ก่อนส่งต่อไปยังพนักงาน
- หากพบไฟล์หรือสิ่งที่สงสัยว่าอาจจะเป็น Virus หรือ Malware ที่ไม่สามารถทำลายได้ด้วยโปรแกรม Anti-Virus พนักงานทุกคนต้องแจ้งพนักงานฝ่ายเทคโนโลยีสารสนเทศเพื่อตรวจสอบและดำเนินการโดยทันที
- ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีการฝึกอบรมและสื่อสารข้อมูลเกี่ยวกับการป้องกัน Virus หรือ Malware อย่างสม่ำเสมอ โดยกำหนดให้มีการแจ้งอัพเดทข้อมูลต่างๆ เป็นประจำทุกเดือนผ่านทางอีเมลหรือช่องทางการสื่อความอื่นๆ และจัดให้มีการฝึกอบรมด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นประจำ นอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศกำหนดช่องทางในการสื่อสาร เพื่อให้พนักงานสามารถติดต่อขอความช่วยเหลือหรือขอคำปรึกษาในการแก้ปัญหาการใช้งาน (IT Help Desk or IT Hotline)

7.4 การสำรองและกู้คืนข้อมูล

บริษัทกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล รวมถึงโปรแกรมระบบปฏิบัติการ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน เพื่อเตรียมความพร้อมรองรับเหตุการณ์ฉุกเฉินต่างๆ ที่อาจเกิดขึ้น และเพื่อให้บริษัทมีข้อมูลสำหรับการปฏิบัติงานอย่างต่อเนื่อง และมีประสิทธิภาพรวมถึงการทดสอบการกู้และความพร้อมใช้งานของข้อมูล ดังนี้

พนักงานฝ่ายเทคโนโลยีสารสนเทศกำหนดแผนการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูล โดยจำนวนครั้งหรือความถี่ในการสำรองข้อมูล และการทดสอบข้อมูล ตามระดับชั้นความลับและความสำคัญของข้อมูลสารสนเทศโดยอ้างอิงนโยบาย GITC-OPS-01 การสำรองข้อมูลระบบเทคโนโลยีสารสนเทศ และ GITC-OPS-02 การทดสอบการกู้คืนข้อมูลระบบเทคโนโลยีสารสนเทศ

พนักงานฝ่ายเทคโนโลยีสารสนเทศทดสอบการกู้คืนข้อมูลสำรองตามตารางที่กำหนด โดยการกู้คืนข้อมูลสำรองต้องได้รับการอนุมัติจากผู้บังคับบัญชาสูงสุดของฝ่ายงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และกำหนดขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสารองจากสื่อบันทึกมาใช้งาน นอกจากนี้ พนักงานฝ่ายเทคโนโลยีสารสนเทศดำเนินการทดสอบการกู้คืนข้อมูลสำรอง และยืนยันความครบถ้วนและความถูกต้องของข้อมูลจากพนักงานเจ้าของข้อมูล โดยอ้างอิงนโยบาย GITC-OPS-02 การทดสอบการกู้คืนข้อมูลระบบเทคโนโลยีสารสนเทศ

พนักงานฝ่ายเทคโนโลยีสารสนเทศบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของ พนักงานเพื่อ

ตรวจสอบความถูกต้องครบถ้วน และ ควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอพนักงานผู้เป็นเจ้าของสินทรัพย์เป็นผู้มีหน้าที่รับผิดชอบต่อข้อมูลสำคัญที่จัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์ของตนเอง

ข้อมูลสำรองที่สำคัญและอ่อนไหว (Critical and Sensitive Information) ต้องจัดเก็บในอุปกรณ์สำรองที่เข้ารหัส และป้องกันทางกายภาพอย่างเหมาะสม ตามที่กำหนดในข้อ 5. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

บริษัทกำหนดให้จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงาน ได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กำหนดในข้อ 5. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

หากบริษัทมีความจำเป็นที่จะต้องจัดเก็บข้อมูลสำรองเป็นระยะเวลานาน ฝ่ายเทคโนโลยีสารสนเทศพิจารณาวิธีการนำข้อมูลสำรองดังกล่าวกลับมาใช้งาน เช่น หากฝ่ายเทคโนโลยีสารสนเทศจัดเก็บข้อมูลสำรองไว้ในอุปกรณ์บันทึกรุ่นเก่า ฝ่ายเทคโนโลยีสารสนเทศต้องจัดเก็บอุปกรณ์ที่รองรับข้อมูลดังกล่าวไว้ด้วย เป็นต้น

พนักงานฝ่ายเทคโนโลยีสารสนเทศติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกข้อมูลสำรองผิดพลาด

การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

ฝ่ายเทคโนโลยีสารสนเทศกำหนดขั้นตอนการปฏิบัติการทำลายข้อมูลที่สำคัญและสื่อบันทึกข้อมูลสำรองที่ไม่ใช้งานแล้ว รวมถึงข้อมูลสำคัญอื่นๆ ที่ไม่ใช้งานแล้วที่ยังคงเหลืออยู่ในระบบเทคโนโลยีสารสนเทศของบริษัท

7.5 การบันทึกข้อมูลกิจกรรมการใช้งาน (Log Control)

บริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศบันทึกข้อมูลกิจกรรมการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท(Log Control) การปฏิเสธการใช้งาน และข้อมูลเหตุการณ์ต่างๆ ด้านเทคโนโลยีสารสนเทศ เช่น บันทึกการเข้าออกระบบ (login-logout logs) บันทึกการพยายามเข้าสู่ระบบ (login attempts) บันทึกการใช้ command line และ firewall log บันทึกการเข้าออกระบบของผู้ดูแลระบบ (System Administrator) หรือ Operator เป็นต้น ข้อมูลกิจกรรมการใช้งาน (Log Control) ที่บันทึก ต้องมีการป้องกันการเข้าถึงอย่างเหมาะสม เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต บริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศจัดเก็บบันทึกข้อมูลกิจกรรมการใช้งาน (Log Control) อย่างน้อย 6 เดือน หรือตามข้อกำหนดในกฎหมายหรือข้อบังคับของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

ฝ่ายเทคโนโลยีสารสนเทศบันทึก ควบคุม และดูแลปัญหาหรืออุปสรรคด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นกับพนักงานอย่างสม่ำเสมอ เพื่อพิจารณาและปรับปรุงการปฏิบัติงานให้ดีขึ้น

ฝ่ายเทคโนโลยีสารสนเทศตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ และกำหนดวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าบันทึกต่างๆ

บริษัทกำหนดให้อุปกรณ์และระบบเทคโนโลยีสารสนเทศของบริษัทกำหนดเวลาตามเวลาท้องถิ่น (Clock synchronization) อย่างถูกต้องและเหมือนกัน เพื่อให้ข้อมูลด้านเวลาที่ถูกต้องตรงกัน นอกจากนี้ การกำหนดเวลาอัตโนมัติ หรือ Network Time Protocol เพื่อให้อุปกรณ์และระบบเทคโนโลยีสารสนเทศของบริษัทกำหนดเวลาที่เป็นมาตรฐานเดียวกัน

7.6 การตรวจสอบระบบเทคโนโลยีสารสนเทศ

พนักงานฝ่ายเทคโนโลยีสารสนเทศตรวจสอบระบบเทคโนโลยีสารสนเทศที่สำคัญของบริษัทอย่างน้อยปีละ 1 ครั้ง และ/หรือกำหนดให้หน่วยงานตรวจสอบภายในตรวจสอบระบบเทคโนโลยีสารสนเทศของบริษัทเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศของบริษัทมีความสอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ หรือความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่างๆ และเพื่อให้ข้อเสนอแนะและแนวทางการปรับปรุงระบบเทคโนโลยีสารสนเทศให้มีประสิทธิ์ภาพมากยิ่งขึ้น โดยการตรวจสอบระบบเทคโนโลยีสารสนเทศควรพิจารณาความเสี่ยงอย่างน้อยดังต่อไปนี้

- ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ (IT Management Risk)
- ความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูล (IT Security Risk)
- ความเสี่ยงด้านความถูกต้องและนำเชื่อถือของข้อมูลสารสนเทศ (Information Integrity Risk)
- ความเสี่ยงด้านความพร้อมการใช้งาน หรือความเสียหายต่อข้อมูลและระบบเทคโนโลยีสารสนเทศ (Availability Risk)ความเสี่ยงด้านการปฏิบัติตามกฎหมาย กฎระเบียบ หรือข้อบังคับที่เกี่ยวข้อง (Regulatory Compliance Risk)
- ความเสี่ยงด้านชื่อเสียงของบริษัท (Reputation Risk)

นอกจากนี้ บริษัทจะพิจารณาว่าจ้างที่ปรึกษาจากภายนอก ตรวจสอบและประเมินความมีประสิทธิ์ผลของระบบเทคโนโลยีสารสนเทศของบริษัท และการควบคุมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นระยะ เพื่อให้มั่นใจว่าบริษัทมีการควบคุมระบบเทคโนโลยีสารสนเทศที่ดี มีประสิทธิ์ผล และเป็นไปตามมาตรฐานปฏิบัติต่างๆ อย่างเหมาะสม

8. ความมั่นคงปลอดภัยในการบริหารจัดการผู้ให้บริการ (Supplier Security Management)

8.1 การดำเนินการร่วมกับผู้ให้บริการภายนอก (Information security in supplier relationships)

บริษัทกำหนดขั้นตอนปฏิบัติในการดำเนินการร่วมกับผู้ให้บริการภายนอก เพื่อป้องกันสินทรัพย์ด้านเทคโนโลยีสารสนเทศของบริษัท รวมถึงควบคุม ติดตาม และตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอกได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

- ฝ่ายเทคโนโลยีสารสนเทศกำหนดความต้องการด้านความมั่นคงด้านเทคโนโลยีสารสนเทศในด้านต่างๆ รวมถึงแนวปฏิบัติในการบรรเทา ป้องกัน หรือลดความเสี่ยงด้านความมั่นคงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น และสื่อสารให้ผู้ให้บริการภายนอกทราบอย่างชัดเจน
- ฝ่ายงานที่ดำเนินการร่วมกับผู้ให้บริการภายนอก โดยประสานงานร่วมกับฝ่ายเทคโนโลยีสารสนเทศจัดทำข้อกำหนดหรือสัญญาอย่างเป็นลายลักษณ์อักษรร่วมกับผู้ให้บริการภายนอก เพื่อป้องกันการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศการรั่วไหลของข้อมูล โดยกำหนดให้ผู้บริหารภายนอกลงนามในข้อกำหนดหรือสัญญา ดังนี้
  - สัญญาจ้างงาน โดยกำหนดข้อตกลง และความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement: NDA)

- พนักงานฝ่ายเทคโนโลยีสารสนเทศสงวนสิทธิ์ในการตรวจสอบรายงานหรือบันทึกการให้บริการของผู้ให้บริการภายนอกแก่ฝ่ายงานที่ว่าจ้างอย่างสม่ำเสมอ และสามารถจำกัดหรือเพิกถอนสิทธิ์การเข้าถึงข้อมูลสารสนเทศของบริษัทได้ตามความเหมาะสม โดยการอนุมัติของผู้บังคับบัญชาฝ่ายงานและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- พนักงานฝ่ายเทคโนโลยีสารสนเทศของบริษัทกำกับดูแลให้ผู้ให้บริการภายนอกปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและข้อกำหนดอื่นๆ ที่เกี่ยวข้องอย่างเคร่งครัด หากไม่ปฏิบัติตาม บริษัทสามารถยกเลิกสัญญาการให้บริการกับผู้ให้บริการภายนอกได้
- ผู้ให้บริการภายนอกต้องแจ้งแก่ฝ่ายงานที่เกี่ยวข้องและฝ่ายเทคโนโลยีสารสนเทศโดยทันทีหากพบการไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ฝ่ายงานที่ดำเนินการร่วมกับผู้ให้บริการภายนอกควบคุมให้ผู้ให้บริการภายนอกเก็บรักษาข้อมูลทุกประเภทที่ได้รับจากบริษัทอย่างเคร่งครัด
- พนักงานฝ่ายเทคโนโลยีสารสนเทศกำหนดระยะเวลาการอนุญาตสิทธิ์ให้เข้าถึงข้อมูลสารสนเทศของผู้ให้บริการ ภายนอกอย่างชัดเจน และเมื่อครบกำหนดเวลา สิ้นสุดสัญญาจ้าง หรือผู้ให้บริการภายนอกไม่จำเป็นต้องเข้าถึงข้อมูลสารสนเทศของบริษัท พนักงานฝ่ายเทคโนโลยีสารสนเทศเพิกถอนสิทธิ์ดังกล่าวโดยทันที

8.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

บริษัทกำหนดขั้นตอนปฏิบัติในการบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก เพื่อให้ผู้ให้บริการภายนอกรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการให้บริการตามที่ตกลงกันไว้ในสัญญาของผู้ให้บริการ ภายนอก ดังนี้

- บริษัทกำหนดสิทธิ์ในการตรวจสอบสภาพแวดล้อมการปฏิบัติงานของผู้ให้บริการภายนอก ทบทวน ติดตาม และตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ให้บริการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และสามารถให้บริการตามที่ตกลงกันและภายในเวลาที่กำหนด
- สำหรับสัญญาที่สำคัญต่อการปฏิบัติงานของบริษัท เช่น การให้บริการติดตั้งระบบเทคโนโลยีสารสนเทศ การให้บริการบริหารจัดการคลัง เป็นต้น ฝ่ายงานที่เกี่ยวข้องต้องประเมินและตรวจสอบการให้บริการโดยเทียบกับมาตรฐานการให้บริการ (Service Level Agreement) ตามที่ตกลงกัน

- หากมีการเปลี่ยนแปลงการปฏิบัติงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท ฝ่ายงานที่เกี่ยวข้องต้องแจ้งการเปลี่ยนแปลงต่อผู้ให้บริการภายนอกเพื่อรับทราบและถือปฏิบัติ และทบทวนการประเมินการดำเนินการร่วมกับผู้ให้บริการภายนอกอีกครั้ง

9. ความมั่นคงปลอดภัยสาหรับการสื่อสารข้อมูล (Communications Security)

9.1 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายขององค์กร

9.1.1 การควบคุมการเข้าถึงเครือข่าย (Network Control)

1) ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดาเนินการตรวจสอบผู้กระทำการละเมิด
2) การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย
3) ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่หน่วยงานนั้นรับผิดชอบ
4) ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย
5) บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของสำนักงานฯ ด้วย

9.1.2 การความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

1) ระบบเครือข่ายทั้งหมดของสำนักงานฯ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทา Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย
2) ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของสานักงานฯ และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของสำนักงานฯ ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายสำนักงานฯ ได้
3) ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายขององค์กรโดยไม่ได้รับอนุญาตจากแผนกเทคโนโลยีสารสนเทศ
4) ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายขององค์กร โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง
5) ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด
6) ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของสำนักงานฯ ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในสานักงานฯ โดยเด็ดขาด

9.1.3 การจัดแบ่งเครือข่ายภายในองค์กร (Segregation in Network)

1) ออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และโซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
2) จัดทำแผนผังระบบเครือข่าย (Network Diagram) และมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

9.2 การถ่ายโอนข้อมูล (Information Transfer)

เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กรและถ่ายโอนข้อมูลกับภายนอกหน่วยงาน

9.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

1) ต้องมีการจัดทำนโยบาย ขั้นตอนปฏิบัติ หรือมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการและมีการปฏิบัติตามเพื่อป้องกันสารสนเทศที่มีการถ่ายโอนกับหน่วยงานภายนอก
2) ต้องมีการดำเนินการแลกเปลี่ยนสารสนเทศ โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure)

9.2.2 ข้อตกลงสาหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer)

1) ต้องมีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูล โดยปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure)

10. การจัดหา พัฒนา และดูแลรักษาระบบเทคโนโลยีสารสนเทศ (IT System Acquisition, Development, and Maintenance)

10.1 การกำหนดความต้องการด้านระบบ และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศกำหนดความต้องการด้านระบบ และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบที่พัฒนาขึ้นมาใช้งาน หรือจัดซื้อมาใช้งาน เพื่อควบคุม ดูแล และตรวจสอบการจัดหา พัฒนา และดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อให้มีความมั่นคงปลอดภัยที่ครอบคลุมการรักษาความลับ (Confidentiality) ลดความเสี่ยงด้านความไม่ถูกต้องของข้อมูล (Integrity) และสภาพความพร้อมใช้งาน (Availability)

ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการในการป้องกันความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศบนเครือข่ายสาธารณะ โดยป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไขข้อมูลสารสนเทศโดยไม่ได้รับอนุญาตและรักษาความถูกต้องและครบถ้วนของข้อมูลสารสนเทศที่เปิดเผยต่อสาธารณะ

ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการการป้องกันข้อมูลสารสนเทศกรณีที่มีการดำเนินธุรกรรมของบริการสารสนเทศ (Protecting application service transactions) เพื่อป้องกันการส่งข้อมูลที่ผิดพลาด หรือการเปิดเผยข้อมูลที่ไม่ได้รับอนุญาต หรือการส่งข้อมูลไม่ถูกต้องหรือซ้ำซ้อนนอกจากนี้ ฝ่ายเทคโนโลยีสารสนเทศกำหนดขั้นตอนปฏิบัติในการจัดหา พัฒนา และดูแลรักษาระบบเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร และสื่อสารรายละเอียดดังกล่าวให้แก่ผู้ปฏิบัติงานและบุคคลที่เกี่ยวข้องรับทราบอย่างทั่วถึง

10.2 การจัดหาระบบเทคโนโลยีสารสนเทศ

- **พนักงานบันทึกการร้องขอการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ (IT System/Change Request Form) โดยต้องจัดทำบันทึกเป็นลายลักษณ์อักษร**
- **ผู้บังคับบัญชาสูงสุดของแต่ละฝ่ายงานพิจารณาตรวจสอบและอนุมัติการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ และลงนามอนุมัติในบันทึกการการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ (IT System/Change Request Form)**
- **ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศตรวจสอบ พิจารณาตรวจสอบและอนุมัติการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ และลงนามอนุมัติในบันทึกการจัดหาหรือเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ (IT System/Change Request Form)**
- **ฝ่ายเทคโนโลยีสารสนเทศประเมินผลกระทบของการเปลี่ยนแปลงของระบบงานเทคโนโลยีสารสนเทศทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการปฏิบัติงาน (Functionality) รวมถึงกฎเกณฑ์และข้อบังคับของหน่วยงานกำกับดูแล ที่เกี่ยวข้องกับระบบงานที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร พร้อมสรุปอุปสรรค ปัญหา และขั้นตอนในการปรับปรุงละแก้ไข และรายงานให้รองประธานพนักงานบริหารที่กำกับดูแลฝ่ายงานเทคโนโลยีสารสนเทศทราบ**
- **ฝ่ายเทคโนโลยีสารสนเทศควบคุมการร้องขอการจัดหาหรือเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมตามการจัดการการเปลี่ยนแปลงระบบงาน**
- **ในการจัดหาระบบเทคโนโลยีสารสนเทศและผู้ให้บริการจากภายนอก ฝ่ายเทคโนโลยีกำหนดแนวปฏิบัติดังนี้**
- กำหนดให้มีการตรวจสอบ และ/หรือ ทดสอบคุณสมบัติของระบบเทคโนโลยีสารสนเทศร่วมกับผู้ใช้งานเพื่อรวบรวมความต้องการการใช้งานระบบ (Requirement)
- กำหนดระบบมาตรฐาน Platform ของระบบเทคโนโลยีสารสนเทศ โดยคำนึงถึงความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (IT Security) เป็นหลัก
- กำหนดให้มีการทำระบบคอมพิวเตอร์สำรองฉุกเฉิน (Disaster Recovery Solution) สำหรับระบบที่มีความเสี่ยงระดับ Critical
- กำหนดให้มีมาตรฐานในการตรวจสอบช่องโหว่และทดสอบระบบความมั่นคงปลอดภัยสารสนเทศ ในการจัดหาและให้กำหนดระยะเวลาในการตรวจสอบและแก้ไขช่องโหว่ที่เกิดขึ้น

- ฝ่ายเทคโนโลยีสารสนเทศจัดทำข้อกำหนดการว่าจ้าง (TOR) ตามรายละเอียดที่กำหนด และนำเสนอต่อผู้บริหารสูงสุดสายงานเทคโนโลยีสารสนเทศเพื่อพิจารณาและอนุมัติ และเข้าสู่กระบวนการจัดซื้อตามนโยบายการจัดซื้อ OKJ-P2P.-PU0.-1 การจัดการใบสั่งซื้อ ของฝ่ายจัดซื้อที่กำหนดไว้

10.3 การพัฒนาระบบเทคโนโลยีสารสนเทศ (Secure development policy)

- **ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้แบ่งส่วนระบบเทคโนโลยีสารสนเทศที่มีไว้เฉพาะสำหรับการพัฒนาระบบ (Develop environment) ออกจากระบบงานที่ใช้ปฏิบัติงานจริง (Production environment) และกำหนดการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องและได้รับอนุญาตเท่านั้น ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้มีการแยกเครื่องแม่ข่าย (Server) ที่ใช้ในการพัฒนา (Development Server)การทดสอบระบบ (QA Server) การให้บริการ/ใช้งานจริง (Production Server) แยกเป็นอิสระจากกัน พร้อมทั้งกำหนดให้ทีมงานพัฒนาระบบ จัดทำเอกสาร Blueprint และเอกสาร Design Specification ของโครงการ**
- **ในกรณีการว่าจ้างผู้ให้บริการภายนอก ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้มีขั้นตอนการพัฒนาระบบเทคโนโลยีสารสนเทศ (System development Life Cycle : SDLC) ตามหลักการการพัฒนาที่กำหนดกับผู้ให้บริการภายนอก พร้อมทั้งมีการระบุสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ และข้อมูล (Authorization Matrix)**
- **พนักงานผู้ร้องขอ รวมถึงผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในการพัฒนาหรือเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศให้ตรงตามความต้องการ**
- **พนักงานฝ่ายเทคโนโลยีสารสนเทศต้องตระหนักถึงระบบการรักษาความปลอดภัย (Security) และความพร้อมในการใช้งาน (Araciality) ของระบบตั้งแต่ช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง**
- **ผู้พัฒนาระบบเทคโนโลยีสารสนเทศต้องกำหนดมาตรการป้องกันสภาพแวดล้อมการพัฒนาระบบให้ปลอดภัยตลอดทุกขั้นตอนของการพัฒนา**

10.4 การติดตั้งและทดสอบระบบเทคโนโลยีสารสนเทศ

- พนักงานฝ่ายเทคโนโลยีสารสนเทศและพนักงานผู้ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบเพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศที่ได้รับการพัฒนา หรือเปลี่ยนแปลงที่มีประสิทธิ์ภาพ ถูกต้อง เป็นไปตามความต้องการและมั่นใจว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย ก่อนที่จะนำไปใช้จริง
- หากระบบเทคโนโลยีสารสนเทศมีสาระสำคัญต่อบริษัท ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้มีหน่วยงานตรวจสอบภายในหรือผู้ตรวจอิสระตรวจสอบการพัฒนาและทดสอบระบบ ก่อนที่จะนำไปใช้จริงพนักงานฝ่ายเทคโนโลยีสารสนเทศตรวจสอบควบคุม และจำกัดการเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปที่ใช้งาน(Software Packages) โดยกำหนดให้สามารถเปลี่ยนแปลงได้เท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดต้องได้รับการทดสอบและบันทึกอย่างเป็นลายลักษณ์อักษร เพื่อความมั่นคงปลอดภัยของซอฟต์แวร์และการบำรุงรักษาซอฟต์แวร์ดังกล่าวในอนาคต
- พนักงานฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรฐานความมั่นคงปลอดภัยด้านวิศวกรรมระบบ (System engineer เพื่อประยุกต์ใช้งานในการพัฒนาหรือเปลี่ยนแปลงระบบข้อมูลที่นำไปทดสอบต้องได้รับการอนุมัติจากผู้บังคับบัญชาสูงสุดของฝ่ายงานเจ้าของข้อมูลอย่างเป็นลายลักษณ์อักษร และต้องได้รับการป้องกัน และควบคุมอย่างระมัดระวัง เมื่อทดสอบเสร็จสิ้นข้อมูลดังกล่าวต้องได้รับการลบออกจากสภาพแวดล้อมหรือระบบที่ทำการทดลอง (Testing environment) ทันที ทั้งนี้พนักงานฝ่ายเทคโนโลยีต้องบันทึกการทดสอบข้อมูล และการลบข้อมูลออกจากการทดสอบอย่างเป็นลายลักษณ์อักษร และรายงานต่อผู้บังคับบัญชาสูงสุดของฝ่ายงานเจ้าของข้อมูล

10.5 การนำระบบเทคโนโลยีสารสนเทศที่จัดหา พัฒนา หรือเปลี่ยนแปลงไปใช้จริง

- ฝ่ายเทคโนโลยีสารสนเทศต้องตรวจสอบการโอนย้ายระบบให้ถูกต้องและครบถ้วน พร้อมทั้งจัดเก็บข้อมูลรายละเอียดเกี่ยวกับการพัฒนาหรือการเปลี่ยนแปลงของระบบที่ผ่านมา และปรับปรุงเอกสารประกอบระบบทั้งหมด ภายหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน รายชื่อผู้มีสิทธิ์ใช้งาน ขั้นตอนการทำงานของระบบ System specification เป็นต้น โดยเอกสารดังกล่าวต้องจัดเก็บในสถานที่ที่เหมาะสม ปลอดภัย และสะดวกต่อการนำไปใช้งาน

- ฝ่ายเทคโนโลยีสารสนเทศกำหนดให้จัดทำแผนการโอนย้ายข้อมูล (Data Migration Plan) ทุกครั้ง ก่อนการปรับปรุงหรือการโอนย้ายข้อมูลจากระบบเก่าสู่ระบบใหม่ และกำหนดให้มีมาตรฐานในการตรวจสอบช่องโหว่และทดสอบระบบความมั่นคงปลอดภัยสารสนเทศ ในการเปลี่ยนแปลงแก้ไขระบบงานที่ให้บริการ และให้กำหนดระยะเวลาในการตรวจสอบและแก้ไขช่องโหว่ที่เกิดขึ้น
- ฝ่ายเทคโนโลยีสารสนเทศต้องจัดเก็บเวอร์ชั่นของระบบก่อนการพัฒนาไว้ หากระบบที่พัฒนาหรือเปลี่ยนเวอร์ชั่นใหม่ไม่สามารถใช้งานได้
- ฝ่ายเทคโนโลยีสารสนเทศทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่งเพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งานฝ่ายเทคโนโลยีสารสนเทศสื่อสารถึงระบบที่พัฒนาหรือเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องรับทราบและสามารถนำไปใช้งานได้อย่างถูกต้องและเหมาะสม
- ฝ่ายเทคโนโลยีสารสนเทศกำหนดเกณฑ์การยอมรับระบบเทคโนโลยีสารสนเทศใหม่ (System Acceptance) สำหรับระบบเทคโนโลยีสารสนเทศที่พัฒนาเอง หรือการจัดซื้อระบบเทคโนโลยีสารสนเทศอื่นๆ ก่อนการใช้งาน โดยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศต้องตรวจสอบพร้อมลงนามยอมรับระบบก่อนนำไปใช้จริง ทั้งนี้ เกณฑ์การยอมรับระบบเทคโนโลยีสารสนเทศใหม่ (System Acceptance) ครอบคลุมประเด็นที่สำคัญต่าง ๆ เช่น
- การทดสอบการยอมรับระบบโดยผู้ใช้งาน (User acceptance testing)
- การประเมินระบบความปลอดภัยของระบบ (Security assessment)
- การช่วยเหลือโดยผู้พัฒนาระบบหรือผู้ขาย (Help desk or issue management protocol)
- การตรวจสอบคู่มือหรือขั้นตอนการปฏิบัติงาน (Operating procedures testing)
- การแก้ไขปัญหาหรือแผนการปฏิบัติในกรณีฉุกเฉิน (Error recovery and contingency plan)

10.6 การติดตาม และดูแลรักษาระบบเทคโนโลยีสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศกำหนดขั้นตอนปฏิบัติในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ดังนี้

- กำหนดให้มีการป้องกันอย่างสม่ำเสมอและแก้ไขช่องโหว่ที่เกิดขึ้นทุกครั้งที่พบ โดยจะต้องแจ้งและได้รับการอนุมัติจากผู้จัดการระบบ หรือผู้จัดการโครงการทุกครั้ง
- กำหนดระดับความสำคัญของระบบ ดังนี้ Critical System, High System, Medium System และ Low System และจะต้องทำสัญญาการบำรุงรักษาอยู่เสมอกำหนดมาตรฐานและขั้นตอนการปฏิบัติงานเกี่ยวกับการบำรุงรักษาระบบ (MA Standard and Procedure)
- กำหนดให้ระยะเวลาของ MA สิ้นสุดทุกสิ้นปีกำหนดให้มีการจัดทำงบประมาณ MA ทุกปี โดยต้องมีการจัดตั้งงบประมาณ MA สำหรับระบบที่เป็น Critical และ High Impact เสมอ

10.7 การว่าจ้างหน่วยงานภายนอกเพื่อให้บริการ

ในการว่าจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบเทคโนโลยีสารสนเทศของบริษัท บริษัทต้องจัดทำสัญญาจ้างที่มีเนื้อหาชัดเจน และครอบคลุมทั้งในด้านลิขสิทธิ์ซอฟต์แวร์ การรักษาข้อมูลเป็นความลับ การใช้งานระบบ และการตรวจสอบระบบโดยละเอียดก่อนการใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ นอกจากนี้ หน่วยงานภายนอกต้องปฏิบัติตามข้อกำหนดในข้อ 8. ความมั่นคงปลอดภัยในการบริหารจัดการผู้ให้บริการ (Supplier Security Management)

11. การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

11.1 การเตรียมความพร้อมและบริหารจัดการความต่อเนื่องทางธุรกิจ

บริษัทจัดทำข้อปฏิบัติการรับมือเหตุการณ์ฉุกเฉินที่ส่งผลกระทบต่อการดำเนินธุรกิจของบริษัท โดยกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศจัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) เพื่อป้องกันหรือลดผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงักในการดำเนินธุรกิจของบริษัทอันเป็นผลมาจากความล้มเหลวของระบบเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังนี้

ฝ่ายเทคโนโลยีสารสนเทศกำหนดความต้องการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านความต่อเนื่องในการดำเนินธุรกิจ (IT Security and Continuity) แผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ควรครอบคลุมรายละเอียดดังต่อไปนี้

จัดลำดับความสำคัญของแต่ละระบบเทคโนโลยีสารสนเทศ ความสัมพันธ์ของระบบ และระยะเวลาในการกู้คืนระบบ

- ระบุและกำหนดเหตุการณ์หรือสถานการณ์ใดๆ ที่ส่งผลให้ระบบเกิดความล้มเหลวหรือหยุดชะงักพร้อมกำหนดและจัดลำดับความรุนแรงของเหตุการณ์และสถานการณ์นั้นๆ
- กำหนดแนวทางการแก้ไขปัญหา หรือแนวทางการตอบสนองต่อเหตุการณ์หรือสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย
- กำหนดพนักงานผู้รับผิดชอบ และผู้มีอำนาจในการตัดสินใจในการแก้ไขปัญหาอย่างชัดเจน
- กำหนดแนวทางการดำเนินการเพื่อให้บริษัทสามารถดำเนินการได้ต่อเนื่อง เช่น การสำรองข้อมูลและระบบเทคโนโลยีสารสนเทศ รวมถึงอุปกรณ์ที่สำคัญ การกู้ข้อมูล เป็นต้น
- บันทึกรายละเอียดของอุปกรณ์และระบบเทคโนโลยีสารสนเทศที่จำเป็นต้องใช้ในกรณีฉุกเฉินแต่ละระบบงาน เช่น Specification ของระบบและอุปกรณ์ ค่า Configuration อุปกรณ์เครือข่าย รุ่นของอุปกรณ์และระบบต่างๆ เป็นต้น
- กำหนดศูนย์ข้อมูลสารสนเทศสำรอง (ถ้ามี) โดยต้องระบุรายละเอียดอย่างชัดเจน
- กำหนดแนวทางการฟื้นฟูและปรับปรุงความเสียหายให้เข้าสู่การปฏิบัติงานตามปกติ

บริษัทกำหนดให้ฝ่ายเทคโนโลยีปรับปรุงหรือแก้ไขแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ให้ทันสมัยและเป็นปัจจุบันอยู่เสมอ และจัดเก็บแผนดังกล่าวไว้นอกสถานที่ที่ปลอดภัย

ฝ่ายเทคโนโลยีสารสนเทศต้องทดสอบการปฏิบัติตามแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) เป็นประจำอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะของการจำลองสถานการณ์จริง เพื่อให้มั่นใจว่าแผนดังกล่าวสามารถนำไปใช้ได้จริงในทางปฏิบัติ และบันทึกผลการทดสอบอย่างเป็นลายลักษณ์อักษรและนำมาปรับปรุงแผนให้มีประสิทธิ์ผลยิ่งขึ้น ทั้งนี้ ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดแผนการทดสอบแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) อย่างชัดเจนรวมถึงวัตถุประสงค์ ขอบเขตของระบบ ขั้นตอนการทดสอบ ระยะเวลาการทดสอบ สถานที่ อุปกรณ์ที่ใช้ ทรัพยากรที่ใช้ งบประมาณ และผู้รับผิดชอบตั้งแต่เริ่มจนสิ้นสุดกระบวนการทดสอบ

ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีอุปกรณ์หรือระบบเทคโนโลยีสารสนเทศในการประมวลผลข้อมูลสารสนเทศสำรองไว้อย่างเพียงพอ เพื่อรองรับเหตุการณ์ฉุกเฉิน โดยอุปกรณ์และระบบสำรองดังกล่าวต้องได้รับการทดสอบความพร้อมในการใช้งานอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และต้องบันทึกผลการทดสอบอย่างเป็นลายลักษณ์อักษรฝ่ายเทคโนโลยีสารสนเทศควรสื่อสารแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ให้บุคคลที่เกี่ยวข้องทราบเฉพาะเท่าที่จำเป็น

ในกรณีเกิดเหตุการณ์ฉุกเฉิน ฝ่ายเทคโนโลยีสารสนเทศต้องบันทึกข้อมูลของเหตุการณ์โดยละเอียด รวมถึงสาเหตุการแก้ไขและผลกระทบที่เกิดขึ้นทั้งในด้านการเงินและไม่ใช่การเงิน (Financial and non-financial impacts) เพื่อนำข้อมูลมาวิเคราะห์และปรับปรุงแผนดังกล่าวให้มีประสิทธิ์ผลและเหมาะสมยิ่งขึ้น

12. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Incident Management)

12.1 การบริหารจัดการและการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

บริษัทกำหนดขั้นตอนปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และผู้มีหน้าที่และความรับผิดชอบในการบริหารจัดการและแก้ไขปัญหาด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อให้พนักงานหรือผู้ที่พบเหตุการณ์สามารถรายงานและฝ่ายเทคโนโลยีสารสนเทศสามารถตอบสนองต่อเหตุการณ์ดังกล่าวได้อย่างทันเวลาและมีประสิทธิ์ภาพ โดยมีขั้นตอนการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามเอกสารแนบ 3.6 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

พนักงานหรือผู้พบเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ("เหตุการณ์ฯ") ต้องรายงานให้ฝ่ายเทคโนโลยีสารสนเทศทราบผ่านช่องทางการรายงานที่กำหนด เช่น โทรศัพท์ อีเมล์ แจ้งโดยตรงที่ฝ่ายเทคโนโลยีสารสนเทศ เป็นต้น ทันทีที่พบเหตุการณ์ฯ เพื่อให้สามารถตอบสนองและแก้ไขปัญหาได้อย่างทันเวลา

พนักงานหรือผู้พบเหตุการณ์ด้านความมั่นคงปลอดภัย หรือจุดอ่อน หรือการกระทำใดๆ ที่ไม่เหมาะสม (Information Security Weaknesses) ต่อฝ่ายเทคโนโลยีสารสนเทศทันทีที่สังเกตพบหรือเกิดความสงสัย โดยห้ามพิสูจน์หรือตรวจสอบข้อสงสัยเกี่ยวกับจุดอ่อนหรือการกระทำใดๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศด้วยตนเอง เว้นแต่เป็นความรับผิดชอบและหน้าที่ของบุคคลนั้นในการปฏิบัติงาน

พนักงานฝ่ายเทคโนโลยีสารสนเทศต้องบันทึกเหตุการณ์ฯ ในรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศโดยละเอียดเพื่อประเมิน จัดประเภท และจัดลำดับความสำคัญในการตอบสนองหรือแก้ไขเหตุการณ์ฯ ดังกล่าว

12.2 การตรวจสอบและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

บริษัทกำหนดขั้นตอนปฏิบัติในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เพื่อรองรับการแก้ไขและจัดการปัญหาได้อย่างทันเวลาและมีประสิทธิ์ภาพ โดยมีขั้นตอนการตรวจสอบและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามเอกสารแนบ 3.6 การตรวจสอบและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

- พนักงานฝ่ายเทคโนโลยีสารสนเทศวิเคราะห์ปัญหาที่เกิดขึ้น และจัดหาวิธีการตอบสนองและแก้ไขปัญหาที่เกิดขึ้น
- พนักงานฝ่ายเทคโนโลยีสารสนเทศอาจพิจารณาปรึกษาหรือจัดจ้างผู้เชี่ยวชาญจากภายนอกเพื่อแก้ไขปัญหาที่เกิดขึ้นตามความเหมาะสม
- พนักงานฝ่ายเทคโนโลยีสารสนเทศบันทึกวิธีการแก้ไขและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร เพื่อใช้เป็นข้อมูลในการวิเคราะห์และจัดหาแนวทางการป้องกันปัญหาที่อาจเกิดขึ้นซ้ำในอนาคต

12.3 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้ฝ่ายเทคโนโลยีสารสนเทศบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ รวมถึงวิธีการในการแก้ไขปัญหาต่างๆ อย่างเป็นลายลักษณ์อักษร และสอบทานและวิเคราะห์เหตุการณ์ที่เกิดขึ้นอย่างสม่ำเสมออย่างน้อยเดือนละ 1 ครั้ง โดยพิจารณาปริมาณเหตุการณ์ที่เกิดขึ้นและมูลค่าความเสียหายและค่าใช้จ่าย เพื่อจัดทำแนวทางในการแก้ไขและป้องกันปัญหาจากเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิ์ภาพ โดยมีขั้นตอนการเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามเอกสารแนบ 3.6 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

13. การบริหารจัดการข้อมูลส่วนบุคคล

บริษัทกำหนดนโยบายและแนวปฏิบัติในการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดนโยบายและแนวปฏิบัติตามข้อกำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลของบริษัท และการบริหารจัดการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพ และสร้างความมั่นใจให้กับผู้มีส่วนได้เสียที่จะดำเนินงานร่วมกับบริษัท โดยกำหนดนโยบายและแนวปฏิบัติครอบคลุม ดังนี้

- การเก็บรวบรวมข้อมูลส่วนบุคคล
- วัตถุประสงค์ในการเก็บรวบรวม และการใช้ข้อมูลส่วนบุคคล
- แนวทางในการคุ้มครองข้อมูลส่วนบุคคล
- การเปิดเผยข้อมูลส่วนบุคคล
- การมีส่วนร่วมและสิทธิ์ของเจ้าของข้อมูลส่วนบุคคล
- การทบทวนและเปลี่ยนแปลงนโยบายการคุ้มครองข้อมูลส่วนบุคคล

14. การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร (Compliance)

14.1 การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ

นโยบาย

14.1.1 การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

1) องค์กรต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือ สัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร
2) พนักงานภายในองค์กรทุกคน รวมถึงผู้บริหารขององค์กร ต้องรับทราบ ทำความเข้าใจ และปฏิบัติตาม รายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยี สารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการ ตรวจสอบกับกฎหมาย IT และมีรายการดังต่อไปนี้เป็นอย่างน้อย
   - นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
   - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
   - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
   - พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
   - พ.ร.บ. ลิขสิทธิ์
3) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศขององค์กร ถือเป็น สินทรัพย์ขององค์กร (ยกเว้น ข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิ์บัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้องค์กร สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้ง ให้ผู้ใช้งานทราบล่วงหน้า
4) เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศขององค์กร และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ขององค์กร กำหนดไว้

5) องค์กร ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้อง แจ้งให้ทราบล่วงหน้า อย่างไรก็ตามองค์กร จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำ เป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใดๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตาม คำสั่งศาลตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น

6) ห้ามพนักงานในองค์กร ใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศขององค์กร กระทำ การใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

7) การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใดๆ ออกนอกประเทศ ไม่ขัดต่อ ข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้อง ปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

14.1.2 สินทรัพย์ทางปัญญา (Intellectual Property Rights)

1) องค์กรต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด

2) องค์กรต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่าง เคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตาม ลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดง ความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่ตามคู่มือการปฏิบัติงานเรื่องการตรวจสอบการใช้ซอฟต์แวร์ที่ละเมิด สินทรัพย์ทางปัญญา (Monitoring of illegal Software Usage Procedure)

3) ห้ามผู้ใช้งานดำเนินการทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบ เทคโนโลยีสารสนเทศขององค์กร โดยเด็ดขาด

4) เพื่อที่จะให้เกิดความแน่ใจว่าพนักงานในองค์กร มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ ตั้งใจหรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใดๆ ที่ติดตั้งอยู่ในเครื่อง คอมพิวเตอร์ขององค์กร เพื่อจุดประสงค์ใดๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตจากทางแผนกเทคโนโลยีสารสนเทศ และในขณะเดียวกันพนักงานในองค์กร ไม่ควรจะติดตั้งโปรแกรมใดๆ ลงใน เครื่องคอมพิวเตอร์ขององค์กร โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามี ใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

5) องค์กร กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 2 ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าองค์กร มีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาต ซอฟต์แวร์เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น องค์กรอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบ อนุญาตอย่างถูกต้อง อื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

14.1.3 การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

1) องค์กร ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล

14.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

1) องค์กร ต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญาที่ เกี่ยวกับองค์กร

14.1.5 การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

1) องค์กร ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอน ปฏิบัติขององค์กร

นโยบาย

14.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

1) องค์กรต้องมีการทบทวน วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติ ขององค์กร เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย วิธีปฏิบัติงานต่างๆ ให้ถูกต้องและเป็นปัจจุบัน ตามรอบระยะเวลาที่กำหนด เช่น ปีละ 1 ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

14.2.2 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

1) องค์กรต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคง ปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้
2) องค์กรต้องมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึง แบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

14.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

1) องค์กรต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วตาม ระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่า ระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และ ทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

15. การตรวจสอบนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

คณะกรรมการบริษัท และฝ่ายเทคโนโลยีสารสนเทศสอบทานและทบทวนความเหมาะสมของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเป็นประจำทุกปี เพื่อให้มั่นใจว่านโยบายฉบับนี้มีความถูกต้อง สอดคล้อง เป็นปัจจุบัน และเป็นไปตามกฎหมายหรือข้อบังคับที่เกี่ยวข้อง และนำเสนอต่อคณะกรรมการบริษัทเพื่อพิจารณาอนุมัตินโยบาย ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศฉบับนี้ ได้รับอนุมัติจากที่ประชุมคณะกรรมการบริษัท