บริษัท บีพีเอส เทคโนโลยี จำกัด (มหาชน)
25/34-38, 47-51 ถ.สุขุมวิท ต.ปากน้ำ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
Tel : 02-755-2688 Fax : 02-380-5096-99 Tax ID : 0107566000526
BPS Technology Public Company Limited
25/34-38, 47-51 Sukhumvit Rd., Paknam, Muang Samutprakan, Samutprakan 10270

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

(Information Security Policy)

1. บทนำ

บริษัท บีพีเอส เทคโนโลยี จำกัด (มหาชน) (“บริษัท”) กำหนดให้เทคโนโลยีสารสนเทศและการสื่อสาร เป็นปัจจัยสำคัญที่ช่วยส่งเสริมการดำเนินธุรกิจและเพิ่มประสิทธิภาพการทำงาน ฉะนั้น จึงเป็นความรับผิดชอบร่วมกันของพนักงานทุกคน ที่จะต้องใช้เทคโนโลยีสารสนเทศและการสื่อสารภายใต้ข้อบังคับของกฎหมาย คำสั่งบริษัทและตามมาตรฐานที่บริษัทกำหนด และบริษัทได้จัดให้มีการบริหารความปลอดภัยของระบบสารสนเทศ ซึ่งหมายถึง ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ตามมาตรฐานสากล (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือกฎหมายอื่นที่เกี่ยวข้อง) ทั้งนี้ พนักงานบริษัททุกคนมีหน้าที่และข้อปฏิบัติตามนโยบายฉบับนี้

2. การกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

นโยบายสำคัญที่เกี่ยวกับการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) จะแบ่งเป็น 14 หมวดดังนี้

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยขององค์กร
หมวดที่ 2 นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)
หมวดที่ 3 ความมั่นคงปลอดภัยสารสนเทศ
หมวดที่ 4 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล
หมวดที่ 5 การบริหารจัดการทรัพย์สิน
หมวดที่ 6 การควบคุมการเข้าถึง
หมวดที่ 7 การเข้ารหัสข้อมูล (Cryptography)
หมวดที่ 8 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการดำเนินการ
หมวดที่ 10 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล
หมวดที่ 11 การจัดหา พัฒนา และดูแลระบบสารสนเทศ
หมวดที่ 12 ความสัมพันธ์กับผู้ให้บริการภายนอก
หมวดที่ 13 การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ Cloud Computing
หมวดที่ 14 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
หมวดที่ 15 การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ
หมวดที่ 16 ความสอดคล้อง

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

1. นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

1.1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

<u>จุดประสงค์และขอบเขต :</u>

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

นโยบายความปลอดภัยสารสนเทศ ครอบคลุมถึงการปกป้องข้อมูลขององค์กรเป็นหลัก ข้อมูลในนโยบายนี้หมายถึง ข้อมูลในรูปแบบอิเล็กทรอนิกส์ เอกสาร สิ่งพิมพ์ ฟิล์ม หรือแม้แต่ในรูปของการสนทนา อย่างไรก็ตามการปกป้องข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ จะกล่าวถึงเป็นส่วนใหญ่เนื่องจากข้อมูลขององค์กรนั้นจะอยู่ในรูปอิเล็กทรอนิกส์

<u>เนื้อหานโยบาย และการดำเนินการ :</u>

1.1.1. การจัดทำนโยบายความปลอดภัยสารสนเทศ (Information Security Policy

- ต้องจัดทำนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศไว้เป็นลายลักษณ์อักษร เพื่อให้เกิดความเชื่อมั่น และมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยนโยบายดังกล่าวจะต้องได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการ โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นขององค์กร ตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สินสารสนเทศขององค์กร
- ต้องจัดให้มีการสื่อสาร/ประกาศใช้นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้บุคลากรภายในองค์กร หน่วยงานภายนอก และผู้ที่เกี่ยวข้องรับทราบ โดยมีหน้าที่จะต้องสนับสนุน ดำเนินการตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเคร่งครัด การฝ่าฝืนนโยบายนี้ ถือเป็นความผิดที่ร้ายแรง โดยมีบทลงโทษถึงขั้นสูงสุดตามระเบียบขององค์กร

1.1.2. การทบทวนนโยบายความปลอดภัยสารสนเทศ (Review of the Information Security Policy)

- ต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อย 1 ครั้งต่อปี โดยสอดคล้องกับรอบการทบทวนกฎบัตรและนโนบายของบริษัท หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การเปลี่ยนแปลงกลยุทธ์หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงที่สำคัญต่อองค์กร

หมวดที่ 2 นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

2.1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จุดประสงค์และขอบเขต :

ผู้จัดการส่วนเทคโนโลยีมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

เนื้อหานโยบาย และการดำเนินการ :

2.1.1 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)

- ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย(Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้องมีการควบคุมการเข้า-ออกและการใช้งาน การตรวจสอบระบบต่างๆ เช่น ระบบเตือนอุณหภูมิภายในห้อง ระบบเตือนอัคคีภัย เป็นต้น
- ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัท เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้งซึ่งอาจมีมัลแวร์ หรือไวรัสคอมพิวเตอร์ หรือมีช่องโหว่เชื่อมต่อเครือข่ายภายนอก เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น
- ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัท ต้องมีตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่งอีเมล เป็นต้น
- ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ และข้อมูล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูล

2.1.2. การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

- ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี

- ความเสี่ยงจากผู้ปฏิบัติงาน ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลเกินกว่าหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้
- ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น
- ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่ทำการใช้งานอยู่อาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

2.1.3 การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้

จัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

2.1.4 กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

หมวดที่ 3 ความมั่นคงปลอดภัยสารสนเทศ
(Organizational of Information Security)

3. ความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

3.1. โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร (Internal Organization)

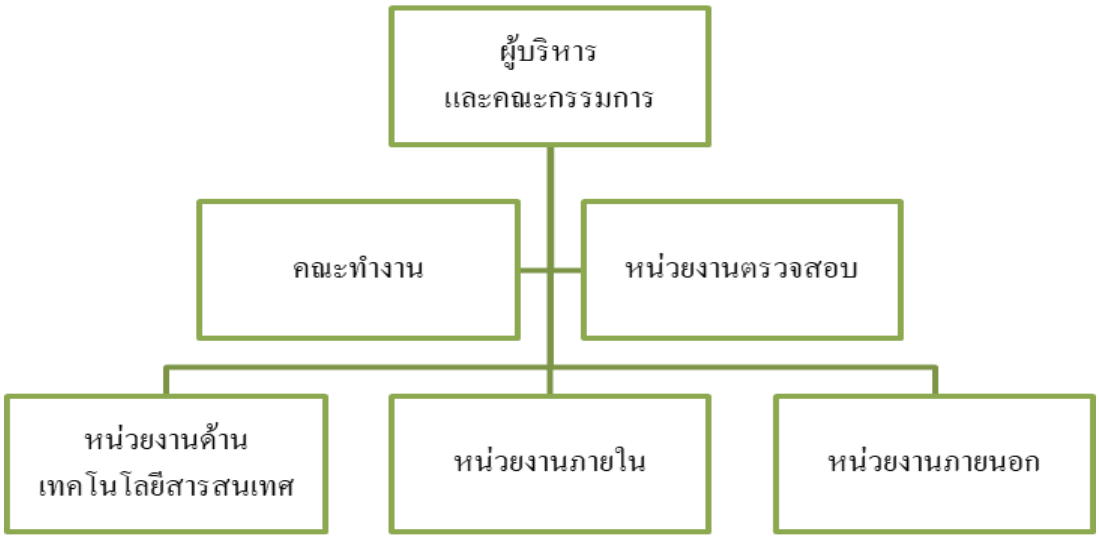
จุดประสงค์และขอบเขต :

เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์ ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย องค์กรจึงได้จัดทำโครงสร้างความปลอดภัยสารสนเทศ รวมถึงการกำหนดบทบาท และหน้าที่ในการบริหารจัดการความปลอดภัยของสารสนเทศภายในองค์กร

เนื้อหานโยบาย และการดำเนินการ :

3.1.1. บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

- ตัวแทนฝ่ายบริหารระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMR: Information Security Management Representative) ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน
- ผู้บริหารให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ โดยอนุมัติให้มีการจัดตั้งคณะกรรมการ หรือกลุ่มผู้ทำงานหลักด้านความปลอดภัยสารสนเทศ ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ดังนี้



โครงสร้างของคณะกรรมการความปลอดภัยสารสนเทศ แสดงดังภาพ

- คณะกรรมการความปลอดภัยสารสนเทศ ประกอบจากผู้บริหารของหน่วยงานต่าง ๆ ดังนี้
    - ประธานเจ้าหน้าที่บริหาร
    - รองประธานเจ้าหน้าที่บริหาร
    - ผู้อำนวยการฝ่ายการตลาด
    - ผู้อำนวยการฝ่ายปฏิบัติการ
    - ผู้อำนวยการฝ่ายบัญชีและการเงิน
- คณะกรรมการความปลอดภัยสารสนเทศมีหน้าที่ดังนี้
    - ตรวจสอบ และอนุมัติ ปรับปรุงนโยบายความปลอดภัยสารสนเทศ ตามกำหนด หรือตามสถานการณ์
    - วางแผนประชาสัมพันธ์ และอบรมบุคลากรทุกหน่วยเข้าใจถึงความปลอดภัยสารสนเทศ
    - ตรวจสอบ และให้ความเห็นชอบโครงการที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ
    - วางแผน ตรวจสอบ และบริหารจัดการความเสี่ยงต่าง ๆ ที่เกิดจากข้อจำกัดของระบบ
    - ตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องด้านความมั่นคงปลอดภัย กรณีฉุกเฉิน

3.1.2. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

คณะกรรมการความปลอดภัย ได้กำหนดบทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องตามโครงสร้างของคณะกรรมการความปลอดภัยสารสนเทศ ดังนี้

- หน้าที่ของประธานเจ้าหน้าที่บริหาร (CEO) กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัทและอนุมัตินโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
- หน้าที่ของของประธานเจ้าหน้าที่บริหาร
    - ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่ารวมทั้งจัดหาและพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท
    - ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ
- หน้าที่ของประธานเจ้าหน้าที่สายงานบัญชีและการเงิน (CFO)
    - ควบคุมและดูแลให้พนักงานสายงานบัญชีและการเงินปฏิบัติตามนโยบายความปลอดภัยสารสนเทศอย่างเคร่งครัด

- ควบคุมการรักษาความลับของข้อมูล สารสนเทศขององค์กรด้านบัญชีและการเงินของพนักงาน
- วางแผน ดูแล และกำกับการใช้งานนโยบายเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับด้านบัญชีและการเงิน

- หน้าที่ของผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ (IT Manager)
  - กำหนดเป้าหมายนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทโดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท
  - จัดการพัฒนานโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ Policy, Standard, Procedure และ Guideline เพื่อให้บริษัทได้มาซึ่ง การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)
  - จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่างๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน
  - มีการบริหารความเสี่ยง และการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจของบริษัท
  - นำเสนอผู้บริหารระดับสูง เช่น ประธานเจ้าหน้าที่บริหาร (CEO) เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง
  - เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ
- หน้าที่ของหน่วยงานตรวจสอบ รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศขององค์กร
- หน่วยงานภายใน คือ พนักงานทุกคนขององค์กร ที่มีส่วนเกี่ยวข้องกับสารสนเทศไม่ว่าทางใดทางหนึ่ง มีหน้าที่รับผิดชอบ ดังนี้
  - ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศอย่างเคร่งครัด
  - รักษาความลับของข้อมูล สารสนเทศขององค์กร และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง
  - รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัยเมื่อเกิดเหตุการณ์ดังกล่าวให้กับหน่วยงานด้านเทคโนโลยีสารสนเทศ
  - ใช้งานข้อมูล และทรัพย์สินทางข้อมูลขององค์กรอย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบ หรือได้รับอนุญาตเท่านั้น

- หน่วยงานภายนอก คือ บุคคลภายนอกที่เข้ามาปฏิบัติงานในองค์กรหรือทำงานให้กับองค์กร ซึ่งมีส่วนเกี่ยวข้องในการใช้ข้อมูลหรือทรัพย์สินสารสนเทศอื่นขององค์กร เช่น ผู้ให้บริการ/ผู้จำหน่าย ระบบคู่สัญญาหรือผู้ที่ได้รับอนุญาตโดยมีหน้าที่ความรับผิดชอบเช่นเดียวกับพนักงานขององค์กร

3.2. อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

<u>จุดประสงค์และขอบเขต :</u>

เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานจากภายนอก และการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

<u>เนื้อหานโยบาย และการดำเนินการ :</u>

3.2.1. นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

ต้องมีการกำหนดและปฏิบัติตามนโยบาย หรือมาตรการสนับสนุน สำหรับการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook, Tablet, Smartphone และอุปกรณ์สื่อสารเคลื่อนที่อื่นๆ) ที่มีการนำมาใช้งาน เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว และควรคำนึงถึงความเสี่ยงของการทำงานในสภาพแวดล้อมที่ไม่ได้รับการป้องกัน โดยให้พนักงานแจ้งทางอีเมล์ หรือช่องทางการสื่อสารอื่นอย่างเป็นลายลักษณ์อักษร ระบุความต้องการขอนำเครื่องประเภทพกพาเข้ามาใช้ภายในบริษัท เพื่อให้ฝ่ายเทคโนโลยีสารสนเทศรับทราบ พร้อมกับสำเนาอีเมล์ให้หัวหน้าหน่วยงานของพนักงานรับทราบด้วย

3.2.2. การปฏิบัติงานจากระยะไกล (Teleworking)

อนุญาตให้บุคลากรขององค์กรที่จำเป็นต้องปฏิบัติงานจากภายนอกสำนักงานฯ โดยให้พนักงานเขียนแบบฟอร์มใบลงทะเบียนและการถอดถอนสิทธิ์ของพนักงาน ส่งให้หัวหน้าหน่วยงานพิจารณาอนุมัติ และส่งให้ฝ่ายเทคโนโลยีสารสนเทศรับทราบและดำเนินการ เพื่อให้มีการตรวจพิสูจน์ตัวตนและควบคุมการทำงานจากระยะไกลโดยการแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในสำนักงานฯ และใช้งานเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

หมวดที่ 4 ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

4. ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

4.1. นโยบายก่อนการจ้างงาน (Prior to Employment Policy)

<u>จุดประสงค์และขอบเขต :</u>

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเอง และมีความเหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงานองค์กร

<u>เนื้อหานโยบาย และการดำเนินการ :</u>

4.1.1. การคัดเลือกบุคลากร (Screening)

- เจ้าหน้าที่ทรัพยากรบุคคล ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นพนักงานประจำ พนักงานชั่วคราว หรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน
- เจ้าหน้าที่ทรัพยากรบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และหน่วยงานว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement : NDA) และให้รับรองว่าไม่มีประวัติในการบุกรุก โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้นๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงาน และผูกพันต่อเนื่อง ภายหลังจากที่สิ้นสุดการว่าจ้างแล้วนำระยะเวลาผูกพันที่ระบุในนโยบายออกเนื่องจากสอดคล้องกับ NDA ที่ใช้ปฏิบัติงานจริงกับพนักงาน ณ ปัจจุบัน

4.1.2. ข้อตกลง และเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

หน่วยงานทรัพยากรบุคคล ต้องกำหนดเงื่อนไขการจ้างงานในสัญญาจ้างกับพนักงาน รวมถึงมีการระบุหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ (Job Description) ที่ชัดเจน โดยเจ้าหน้าที่ทรัพยากรบุคคล ต้องแจ้งให้ฝ่าย IT และหน่วยที่เกี่ยวข้องทราบทันทีเมื่อมีเหตุ ดังนี้

- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

4.2. นโยบายระหว่างการจ้างงาน (During Employment Policy)

<u>จุดประสงค์และขอบเขต :</u>

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนัก และปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร และเพื่อลดความเสี่ยงของสารสนเทศที่เกิดจากบุคลากร ทั้งที่เกิดจากการละเมิดความปลอดภัยสารสนเทศโดยเจตนาและไม่ได้เจตนา หรือจากการละเลยต่อการปฏิบัติหน้าที่ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

เนื้อหานโยบาย และการดำเนินการ :

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

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

- พนักงานขององค์กรทุกคนต้องได้รับการอบรมให้ความรู้ โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล
- ต้องจัดอบรมให้ความรู้แก่เจ้าหน้าที่ภายในองค์กร เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย การเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรด้วย
- พนักงานที่เข้าใหม่ทุกคนจะต้องได้รับการอบรมเกี่ยวกับนโยบายรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร หรือได้รับเอกสารนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศฉบับย่อ และระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานภายใน 30 วันนับจากเข้าทำงานในหน่วยงาน เพื่อให้พนักงาน หรือผู้ที่เกี่ยวข้องได้ศึกษา และถือปฏิบัติโดยอาจเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย
- เจ้าหน้าที่ทรัพยากรบุคคล และเจ้าหน้าที่ IT มีหน้าที่ในการแจ้งให้ทราบ เกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรให้แก่บุคลากรด้วย

4.2.2. กระบวนการทางวินัย (Disciplinary Process)

ผู้บริหาร ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือ ระเบียบปฏิบัติขององค์กร โดยพนักงานทุกคนต้องลงลายมือชื่อรับทราบในแบบฟอร์มการรับทราบเงื่อนไขการใช้งานระบบสารสนเทศ ซึ่งกระบวนการทางวินัยที่กำหนดขึ้นนี้เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยการฝ่าฝืนหรือละเลยต่อหน้าที่และนโยบายถือว่ามีความผิด ต้องพิจารณาตามบทลงโทษขององค์กร ซึ่งขึ้นอยู่กับความรุนแรงของผลกระทบที่เกิดขึ้นกับองค์กร

4.3. นโยบายหลังการสิ้นสุด หรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment Policy)

จุดประสงค์และขอบเขต :

เป็นการควบคุมความปลอดภัยของสารสนเทศให้ดียิ่งขึ้น และเพื่อป้องกันผลประโยชน์ขององค์กร ซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

เนื้อหานโยบาย และการดำเนินการ :

4.3.1. การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

หน่วยงานทรัพยากรบุคคลและหน่วยงานต่าง ๆ ร่วมกันกำหนดขั้นตอนการปฏิบัติ ของพนักงานที่ออกจากองค์กร เมื่อสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อมีการเปลี่ยนการจ้างงาน ดังนี้

- หน่วยงานที่เกี่ยวข้อง มีหน้าที่แจ้งไปยังหน่วยงานทรัพยากรบุคคล ถึงเรื่องการลาออก หรือการปรับเปลี่ยนตำแหน่งของพนักงาน
- หน่วยงานทรัพยากรบุคคล แจ้งให้หน่วยงานด้านเทคโนโลยีสารสนเทศทราบทันทีที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานขององค์กรเพื่อทำการถอดถอนสิทธิ การเข้าใช้ระบบงานต่าง ๆ และการเข้า-ออกพื้นที่ขององค์กร โดยให้ปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการลาออก (QP-HRD-011) ของฝ่ายทรัพยากรบุคคล เพื่อดำเนินการเพิกถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ์
- หน่วยงานด้านเทคโนโลยีสารสนเทศ ทำการสำรองข้อมูลที่จำเป็นของพนักงาน และแจ้งให้ให้หน่วยงานที่เกี่ยวข้องทราบถึงวิธีเข้าถึงข้อมูลดังกล่าว

หมวดที่ 5 การบริหารจัดการทรัพย์สิน
(Asset Management)

5. การบริหารจัดการทรัพย์สิน (Asset Management)

5.1. นโยบาย และหน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets Policy)

<u>จุดประสงค์และขอบเขต</u>

ทรัพย์สิน หมายถึง ทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ข้อมูล ซอฟต์แวร์ หรืออุปกรณ์ที่เกี่ยวข้องในการประมวลผล นอกจากนี้องค์กรควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน แต่อย่างไรก็ตามเจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว เพื่อให้มีการระบุทรัพย์สินขององค์กร และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

<u>เนื้อหานโยบาย และการดำเนินการ</u>

5.1.1. การจัดการบัญชีทรัพย์สิน (Inventory of Assets)

- ต้องจัดทำและเก็บทะเบียนสินทรัพย์ ซึ่งรวมถึงสินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ (Software Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ของสำนักงานฯ โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการควบคุมสินทรัพย์ถาวร ของฝ่ายบัญชี
- ต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภท ตามระยะเวลาที่กำหนดไว้ ตรวจนับร่วมกับฝ่ายบัญชี ปีละ 1 ครั้ง และสุ่มตรวจนับโดยฝ่ายเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง
- ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

5.1.2. ผู้ถือครองทรัพย์สิน (Ownership of Assets)

หน่วยงานผู้รับผิดชอบข้อมูลและสินทรัพย์ มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น เจ้าของทรัพย์สิน ต้องสอบทานความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สินตลอดจนการแจ้งถึงการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินทราบ

5.1.3. การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets)

- ต้องมีการกำหนดกฎเกณฑ์สำหรับการใช้งานสารสนเทศอย่างเหมาะสม และกฎการอนุญาตให้ใช้ข้อมูลและทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ โดยแสดงบันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูล ตามระเบียบบริษัทเรื่องการแจ้งจัดเตรียมอุปกรณ์คอมพิวเตอร์และระบบงานสำหรับพนักงานใหม่ และเรื่องการขอยืมใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ IT ชั่วคราว

- การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์ มีดังนี้
  - ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่บริษัทฯ เป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของบริษัทฯ การใช้งานระบบและอุปกรณ์ต่างๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวน หรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
  - เจ้าหน้าที่ ตลอดจนหน่วยงานภายนอกที่ได้รับการว่าจ้างโดยบริษัทฯ จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูลและระบบสารสนเทศของบริษัทฯ
  - ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ของสำนักงานฯ อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
  - เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของบริษัทฯ ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
  - ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของบริษัทฯ รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใดๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทฯ ก่อนได้รับอนุญาตจากผู้บริหาร/ผู้มีอำนาจ
  - เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัทฯ อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกัน สปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนำที่ระบุไว้ตามหัวข้อ 3.2.1 นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)
  - อุปกรณ์คอมพิวเตอร์ของสำนักงานฯต้องไม่ถูกดัดแปลงหรือติดตั้งอุปกรณ์เพิ่มเติมใดๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้นๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์ หรือซอฟต์แวร์ใดๆ บนเครื่องคอมพิวเตอร์ของสำนักงานฯ อย่างเด็ดขาด

- การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้
    - ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัทฯ
    - ซอฟต์แวร์ที่นำมาใช้ ในการประมวลผล และจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของสำนักงานฯ ทั้งที่ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสม โดยเป็นไปตามกรอบอำนาจอนุมัติก่อนนำมาติดตั้งก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัทฯ
    - ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของบริษัทฯ มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้
    - รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทฯ เท่านั้น
- การอนุญาตให้ใช้งานอินเทอร์เน็ต มีดังนี้
    - บริษัทฯ จัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำวิจัยการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงาน และการให้บริการของบริษัทฯ
    - ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทฯ และบุคคลผู้ที่เกี่ยวข้องกับบริษัทฯ เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
    - การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้บริษัทฯ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
    - หลีกเลี่ยงการคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต แต่หากดำเนินการโดยมิได้เจตนาให้แจ้งฝ่ายเทคโนโลยีสารสนเทศให้ทราบโดยทันที

- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
- ห้ามใช้สินทรัพย์ของบริษัทแสดงความคิดเห็นส่วนตัวของเจ้าหน้าที่ ในรูปแบบอิเล็กทรอนิกส์ทุกรูปแบบ โดยความเสียหายใดๆจากการแสดงความคิดเห็นดังกล่าวถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

- การอนุญาตให้ใช้งานอีเมล์ มีดังนี้
  - ผู้ใช้งานอีเมล์ทั้งหมดของสำนักงานฯ ควรมี E-mail Account เป็นของตนเอง หรืออย่างน้อยทุกแผนก/ส่วนงานต้องมี email กลาง เพื่อให้พนักงานสามารถใช้งานemailกลางร่วมกันได้
  - E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ ไปใช้ในทางที่ผิด
  - E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น info@big-electric.com อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป
  - E-mail Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของสำนักงานฯ ถือเป็นสินทรัพย์ของบริษัทฯ
  - ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือติดต่อสื่อสารกับระบบอีเมล์ของบริษัทฯ
  - ขนาดของอีเมล์และไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้
  - ผู้ใช้งานต้องลบอีเมล์ที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ ให้เป็นไปตามขนาดที่สำนักงานฯ กำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงาน และอีเมล์ตามที่กฎหมายกำหนดไว้เท่านั้น
  - ห้ามใช้ E-mail Account ของบริษัทฯ เพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
  - ห้ามใช้ E-mail Account ของบริษัทฯ ในการประกาศข้อมูลใดๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับบริษัทฯ

- ซอฟต์แวร์สำหรับใช้งานอีเมล์ควรได้รับการตั้งค่าให้อีเมล์ส่งออกทุกฉบับ มีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน สำนักงานฯ และเบอร์โทรศัพท์ติดต่อ
- ห้ามผู้ใช้งานทำสำเนาข้อความ หรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์ นั้นในนามตัวแทนของบริษัทฯ
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-mail Account ของตน เว้นแต่เกิดจากกรณีจำเป็นและต้องให้ความยินยอมอย่างเป็นลายลักษณ์อักษร
- ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail) เป็นต้น
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใดๆ กับการส่งอีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติหรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงาน และส่งผลเสียต่อบริษัทฯ
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษ เมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่าเครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

- การอนุญาตให้ใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้
  - ผู้ใช้งานต้องปกป้องความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่เมื่อจำเป็นต้องส่งข้อมูลนั้นผ่านเครื่องโทรสาร

- ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิดหมายเลขผิดส่วนงาน เป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น
- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น
- ห้ามผู้ใช้งานบันทึกหรือฝากข้อความที่มีข้อมูลลับในเครื่องตอบรับโทรศัพท์อัตโนมัติหรือระบบวอยซ์เมล์โดยเด็ดขาด
- ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลำโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่น Voice Over IP หรือในระหว่างการประชุมทางไกล เว้นแต่ผู้เข้าร่วมการประชุมทุกหน่วยงานได้รับการพิสูจน์ตัวตนแล้วว่า เป็นผู้ที่เกี่ยวข้องและมีสิทธิ์รับทราบข้อมูล
- ผู้ที่เกี่ยวข้องต้องตรวจสอบอย่างรอบคอบและระมัดระวัง เพื่อให้มั่นใจว่าไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลที่สนทนาอยู่
- การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสมสามารถป้องกันเสียงลอดออกมาได้ เป็นต้น
- ผู้ใช้งานต้องระมัดระวังการใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสารเพื่อป้องกันข้อมูลลับถูกเปิดเผย แก่บุคคลที่ไม่ได้รับอนุญาต
- ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใดๆ ทางโทรศัพท์ ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้น เป็นผู้ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าวก่อนที่จะเปิดเผยข้อมูล
- ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสารที่มีข้อมูลลับ โดยสำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับ
- เจ้าหน้าที่ต้องไม่เปิดเผยสถานที่ตั้งของห้องเครื่องคอมพิวเตอร์แม่ข่ายต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน

5.1.4. การคืนทรัพย์สิน (Return of Assets)

พนักงาน และลูกจ้างของหน่วยงานภายนอก ทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง ภายใน 3 วันก่อนวันสุดท้ายของการทำงาน (เป็นไปตามกฎระเบียบบริษัท เรื่องการลาออก) โดยทรัพย์สินที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจะต้องมีการตรวจสภาพทรัพย์สินจากฝ่ายเทคโนโลยีสารสนเทศเสียก่อน หากผลการตรวจสอบพบว่ามี

ความชำรุดเสียหาย หรือมีข้อมูลบางอย่างขาดหายไป ผู้รับผิดชอบจะต้องได้รับผิดชอบตามข้อกำหนดที่ได้ตกลงไว้ โดยปฏิบัติตามระเบียบบริษัท เรื่องการลาออก ของฝ่ายทรัพยากรบุคคล

5.2. นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)

<u>จุดประสงค์และขอบเขต :</u>

นโยบายได้กำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้น และได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้นโยบายยังได้กำหนดถึงบทบาทของเจ้าของข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้องกับการจัดลำดับชั้นของข้อมูล เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

<u>เนื้อหานโยบาย และการดำเนินการ :</u>

5.2.1. ชั้นความลับสารสนเทศ (Classification of Information)

บริษัทต้องกำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสมเอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วนให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลนั้น

- ชั้นที่ 1 ข้อมูลเปิดเผยได้
  - ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย
- ชั้นที่ 2 ข้อมูลใช้ภายในองค์กรเท่านั้น
  - เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้พนักงานทุกคนภายในองค์กรทราบได้ แต่ไม่สามารถเปิดเผยต่อบุคคลภายนอกองค์กรได้ เนื่องจากอาจสร้างความเสียหายให้กับองค์กรได้
- ชั้นที่ 3 ข้อมูลลับ
  - เป็นข้อมูลใช้ภายในองค์กรที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน
- ชั้นที่ 4 ข้อมูลลับมาก
  - เป็นข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้ใช้บางกลุ่มขององค์กร (ส่วนใหญ่เป็นผู้บริหารเท่านั้น) และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เนื่องจากข้อมูลประเภทนี้ มีความจำเป็นต่อการปฏิบัติงานขององค์กรและจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือ ทำให้เกิดผลเสียหายร้ายแรงต่อองค์กร

5.3. นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัทฯ โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

<u>เนื้อหานโยบาย และการดำเนินการ</u>

5.3.1. การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูล ต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างนี้ที่นำส่ง หรือขนย้ายสื่อบันทึกข้อมูลนั้นต้องกำหนดวิธีปฏิบัติ และสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูล โดยให้พนักงานแจ้งความประสงค์ในแบบฟอร์มขอใช้งาน Computer and Software ส่งผู้มีอำนาจพิจารณาและให้ฝ่ายเทคโนโลยีสารสนเทศรับทราบและปฏิบัติ อาทิเช่น

- สื่อบันทึกข้อมูลต้องตั้งชื่อตามที่กำหนด และต้องมีทะเบียนควบคุมการใช้งาน
- การเบิกและจ่ายสื่อบันทึกข้อมูลจะต้องผ่านการอนุมัติจากผู้มีอำนาจของหน่วยงานผู้ใช้
- สื่อบันทึกข้อมูลต้องมีการตรวจนับอย่างน้อยปีละ 1 ครั้ง

5.3.2. การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน ดังนี้

- เจ้าหน้าที่ IT จัดทำสรุปรายการสื่อบันทึกข้อมูล ที่ต้องการทำลายทิ้ง และจัดทำบันทึกภายใน (MEMO) ขออนุมัติทำลายฯ
- ผู้จัดการฝ่าย IT ตรวจทานเรื่องการขออนุมัติทำลายฯ
- ผู้อำนวยการสายงานบัญชีและการเงิน (CFO) พิจารณาอนุมัติการทำลาย
- ควรทำลายสื่อที่ใช้ในการบันทึกข้อมูล เอกสาร และอุปกรณ์สำนักงานภายใต้สิ่งแวดล้อมที่ได้มีการควบคุม (Controlled Environment)

5.3.3. การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น และต้องมีวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศหรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย โดยให้พนักงานแจ้งผู้จัดการฝ่ายพิจารณาอนุมัติ โดยเป็นลายลักษณ์อักษร

หมวดที่ 6 การควบคุมการเข้าถึง
(Access Control)

6. การควบคุมการเข้าถึง (Access Control)

6.1. การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

<u>จุดประสงค์และขอบเขต</u>

เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย และเพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็น และความต้องการทางธุรกิจ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

6.1.1. การควบคุมการเข้าถึง (Access Control)

- มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยปฏิบัติตามระเบียบปฏิบัติเรื่องการบริหารจัดการบัญชีผู้ใช้งานระบบ
- ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน ก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยปฏิบัติตามระเบียบปฏิบัติเรื่องการบริหารจัดการบัญชีผู้ใช้งานระบบ
- ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้
- ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ
    - ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น
    - ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ
    - การเข้าถึงข้อมูลและระบบสารสนเทศของสำนักงานฯ จะกระทำได้ก็ต่อเมื่อ ได้รับการอนุมัติโดยผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น ๆ เท่านั้น ความปลอดภัยของข้อมูลและกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบายและขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึง การให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูล และการกู้ข้อมูลที่เสียหายกลับคืนมา

6.1.2. การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services) ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึง เท่านั้น

- ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูล และระบบเทคโนโลยีสารสนเทศ อาทิ
- ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย อาทิ Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP)
- จำกัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ-ส่งไฟล์ขนาดใหญ่ ฟังเพลงออนไลน์ ดูทีวีออนไลน์ หรือ เล่นเกมส์ออนไลน์ ในช่วงเวลาทำการ ยกเว้นกรณีที่ได้รับอนุญาตจากผู้บริหาร/ผู้มีอำนาจ
- ผู้ใช้งานจะต้องสามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ
- อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดต้องได้รับการตั้งค่าให้มีความปลอดภัย และการมีการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย
- ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรม และได้รับการติดตั้งโดยผู้ที่มีความชำนาญที่ผ่านการพิจารณาอนุมัติแล้ว
- อุปกรณ์เครือข่าย อาทิ Router, Firewall, Switch, Wireless Access Point ต้องได้รับการตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้นๆ หรือตามคำแนะนำของสำนักงาน ฯ ด้านความมั่นคงปลอดภัยต่าง ๆ อาทิ SANS Institute หรือ NSA
- IP Address ต้องได้รับการลงทะเบียน แจกจ่าย และบริหารจัดการโดยแผนก IT
- อุปกรณ์เครือข่ายที่สำคัญ เช่น Router, Core Switch ต้องมีอุปกรณ์สำรองไฟฟ้า (UPS) เสมอ
- การเปลี่ยนแปลงระบบเครือข่ายหรืออุปกรณ์เครือข่ายต้องได้รับการควบคุมโดยปฏิบัติตามเอกสารวิธีการปฏิบัติงานเรื่องการขอสร้างหรือเปลี่ยนแปลงระบบงาน
- ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)
- ข้อตกลงการให้บริการเครือข่ายต้องระบุถึงรายละเอียด และข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ และการบริหารจัดการบริการเครือข่ายทั้งหมด หากบริการเครือข่ายนั้นได้รับการดำเนินการโดยหน่วยงานภายนอก ต้องมีการระบุถึงสิทธิของบริษัทฯ ในการติดตามตรวจสอบ และตรวจประเมินการทำงานของหน่วยงานภายนอกด้วย

6.2. นโยบายการควบคุมการเข้าถึงระบบ (System and Application Access Control Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิเข้าใช้งานในระดับระบบปฏิบัติการ (Operating System) หน่วยงานด้านเทคโนโลยีสารสนเทศ การตรวจสอบผู้ใช้และการบริหารรหัสผ่านสำหรับผู้ใช้งาน รวมถึงการควบคุมเวลาในการเชื่อมต่อสู่ระบบ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

6.2.1. การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึง ทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท

6.2.2. การบริหารจัดการสิทธิ์ตามระบบสิทธิ์การเข้าถึง (Management of Privileged Access Right)

- ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย
- ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ

6.2.3. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

- ต้องมีกระบวนการจัดการการส่งมอบข้อมูล เพื่อพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นความลับ และการเก็บรักษาข้อมูลความลับของตัวเอง การส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ
- เจ้าหน้าที่ IT ต้องปฏิบัติตามระเบียบปฏิบัติงานเรื่องการบริหารจัดการบัญชีผู้ใช้งานระบบ

6.2.4. การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

ทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ตามระเบียบปฏิบัติงานเรื่องการบริหารจัดการบัญชีผู้ใช้งานระบบ

6.2.5. การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights)

- สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องได้รับการถอดถอน เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ
- ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้
-

6.3. นโยบายบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

<u>จุดประสงค์และขอบเขต :</u>

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์ตัวตน

<u>เนื้อหานโยบาย และการดำเนินการ :</u>

6.3.1. ใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

- การใช้งานและเก็บรักษาข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน ต้องดำเนินการตามนโยบายหรือวิธีปฏิบัติขององค์กร สำหรับการใช้งานข้อมูลพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ เช่น
  - เก็บรักษา Username และ Password ต้องเป็นความลับห้ามเปิดเผยให้บุคคลอื่นทราบ
  - หลีกเลี่ยงการเก็บบันทึกข้อมูลการตรวจสอบความลับ เว้นแต่สามารถเก็บไว้อย่างปลอดภัยได้และ เมื่อได้รับข้อมูล Password ซึ่งเป็นข้อมูล Default ควรมีการแก้ไขทันทีเมื่อเข้าใช้งานระบบครั้งแรก

6.4. การควบคุมการเข้าถึงระบบ (System and Application Access Control)

<u>จุดประสงค์และขอบเขต</u>

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อมุ่งเน้นให้ผู้ใช้งานระบบมีความตระหนักถึงความปลอดภัยในการใช้งานระบบข้อมูล โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่าน และต้องทราบถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานคอมพิวเตอร์

<u>เนื้อหานโยบาย และการดำเนินการ</u>

6.4.1. นโยบายหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy)

- ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน
- บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น
- บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการสื่อสาร (IT Security Policy) ของบริษัทฯ อย่างเคร่งครัดก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของสำบริษัทฯ

6.4.2. ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure)

- ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 5 ครั้ง

6.4.3. ระบบบริหารจัดการรหัสผ่าน (Password Management System)

ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูล การพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับดังต่อไปนี้

- ผู้ใช้ต้องกำหนดและใช้รหัสผ่านที่มีประกอบด้วย ตัวเลข สัญลักษณ์ และตัวอักษร รวมกัน 8-12 ตัวอักษร
- ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ ทุก ๆ 90 วัน ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตาม และผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำกับของเดิม หรือไม่ใช้วิธีเปลี่ยนตัวเลขต่อท้ายในรหัสผ่าน

6.4.4. การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

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

6.4.5. การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)

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

หมวดที่ 7 การเข้ารหัสข้อมูล
(Cryptography)

7. การเข้ารหัสข้อมูล (Cryptography)

7.1. นโยบายการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

<u>จุดประสงค์และขอบเขต :</u>

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องการความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

<u>เนื้อหานโยบาย และการดำเนินการ :</u>

7.1.1. การใช้มาตรการเข้ารหัสข้อมูล (Use of Cryptographic Controls)

- บริษัทฯ ต้องมีนโยบายการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

7.1.2. การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

- นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ โดยองค์กรควรมีการกำหนดมาตรการในการเก็บ Key ที่เป็นข้อมูลลับของแต่ละบุคคล

หมวดที่ 8 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

8. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

8.1. นโยบายเกี่ยวกับบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

จุดประสงค์และขอบเขต :

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพ ที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ของบริษัทฯ และเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต

เนื้อหานโยบาย และการดำเนินการ :

8.1.1. การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

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

8.1.2. การควบคุมการเข้าออก (Physical Entry Controls)

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

- ต้องกำหนด “พนักงานแผนก IT” และหรือผู้ที่ได้รับสิทธิ์จากผู้บริหาร/ผู้มีอำนาจ ที่มีสิทธิ์ผ่านเข้าออกช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน
- หากมีบุคคลอื่นใดที่ไม่ใช่ “พนักงานแผนก IT” ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคล และการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่อนุญาตให้เข้าพื้นที่) และต้องบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Data Center) ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี
- เจ้าหน้าที่ของบริษัทฯ ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

8.1.3. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing Offices, Room and Facilities)

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

8.1.4. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environmental Threats)

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

8.1.5. การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

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

8.2. นโยบายเกี่ยวกับการจัดการอุปกรณ์ (Equipment Management Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์ คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

8.2.1. การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

จัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัย รวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

8.2.2. การติดตามการทำงานของเครื่องแม่ข่าย (Server Monitor)

มีการจัดทำรายงานสถานการณ์ทำงานของเครื่องแม่ข่ายต่าง ๆ รวมถึงอุปกรณ์รอบข้างที่จำเป็น เป็นประจำทุกวัน โดยผู้ปฏิบัติจะทำการบันทึกสถานการณ์การทำงานต่าง ๆ ทางกายภาพ และมีการจัดทำรายงานสรุปสถานการณ์ทำงานภายในห้อง Server เพื่อนำเสนอข้อมูลให้ผู้บริหารให้ทราบเป็นประจำทุกไตรมาส

8.2.3. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้องได้รับการป้องกันการล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่น ๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบ และอุปกรณ์สนับสนุนการทำงานต่าง ๆ

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

หมวดที่ 9. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

9. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

9.1. นโยบายการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

<u>เนื้อหานโยบาย และการดำเนินการ</u>

9.1.1. การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

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

9.1.2. การจัดการการเปลี่ยนแปลง (Change Management)

- มีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ทุกครั้ง โดยปฏิบัติตามระเบียบปฏิบัติงานเรื่องการขอใช้บริการฝ่าย IT
- เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ เช่น ระบบปรับอากาศ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ ฯลฯ เจ้าหน้าที่ต้องประสานงานหรือรายงานกับคณะกรรมการ
- เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง
- มีการประชุมเป็นประจำเพื่อตรวจสอบ คำร้องขอการเปลี่ยนแปลง (Change Request) และพิจารณาตรวจสอบการเปลี่ยนแปลงต่าง ๆ ให้เป็นที่พอใจและยอมรับได้
- ตาราง และ/หรือ แผนการเปลี่ยนแปลงทุกครั้งต้องได้รับความเห็นชอบจากผู้บริหาร/ผู้มีอำนาจอนุมัติก่อนจะทำการเปลี่ยนแปลง
- บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบโดยบันทึกฯ ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
  - วันที่รับเรื่อง และวันที่ทำการเปลี่ยนแปลง
  - เจ้าของข้อมูล และผู้ดูแลระบบ
  - วิธีการเปลี่ยนแปลง
  - ผลของการเปลี่ยนแปลง (สำเร็จ หรือล้มเหลว)

9.1.3. การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

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

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

- ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบออกจากกับเครื่องที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย

9.2. นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย และได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี เพื่อควบคุม และป้องกันซอฟต์แวร์ และข้อมูลจากโปรแกรมที่ไม่ประสงค์ดี และซอฟต์แวร์อันตราย

<u>เนื้อหานโยบาย และการดำเนินการ</u>

9.2.1. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against Malware)

มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการ สร้างความตระหนักผู้ใช้งานที่เหมาะสม

- หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกัน Virus Version ล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่อง Server โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา
- หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้โปรแกรมค้นหา Virus ทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย การติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก 6 เดือน และต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย

- ห้ามเจ้าหน้าที่ทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติจากแผนก IT หลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัสก่อนการใช้งาน
- ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตควรมีการตรวจหา Virus ก่อนนำไปใช้งาน โดยมีการติดตั้งระบบตรวจจับ Virus ที่ใช้ร่วมกันในบริษัท
- ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใดๆ เช่น ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง อีเมล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ของบริษัทฯ
- ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้นต้องตรวจสอบ Virus คอมพิวเตอร์ก่อนใช้งานทุกครั้ง
- เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชั่นการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

9.3. นโยบายการสำรองข้อมูล (Backup Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย และเพื่อป้องกันการสุญหายของข้อมูล

<u>เนื้อหานโยบาย และการดำเนินการ</u>

9.3.1. การสำรองข้อมูล (Information Backup)

ข้อมูลสำหรับสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการดำเนินการสำรองไว้ และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอ ตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้

- ต้องกำหนดความถี่ในการทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบโดยปฏิบัติตามระเบียบปฏิบัติงานเรื่องการสำรองข้อมูลและการกู้คืน Backup & Restore Procedure
- จัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ สามารถใช้งานได้ตลอดเวลา
- มีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ
- กำหนดระยะเวลาในการสำรองข้อมูลตามระดับการบริหารความเสี่ยง
- ต้องมีกระบวนการสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องมีการทำเอกสาร และมีการตรวจสอบเป็นระยะ ๆ
- ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง
- ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

- ต้องลงบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูล ต้องได้รับการตรวจสอบเป็นประจำทุกปี
- กระบวนการในการเก็บข้อมูลระหว่างสถานที่ระบบคอมพิวเตอร์และสถานที่เก็บข้อมูลต้องได้รับการตรวจสอบอย่างน้อยปีละ 1 ครั้ง
- สื่อที่ใช้เก็บข้อมูลต้องมีป้ายบอกรายละเอียด ซึ่งประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
  - ชื่อระบบ
  - วันสร้าง
  - ระดับความสำคัญของข้อมูล
  - รายละเอียดติดต่อผู้ดูแลข้อมูล

9.4. นโยบายการบันทึกข้อมูลล็อก และการเฝ้าระวัง (Logging and Monitoring Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

<u>เนื้อหานโยบาย และการดำเนินการ</u>

9.4.1. การบันทึกข้อมูลล็อก แสดงเหตุการณ์ (Event Logging)

- ข้อมูล Log แสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บ และทบทวนอย่างสม่ำเสมอ อุปกรณ์บันทึกข้อมูล Log จะได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไข และการเข้าถึงโดยไม่ได้รับอนุญาต

9.4.2. การป้องกันข้อมูลล็อก (Protection of Log Information)

- ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

9.4.3. ข้อมูลล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ (Administrator and Operator Logs)

- ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น ๆ รวมถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย

9.4.4. การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

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

9.5. นโยบายการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

เนื้อหานโยบาย และการดำเนินการ

9.5.1. การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

- ซอฟต์แวร์คอมพิวเตอร์ทุกเครื่อง จะถูกต้องตั้งโดย หน่วยงานเทคโนโลยีสารสนเทศ เท่านั้น โดยมีการตรวจสอบตามข้อกำหนด เรื่อง การบริหารจัดการสินทรัพย์ (Asset Management)
- ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ Library ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริง จะต้องผ่านการทดสอบ การใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

9.6. นโยบายการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management Policy)

จุดประสงค์และขอบเขต

เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ และเพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

เนื้อหานโยบาย และการดำเนินการ

9.6.1. การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

- ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับ เพื่อลดความเสี่ยงดังกล่าว

9.6.2. การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

- บริษัทฯ ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญา ที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด
- บริษัทฯ ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่ โดยฝ่ายเทคโนโลยีสารสนเทศ ทำการตรวจสอบการติดตั้งซอฟต์แวร์ของพนักงานทุกคน อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่า ไม่มีการใช้ซอฟต์แวร์ที่ละเมิดสินทรัพย์ทางปัญญา
- ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ บนระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยเด็ดขาด
- เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่สำนักงานฯ มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ตั้งใจ หรือพลั้งเผลอ จึงไม่ควรจะทำสำเนาซอฟต์แวร์ใด ๆ ที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของสำนักงานเพื่อจุดประสงค์ใด ๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตจากผู้บริหาร/ผู้มีอำนาจ และในขณะเดียวกันพนักงานของบริษัทฯ ไม่ควรจะติดตั้งโปรแกรมใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทฯ โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

- บริษัทฯ กำหนดให้มีการตรวจสอบเครื่องคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง เพื่อตรวจดูรายการของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ และเพื่อให้แน่ใจว่าสำนักงานมีใบอนุญาตการใช้งานสำหรับผลิตภัณฑ์ซอฟต์แวร์แต่ละตัวในเครื่องคอมพิวเตอร์ ถ้าพบว่ามีซอฟต์แวร์ที่ไม่ได้รับอนุญาตซอฟต์แวร์ เหล่านั้นจะถูกลบทิ้ง และถ้าหากมีความจำเป็น สำนักงานอาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มี ใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้

9.7. นโยบายพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

<u>เนื้อหานโยบาย และการดำเนินการ</u>

9.7.1. การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)

- ต้องวางแผนการตรวจสอบระบบและตกลงร่วมกันอย่างระมัดระวัง เพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ หน่วยงานเทคโนโลยีสารสนเทศ
- จะทำการกำหนดแผนการประเมินระบบสำคัญต่าง ๆ รวมกับฝ่ายตรวจสอบภายใน โดยฝ่ายตรวจสอบภายใน มีหน้าที่จัดทำรายการตรวจประเมินระบบภายใต้การบริหารความเสี่ยงระบบและนำผลการตรวจประเมินเสนอคณะกรรมการบริหารความมั่นคงตามกำหนดระยะเวลาการประชุม

หมวดที่ 10 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

10. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

10.1. นโยบายการจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

<u>จุดประสงค์และขอบเขต</u>

เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัทฯ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

10.1.1. การควบคุมการเข้าถึงเครือข่าย (Network Control)

เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่าง ๆ หัวหน้าหน่วยงานควบคุมระบบเครือข่าย ต้องรับผิดชอบในการจัดให้มีการควบคุมการปฏิบัติการด้านเครือข่ายดังต่อไปนี้

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

10.1.2. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

- ระบบเครือข่ายทั้งหมดของสำนักงานฯ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้ง ต้องมีความสามารถในการตรวจจับไวรัสด้วย
- ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของสำนักงานฯ และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะ และติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของสำนักงานฯ ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้ หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายของบริษัทฯ ได้
- ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัทฯ โดยไม่ได้รับอนุญาตจากฝ่าย IT
- ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของสำนักงานฯ โดยเด็ดขาด หากมีความจำเป็นต้องใช้งาน ต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง
- ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด
- ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของสำนักงานฯ ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในสำนักงานฯ โดยเด็ดขาด

10.1.3. การจัดแบ่งเครือข่ายภายในสำนักงานฯ (Segregation in Network)

- ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และโซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

10.2.นโยบายการถ่ายโอนข้อมูล (Information Transfer)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กร และถ่ายโอนข้อมูลกับภายนอกหน่วยงาน

<u>เนื้อหานโยบาย และการดำเนินการ</u>

10.2.1. นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

- ต้องมีการจัดทำนโยบาย ขั้นตอนปฏิบัติหรือมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการ และมีการปฏิบัติตาม เพื่อป้องกันสารสนเทศที่มีการถ่ายโอนกับหน่วยงานภายนอก
- ต้องมีการดำเนินการแลกเปลี่ยนสารสนเทศ พนักงานผู้ถ่ายโอนสารสนเทศ ต้องแจ้งขออนุมัติการถ่ายโอนฯ ต่อผู้จัดการฝ่ายต้นสังกัด ทุกครั้งก่อนทำการถ่ายโอน โดยต้องมีการระบุรายละเอียดข้อมูลสารสนเทศที่ถ่ายโอน เช่น วัตถุประสงค์การถ่ายโอน รายละเอียดของข้อมูลที่ถ่ายโอน และชื่อองค์กร ชื่อผู้รับถ่ายโอน ปลายทาง
- ต้องมีการจัดข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer)

10.2.2. การรักษาความมั่นคงปลอดภัยการส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging)

- ต้องมีการกำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์ รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

10.2.3. การตรวจสอบรายการการใช้งานเครือข่าย (Network Monitoring)

- หน่วยงานสารสนเทศมีการตรวจสอบการใช้งานเครือข่าย ของฝ่ายต่าง ๆ และมีการจัดทำรายงานสรุปการใช้งานเครือข่าย และนำเสนอต่อคณะกรรมการบริหาร ตามกำหนดระยะเวลาการประชุม

10.2.4. การรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements)

- ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) ซึ่งเป็นไปตามความต้องการด้านการป้องกันข้อมูลของบริษัทฯ และมีการทบทวนอย่างสม่ำเสมอ
- พนักงาน บุคคล หรือผู้ติดต่อจากหน่วยงานอื่น ที่มีส่วนต้องเข้าถึงสารสนเทศของ สำนักงานฯ ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่/ผู้ว่าจ้าง” และ “ผู้ติดต่อ/ผู้รับจ้าง/ผู้ให้บริการ” ว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement: NDA)

หมวดที่ 11. การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

11. การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

11.1. การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

11.1.1. การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification

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

11.1.2. ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

- สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการป้องกัน และการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

11.1.3. การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

- สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

11.2.นโยบายสำหรับกระบวนการในการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ (development lifecycle)

<u>เนื้อหานโยบาย และการดำเนินการ</u>

11.2.1. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

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

11.2.2. กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

- ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการ เพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น
  - คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
  - ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
  - ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
  - เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
  - ต้องเก็บรายละเอียดของคำขอไว้ในแบบฟอร์มขอใช้งานหรือยกเลิกระบบสารสนเทศ โดยปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การจัดทำหรือเปลี่ยนแปลงระบบงาน

11.2.3. การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)

- เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ต่างๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

11.2.4. การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

- เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบ และจัดทำเป็นเอกสาร เพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

11.2.5. หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

- เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรม ระบบต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ โดยให้คณะกรรมการความปลอดภัยฯ มีหน้าที่ดูแล ระบบด้านความมั่นคงปลอดภัยด้านโครงสร้างสำนักงาน

11.2.6. การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development)

- ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทฯ ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

11.2.7. การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

- โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา

11.2.8. การทดสอบเพื่อรับรองระบบ (System acceptance testing)

- มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่และระบบที่ปรับปรุง
- ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มีการเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ และลายเซ็นผู้ตรวจรับ ในแบบฟอร์มใบขอสร้างและแก้ไขระบบ หรือแบบฟอร์มการรับมอบงาน UAT โดยปฏิบัติตามระเบียบปฏิบัติงานเรื่อง การขอสร้างหรือเปลี่ยนแปลงระบบงาน

11.3.นโยบายข้อมูลสำหรับการทดสอบ (Test data)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

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

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกัน เพื่อลดความเสี่ยงของการเข้าถึง หรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

- ในการพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) และระบบที่ใช้งานจริง (Production System)
- ต้องจัดให้มีระเบียบปฏิบัติที่ชัดเจนในการโอนย้ายโปรแกรมที่พัฒนาเสร็จแล้ว ไปยังระบบที่ใช้งานจริง

- ต้องไม่มีการติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาโปรแกรมอื่น ๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง

11.3.2. การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

- ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยัง ผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวดที่ 12. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

12. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

12.1. นโยบายเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

จุดประสงค์และขอบเขต

เพื่อให้มีการป้องกันสินทรัพย์ขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

เนื้อหานโยบาย และการดำเนินการ

12.1.1. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

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

12.1.2. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)

- เจ้าหน้าที่ IT ต้องมีส่วนร่วมกับฝ่ายจัดซื้อจัดจ้าง ในการระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่างบริษัทกับผู้ให้บริการภายนอก ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ ต้องปฏิบัติตามระเบียบปฏิบัติเรื่องการจัดซื้อจัดจ้าง ของบริษัท และเมื่อมีความจำเป็นต้องให้ผู้ให้บริการภายนอกนั้น เข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ และก่อนที่จะอนุญาตให้สามารถเข้าถึงได้ ผู้ให้บริการภายนอกต้องมีการลงทะเบียนใช้งานระบบสารสนเทศ ไว้กับฝ่ายเทคโนโลยีสารสนเทศ

12.2. นโยบายการบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

จุดประสงค์และขอบเขต

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ใน ข้อตกลงการให้บริการของผู้ให้บริการภายนอก

เนื้อหานโยบาย และการดำเนินการ

12.2.1. การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

- บริษัทฯ ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับสำนักงานฯ ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก

- ต้องมีการตรวจสอบการให้บริการจากหน่วยงานภายนอกผู้ทำหน้าที่ตรวจสอบจำเป็นต้องมีความรู้ ความเข้าใจในเรื่องความปลอดภัยสารสนเทศ ตลอดจนเงื่อนไขและข้อตกลงต่าง ๆ
- ในกรณีที่มีเหตุการณ์ที่กระทบต่อความปลอดภัยโดยที่มีสาเหตุมาจากบุคคลภายนอก ต้องมีการดำเนินการ เพื่อรักษาความถูกต้องทางด้านหลักฐานและดำเนินการทางกฎหมายในกรณีที่จำเป็น
- ต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ โดยมีการตรวจประเมินผู้ให้บริการจากภายนอกทุกปี

12.2.2. การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

- การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของสำนักงานฯ ทุกครั้ง ต้องเป็นไปตามกระบวนการเรื่องการคัดเลือกและประเมินผู้ขาย/ ผู้ให้บริการ ของบริษัทฯ
- การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบัน ต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจ ที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

13. การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ Cloud Computing

13.1 นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ Cloud Computing

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้บริษัทมีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่สอดคล้องกับความต้องการของกิจการรวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศในส่วนที่เป็นเทคโนโลยีที่เกี่ยวกับบริการคลาวด์มาใช้ในการสนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความสี่ยง รวมถึงเพื่อให้กิจการสามารถรบรรลุวัตถุประสงค์และเป้าหมายหลักของกิจการ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

13.1.1 บริษัทได้กำหนดแนวทางการกำกับดูแลและบริหารจัดการการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ตามความต้องการของผู้ใช้งาน หรือ Cloud Computing ที่ครอบคลุมกระบวนการสำคัญตั้งแต่การกำหนดกรอบการกำกับดูแลการใช้งาน Cloud Computing การกำหนดแนวทางเชิงกลยุทธ์ในการใช้งาน การกำกับผู้ให้บริการ ตลอดจนการยกเลิกหรือสิ้นสุดการใช้งาน

13.1.2 ประเภทของ Cloud Computing (Service Models) ที่อนุญาตให้ใช้งาน

- Software-as-a-Service (SaaS) หมายถึง บริการด้านแอปพลิเคชันที่ทำงานบนโครงสร้างพื้นฐานระบบ Cloud Computing ซึ่งผู้ใช้บริการสามารถเข้าใช้งานแอปพลิเคชันผ่านเครือข่ายผ่านโปรแกรมบนอุปกรณ์ของผู้ใช้บริการ เช่น เว็บเบราว์เซอร์ แอปพลิเคชันบนมือถือ เป็นต้น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย ระบบจัดเก็บข้อมูล รวมถึงค่าพื้นฐานของแอปพลิเคชัน

- Platform-as-a- Service (PaaS) หมายถึง บริการด้านแฟลตฟอร์มที่ทำงานบนโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งผู้ใช้บริการสามารถเข้าแฟลตฟอร์มในการพัฒนาแอปพลิชั่น โดยผู้ให้บริการทำหน้าที่บริหารจัดการโครงสร้างพื้นฐานระบบคลาวด์ ซึ่งครอบคลุมถึง ความปลอดภัยทางกายภาพระบบปฏิบัติการ ระบบเครือข่าย และระบบให้บริการ เช่น เว็บเซอร์วิส ระบบจัดการฐานข้อมูล เป็นต้น อย่างไรก็ตาม การควบคุมที่เกี่ยวกับการบริหารจัดการแอปพลิเคชัน เช่น การแก้ไขเปลี่ยนแปลงโปรแกรม ผู้ใช้บริการจะเป็นผู้ดำเนินการ

- Infrastructure-as-a-Service (IaaS) หมายถึง บริการด้านโครงสร้างพื้นฐานระบบคลาวด์ที่มีการใช้งานทรัพยากรทางด้านระบบสารสนเทศร่วมกัน เช่น ระบบปฏิบัติการ ระบบเครือข่าย หรือระบบจัดเก็บข้อมูล โดยทางผู้ให้บริการทำหน้าที่ดูแลทางกายภาพ และทรัพยากรสารสนเทศที่ใช้ในการสนับสนุนการทำงานของโครงสร้างพื้นฐานระบบคลาวด์

13.1.3 รูปแบบของการนำไปใช้งาน (Deployment Models)

- Public Cloud หมายถึงโครงสร้างพื้นฐานระบบคลาวด์ที่เปิดให้ใช้งานผ่านเครือข่ายสาธารณะ
- Private Cloud หมายถึง โครงสร้างพื้นฐานระบบคลาวด์ที่จัดเตรียมไว้สำหรับการใช้งานโดยหน่วยงานภายในองค์กรเดียวกัน
- Hybrid Cloud หมายถึง โครงสร้างพื้นฐานระบบคลาวด์ที่ประกอบด้วยโครงสร้างพื้นฐานระบบคลาวด์ที่แตกต่างกันตั้งแต่สองรูปแบบขึ้นไป (Public และ Private)

13.1.4 การประเมินความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยทางไซเบอร์จากการใช้งาน Cloud Computing

13.1.5 ประเมินความเสี่ยงและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัย ทางไซเบอร์จากการใช้งาน Cloud Computing

- ความเสี่ยงด้านกลยุทธ์ เช่น ความเสี่ยงจากการพึ่งพิงผู้ให้บริการภายนอกและความสามารถในการเปลี่ยนแปลง ผู้ให้บริการ (vendor locked-in)
- ความเสี่ยงด้านปฏิบัติการ เช่น ระบบประมวลผลผิดพลาดจากระบบให้บริการหรือบุคลากรผู้ให้บริการ การใช้งานเทคโนโลยีร่วมกัน (Share technology risk) การละเมิดข้อกำหนดและข้อตกลงการใช้งาน Cloud Computing หรือความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลหรือการจำกัดการเข้าถึงของข้อมูลจากผู้ให้บริการ
- ความเสี่ยงด้านกฎหมาย เช่น การไม่ปฏิบัติตามกฎหมาย หลักเกณฑ์และข้อกำหนดของทางการ ทั้งภายในประเทศและต่างประเทศ
- ความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น การเรียกใช้โปรแกรม (APIs) หรือช่องทาง บริหารจัดการที่ไม่ปลอดภัย
- ความเสี่ยงด้านข้อมูลส่วนบุคคล (data privacy) และการรักษาความปลอดภัยของข้อมูล (data security)
- ความเสี่ยงจากการใช้ผู้ให้บริการภายนอกที่มีการใช้ผู้ให้บริการภายนอกอื่นรับช่วงจัดการงาน (sub-contract)

13.1.6 จัดเตรียมและพัฒนาองค์ความรู้ด้านการบริหารจัดการ Cloud Computing ให้แก่ผู้ดูแลระบบ (Administrator) และบุคลากรที่เกี่ยวข้องอย่างเพียงพอ

13.1.7 กำหนดให้มีการประเมินและคัดเลือกผู้ให้บริการ (Due Diligence) ดังนี้

- ตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการเพื่อให้มั่นใจว่าผู้ให้บริการสามารถให้บริการได้อย่างต่อเนื่อง โดยคำนึงถึงปัจจัยสำคัญ ได้แก่ ความรู้ความสามารถ ประสบการณ์ ความสามารถทางการเงินที่สามารถ ในการให้บริการอย่างต่อเนื่อง
- ประเมินมาตรฐานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ได้แก่ การรักษาความลับข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และ ความ

ต่อเนื่องของการให้บริการ (Availability) เช่น ผลการประเมินมาตรฐานความปลอดภัยที่เป็นที่ยอมรับในสากล ได้แก่ ISO27001, ISO27017, PCI/DSS, TIA เป็นต้น

- ประเมินผลรายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ ด้านมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น System and Organization Control (SOC) Report โดยพิจารณาถึงขอบเขตการตรวจสอบ ระยะเวลาที่ครอบคลุมในรายงานการตรวจสอบ ผลการตรวจสอบและประเด็นสำคัญในผลการตรวจสอบ ความสามารถและความน่าเชื่อถือของผู้ตรวจสอบ เป็นต้น

- ประเมินความสอดคล้องกันของแนวทางการรักษาความต่อเนื่องของการให้บริการของผู้ให้บริการระบบ Cloud Computing และผลการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) ของระบบงานที่จะมีการใช้บริการบนระบบ Cloud Computing อันประกอบไปด้วย ระยะเวลาการหยุดชะงักของระบบให้บริการที่ยอมรับได้ (Maximum Tolerable Downtime: MTD) ระยะเวลาที่ยอมรับได้ในการกู้คืนระบบงานและข้อมูล (Recovery Time Objective: RTO) และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO)

- ประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและความต่อเนื่องในการให้บริการในกรณีที่ผลการประเมินผู้ให้บริการไม่เป็นไปตามข้อกำหนดหรือมาตรฐานความปลอดภัยที่กำหนดไว้

13.1.8 จัดทำสัญญาและข้อตกลงการให้บริการ (Engage) ซึ่งมีรายละเอียดในเรื่องดังต่อไปนี้เป็นอย่างน้อย

- หน้าที่และความรับผิดชอบของผู้ให้บริการ รวมถึงความรับผิดชอบต่อบริษัทในกรณีที่ผู้ให้บริการ ไม่สามารถปฏิบัติตามข้อตกลงได้

- ขอบเขตการให้บริการ ประเภท และเงื่อนไขการให้บริการ

- เงื่อนไขความเป็นเจ้าของข้อมูลของผู้ใช้บริการ สิทธิการใช้และลิขสิทธิ์ที่เกี่ยวข้อง โดยผู้ใช้บริการควรเป็นเจ้าของสิทธิในข้อมูล

- ข้อกำหนดด้านเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามที่กำหนดในข้อตกลง ทั้งนี้ บริษัทควรพิจารณาถึงเงื่อนไขการประเมินความเสียหาย รวมถึงข้อจำกัดในกรณีมีเงื่อนไขการจำกัดความรับผิดในสัญญาระหว่างผู้ใช้บริการและผู้ให้บริการ

- ข้อกำหนดด้านการเข้าถึงข้อมูลของผู้ให้บริการ ประกอบด้วยสิทธิการเข้าถึงและเงื่อนไขการเปิดเผยข้อมูล โดยผู้ให้บริการจากความยินยอมของผู้ใช้บริการ หรือการเปิดเผยข้อมูลโดยข้อกำหนดทางกฎหมายของประเทศ ที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล ทั้งนี้ ต้องมีการแจ้งให้ผู้ใช้บริการรับทราบ

- ข้อกำหนดด้านการสำรองข้อมูลและการจัดทำแผนสำรองฉุกเฉิน และแผนความต่อเนื่องทางธุรกิจสำหรับ การให้บริการ โดยมีเงื่อนไขที่ชัดเจนทางด้าน

    - สถานที่ในการกู้คืนข้อมูล (Location)
    - ระยะเวลากู้คืนระบบให้บริการ (Service Restoration)
    - ระยะเวลากู้คืนข้อมูล (Recovery Time Objective: RTO)

- ชุดข้อมูลล่าสุดที่กู้คืนได้ (Recovery Point Objective: RPO)

- ข้อกำหนดและเงื่อนไขการส่งมอบข้อมูลเมื่อมีการยกเลิก หรือสิ้นสุดการใช้บริการ

- ข้อกำหนดด้านเงื่อนไขในกรณีที่ผู้ให้บริการจะให้ผู้ให้บริการรายอื่นรับดำเนินการช่วง (Subcontract of the cloud provider)

- ข้อกำหนดและมาตรการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

- ข้อกำหนดด้านสิทธิในการตรวจสอบ (Rights to Audit)

- ช่องทางติดต่อและผู้รับผิดชอบด้านปัญหาการใช้งาน และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ

13.1.9 บริษัทฯ กำหนดให้มีการติดตาม และ ประเมินผลด้านประสิทธิภาพและการปฏิบัติตามข้อตกลงการให้บริการ อย่างน้อยปีละ 1 ครั้ง

13.1.10 ติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ

13.1.11 ต้องพิจารณาความเสี่ยงที่เกี่ยวข้องในการยกเลิกการใช้บริการระบบประมวลผลร่วมกันผ่านเครือข่าย อย่างรอบด้านเพื่อกำหนดกลยุทธ์และจัดทำแผนการยกเลิกการใช้บริการอย่างเหมาะสม เพื่อป้องกันหรือลดผลกระทบ อันอาจจะเกิดขึ้นจากความเสี่ยง เช่น ความเสี่ยงด้านการหยุดชะงักของระบบให้บริการ ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความลับข้อมูล ความเสี่ยงด้านความถูกต้องของระบบประมวลผล เป็นต้น

หมวดที่ 14 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

14. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

14.1. นโยบายการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทฯ ได้รับการดำ เนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และเพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

14.1.1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

- ต้องกำหนดหน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงาน และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี เพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ โดยจัดทำระบบแจ้งซ่อมระบบสารสนเทศ Online (IT-Web)
- ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสำนักงานฯ โดยผ่านช่องทางรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ โดยปฏิบัติตามระเบียบปฏิบัติเรื่องการขอใช้บริการฝ่าย IT
- ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในสำนักงานฯ ต่อผู้บังคับบัญชา หรือหน่วยงานจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที
- ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อผู้บริหารหรือคณะกรรมการทันที
- ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อผู้บริหารหรือคณะกรรมการทันที
- ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในสำนักงาน ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย (Security Management) และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง
- การกระทำอื่นๆ ที่ถือเป็นข้อห้ามของบริษัทฯ มีดังนี้

- การกระทำใดๆ ที่กฎหมายบัญญัติว่าเป็นความผิด ตลอดจนการกระทำในลักษณะอื่นๆ ที่กล่าวถึงด้านล่างนี้ ถือเป็นข้อห้ามของสำนักงานฯ ไม่ยินยอมให้พนักงานดำเนินการโดยเด็ดขาด ทั้งนี้บริษัทฯ มิได้เขียนระบุถึงข้อห้ามทั้งหมดที่ห้ามกระทำไว้ แต่เขียนเพื่อเป็นแนวทางให้แก่ผู้ใช้งานได้รับทราบเท่านั้น หมายเหตุ : เจ้าหน้าที่บางส่วนอาจได้รับยกเว้นจากข้อห้ามบางข้อที่กล่าวไว้ด้านล่างนี้ (ตราบเท่าที่ไม่ขัดต่อกฎหมาย) หากเป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย เช่น ผู้ดูแลระบบสามารถระงับการเข้าถึงระบบเครือข่ายของอุปกรณ์ใด ๆ หากการเข้าถึงนั้นรบกวนการทำงานของระบบเทคโนโลยีสารสนเทศ
- การใช้งานทรัพยากรของสำนักงาน ฯ เพื่อการจัดหาหรือส่งต่อวัสดุ เอกสาร หรือรูปภาพ ลามกอนาจาร หรือที่ขัดต่อกฎหมาย
- การฉ้อโกงโดยใช้ User ID และรหัสผ่านที่บริษัทฯ กำหนดให้ เพื่อเสนอขายสินค้าหรือบริการใด
- การพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่าย ตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย ได้แก่ การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์ แม่ข่ายที่ตนไม่ได้รับอนุญาต เป็นต้น ส่วนตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ Sniffing, Pinged Floods, Pack Spoofing, Denial of Service และ Forged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น
- การใช้งาน Bandwidth จำนวนมากโดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P File Sharing
- การทำ Port Scanning และ Security Scanning เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
- การดักฟังหรือดักจับข้อมูลที่พนักงานไม่ได้รับอนุญาต ให้รับรู้ด้วยวิธีการใด ๆ เว้นแต่เป็นการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
- การค้นหาจุดบกพร่องของระบบ เพื่อทำการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
- การหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ระบบเครือข่ายใด ๆ
- การใช้โปรแกรม/สคริปต์/คำสั่ง หรือการส่งข้อความใด ๆ โดยมีเจตนารบกวน ลดประสิทธิภาพการให้บริการ หรือระงับการใช้งานของผู้ใช้งาน ทั้งโดยผ่านระบบภายใน หรือผ่านระบบเครือข่ายต่าง ๆ

- การให้ข้อมูลลับเกี่ยวกับรายชื่อพนักงาน รายชื่อลูกค้า ความลับของสำนักงานฯ และข้อมูลลับอื่น ๆ แก่บุคคลภายนอก
- การข่มขู่คุกคามทุกรูปแบบผ่านอีเมล์ โทรศัพท์ หรือระบบส่งข้อความ ไม่ว่าจะด้วยภาษา ความถี่ หรือขนาดของข้อความการแสดงความคิดเห็น หรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการทำงานไปหาบุคคลจำนวนมาก (Newsgroup Spam)
- การละเมิดสิทธิ์ส่วนบุคคล ลิขสิทธิ์ของสำนักงานฯ ความลับของสำนักงานฯ สิทธิบัตร ทรัพย์ สินทางปัญญา หรือกฎหมายอื่นใด

14.1.2. การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

- ประเด็นปัญหาต่าง ๆ ที่ได้รับแจ้ง และได้ดำเนินการแก้ไขเสร็จแล้วตามกำหนดระยะเวลา จะถูกนำข้อมูลดังกล่าวมาประมวลผล เพื่อสรุปออกมาเป็นรายงาน เพื่อแสดงให้เห็นว่าในช่วงเวลาที่ผ่านมานั้น มีปัญหาเรื่องอะไรมากที่สุด สาเหตุของปัญหาดังกล่าวเกิดจากอะไร และจะมีวีการป้องกันไม่ให้ปัญหานั้นเกิดขึ้นมาได้อย่างไร โดยหน่วยงานเทคโนโลยีสารสนเทศ จะทำรายงานสรุปดังกล่าว เพื่อนำเสนอคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ เป็นประจำทุก 1 ปี เพื่อร่วมพิจารณาปัญหาและวางแนวทางป้องกันปัญหาที่เกิดขึ้นในอนาคต

หมวดที่ 15 การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

15. การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ(Information Security Aspects of Business Continuity Management)

15.1. นโยบายความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity Policy)

<u>จุดประสงค์และขอบเขต</u>

เพื่อป้องกันการหยุดชะงักในการดำเนินงานของสำนักงานฯ ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ ไม่ว่าจะด้วยอุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหาย ต่อองค์กรไม่มากก็น้อย ดังนั้นจึงควรจัดทำแผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ เพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักขององค์กรต่อไปได้

<u>เนื้อหานโยบาย และการดำเนินการ</u>

15.1.1. การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

- องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ
- ต้องจัดทำแนวทางปฏิบัติ ในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ควรพิจารณา ดังนี้
  - การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้ เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานของบริษัทฯ และกาให้บริการด้านเทคโนโลยีสารสนเทศสำนักงานฯ
  - การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของ ความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
  - การดำเนินการเพื่อให้สำนักงานฯ สามารถดำเนินงานเป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
  - การกลับคืนสู่การทำงานปกติ เพื่อให้การดำเนินงานของบริษัทฯ กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

15.1.2. การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement information security continuity)

- ต้องจัดตั้งแผนสร้างความต่อเนื่องให้กับธุรกิจของระบบเทคโนโลยีสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงาน เจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลข้อมูล เป็นต้น

- ต้องจัดทำแผนรองรับ เหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ 1 ครั้ง โดยปฏิบัติตามเอกสารนโยบายบริษัท เรื่องแผนความต่อเนื่องของธุรกิจ ด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)

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

- ต้องกำหนดเวลาการ ทดสอบแผน กำหนดการทดสอบแผนฉุกเฉินที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ
- ต้องกำหนดเหตุการณ์ จำลองที่จะใช้ทดสอบและรายละเอียด ในการกำหนดรายละเอียดของเหตุการณ์ จำลอง ควรระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน ฉุกเฉิน
- ต้องกำหนดทรัพยากรต่างๆ ที่ใช้ในการทดสอบแผนฉุกเฉิน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่และอุปกรณ์เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย
- ต้องกำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

15.2.นโยบายการเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)

<u>จุดประสงค์และขอบเขต</u>

เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

15.2.1. สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

- อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนด

หมวดที่ 16 ความสอดคล้อง
(Compliance)

16. ความสอดคล้อง (Compliance)

16.1. นโยบายปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

<u>จุดประสงค์และขอบเขต</u>

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญา/ทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ

<u>เนื้อหานโยบาย และการดำเนินการ</u>

16.1.1. การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

- บริษัทฯ ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน
- เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด และมีรายการดังต่อไปนี้เป็นอย่างน้อย
  - นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
  - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
  - พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
  - พ.ร.บ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
  - พ.ร.บ. ลิขสิทธิ์
  - พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถือเป็นสินทรัพย์ของบริษัทฯ (ยกเว้น ข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้สำนักงานฯ สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า
- เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งาน เพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของบริษัทฯ กำหนดไว้

- บริษัทฯ ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมล์ของผู้ใช้งาน โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า อย่างไรก็ตามสำนักงานฯ จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผยข้อมูลใดๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาลตามบทบังคับของกฎหมาย หรือด้วยความยินยอมจากผู้ใช้งานเท่านั้น
- ห้ามพนักงานบริษัทฯ ใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัทฯ กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม
- การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใดๆ ออกนอกประเทศไม่ขัดต่อข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

16.1.2. สินทรัพย์ทางปัญญา (Intellectual Property Rights)

- ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานสินทรัพย์ทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด
- ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่าง เคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตาม ลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่ โดยให้เจ้าหน้าที่ IT ทำการตรวจสอบการติดตั้ง/การใช้งานซอฟต์แวร์ของพนักงาน อย่างน้อยปีละ 1 ครั้ง หากพบการใช้งานที่ไม่ถูกต้องต้องดำเนินการลบการติดตั้งทันที และพิจารณาโทษ ตามกระบวนการพิจารณาของฝ่ายทรัพยากรบุคคล และถ้าหากมีความจำเป็น สำนักงานฯ อาจจะมีการพิจารณาให้นำซอฟต์แวร์ที่มีใบอนุญาตอย่างถูกต้องอื่นมาใช้แทนซอฟต์แวร์ดังกล่าวได้
- ห้ามผู้ใช้งานดำเนินการทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบ เทคโนโลยีสารสนเทศของสำนักงานฯ โดยเด็ดขาด
- เพื่อที่จะให้เกิดความแน่ใจว่าเจ้าหน้าที่สำนักงานฯ มิได้ละเมิดลิขสิทธิ์โดยไม่ได้ ตั้งใจหรือพลั้งเผลอ จึงไม่ควรทำสำเนาซอฟต์แวร์ใดๆ ที่ติดตั้งอยู่ในเครื่อง คอมพิวเตอร์ของสำนักงานฯ เพื่อจุดประสงค์ใดๆ ก็ตาม โดยที่ไม่ได้รับอนุญาตจาก ISMR และในขณะเดียวกันเจ้าหน้าที่สำนักงานฯ ไม่ควรจะติดตั้งโปรแกรมใดๆ ลงในเครื่องคอมพิวเตอร์ของสำนักงานฯ โดยไม่ได้รับการอนุญาต ทั้งนี้เพื่อที่จะให้แน่ใจว่ามีใบอนุญาตที่ครอบคลุมการติดตั้งดังกล่าว

16.1.3. การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

- ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล

16.1.4. ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

- ต้องมีการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญาที่เกี่ยวกับบริษัทฯ

16.1.5. การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

- ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

16.2.นโยบายการทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

<u>จุดประสงค์และขอบเขต</u>

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบาย และขั้นตอนปฏิบัติงานขององค์กร

<u>เนื้อหานโยบาย และการดำเนินการ</u>

16.2.1. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

- ต้องมีการทบทวน วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติขององค์กร เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย วิธีปฏิบัติงานต่างๆ ให้ถูกต้องและเป็นปัจจุบัน ตามรอบระยะเวลาที่กำหนด เช่น ปีละ 1 ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

16.2.2. การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

- ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้
- ต้องมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

16.2.3. ทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

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

บริษัท บีพีเอส เทคโนโลยี จำกัด (มหาชน)
25/34-38, 47-51 ถ.สุขุมวิท ต.ปากน้ำ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
Tel : 02-755-2688 Fax : 02-380-5096-99 Tax ID : 0107566000526
BPS Technology Public Company Limited
25/34-38, 47-51 Sukhumvit Rd., Paknam, Muang Samutprakan, Samutprakan 10270

ประกาศ ณ วันที่ 12 พฤศจิกายน 2567

บริษัท บีพีเอส เทคโนโลยี จำกัด (มหาชน)

.....

(นายบุญช่วย ก่อกิจโรจน์)

ประธานกรรมการบริษัท