TQMalpha
บริษัท ทีคิวเอ็ม อัลฟา จำกัด (มหาชน)
123 ถนนลาดปลาเค้า แขวงจระเข้บัว เขตลาดพร้าว กรุงเทพฯ 10230 โทรศัพท์ 1737, 0-2119-8888 โทรสาร 0-2119-9000 www.tqmalpha.co.th

นโยบาย

เรื่อง
การรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
(IT Security Policy)

สายงาน ทุกสายงาน

ฝ่าย ทุกฝ่าย

ส่วน ทุกส่วน

แผนก ทุกแผนก

บริษัท ทีคิวเอ็ม อัลฟา จำกัด (มหาชน)

(ต้นฉบับ)

สารบัญ

หัวข้อ **หน้า**

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

(IT Security Policy)

1. บทนำ

นโยบายความปลอดภัยข้อมูลและระบบคอมพิวเตอร์จัดทำขึ้นเพื่อให้พนักงานใช้งานและดูแลระบบคอมพิวเตอร์อย่างเหมาะสม เพื่อป้องกันระบบคอมพิวเตอร์และข้อมูลของบริษัท มิให้ได้รับความเสียหายจากการกระทำที่เจตนาหรือไม่ได้เจตนา อันอาจมีผลทำให้ระบบคอมพิวเตอร์หรือข้อมูลนั้นมีการเปลี่ยนแปลง ถูกทำลาย หรือนำไปเปิดเผยอย่างไม่เหมาะสม และส่งผลกระทบต่อการดำเนินการของบริษัท ตลอดจนหน่วยงานหรือบุคคลที่เกี่ยวข้อง

นโยบายความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ฉบับนี้ เป็นฉบับที่ปรับปรุงเพิ่มเติม และประกาศใช้ใน บริษัท ทีคิวเอ็ม อัลฟา จำกัด (มหาชน) ซึ่งมีบริษัทในเครือ รับผิดชอบงานการดำเนินงานด้านเทคโนโลยีสารสนเทศ โดย บริษัท แคสเมท จำกัด เพื่อให้สอดคล้องกับสภาพแวดล้อมการใช้งานด้านเทคโนโลยีและสารสนเทศที่เปลี่ยนแปลงอยู่เสมอ โดยมีนโยบายที่สอดคล้องกับมาตรฐานความปลอดภัยระดับสากล เพื่อให้พนักงานของบริษัท ทีคิวเอ็ม อัลฟา จำกัด (มหาชน) มีความพร้อมและเข้าใจหลักเกณฑ์ที่ถูกต้อง โดยบริษัท เชื่อในแนวทางความปลอดภัยพื้นฐานตามหัวข้อดังต่อไปนี้

- Confidentially หมายถึง การรักษาข้อมูลและระบบคอมพิวเตอร์ให้ปลอดภัย โดยต้องจัดเตรียมระบบคอมพิวเตอร์ให้กับบุคคลที่ได้รับอนุญาตเท่านั้น
- Integrity หมายถึง ข้อมูลและระบบคอมพิวเตอร์จะต้องมีความถูกต้องสมบูรณ์ ไม่ถูกเปลี่ยนแปลงโดยไม่รับอนุญาต หรือ มีการปลอมแปลงใช้งาน หรือสูญหายโดยไม่ทราบสาเหตุ
- Availability หมายถึง ข้อมูลและระบบคอมพิวเตอร์ จะต้องมีความพร้อมใช้งานอย่างปลอดภัย สอดคล้องตามความต้องการของแต่ละหน่วยงาน
- Authenticity & Non-repudiation หมายถึง การพิสูจน์ตัวตนที่ถูกต้องและมีความน่าเชื่อถือในการทำธุรกรรมและการแลกเปลี่ยนข้อมูลระหว่างกัน ทั้งในและนอกบริษัทฯ

1.1 วัตถุประสงค์

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ จัดทำขึ้นเพื่อควบคุมดูแลการให้บริการด้านระบบสารสนเทศที่มีประสิทธิภาพต่อการบริหารจัดการทางธุรกิจ โดยมีวัตถุประสงค์หลักคือ

1. มีความปลอดภัยของข้อมูล และระบบสารสนเทศ (Confidentiality)
2. มีความครบถ้วนและถูกต้องสมบูรณ์ของข้อมูลสารสนเทศ (Integrity)
3. มีความต่อเนื่องในการทำงานของข้อมูล และระบบสารสนเทศ (Availability)
4. ให้มีมาตรฐานตามข้อกำหนด และเป็นไปตามกฎเกณฑ์ของ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551
5. กำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ และผู้ใช้
6. ป้องกันการบุกรุกและพฤติกรรมการใช้งานที่ไม่ถูกต้อง

1.2 ขอบเขตของนโยบาย (Coverage of Policy)

นโยบายนี้ครอบคลุมถึงการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศทั้งอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย โปรแกรมควบคุมพิวเตอร์ และข้อมูลใดๆ ของบริษัทฯ ที่มีให้บริการแก่พนักงานและผู้ใช้ทั่วไป รวมถึงผู้ให้บริการ คู่สัญญา บุคคล หรือนิติบุคคลอื่นใดที่สามารถเข้าถึงระบบสารสนเทศของบริษัทฯ ได้ จะต้องยึดถือและปฏิบัติตามภายใต้กรอบนโยบายด้านเทคโนโลยีสารสนเทศฉบับนี้

หากมีนโยบายฉบับใดที่ได้มีการประกาศใช้ไปก่อนหน้านี้แล้ว มีข้อความขัด หรือแย้งกับนโยบายฉบับนี้ ให้ยึดปฏิบัติตามนโยบายฉบับนี้เป็นสำคัญ

1.3 นิยาม

ในนโยบายความปลอดภัยข้อมูลและระบบคอมพิวเตอร์-การจัดการฉบับทั่วไปนี้

“บริษัทฯ” หมายถึง บริษัท ทีคิวเอ็ม อัลฟา จำกัด (มหาชน)

“พนักงาน” หมายถึง พนักงานประจำ พนักงานบริษัท ทีคิวเอ็ม อัลฟา จำกัด (มหาชน) อันได้แก่ บริษัท ทีคิวเอ็ม อินชัวร์รันส์ โบรคเกอร์ จำกัด ,บริษัท ทีคิวเอ็มไลฟ์ อินชัวร์รันส์ โบรคเกอร์ จำกัด ,บริษัท แคสแมท จำกัดและบริษัทฯในเครือ พนักงานสัญญาจ้าง พนักงานชั่วคราวตามระเบียบของบริษัทฯ ในเรื่องการบริหารงานบุคคล

“ระบบคอมพิวเตอร์” หมายถึง ระบบเครือข่าย (Network) ระบบปฏิบัติการ (Operating System) ระบบ Application และข้อมูล (Data) สำหรับการใช้งานและทดสอบ

“ข้อมูล” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของ เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ โดยคำว่าข้อมูลให้หมายรวมถึงข้อมูลส่วนบุคคลด้วย

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลที่สามารถบ่งชี้ได้ว่าข้อมูลนั้นเป็นของใคร สามารถระบุไปยังตัวบุคคลได้

“ผู้ดูแลระบบคอมพิวเตอร์” หมายถึง พนักงานที่ได้รับมอบหมายจากบริษัทฯ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์ให้สามารถทำงานได้ตามนโยบายของบริษัทฯ

“ผู้ดูแลความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์” หมายถึง พนักงานที่ได้รับมอบหมายจากบริษัทฯ ให้มีหน้าที่รับผิดชอบในการดูแลและตรวจสอบในด้านความปลอดภัยของระบบคอมพิวเตอร์

"ภัยคุกคาม" หมายถึง เหตุการณ์ หรือ การกระทำที่เกิดขึ้นโดยไม่พึงประสงค์ และ มีผลต่อการทำงานของระบบคอมพิวเตอร์ เช่น ทำงานผิดพลาด, ทำงานช้า, ข้อมูลรั่วไหล, ข้อมูลเสียหาย เป็นต้น อันอาจจะก่อให้เกิดความเสี่ยงในการดำเนินการของบริษัทฯ

"ช่องโหว่" หมายถึง จุดอ่อน หรือ ข้อบกพร่อง หรือ การใช้งานระบบคอมพิวเตอร์ที่ไม่เหมาะสมเสี่ยงต่อการทำให้เกิดภัยคุกคาม ซึ่งจะต้องได้รับการปรับปรุงแก้ไขให้อยู่สภาพที่เหมาะสมต่อไป

1.4 มาตรฐานและกฎหมายอ้างอิง

นโยบายความปลอดภัยฉบับนี้ จัดทำขึ้นโดยมีเนื้อหาสอดคล้องกับมาตรฐานและกฎหมายต่าง ๆ เพื่อให้มั่นใจว่า การบริหารและการควบคุมดูแลการใช้ระบบคอมพิวเตอร์และข้อมูลให้มีความปลอดภัยได้ปฏิบัติตามหลักเกณฑ์ที่ได้มาตรฐานสากล โดยบริษัทยึดถือมาตรฐานและกฎหมายที่ใช้เป็นแนวทางในการจัดทำนโยบายความปลอดภัยดังต่อไปนี้

- ☐ ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements
- ☐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ,ฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551

2. บทบาทหน้าที่และความรับผิดชอบ (Roles and Areas of Responsibility)

ความรับผิดชอบด้านการรักษาความปลอดภัยในภาพรวม มุ่งเน้นความมีประสิทธิภาพและสอดคล้องตามกฎหมาย และข้อกำหนดในสัญญา โดยผู้บริหารสายงานเทคโนโลยีสารสนเทศและการสื่อสารมีความรับผิดชอบโดยรวมในการรักษาความมั่นคงปลอดภัยข้อมูลของบริษัทฯ รวมทั้งการรักษาความปลอดภัยข้อมูลเกี่ยวกับบุคลากรและความมั่นคงด้านไอที

2.1 เจ้าของนโยบายความปลอดภัย

ประธานบริษัทเป็นเจ้าของนโยบายความปลอดภัย โดยมอบความรับผิดชอบต่อเอกสารที่เกี่ยวข้องกับการรักษาความปลอดภัยแก่ผู้บริหารสายงานเทคโนโลยีสารสนเทศและการสื่อสาร การเปลี่ยนแปลงในนโยบายทั้งหมดต้องได้รับการอนุมัติและลงนามโดยผู้บริหารสายงานเทคโนโลยีสารสนเทศและการสื่อสาร

2.2 ผู้บริหารสายงานเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้บริหารสายงานเทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่รับผิดชอบหลักในการรักษาความปลอดภัยข้อมูลของบริษัทฯ

2.3 เจ้าของระบบ (System Owner)

เจ้าของระบบ มีหน้าที่รับผิดชอบในการให้คำปรึกษากับแผนกไอทีในการจัดซื้อ การพัฒนา การบำรุงรักษาข้อมูลและระบบสารสนเทศที่เกี่ยวข้อง ระบบทั้งหมดและทุกประเภทข้อมูลต้องมีเจ้าของระบบที่กำหนดไว้

เจ้าของระบบต้องกำหนดผู้ใช้หรือกลุ่มผู้ใช้ที่ได้รับอนุญาต กำหนดการเข้าถึงข้อมูลและ ต้องมีการจัดทำเอกสารอธิบายการใช้ข้อมูลตลอดจนความเป็นเจ้าของระบบ

2.4 ผู้ดูแลระบบ (System Administrator)

ผู้ดูแลระบบ คือ ผู้ดูแลระบบสารสนเทศและข้อมูลของบริษัทฯ เป็นผู้ที่ได้รับความไว้วางใจจากบริษัทฯ และบุคคลอื่นๆ ที่เกี่ยวข้อง ข้อมูลและระบบแต่ละประเภทต้องมีผู้ดูแลระบบโดยเฉพาะอย่างน้อยหนึ่งท่าน ซึ่งมีหน้าที่ในการปกป้องข้อมูล รวมทั้งการใช้ระบบการควบคุมการเข้าถึง การรักษาความลับ และดำเนินการสำรองข้อมูลเพื่อให้มั่นใจว่าข้อมูลที่มีความสำคัญจะไม่สูญหาย โดยต้องดำเนินการบำรุงรักษาระบบรักษาความปลอดภัยตามนโยบายความปลอดภัย

2.5 ผู้ใช้ระบบ (Users)

พนักงานต้องมีความรับผิดชอบในการศึกษา และปฏิบัติตามกฎระเบียบด้านเทคโนโลยีสารสนเทศ หากมีข้อสงสัยหรือคำถามเกี่ยวกับการบริหารข้อมูลประเภทต่างๆ ควรสอบถามกับเจ้าของระบบของข้อมูลที่เกี่ยวข้อง (System Owner) หรือผู้ดูแลระบบ (System Administrator)

2.6 ที่ปรึกษาและคู่ค้าตามสัญญา (Consultants and Contractual Partners)

คู่ค้าตามสัญญาและที่ปรึกษาที่ทำสัญญากับบริษัทฯ จะต้องลงนามในข้อตกลงการรักษาความลับ (Confidentiality Agreement) ก่อนที่จะเข้าถึงข้อมูลที่เป็นความลับ เจ้าของระบบจะต้องเป็นผู้รับผิดชอบในการตรวจสอบว่ามีการปฏิบัติตามนโยบายนี้

3. หลักการสำคัญสำหรับการรักษาความปลอดภัยของสารสนเทศ

3.1 หน่วยงานรักษาความปลอดภัยข้อมูล (Security organization)

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยขององค์กร มีการบริหารงาน และการทำงานที่ชัดเจนตามสายงานที่รับผิดชอบอย่างเหมาะสม จึงกำหนดเป็นแนวทางปฏิบัติงานดังนี้

3.1.1 ประธานบริษัทฯ เป็นผู้รับผิดชอบหลัก หรือแต่งตั้งคณะทำงานหรือมอบหมายอำนาจหน้าที่ด้านการรักษาความปลอดภัยสารสนเทศให้แก่ (Chief Information Officer: CIO) เพื่อทำหน้าที่ในการรักษาความปลอดภัยของข้อมูลและเป็นผู้ควบคุมตามนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กำกับดูแลระบบรักษาความปลอดภัยของบริษัทฯ ซึ่งหมายรวมถึงความปลอดภัยของข้อมูลและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.1.2 แผนกและส่วนงานต่างๆ มีหน้าที่รับผิดชอบในการดำเนินการด้านความปลอดภัยข้อมูลของหน่วยงานโดยผู้จัดการของแต่ละหน่วยงาน ต้องแต่งตั้งผู้ดูแลความปลอดภัยแยกต่างหาก

3.1.3 รองประธานสายงานเทคโนโลยีสารสนเทศและการสื่อสาร (Executive Vice President: EVP) รับผิดชอบเกี่ยวกับความปลอดภัยข้อมูลในด้านระบบเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐาน

3.1.4 ผู้จัดการฝ่ายปฏิบัติการฝ่ายบริหารงานซอฟต์แวร์ และฝ่ายโครงสร้างพื้นฐาน มีหน้าที่รับผิดชอบด้านความมั่นคงสารสนเทศในด้านการพัฒนาซอฟต์แวร์ โครงสร้างพื้นฐาน และคุณภาพงานทั้งหมด

3.1.5 ผู้อำนวยการฝ่ายบุคคลมีหน้าที่รับผิดชอบด้านความปลอดภัยของข้อมูลตามกฎหมายว่าด้วยข้อมูลส่วนบุคคลและเป็นผู้ควบคุมข้อมูลส่วนบุคคลของพนักงาน ตลอดจนการรักษาความปลอดภัยข้อมูลเกี่ยวกับระบบ Human Resource System

3.1.6 โครงการต่าง ๆ ต้องดำเนินการตามคู่มือที่เกี่ยวข้องกับโครงการ โดยควรกำหนดแนวทางการจัดการความมั่นคงสารสนเทศสำหรับโครงการนั้นๆ

3.1.7 การรักษาความปลอดภัยข้อมูลของบริษัทฯ จะได้รับการปรับปรุงให้เป็นปัจจุบันเท่าที่จำเป็น โดยมีการควบคุมภายใน และความช่วยเหลือจากผู้ตรวจสอบเทคโนโลยีสารสนเทศภายนอก (External IT Auditor)

3.1.8 บริษัทฯ จะจัดกิจกรรมสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อส่งเสริมให้เกิดการปฏิบัติอย่างต่อเนื่อง ดังนี้

- กิจกรรมเพื่อทบทวนและแนะนำนโยบายด้านความปลอดภัยข้อมูล เพื่อจัดทำบันทึกเป็นลายลักษณ์อักษร รวบรวมเอกสารประกอบที่เกี่ยวข้อง และกระจายความรับผิดชอบไปยังผู้เกี่ยวข้อง
- ติดตามการเปลี่ยนแปลงที่สำคัญที่ส่งผลต่อภัยคุกคามต่อทรัพย์สินข้อมูลขององค์กร (Information Assets)
- ทบทวนและตรวจสอบรายงานเหตุการณ์ความปลอดภัย (Security Incident)
- อนุญาตให้มีการริเริ่มเพื่อเสริมสร้างความมั่นคงด้านข้อมูลยิ่งขึ้น

3.2 การกำหนดชั้นความลับข้อมูล (Data Classification and control of assets)

3.2.1 "ทรัพย์สิน (Assets)" หมายถึง ข้อมูลและ/หรือสารสนเทศ และ เครื่องมือ เครื่องใช้ คอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่เป็นของบริษัทฯ

3.2.2 ข้อมูล และ/หรือ สารสนเทศ และโครงสร้างพื้นฐานต่าง ๆ ที่เกี่ยวข้อง รวมถึงข้อมูลส่วนบุคคล ต้องกำหนดให้ มีการจำแนกตามระดับการรักษาความปลอดภัย และการควบคุมการเข้าถึง

3.2.3 การกำหนดชั้นความลับข้อมูล (Data Classification)

- เนื่องด้วยข้อมูลที่ใช้ร่วมกันภายในบริษัทมีความหลากหลาย จำเป็นต้องกำหนดชั้นความลับข้อมูลให้ชัดเจนเพื่อให้เกิดความปลอดภัยในการเผยแพร่ หรือนำข้อมูลไปใช้งานอย่างถูกต้องเหมาะสม
- การจัดชั้นลำดับความลับข้อมูล จัดแบ่งตามลำดับความสำคัญของข้อมูลออกเป็น 3 ระดับ คือ

  ระดับที่ 1: confidentiality คือ ข้อมูลที่มีความสำคัญสูง คือข้อมูลที่อาจก่อให้เกิดความเสียหายต่อบริษัทฯ หรือมีผลต่อความได้เปรียบเสียเปรียบในการแข่งขันทางธุรกิจ หากข้อมูลนั้นถูกเผยแพร่ออกไป เช่น ข้อมูลพนักงาน ข้อมูลด้านบัญชีการเงิน ข้อมูลลูกค้า ข้อมูลส่วนบุคคล เป็นต้น

  ระดับที่ 2: Internal use คือ ข้อมูลเพื่อการปฏิบัติงานภายในบริษัทฯ คือข้อมูลที่เกิดจากขั้นตอนการปฏิบัติงานต่างๆ ของบริษัทฯ ซึ่งเป็นข้อมูลที่ไม่ก่อให้เกิดผลเสียหายต่อบริษัทฯ หากมีการเผยแพร่ออกไปภายนอก แต่จะมีการป้องกันข้อมูลเหล่านั้นมิให้ผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลได้เห็นข้อมูลเหล่านี้ได้ เช่น Log Files เอกสารรายงานต่าง ๆ เป็นต้น

  ระดับที่ 3: Publish คือ ข้อมูลเผยแพร่ทั่วไป คือข้อมูลที่บริษัทฯ เปิดเผยให้บุคคลทั่วไปรับทราบ เช่น ข้อมูลที่เผยแพร่ผ่านทาง web site ของบริษัทฯ เป็นต้น

3.2.4 บริษัทฯ ต้องบริหารและดูแลข้อมูลผู้ใช้ และควรจัดให้มีการเก็บรักษาข้อมูล ตามลำดับความลับของข้อมูลที่เหมาะสม

3.2.5 เอกสารที่เป็นความลับต้องมีการบ่งชี้ที่ชัดเจน

3.2.6 ต้องมีการจำแนกอุปกรณ์ต่างๆ ตามลำดับความลับของข้อมูล และจัดให้มีในแผนสำรองเมื่อเกิดเหตุการณ์ฉุกเฉิน

3.2.7 ต้องมีการจัดทำแผนในการจัดเตรียมพื้นที่เก็บข้อมูลและเอกสารอิเล็กทรอนิกส์

3.3 การรักษาความปลอดภัยข้อมูลในการเชื่อมต่อกับผู้ใช้บริการของแคทแมส (Information security in connection with users of services)

3.3.1 ก่อนการจ้างงาน (Prior to employment)

- ☐ ต้องมีการอธิบายสัญญาจ้างและหน้าที่และความรับผิดชอบของพนักงานในด้านการรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์
- ☐ ต้องมีการตรวจสอบประวัติพนักงานในตำแหน่งต่างๆ ที่จะรับเข้าทำงานในบริษัทฯ ตามกฎหมาย กฎระเบียบ และแนวทางที่กำหนด
- ☐ ต้องให้พนักงาน ผู้รับจ้าง ที่ปรึกษา และบุคคลอื่นๆ ที่เข้าถึงข้อมูลที่เป็นความลับหรือข้อมูลภายในเซ็นสัญญาการไม่เปิดเผยข้อมูล
- ☐ กำหนดให้มีการขอความยินยอม เก็บรวมรวม ใช้ หรือเปิดเผยข้อมูล จากผู้มาสมัครงาน

3.3.2 ระหว่างการจ้างงาน (During employment)

- ☐ พนักงานทุกคนจะได้รับสิทธิ์พื้นฐานที่เพียงพอในการใช้ระบบคอมพิวเตอร์ตั้งแต่วันแรกที่เข้าทำงาน คือ รหัสผ่านสำหรับการใช้ Domain, Email
- ☐ พนักงานต้องได้รับการระบุสิทธิ์ของตนเองในการใช้ทรัพยากรคอมพิวเตอร์ของบริษัท และใช้งานภายใต้ขอบเขตหน้าที่ของตนเองเท่านั้น
- ☐ ในกรณีพนักงานต้องปฏิบัติงานตามคำสั่งพิเศษ เช่น ปฏิบัติงานในต่างประเทศ และต้องการเปลี่ยนแปลงสิทธิในการใช้ระบบคอมพิวเตอร์เป็นการชั่วคราว ให้แจ้งความต้องการไปที่ผู้บังคับบัญชาเพื่อขออนุมัติ และส่งคำอนุมัติดังกล่าวไปยังหน่วยงาน IT Helpdesk เพื่อดำเนินการต่อไป โดยจะพิจารณาความต้องการดังกล่าว ไม่มีความเสี่ยงหรือละเมิดนโยบายของบริษัท
- ☐ สิทธิ์การใช้ระบบคอมพิวเตอร์จะถูกระงับหรือไม่อนุญาตให้ใช้เป็นการชั่วคราว โดยให้ยึดถือตามประกาศของฝ่าย IT เป็นครั้งคราวไป

- กำหนดให้มีการขอความยินยอม เก็บรวมรวม ใช้ หรือเปิดเผยข้อมูล จากพนักงานเพิ่มเติม เนื่องจากข้อมูลที่ขอตอนมาสมัครงาน และข้อมูลที่ขอในระหว่างที่เป็นพนักงานแล้ว ข้อมูลขอมากขึ้นและวัตถุประสงค์ในการขอความยินยอมมีเพิ่มขึ้น จึงจำเป็นต้องขอความยินยอมเพิ่ม

3.3.3 การเลิกจ้างหรือเปลี่ยนแปลงการจ้างงาน

- เมื่อมีการโยกย้ายหน่วยงาน สิทธิ์การใช้ระบบคอมพิวเตอร์จะถูกเปลี่ยน ยกเลิก หรือลบทิ้ง เพื่อให้เหมาะสมกับหน้าที่ในตำแหน่งงานใหม่ทุกครั้ง ทั้งนี้ทาง IT Helpdesk จะดำเนินการโอนย้ายให้ตามคำสั่งที่เป็นทางการจากฝ่ายบุคคลเท่านั้น
- สิทธิ์การใช้ระบบคอมพิวเตอร์จะถูกเพิกถอน หรือ ยกเลิก เมื่อพนักงานพ้นสภาพจากการเป็นพนักงานของบริษัทแล้ว โดย IT Helpdesk จะดำเนินการระงับสิทธิ์การใช้ระบบคอมพิวเตอร์ในเบื้องต้น หรือ เปลี่ยนรหัสผ่าน แล้วจึงดำเนินการถอดสิทธิ์ทั้งหมดต่อไป เมื่อพิจารณาแล้วว่าไม่มีผลกระทบต่อการทำงาน ทั้งนี้ทาง IT Helpdesk จะดำเนินการส่งเรื่องให้เจ้าหน้าที่ดำเนินการเพิกถอนหรือยกเลิกตามคำสั่งที่เป็นทางการจากฝ่ายบุคคลเท่านั้น

3.4 การจัดการสภาวะแวดล้อมทางกายภาพของการรักษาความปลอดภัยของข้อมูล (Information security regarding physical conditions)

3.4.1 การรักษาความปลอดภัยของพื้นที่ (Security areas)

- ข้อมูล คอมพิวเตอร์และอุปกรณ์ต่างๆ ที่เกี่ยวข้องที่เป็นความลับต้องได้รับการป้องกัน และจัดเก็บในสถานที่ที่มีการรักษาความปลอดภัยและมีควบคุมการเข้าถึงตามสิทธิ์ที่ได้กำหนดไว้ ดังแสดงไว้ในตารางดังนี้

ระดับการรักษาความปลอดภัย	พื้นที่	การรักษาความปลอดภัย
เขียว	- พื้นที่ไม่จำกัดการเข้าออก	- ไม่มีการควบคุมการเข้าออกในระหว่างเวลาทำงานปกติ - ข้อมูลภายในและข้อมูลที่เป็นความลับไม่ควรจะมีการพิมพ์ที่พื้นที่นี้
เหลือง	- พื้นที่ที่มีการใช้ข้อมูลภายในระหว่างเวลาทำการ - พื้นที่ทำงาน ห้องประชุม ห้องเก็บของ และห้องปฏิบัติการบางประเภท เช่น ห้องแล็ป ห้องพริ้นท์เตอร์	- เอกสารที่จะพิมพ์ออกมาผู้สั่งพิมพ์จะต้องไปรอรับที่เครื่อง (Follow me function) - มีการควบคุมการเข้าถึงข้อมูล (Access control) หรือมีคีย์การ์ด เป็นต้น
แดง	- พื้นที่ควบคุมต้องมีการกำหนดสิทธิพิเศษ (Special authorization) จึงจะเข้าได้ เช่น ห้องเก็บข้อมูล ห้องคอมพิวเตอร์ หรือห้องเซิร์ฟเวอร์) ที่เก็บข้อมูลที่เป็นความลับ	- เอกสารที่จะพิมพ์ออกมาผู้สั่งพิมพ์จะต้องไปรอรับที่เครื่อง (Follow me function) - มีการควบคุมการเข้าถึงข้อมูล (Access control) หรือมีคีย์การ์ด เป็นต้น

- ☐ ต้องมีการจัดทำแผนผังแสดงขอบเขตของพื้นที่ต่างๆ ตามตารางข้างต้นอย่างชัดเจน
- ☐ ในพื้นที่ที่เก็บรักษาข้อมูลที่เป็นความลับต้องจัดให้มีบันทึก (log) และตรวจสอบการเข้า-ออกอย่างเหมาะสม
- ☐ ผู้รับจ้าง ที่ปรึกษา และบุคคลอื่นๆ ที่จะเข้าไปยังพื้นที่สีแดงและสีเหลืองต้องได้รับการควบคุมและติดตามอย่างเหมาะสม

3.4.2 การรักษาความปลอดภัยของอุปกรณ์ (Securing equipment)

- ☐ คอมพิวเตอร์ และอุปกรณ์ต่างๆ ที่ได้รับการจัดลำดับชั้น “สูง” ต้องได้รับการป้องกันจากอุบัติภัยต่างๆ เช่น ไฟไหม้ น้ำท่วม อุณหภูมิที่เปลี่ยนแปลง เป็นต้น การจัดลำดับชั้นของคอมพิวเตอร์ และอุปกรณ์ต่างๆ ต้องดำเนินการโดยการประเมินความเสี่ยงที่กำหนดไว้
- ☐ ข้อมูลที่เป็น “ความลับ” ต้องไม่ถูกจัดเก็บไว้ในคอมพิวเตอร์เคลื่อนที่หรืออุปกรณ์พกพา เช่น โน๊ตบุ๊ค มือถือ เป็นต้น แต่ถ้ามีความจำเป็นที่จะต้องจัดเก็บต้องมีการป้องกันข้อมูล โดยการใช้พาสเวิร์ดและการเข้ารหัสตามกระบวนการหรือแนวทางที่กำหนดไว้

3.5 การบริหารการปฏิบัติงานและการติดต่อสื่อสารของระบบสารสนเทศ (IT communications and operations management)

3.5.1 ขั้นตอนปฏิบัติงานและขอบเขตความรับผิดชอบ (Operational procedures and areas of responsibility)

- ☐ การซื้อและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศต้องได้รับการอนุมัติจากแผนกเทคโนโลยีสารสนเทศ
- ☐ การซื้อและติดตั้งซอฟต์แวร์สำหรับอุปกรณ์เทคโนโลยีสารสนเทศต้องได้รับการอนุมัติจากแผนกเทคโนโลยีสารสนเทศ
- ☐ แผนกเทคโนโลยีสารสนเทศควรตรวจสอบเอกสารของระบบเทคโนโลยีสารสนเทศตามมาตรฐานของบริษัทฯ
- ☐ การเปลี่ยนแปลงใดๆ เกี่ยวกับระบบเทคโนโลยีสารสนเทศ ต้องมีการพิจารณาผลกระทบทางด้านธุรกิจและความปลอดภัย ก่อนดำเนินการเสมอ
- ☐ แผนกเทคโนโลยีสารสนเทศต้องมีขั้นตอนรองรับสถานการณ์ฉุกเฉิน เพื่อลดผลกระทบจากการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศในกรณีที่เกิดข้อผิดพลาด
- ☐ ต้องมีการจัดทำเอกสารขั้นตอนการปฏิบัติงาน และต้องได้รับการปรับปรุงให้เป็นปัจจุบัน
- ☐ ต้องมีการวางแผน และประเมินความเสี่ยงก่อนการนำระบบเทคโนโลยีสารสนเทศมาใช้จริง เพื่อหลีกเลี่ยงข้อผิดพลาด นอกจากนี้ควรมีการตรวจสอบและจัดการกับปัญหาที่อาจจะเกิดขึ้นโดยคาดไม่ถึง
- ☐ ควรจำแนกหน้าที่และความรับผิดชอบออกจากกันอย่างชัดเจน เพื่อลดโอกาสการนำทรัพย์สินทางด้านเทคโนโลยีสารสนเทศ ไปใช้ในทางที่ผิดทั้งโดยเจตนาหรือไม่เจตนา

- การพัฒนา การทดสอบและการบำรุงรักษาเทคโนโลยีสารสนเทศ ควรมีการจัดการโดยแยกการปฏิบัติงานออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และเพื่อลดความเสี่ยงในการเกิดความผิดพลาด

3.5.2 บริการของบุคคลภายนอก (Third party services)

สัญญาต่างๆ เกี่ยวกับระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก ควรระบุข้อมูลสำคัญดังนี้

- ข้อกำหนดด้านความปลอดภัยข้อมูลรวมทั้งความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน (availability)
- การอธิบายเกี่ยวกับระดับความปลอดภัยที่จะทำข้อตกลงระหว่างกัน
- กำหนดข้อตกลงความร่วมมือในการแลกเปลี่ยนข้อมูล
- ความต้องการสำหรับการรายงานเหตุการณ์ด้านความปลอดภัย (Security Incidents) จากบุคคลที่สาม
- การอธิบายวิธีการตรวจสอบการปฏิบัติตามสัญญา
- การอธิบายถึงสิทธิ์ของบริษัทฯ ในการตรวจสอบบุคคลภายนอก

3.5.3 การวางแผนและการตรวจรับระบบ (System planning and acceptance)

- ต้องพิจารณาความต้องการด้านความปลอดภัยข้อมูลในการออกแบบ การทดสอบ การติดตั้งและการอัพเกรดระบบเทคโนโลยีสารสนเทศ ตลอดจนระหว่างการเปลี่ยนแปลงระบบ ต้องมีการพัฒนากระบวนการปฏิบัติงานเพื่อการจัดการการเปลี่ยนแปลง และการพัฒนา/การบำรุงรักษาระบบ
- ระบบเทคโนโลยีสารสนเทศต้องมีการกำหนดความต้องการด้าน Capacity หรือโหลดในด้านต่างๆ เพื่อการตรวจสอบเป็นระยะ และวางแผนการอัพเกรดและการปรับเปลี่ยนในเวลาที่เหมาะสม ซึ่งเป็นกิจกรรมสำคัญอย่างยิ่งสำหรับระบบเทคโนโลยีสารสนเทศที่รองรับธุรกิจสำคัญของบริษัทฯ

3.5.4 การป้องกันรหัสโปรแกรมที่เป็นอันตราย (Protection against malicious code)

- อุปกรณ์คอมพิวเตอร์ต้องได้รับการป้องกันไวรัสและรหัสโปรแกรมที่เป็นอันตรายอื่นๆ ซึ่งเป็นหน้าที่ของผู้จัดการฝ่ายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.5.5 การสำรองข้อมูล (Backup)

- ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการดำเนินการสำรองข้อมูลและเรียกคืนการสำรองข้อมูล รวมทั้งการจัดเก็บข้อมูลในระบบเทคโนโลยีสารสนเทศของบริษัทฯ ตามที่ได้จำแนกประเภทไว้ (Data Classification)
- การสำรองข้อมูลควรจัดเก็บไว้ภายนอกหรือในโซนที่มีการป้องกันแยกต่างหาก

3.5.6 การบริหารเครือข่าย (Network administration)

- ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการป้องกันเครือข่ายภายในของบริษัทฯ
- ควรมีการจัดเก็บทะเบียนทรัพย์สินของอุปกรณ์เครือข่ายที่มีการเชื่อมโยงถึงกัน (Network Inventory)
- ควรบันทึกกิจกรรมการเข้าสู่ระบบเครือข่าย (Logging) ทั้งหมดของบริษัทฯ

3.5.7 การจัดการสื่อบันทึกข้อมูล (Management of storage media)

- ☐ ควรมีขั้นตอนในการจัดการสื่อบันทึกข้อมูลแบบภายนอก และให้ถือเป็นความรับผิดชอบของพนักงานทุกคนให้ปฏิบัติตาม
- ☐ กรณีการทำลายสื่อบันทึกข้อมูลที่ไม่ใช้แล้ว ต้องมีการกำจัด/ทำลายอย่างปลอดภัย โดยใช้ขั้นตอนการดำเนินการอย่างเป็นทางการ

3.5.8 การแลกเปลี่ยนข้อมูล (Exchange of information)

- ☐ ควรมีขั้นตอนและการควบคุม ด้านการแลกเปลี่ยนข้อมูล และการถ่ายโอนข้อมูลกับภายนอก โดยบุคคลหรือหน่วยงานภายนอกต้องปฏิบัติตามขั้นตอนเหล่านี้
- ☐ บริษัทฯ มีสิทธิ์เข้าถึงอีเมล์ส่วนบุคคลและข้อมูลส่วนตัวอื่นๆ ที่เก็บอยู่ในเครือข่ายคอมพิวเตอร์ของบริษัทฯ

3.5.9 การเข้ารหัส (Use of encryption)

- ☐ ควรเข้ารหัสหรือป้องกันการจัดเก็บและถ่ายโอนข้อมูลที่สำคัญ

3.5.10 การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic exchange of information)

- ☐ กรณีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จะต้องมีการป้องกันข้อมูล เพื่อป้องกันจากการฉ้อโกง การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
- ☐ แผนกเทคโนโลยีสารสนเทศ ควรตรวจสอบข้อมูลที่สามารถเข้าถึงได้จากสาธารณะ เช่น บริการข้อมูลทางเว็บไซต์ของบริษัทฯ จะต้องได้รับการป้องกันอย่างเพียงพอจากการเข้าถึงโดยไม่ได้รับอนุญาต

3.5.11 การเฝ้าระวังการเข้าถึงและการใช้ระบบ (Monitoring of system access and usage)

- ☐ ควรมีการบันทึกและตรวจสอบ การเข้าถึงและการใช้ระบบเทคโนโลยีสารสนเทศ เพื่อตรวจสอบกิจกรรมการประมวลผลข้อมูลที่ไม่ได้รับอนุญาต
- ☐ การใช้ระบบและการตัดสินใจต่างๆ เกี่ยวกับระบบต้องสามารถสอบทานได้ถึงระดับบุคคล หรือระบบ
- ☐ แผนกเทคโนโลยีสารสนเทศ ควรบันทึกเหตุการณ์ การหยุดชะงัก (Disruptions) ความผิดปกติในการดำเนินงานของระบบ (Irregularities of System Operations) และสาเหตุที่อาจเกิดขึ้นจากข้อผิดพลาด
- ☐ ควรมีการตรวจสอบ ความสามารถในการทำงานและคุณภาพของระบบอย่างเพียงพอ เพื่อสร้างความมั่นใจในการใช้งานและความพร้อมใช้งานที่เชื่อถือได้
- ☐ แผนกเทคโนโลยีสารสนเทศ ควรบันทึกเหตุการณ์ด้านความปลอดภัย (Security Incidents) สำหรับระบบที่จำเป็นทั้งหมด
- ☐ แผนกเทคโนโลยีสารสนเทศ ควรมีการตรวจสอบเวลาของเครื่องแม่ข่าย (System Clock) และการ Sync กับเวลามาตรฐานเพื่อความถูกต้อง
- ☐ จะต้องมีการควบคุมการใช้ระบบสารสนเทศที่มีข้อมูลส่วนบุคคล

3.6 การควบคุมการเข้าถึงข้อมูล (Access control)

3.6.1 ความต้องการทางธุรกิจ (Business requirements)

- ☐ ให้มีการกำหนดแนวทางในการควบคุมการเข้าถึงข้อมูลและการกำหนดพาสเวิร์ดให้สอดคล้องกับความต้องการทางธุรกิจและการรักษาความปลอดภัยและให้มีการทบทวนแนวทางที่กำหนดขึ้นเป็นระยะ
- ☐ แนวทางที่กำหนดขึ้นควรกำหนดให้มีความต้องการที่จำเป็นของพาสเวิร์ด (ระยะเวลาในการเปลี่ยน ความยาวขั้นต่ำชนิดของตัวอักษรเป็นต้น) และมีระเบียบในการจัดเก็บพาสเวิร์ด

3.6.2 การเข้าถึงข้อมูล

- ☐ กำหนดให้การเข้าถึงข้อมูลในระดับที่ 1 (ข้อมูลที่มีความสำคัญสูง) และระดับที่ 2 (ข้อมูลเพื่อการปฏิบัติงานภายในบริษัท) จะต้องมีการควบคุม และการจำกัดสิทธิ์ในการเข้าถึงข้อมูลของแต่ละระบบงานตามลำดับความรับผิดชอบของเจ้าหน้าที่ในแต่ละหน่วยงาน
- ☐ การนำข้อมูลในระดับที่ 1 (ข้อมูลที่มีความสำคัญสูง) ออกไปเปิดเผยให้บุคคลอื่นที่ไม่ได้รับสิทธิ์การเข้าถึงข้อมูลได้รับทราบ หรือนำไปเปิดเผยให้บุคคลภายนอกได้รับทราบจะได้รับการพิจารณาโทษทางวินัยตามระเบียบบริษัทต่อไป
- ☐ ข้อมูลในระดับที่ 2 (ข้อมูลเพื่อการปฏิบัติงานภายในบริษัทฯ) เป็นข้อมูลการปฏิบัติงานภายในของแต่ละฝ่าย ดังนั้นจึงถือว่าเป็นความรับผิดชอบของผู้ได้รับสิทธิ์โดยตรงที่จะต้องทำการรักษาข้อมูลและไม่ควรนำข้อมูลไปเปิดเผยให้บุคคลอื่นที่ไม่มีส่วนเกี่ยวข้อง หรือไม่ได้รับสิทธิ์ในการเข้าถึงข้อมูลนั้นๆ ได้รับทราบ
- ☐ การเข้าถึงข้อมูลใดๆจะต้องได้รับอนุญาตจากเจ้าของข้อมูล (Data owner) ก่อนเสมอ โดยจะต้องมีการบันทึกความต้องการและอนุมัติจากผู้บริหารสูงสุดของหน่วยงาน และต้องกำหนดระดับการเข้า (Authorization) ตามสิทธิ์ที่ได้รับมอบหมาย
- ☐ ผู้ใช้จะต้องได้รับการยืนยันตัวบุคคล (Authentication) ก่อนการเข้าถึงข้อมูลตามวิธีการที่กำหนด

3.6.3 การเข้ารหัสข้อมูล

ต้องมีการเข้ารหัสข้อมูล (Encryption) เมื่ออยู่ในสถานการณ์ ต่อไปนี้

- ☐ การโอนข้อมูลระหว่างเครื่องคอมพิวเตอร์
- ☐ การติดต่อกับหน่วยงานภายนอกผ่านระบบ Internet
- ☐ การเก็บข้อมูลสำคัญ เช่น รหัสและรหัสผ่านผู้ใช้ (Username and Password Policy)

โดยกำหนดมาตรฐานควบคุมเกี่ยวกับรหัสและรหัสผ่านสำหรับผู้ใช้งานที่มีสิทธิสูงและผู้ใช้งานที่มีสิทธิสูงสุด รหัสและรหัสผ่านผู้ใช้ระบบทั่วไป และมีมาตรฐานการเข้ารหัสข้อมูล (Encryption policy) ดังนี้

<u>มาตรฐานเกี่ยวกับรหัสผู้ใช้ และ รหัสผ่าน</u>

1. ผู้ใช้ระบบต้องมีรหัสผู้ใช้งานเป็นของตัวเอง (Unique Identity) ห้ามใช้รหัสร่วมกับบุคคลอื่น ยกเว้นรหัสผู้ใช้ประจำเครื่อง (Root, Administrator)
2. การบันทึกรหัสผ่านในระบบงานใดๆ ต้องมีการเข้ารหัส (Password encryption)

3. บัญชีผู้ใช้งานที่มีสิทธิสูง และผู้ใช้งานที่มีสิทธิสูงสุด กำหนดให้มีขั้นตอนการควบคุมการใช้งานที่เหมาะสมกับระบบ เช่น การเปลี่ยนรหัสผ่าน การเบิกใช้รหัสผ่าน รวมถึงการเก็บรักษารหัสผ่านของบัญชีผู้ใช้งานที่มีสิทธิสูงควรเก็บให้เป็นความลับและจัดเก็บในสถานที่ที่ปลอดภัย
4. ต้องใช้รหัสผ่านที่เดาได้ยาก (Complex/Strong Password) เช่น
   - รหัสผ่านมีความยาวอย่างน้อย 8 หลัก
   - ประกอบไปด้วยตัวอักษร ตัวเลข และ อักขระพิเศษ
   - ถ้าเป็นอักษรภาษาอังกฤษ ควรมีอักษรตัวใหญ่ตัวเล็กผสมกัน
   - ไม่ใช้คำที่อยู่ในพจนานุกรม
   - ไม่ใช้คำที่เกี่ยวข้องกับตัวผู้ใช้ เช่น วันเกิด,หมายเลขโทรศัพท์
   - สามารถใช้รหัสผ่านเป็นภาษาไทยได้
5. ต้องกำหนดระยะเวลาหมดอายุของรหัสผ่าน และ บังคับให้เปลี่ยนทันทีเมื่อครบเวลา
   - จำนวนวันหมดอายุขั้นต่ำ 90 วัน
   - ควรมีระบบแจ้งเตือนก่อนหมดอายุล่วงหน้า หากสามารถทำได้
6. ควรมีระบบที่สามารถบังคับให้เปลี่ยนรหัสผ่านที่ถูกใช้ครั้งแรก
7. ผู้ใช้ระบบสามารถเปลี่ยนรหัสผ่านได้ตลอดเวลา
8. ในกรณีที่ผู้ใช้งานไม่ได้นั่งหน้าเครื่องคอมพิวเตอร์ของตนเอง ควรตั้งโปรแกรมรักษาจอภาพที่มีการใช้รหัสผ่านแทน เพื่อป้องกันไม่ให้ผู้อื่นแอบใช้หรือดูข้อมูลภายในเครื่อง
9. ระบบป้อนรหัสผ่านต้องไม่ถูกเปิดเผยหรือใช้เครื่องมือดักจับได้โดยง่าย
10. ในกรณีที่ระบบใดๆมีข้อจำกัดไม่สามารถปฏิบัติตามได้ หรือ ต้องให้บริการต่อบุคคลภายนอกให้ผู้จัดทำระบบปรึกษาผู้ดูแลความปลอดภัยระบบงานเพื่อกำหนดขอบเขตการใช้งานที่เหมาะสมต่อไป

<u>มาตรฐานการเข้ารหัสข้อมูล</u>

1. ต้องมีการเข้ารหัสข้อมูลที่มีความสำคัญ เช่น รหัสผ่าน เป็นต้น
2. เมื่อมีการสื่อสารระหว่างสถานที่ หรือ เป็นการติดต่อไปยังระบบซึ่งมีความสำคัญสูง
3. เลือกใช้การเข้ารหัสที่น่าเชื่อถือและเหมาะสมต่อระบบงานนั้นทั้งแบบ Symmetric หรือ Asymmetric โดยพิจารณาจากลักษณะของระบบงาน การ encryption ที่เหมาะสมต่อการใช้งาน เช่น AES 256, SSL, RSA, ,3DES, MD5, SHA-1, PKI, DH เป็นต้น
4. การใช้งานแบบ PKI ต้องเลือกผู้ใช้ให้บริการ CA ที่มีคุณสมบัติน่าเชื่อถือ ยกเว้นเป็นการใช้ภายในระบบเครือข่ายของบริษัทฯ ให้ใช้งานแบบ Self Sign ได้
5. เลือกใช้ขนาดของการเข้ารหัส (KEY) สูงที่สุดที่สามารถทำได้โดยไม่มีผลกระทบต่อประสิทธิภาพของระบบ เช่น SSL 256 bits
6. ต้องปกปิด key ของการเข้ารหัสเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
7. ไม่บันทึก key ของการเข้ารหัสไว้ในสื่อใดๆ ที่สามารถเรียกขึ้นมาดูได้

3.6.4 นโยบายความปลอดภัยของระบบเครือข่าย

ระบบเครือข่ายจัดเป็นหัวใจสำคัญอย่างหนึ่งของการบริหารระบบคอมพิวเตอร์ เพราะเป็นช่องทางสื่อสารระหว่างเครื่องคอมพิวเตอร์ทั้งภายในและภายนอกบริษัท ปัจจุบันมีอันตรายหรือการโจมตีผ่านระบบเครือข่ายจำนวนมาก

- การเข้าใช้งานระบบเครือข่าย

อุปกรณ์คอมพิวเตอร์ที่จะเชื่อมต่อเพื่อใช้งาน (Network access) ในระบบเครือข่ายของบริษัท จะต้องผ่านการขออนุญาต (Authentication) ด้วยวิธีที่ปลอดภัย เช่น การระบุรหัสผู้ใช้ และรหัสผ่านหรือใช้รหัสประจำเครื่องเช่น Mac Address พนักงานจะต้องไม่เชื่อมอุปกรณ์เข้าระบบเครือข่ายโดยไม่ได้รับอนุญาต เพราะอาจจะก่อให้ระบบเครือข่ายหยุดทำงาน หรือ เป็นช่องทางการแพร่ระบาดของไวรัสได้

- การแยกเขตใช้งานในระบบเครือข่าย (Network segregation)

บริษัทฯ จะแบ่งเขต (Zone) การใช้งานของระบบเครือข่าย เพื่อให้มีความปลอดภัย และสะดวกต่อการดูแล โดยเจ้าหน้าที่ระบบเครือข่ายจะเป็นผู้จัดการเปิดสิทธิ์การใช้งานตามความต้องการของระบบงานและหน่วยงานต่างๆ และจะต้องบันทึกการเปลี่ยนแปลงตามนโยบายการบริหารความเปลี่ยนแปลงทุกครั้ง

- การรักษาความปลอดภัยในระบบเครือข่าย

เจ้าหน้าที่บริหารระบบเครือข่ายจะต้องดูแลระบบเครือข่ายให้อยู่ในสภาพพร้อมใช้งาน และมีความปลอดภัยต่อผู้ใช้งานทั้งภายในและภายนอกบริษัทอย่างเหมาะสม เช่น การติดตั้ง Firewall, การเลือกใช้ระบบ encryption เป็นต้น

- การดูแลและบำรุงรักษาระบบเครือข่าย

เจ้าหน้าที่บริหารระบบเครือข่ายจะต้องดูแลและบำรุงระบบเครือข่ายให้มีความสามารถในการรองรับการใช้งานทั้งภายในและภายนอกบริษัทฯ

- การใช้ Internet และ Email

บริษัทฯ ได้จัดบริการเกี่ยวกับ Internet และ Email เพื่อใช้ติดต่อสื่อสารทั้งภายในและภายนอกบริษัทฯได้ โดยมีข้อกำหนดดังต่อไปนี้

- อนุญาตให้ใช้ Internet เพื่อค้นคว้าข้อมูลที่จำเป็นต่อการทำงานเท่านั้น
- ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- ไม่อนุญาตให้ดาวน์โหลดโปรแกรมใดๆ ที่ไม่มีลิขสิทธิ์ถูกต้อง หรือไม่เกี่ยวข้องกับงาน สำหรับการดาวน์โหลดข้อมูลที่มีปริมาณมาก ควรหลีกเลี่ยงที่จะกระทำในช่วงเวลาทำการหรือมีการใช้งานหนาแน่น เพื่อป้องกันไม่ให้เกิดการขัดข้องในระบบเครือข่าย
- พนักงานไม่ควรเข้า web site ที่ไม่เหมาะสม เช่น web ให้บริการทางเพศ หรือ การพนัน
- พนักงานจะได้สิทธิ์ในการรับส่งเมล์ที่มีไฟล์แนบตามข้อกำหนด (รับ-ส่งได้ไม่เกินครั้งละ 10 MB)
- พนักงานไม่ควรนำ Email ไปประกาศใน Internet โดยไม่จำเป็น เพราะอาจจะเป็นสาเหตุถูกนำไปรับ Spam mail

- พนักงานไม่ควรสร้าง หรือ ส่งต่อ Mail ที่เข้าข่ายจดหมายลูกโซ่,จดหมายหลอกหลวง หรือ เมล์ที่อาจจะก่อให้เกิดผลทางกฎหมาย

3.6.5 อุปกรณ์เคลื่อนที่และการทำงานจากระยะไกล (Mobile equipment and remote workplaces)

- การเข้าถึงอุปกรณ์คอมพิวเตอร์และบริการของบริษัทฯ จากระยะไกล จะได้รับอนุญาตเฉพาะเมื่อมีการอ่านและทำความเข้าใจนโยบายความปลอดภัยและลงนามในระเบียบข้อบังคับด้านเทคโนโลยีสารสนเทศเท่านั้น
- การเข้าถึงเครือข่ายของบริษัทฯ จากระยะไกลสามารถใช้งานได้เฉพาะวิธีที่ได้รับอนุมัติจากแผนกเทคโนโลยีสารสนเทศ ด้านความปลอดภัยเท่านั้น
- อุปกรณ์เคลื่อนที่ต่างๆ ต้องได้รับการป้องกันด้านการรักษาความปลอดภัยอย่างเพียงพอ
- ต้องเข้ารหัสข้อมูลที่มีความสำคัญ หากเก็บไว้ในสื่อแบบพกพา เช่น หน่วยความจำ External Disk, DVD และโทรศัพท์มือถือ

3.7 การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

เพื่อให้การพัฒนาระบบงานหรือการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ได้ดำเนินการอย่างรอบคอบและเป็นไปตามความต้องการของผู้ใช้งานโดยมีเป้าหมาย เพื่อลดความเสี่ยงที่จะเกิดผลกระทบต่อความปลอดภัยของระบบคอมพิวเตอร์ของบริษัทฯ ดังนั้นเมื่อต้องการเปลี่ยนแปลงใดๆ จะต้องดำเนินงานตามขั้นตอนต่อไปนี้

3.7.1 การร้องขอเพื่อเปลี่ยนแปลง (Request for Change:RFC)

- ผู้ที่ต้องการร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำรายการที่ต้องการ โดยระบุวัตถุประสงค์หรือสาเหตุของการเปลี่ยนแปลงนั้นๆ โดยมีการอนุมัติจากผู้บริหารสูงสุดของหน่วยงาน และ แจ้งความต้องการไปยัง IT Helpdesk เพื่อบันทึกรายการและผลิตตามการทำเปลี่ยนแปลง
- ผู้ร้องขอ และ ผู้ที่จะดำเนินการเปลี่ยนแปลง จะต้องร่วมกันประเมินความเสี่ยง หรือ ผลกระทบที่อาจจะเกิดขึ้นจากการเปลี่ยนแปลง และ ระบุวิธีการบรรเทาความเสี่ยง หรือ ผลกระทบนั้นๆ และหากเป็นระบบสำคัญที่อาจจะมีผลกระทบต่อการทำงานของคนจำนวนมากจะต้องเตรียมแผนสำรองฉุกเฉิน (Business Continuity Planning) เพื่อรองรับในกรณีที่เกิดสาเหตุสุดวิสัยที่ทำให้ระบบไม่สามารถใช้งานได้ตามปกติ (System outage)

3.7.2 ถ้าการเปลี่ยนแปลงใดๆ มีผลกระทบดังต่อไปนี้ ให้นำเข้าปรึกษาในที่ประชุมคณะทำงานพิจารณาการเปลี่ยนแปลง (Change Control Board)

- การเปลี่ยนแปลงที่ทำให้ระบบต้องหยุดทำงานเป็นเวลานาน เกินจากที่ได้ตกลงกันระหว่างผู้ใช้งานและผู้ดูแลระบบ) หรือ มีผลกระทบต่อบุคคล/หน่วยงานภายนอก
- การเปลี่ยนแปลงที่ต้องใช้งบประมาณจำนวนมาก
- การเปลี่ยนแปลงที่ทำให้วิธีใช้งานไม่เหมือนเดิม
- การเปลี่ยนแปลง Hardware หรือ Software เป็นการใช้ชุดใหม่

3.7.3 การควบคุมสภาพแวดล้อมของการเปลี่ยนแปลง

- ☐ ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop environment) ออกจากส่วนที่ใช้งานจริง (Production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น
- ☐ ควรตระหนักถึงระบบรักษาความปลอดภัย(Security Awareness) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนาหรือการแก้ไขเปลี่ยนแปลง

3.7.4 ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

3.7.5 การทดสอบก่อนเปลี่ยนแปลง

- ☐ ผู้ที่ร้องขอและเจ้าหน้าที่สายงานเทคโนโลยีสารสนเทศ รวมทั้งผู้ที่ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง
- ☐ ในระบบงานที่สำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบก่อนที่จะโอนย้ายไปใช้งานจริง

3.7.6 การโอนย้ายระบบงาน (Release Management)

- ☐ ก่อนที่จะมีการโอนย้ายระบบงานเพื่อใช้งานจริง (production) จะต้องมีการสอบทานแผนการโอนย้ายระบบงาน (release plan) ให้ถูกต้องครบถ้วนเสมอ
- ☐ ให้เจ้าหน้าที่ส่วน Operation ของ IT Division จะเป็นผู้โอนย้ายระบบงานจากระบบที่ใช้เพื่อการพัฒนา หรือ เพื่อการทดสอบเข้าสู่ระบบหลัก (production) เท่านั้น หากมีความจำเป็นที่ต้องทำโดยบุคคลอื่นให้แจ้งเหตุผลเป็นกรณีพิเศษ

3.7.7 การจัดทำเอกสารและรายละเอียดประกอบการเปลี่ยนแปลง (Documentation and Version Control)

- ☐ ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรม และ ระบบต่างๆ ที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
- ☐ ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล รายละเอียดระบบเครือข่ายและ Server คู่มือระบบงาน ทะเบียนรายชื่อผู้ที่มีสิทธิ์ใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
- ☐ ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนา หรือ เปลี่ยนแปลง และ ค่าติดตั้ง (parameter) ไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

3.7.8 การทดสอบหลังการใช้งาน (post- implementation test) ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือ แก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งาน ระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

3.8 นโยบายการตรวจสอบและรายงานเหตุการณ์ผิดปกติ (Incident management)

3.8.1 การตรวจสอบเหตุการณ์ผิดปกติ (Incident Monitoring)

3.8.2 เจ้าหน้าที่ประจำ System Admin จะต้องทำการตรวจสอบเหตุการณ์ผิดปกติในระบบคอมพิวเตอร์ของบริษัทอย่างสม่ำเสมอ

3.8.3 การบันทึกเหตุการณ์ผิดปกติ (Incident Recording) ให้บันทึกเหตุการณ์ผิดปกติที่ตรวจพบ เพื่อหาสาเหตุหรือแหล่งที่มา ตลอดจนถึงบันทึกวิธีการแก้ไขเหตุการณ์ผิดปกติดังกล่าวด้วย

3.8.4 การรายงานเหตุการณ์ผิดปกติ (Incident Reporting)

- ☐ ในกรณีที่พนักงานพบเหตุการณ์ผิดปกติของระบบคอมพิวเตอร์ เช่น พบการเตือนของ โปรแกรมป้องกันไวรัส หรือพบว่ามี Email แปลกปลอมเข้าสู่เครื่องของตนเอง ให้แจ้งเหตุการณ์ผิดปกติดังกล่าวไปที่ IT Helpdesk เพื่อบันทึกและตรวจสอบเหตุการณ์นั้นต่อไป
- ☐ ในกรณีที่เหตุการณ์ผิดปกติมีผลกระทบอย่างมากต่อบริษัท และ/หรือ บุคคล ตลอดจนหน่วยงานภายนอก ให้นำเสนอเหตุการณ์นั้นต่อผู้บริหารสูงสุดของสายงานเทคโนโลยีสารสนเทศโดยด่วน เพื่อพิจารณาแนวทางป้องกันหรือแก้ไขดำเนินการที่เหมาะสมในอนาคตต่อไป

3.9 แผนสำรองเมื่อเกิดเหตุการณ์ฉุกเฉิน (Disaster recovery and Business Continuity)

ความเสี่ยงที่มีผลทำให้เกิดการหยุดชะงักในการดำเนินงานของธุรกิจ เป็นสิ่งจำเป็นอย่างยิ่งที่ จะต้องมีการเตรียมความพร้อมด้านการวางแผนสำรองฉุกเฉิน เพื่อการกอบกู้ระบบให้สามารถดำเนินธุรกรรมให้เป็นไปอย่างต่อเนื่อง และมีผลกระทบต่อธุรกิจให้น้อยที่สุดตามเงื่อนไข

- ☐ จัดให้มีการทำแผนสำรองฉุกเฉินของระบบงานที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัทฯ
- ☐ จัดลำดับความสำคัญของระบบงานที่เกี่ยวข้องในการกอบกู้ระบบให้เป็นไปอย่างมีประสิทธิภาพ
- ☐ ต้องมีการสำรองข้อมูลและชุดคำสั่งให้มีความครบถ้วน และจัดเก็บไว้กับผู้ให้บริการรับฝากสื่อบันทึกข้อมูลที่ได้มาตรฐานเป็นที่ยอมรับ
- ☐ ต้องมีการจัดทำขั้นตอนในการปฏิบัติที่ครอบคลุมถึงวิธีการสำรองข้อมูล ความถี่ของการบันทึก และการจัดเก็บรักษาที่ได้มาตรฐาน
- ☐ กำหนดให้มีการทดสอบแผนสำรองฉุกเฉินโดยการจำลองสถานการณ์อย่างน้อยปีละ 1 ครั้ง
- ☐ กำหนดให้มีการทบทวน และปรับปรุงแผนสำรองฉุกเฉินให้มีความพร้อมสามารถใช้งานได้จริงอย่างน้อยปีละ 1 ครั้ง

3.10การทำงานจากที่บ้าน (Work From Home)

การทำงานจากที่บ้าน โดยที่ไม่ต้องเข้าออฟฟิต (Work From Home) กรณีมีความจำเป็นให้พนักงานสามารถทำงานจากที่บ้านได้ จะต้องได้รับการอนุมัติจากรองประธานสายงานขึ้นไป โดยสามารถเข้าถึงระบบจากภายนอกได้ ดังนี้

3.10.1โปรแกรมควบคุมเครื่องคอมพิวเตอร์จากระยะไกล (Remote Desktop)

3.10.2เครือข่ายส่วนตัวเสมือน (Virtual Private Network)

3.11 การฝึกอบรมและให้ความรู้เกี่ยวกับความปลอดภัย (Training Policy)

พนักงานทุกคนจะต้องได้รับการฝึกอบรมดังต่อไปนี้

3.11.1 พนักงานที่เริ่มงานใหม่กับบริษัทฯ จะได้รับการปฐมนิเทศเกี่ยวกับความรู้เบื้องต้นของความปลอดภัยด้านเทคโนโลยีสารสนเทศ และรับทราบนโยบายความปลอดภัยของบริษัทฯ

3.11.2 พนักงานแต่ละระดับได้รับการฝึกอบรมเกี่ยวกับความปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับที่เหมาะสมต่อการทำงาน

3.11.3 สายงานเทคโนโลยีสารสนเทศจะจัดให้มีการบรรยายความรู้เกี่ยวกับความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละครั้ง เพื่อให้พนักงานได้รับความรู้ทันสมัยอยู่เสมอ

3.12 บทลงโทษ

พนักงานที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายที่กำหนดไว้โดยไม่มีเหตุผลอันควร บริษัทฯ มีอำนาจในการพิจารณาลงโทษพนักงานที่ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบาย โดยพิจารณาลงโทษตามกระบวนการที่กำหนดไว้ในระเบียบบริษัท ว่าด้วยการบริหารงานบุคคล

3.13 การจัดการ และทบทวนนโยบาย (Policy Management & Revision)

การสอบทานและดูแลหลักเกณฑ์ข้อกำหนดนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นหน้าที่ของผู้บังคับบัญชาสายงานเทคโนโลยีสารสนเทศ และหน่วยงานเทคโนโลยีสารสนเทศจะต้องรับผิดชอบให้มีการทบทวน อย่างน้อยปีละ 1 ครั้ง และปรับเปลี่ยนตามความจำเป็นและความเหมาะสมของวิวัฒนาการที่เปลี่ยนแปลงไปทางด้านเทคโนโลยีสารสนเทศ