นโยบายด้านเทคโนโลยีสารสนเทศ
(IT Policy)

PPS

บริษัท โปรเจค แพลนนิ่ง เซอร์วิส จำกัด (มหาชน)
และบริษัทในเครือ

โดย
ฝ่ายวิจัยและพัฒนานวัตกรรม

นโยบายด้านเทคโนโลยีสารสนเทศฉบับนี้ เป็นฉบับปรับปรุงครั้งที่ 2/2565 ทบทวนโดยฝ่ายวิจัยและพัฒนานวัตกรรม มีผลบังคับใช้ตั้งแต่วันที่ 15 พฤศจิกายน 2565 เป็นต้นไป

ผู้จัดทำ	ผู้ตรวจทาน
(นางสาวศิวพร สุวรรณศรี)	(นายชาญชัย ริ้วกุลประเสริฐ)
เจ้าหน้าที่ไอทีอาวุโส	ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

ผู้อนุมัติ

(นายประสงค์ ธาราไชย)

ประธานบริษัท

นโยบายด้านเทคโนโลยีสารสนเทศ
บริษัท โปรเจค แพลนนิ่ง เซอร์วิส จำกัด (มหาชน) และบริษัทในเครือ

1. วัตถุประสงค์ของนโยบาย

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท โปรเจค แพลนนิ่ง เซอร์วิส จำกัด (มหาชน) และบริษัทในเครือ หรือต่อไปนี้เรียกว่า "องค์กร" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ องค์กรจึงเห็นสมควรกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 นโยบายนี้จะต้องทำการเผยแพร่ให้ผู้บริหารและพนักงานทุกระดับในองค์กรได้รับทราบ และทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร พนักงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

2. องค์ประกอบของนโยบาย

นโยบายด้านเทคโนโลยีสารสนเทศของบริษัท โปรเจค แพลนนิ่ง เซอร์วิส จำกัด (มหาชน) จัดทำขึ้นเพื่อกำหนดแนวทางการปฏิบัติให้สอดคล้องตามข้อกำหนดในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามที่สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ได้มีประกาศไว้ โดยมีสาระสำคัญดังนี้

1) แนวปฏิบัติของนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร (IT Policy)

เป็นการกำหนดแนวทางการจัดทำนโยบาย เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย และการปฏิบัติตามนโยบาย

2) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

เป็นการกำหนดนโยบายเพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้าน infrastructure risk

3) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

เป็นการกำหนดนโยบายเพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ และระบบป้องกันความเสียหายต่างๆ ที่ควรจัดให้มีภายในศูนย์คอมพิวเตอร์

4) การรักษาความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

เป็นการกำหนดนโยบายเพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึงข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง และป้องกันบุคคล ไวรัส รวมทั้งโปรแกรมไม่พึงประสงค์ต่างๆ มิให้เข้าถึงข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

5) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

เป็นการกำหนดนโยบายเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

6) การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

เป็นการกำหนดนโยบายเพื่อให้ผู้ใช้ให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามอย่างเคร่งครัด

7) การสำรองข้อมูลและระบบคอมพิวเตอร์ (Backup)

เป็นการกำหนดนโยบายเพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และทันเวลาที่ต้องการ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา

8) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

เป็นการกำหนดนโยบายเพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

9) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

เป็นการกำหนดนโยบายเพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ

10) การควบคุมการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

เป็นการกำหนดนโยบายเพื่อให้บริษัทฯ ใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

11) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

นโยบายเพื่อให้บริษัทฯ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สำหรับเป็นแนวทางในการป้องกัน และลดระดับความเสี่ยงที่อาจเกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้

3. หลักการในการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศ

3.1 มุ่งเน้นการกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศ ให้มีการรักษาความลับ (Confidentiality) มีความถูกต้องครบถ้วน (Integrity) และมีสภาพพร้อมใช้งานอยู่เสมอ (Availability) โดยกำหนดเป็นแนวปฏิบัติดังนี้

1) ในด้านการรักษาความลับ (Confidentiality) เพื่อป้องกันการเข้าถึงข้อมูลในระบบสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต จึงต้องมีการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) ระบบปฏิบัติการ (Operating System Access Control) แอพพลิเคชั่นหรือโปรแกรมประยุกต์ (Application and Information Access Control) การควบคุมทางกายภาพ (Physical Security) และการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

2) ในด้านการรักษาความถูกต้องครบถ้วน (Integrity) เพื่อให้ข้อมูลสารสนเทศมีความถูกต้อง ครบถ้วน ไม่ถูกเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหายหรือถูกทำลายโดยไม่ได้รับอนุญาต จึงต้องมีการกำหนดการเข้าถึงและควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control) และการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3) ในด้านการรักษาสภาพพร้อมใช้งาน (Availability) เพื่อให้ระบบสารสนเทศสามารถเข้าถึงหรือใช้งานได้ในเวลาที่ต้องการ จึงต้องมีระบบสำรองข้อมูล เพื่อเตรียมความพร้อมในกรณีฉุกเฉิน

3.2 การสร้างความเข้าใจให้กับผู้ใช้งานระบบ เพื่อให้เกิดความตระหนักถึงผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

3.3 ทบทวนนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร ให้สอดคล้องกับสภาพแวดล้อมและกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง

4. ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศขององค์กร

เพื่อให้การดำเนินตามนโยบายด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ จะต้องมีการกำหนดหน้าที่รับผิดชอบให้แก่ผู้ที่เกี่ยวข้อง เพื่อดูแล ควบคุมให้เป็นไปตามที่กำหนด ดังนี้

- ผู้จัดการฝ่ายวิจัยและพัฒนานวัตกรรม หรือ ผู้จัดการฝ่ายไอที

รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางการแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงาน และตรวจสอบระบบความปลอดภัยของระบบสารสนเทศ พร้อมรายงานผลการดำเนินงาน รวมทั้งรับผิดชอบ ดังนี้

1) ควบคุมการเข้า-ออกห้องแม่ข่าย ตามการกำหนดสิทธิการเข้าถึง
2) กำกับดูแล ติดตาม ตรวจสอบ การเข้าใช้งาน และการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ
3) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์เครื่อง Server และอุปกรณ์เครือข่าย (Network) ให้สามารถใช้งานได้ตามปกติตลอดเวลา
4) กำกับดูแล การติดตั้ง รื้อถอน ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายระบบ LAN, Internet, Intranet ที่ให้บริการภายในองค์กร
5) กำกับ ดูแล รักษา ตรวจสอบ การทำงานของระบบแจ้งเตือนภัยภายในห้องแม่ข่าย ให้มีการทำงานเป็นปกติอยู่ตลอดเวลา
6) แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยง และความเสียหายที่เกิดขึ้นกับระบบสารสนเทศขององค์กร
7) กำกับ ดูแล การป้องกันการถูกคุกคามทางระบบสารสนเทศ และแก้ไขปัญหาการถูกบุกรุกจากบุคคลภายนอกที่ไม่ได้รับอนุญาต (Hacker)
8) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกบุกรุกจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ภายใน Server ให้สามารถใช้งานได้ปกติตลอดเวลา
9) กำกับดูแล ตรวจสอบ การกำหนดหรือแก้ไขเปลี่ยนแปลงค่าพารามิเตอร์ต่างๆของระบบ

10) รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบ

- เจ้าหน้าที่ดูแลระบบสารสนเทศ (System Administrator) หรือ เจ้าหน้าที่ไอที รับผิดชอบดังนี้
  1) ทำการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery) ตามระยะเวลาที่กำหนด
  2) บริหารจัดการสิทธิการเข้าถึงเครื่องแม่ข่าย (Server) เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
  3) บำรุงรักษาอุปกรณ์แม่ข่าย (Server) ให้สามารถใช้งานได้เป็นปกติตลอดเวลา
  4) แก้ไขปัญหา อุปสรรค หรือความเสี่ยงต่างๆที่เกิดขึ้นกับระบบงานเครื่องแม่ข่าย
  5) กำหนด แก้ไข หรือเปลี่ยนแปลงค่าพารามิเตอร์ของระบบต่างๆ
  6) บริหารจัดการสิทธิการเข้าถึงข้อมูลของระบบสารสนเทศต่างๆ (User Access Management) ตามอำนาจหน้าที่และความจำเป็น และตรวจสอบสิทธิผู้ใช้งานตามรอบระยะเวลาที่กำหนด
  7) แก้ไขปัญหา อุปสรรคต่างๆ ในการใช้งานระบบสารสนเทศ
  8) ควบคุมการใช้ทรัพยากร ทั้งฮาร์ดแวร์และซอฟต์แวร์ ให้เป็นไปตามนโยบายที่กำหนด
  9) อื่นๆตามที่ได้รับมอบหมาย

- เจ้าหน้าที่อื่นๆ ที่เกี่ยวข้อง ตามอำนาจหน้าที่ที่ได้รับมอบหมาย ให้เป็นผู้ปฏิบัติและมีหน้าที่รับผิดชอบเกี่ยวกับระบบสารสนเทศขององค์กร

5. ผู้ที่ต้องปฏิบัติตามนโยบาย

นโยบายด้านเทคโนโลยีสารสนเทศ จัดทำขึ้นเพื่อให้ทุกส่วนขององค์กรปฏิบัติตามอย่างเคร่งครัด

6. การบังคับใช้นโยบาย

นโยบายฉบับนี้มีผลบังคับนับแต่วันที่ประกาศใช้

สารบัญ

บทที่ 1 แนวปฏิบัติของนโยบายด้านเทคโนโลยีสารสนเทศขององค์กร

(IT Policy Guideline)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและผู้ที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่ ความรับผิดชอบ และแนวทางในการควบคุมความเสี่ยงต่างๆ

แนวปฏิบัติ

1. การกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ
    - 1.1 ฝ่ายไอทีทุกคนต้องมีส่วนร่วมในการจัดทำนโยบาย และต้องได้รับการอนุมัติจากคณะกรรมการบริหาร หรือคณะกรรมการบริษัท
    - 1.2 การกำหนดบังคับใช้จะมีผลทันทีที่ได้รับการอนุมัติจากคณะกรรมการบริหาร หรือคณะกรรมการบริษัท
    - 1.3 เผยแพร่นโยบายทันทีที่คณะกรรมการบริหาร หรือคณะกรรมการบริษัทอนุมัติ และประกาศใช้
    - 1.4 กรณีมีบุคลากรเข้าใหม่ ต้องแจ้งนโยบายเทคโนโลยีสารสนเทศให้รับทราบ
    - 1.5 เมื่อมีการเปลี่ยนแปลงนโยบายทุกครั้ง จะต้องเผยแพร่นโยบายให้ทุกคนในองค์กรรับทราบ
2. การทบทวนนโยบายด้านเทคโนโลยีสารสนเทศ
    - 2.1 ต้องทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง
    - 2.2 ต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง และจัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ อย่างน้อยปีละ 1 ครั้ง
    - 2.3 ประกาศนโยบายให้กับผู้ใช้งานและบุคคลที่เกี่ยวข้องทุกครั้ง หลังมีการทบทวนและปรับปรุง
    - 2.4 จัดเก็บนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้โดยง่าย

บทที่ 2 การแบ่งแยกอำนาจหน้าที่

(Segregation of Duties)

วัตถุประสงค์

เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคคล ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure Risk

แนวปฏิบัติ

1. การควบคุมการเข้าถึงระบบ (Access Control Policy)
   - 1.1 กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของบริษัท เพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศ จะต้องขออนุญาตต่อผู้ดูแลระบบ (System Administrator)
   - 1.2 ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบ (Developer) ออกจากการทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานในส่วนของระบบที่ใช้งานจริง
   - 1.3 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์ในการเข้าถึงข้อมูลและระบบ ให้เหมาะสมกับการ ใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้ รวมถึงต้องมีการตรวจทานสิทธิ์การใช้งานอยู่เสมอ
   - 1.4 ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงต่างๆ และการผ่านเข้า-ออก สถานที่ตั้งของระบบ เพื่อเป็นหลักฐานในการตรวจสอบ
   - 1.5 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดขั้นตอนในการลงทะเบียนบุคคลากรใหม่ของบริษัท ให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติในการยกเลิกสิทธิ์ เช่น กรณีลาออก หรือเปลี่ยนแปลงตำแหน่งงาน เป็นต้น
   - 1.6 ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการใช้งานเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ประยุกต์ (Application) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่
2. การบริหารจัดการการเข้าถึงระบบสารสนเทศ

   ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้
   - 2.1 การกำหนดสิทธิ์ผู้ใช้ของบุคลากรใหม่ ต้องได้รับการร้องขอเป็นลายลักษณ์อักษร
   - 2.2 กำหนดให้ทำการยกเลิกการใช้งานสำหรับทุก User ID ที่พ้นสภาพจากการจ้างงานแล้ว ซึ่งต้องได้รับการแจ้งจากฝ่ายบุคคล
   - 2.3 การกำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
   - 2.4 กรณีที่มีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องกำหนดระยะเวลาการใช้งานเริ่มต้นและสิ้นสุดเป็นลายลักษณ์อักษรอย่างชัดเจน โดยได้รับการอนุมัติจากผู้มีอำนาจสูงสุดในสายงาน และผู้ดูแลระบบสูงสุด เมื่อครบเวลาที่กำหนดจะถูกระงับการใช้สิทธิ์นั้นทันที

บทที่ 3 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

1. เพื่อป้องกันไม่ให้ผู้ไม่มีอำนาจหน้าที่เข้าถึง ล่วงรู้ (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability Risk)
2. เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมและภัยพิบัติต่างๆ (Availability Risk)

แนวปฏิบัติ

1. การควบคุมศูนย์คอมพิวเตอร์ (ห้อง Server)
   - 1.1 ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง ได้แก่
     - 1.1.1 บุคลากรของบริษัท
       1) เจ้าหน้าที่ไอที ที่มีหน้าที่รับผิดชอบดูแลเครื่องแม่ข่าย
       2) เจ้าหน้าที่ฝ่ายอื่น ที่มีหน้าที่ดูแลอุปกรณ์ที่ติดตั้งอยู่ภายในห้องที่นอกเหนือจากอุปกรณ์เครื่องแม่ข่าย
     - 1.1.2 บุคคลภายนอก ซึ่งมีหน้าที่ติดตั้ง บำรุงรักษา หรือให้คำปรึกษา ในงานเกี่ยวกับอุปกรณ์ที่ติดตั้งภายในศูนย์คอมพิวเตอร์
   - 1.2 การเข้าใช้งานศูนย์คอมพิวเตอร์ (ห้อง Server)
     - 1.2.1 กำหนดให้มีการยืนยันตัวตนในการเข้าออกห้อง Server โดยติดตั้งระบบสแกนลายนิ้วมือ (Finger Scan) และกำหนดสิทธิ์เฉพาะเจ้าหน้าที่ที่รับผิดชอบดูแลเครื่องแม่ข่าย
     - 1.2.2 ผู้ที่จะเข้าใช้ห้อง Server จะต้องได้รับอนุมัติจากเจ้าหน้าที่ไอทีที่รับผิดชอบก่อน
     - 1.2.3 ระยะเวลาการขอเข้าใช้ห้อง Server อยู่ในช่วงเวลาทำงานปกติ คือ วันจันทร์ถึงวันศุกร์ เวลา 08.00 ถึง 17.00 น. ยกเว้นวันหยุดราชการ
     - 1.2.4 กรณีที่มีเหตุฉุกเฉินที่จำเป็นต้องเข้าห้อง Server ให้รีบแจ้งเจ้าหน้าที่ เพื่อให้ทราบถึงสาเหตุและความจำเป็นที่จะต้องเข้าใช้งาน
2. การป้องกันความเสียหาย
   - 2.1 ต้องติดตั้งอุปกรณ์แจ้งเตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
   - 2.2 ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ และต้องให้มีการแจ้งเตือนมายังผู้ดูแลกรณีที่เกิดเหตุขัดข้อง หรือมีความผิดปกติของอุปกรณ์สำรองไฟ เพื่อให้การดำเนินงานมีความต่อเนื่อง
   - 2.3 ต้องควบคุมสภาพแวดล้อมให้มีความเหมาะสม โดยควรตั้งอุณหภูมิของเครื่องปรับอากาศ และตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสมได้

บทที่ 4 การรักษาความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

1. เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง
2. เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

แนวปฏิบัติ

1. การบริหารจัดการข้อมูล (Data Management)
   - 1.1 บริษัทต้องกำหนดชั้นความลับของข้อมูล การจัดเก็บข้อมูลในแต่ละชั้นความลับ และการเข้าถึงข้อมูลแต่ละชั้น ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลในแต่ละระดับชั้น
     - 1.1.1 ข้อมูลที่เป็นความลับอย่างยิ่ง
       1) ข้อมูลเงินเดือน
       2) ข้อมูลกำไร ต้นทุนต่างๆ ที่อาจเอื้อประโยชน์ต่อคู่แข่ง
       3) เอกสารพิเศษ
     - 1.1.2 ข้อมูลที่เป็นความลับ
       1) ข้อมูล Username และ Password เข้าสู่ระบบต่างๆ
       2) ข้อมูลทางบัญชีและการเงิน
       3) ข้อมูลทางกฎหมาย
       4) ข้อมูลส่วนบุคคล
     - 1.1.3 ข้อมูลที่ใช้เฉพาะในแต่ละส่วนงาน
       1) ข้อมูลใน PPS Drive ที่แชร์เฉพาะในหน่วยงานที่เกี่ยวข้อง
       2) ข้อมูลในโปรแกรม Project Live ของแต่ละโครงการ
   - 1.2 กรณีที่มีการจัดเก็บข้อมูลชุดเดียวกันไว้หลายที่ (distributed database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้อง ครบถ้วน ตรงกัน
   - 1.3 ต้องมีการพิสูจน์ตัวตนทุกครั้ง ก่อนมีการเข้าถึงข้อมูลสำคัญของบริษัท
   - 1.4 ต้องมีมาตรการรักษาความปลอดภัยของข้อมูล ในกรณีที่มีการนำอุปกรณ์คอมพิวเตอร์ออกไปนอกพื้นที่ของบริษัท เช่น มีการทำลายข้อมูลในสื่อบันทึกก่อน เป็นต้น
   - 1.5 ในกรณีที่บริษัทต้องการตรวจสอบข้อมูล อาจแต่งตั้งให้ผู้ที่ทำหน้าที่ตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ
   - 1.6 ผู้ใช้งานต้องตระหนักและระมัดระวังในการใช้งานข้อมูล ไม่ว่าจะเป็นข้อมูลของบริษัท หรือข้อมูลส่วนบุคคล
   - 1.7 ผู้ใช้งานต้องช่วยกันป้องกัน ดูแล รักษา ข้อมูลที่เป็นความลับของบริษัท

1.8 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัทห้ามนำไปใช้ในทางที่ผิด และเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

2. การควบคุมการกำหนดสิทธิพิเศษให้แก่ผู้ใช้งาน (User Privilege ID)

2.1 ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่และได้รับความเห็นชอบจาก ผู้มีอำนาจ รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2.2 ในกรณีมีความจำเป็นต้องใช้ user ที่มีสิทธิพิเศษ ต้องมีการควบคุมอย่างรัดกุมและเข้มงวด ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.3 ควรมีการเปลี่ยนรหัสผ่านทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยนรหัสผ่านทุก 60-90 วัน

2.4 การใช้งาน User ที่มีสิทธิพิเศษ ต้องเป็นผู้ที่ถือรหัสผ่าน หรือบุคคลที่ได้รับมอบหมายโดยผู้ถือรหัสผ่านเท่านั้น

2.5 ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญ มีการให้สิทธิผู้ใช้งานรายอื่นเข้าแก้ไขข้อมูลของตนเองได้ จะต้องเป็นการให้สิทธิเฉพาะบุคคลหรือเฉพาะกลุ่มเท่านั้น และต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลา

3. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password)

3.1 ต้องมีระบบตรวจสอบตัวตนและสิทธิการเข้าใช้งานของผู้ใช้ (Identification and Authentication) ก่อนเข้าสู่ระบบคอมพิวเตอร์ที่รัดกุมเพียงพอ และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง

3.2 ผู้ใช้งานควรเปลี่ยนรหัสผ่าน (Password) หลังจากที่ได้รับมอบสิทธิ์ทันที (E-mail) หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

3.3 ผู้ใช้งานควรตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านที่ดีควรประกอบด้วยตัวอักษรผสมกับตัวเลข และมีความยาวไม่น้อยกว่า 6 ตัว

3.4 หากมีการใส่รหัสผ่าน (password) ผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการระงับการใช้งานชั่วคราว เช่น ระบบ PPS Drive ใส่รหัสผ่านผิดเกิน 10 ครั้งติดต่อกันภายใน 1 นาที จะไม่สามารถ Login เข้าใช้งานได้เป็นเวลา 30 นาที เป็นต้น

3.5 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน โดยแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

3.6 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำที่เกิดจากบัญชีของผู้ใช้งาน (Username) ของตน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

3.7 ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการลบบัญชีรายชื่อผู้ที่ไม่มีสิทธิใช้งานระบบแล้วทันทีที่ตรวจพบหรือได้รับแจ้ง

4. การบริหารจัดการทรัพย์สินคอมพิวเตอร์ (Asset Management)
   4.1 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง การรับหรือคืนทรัพย์สินจะถูกบันทึก และตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่รับผิดชอบ
   4.2 กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลรับผิดชอบทรัพย์สินของบริษัทที่ได้รับมอบหมาย
   4.3 ผู้ใช้งานต้องชดใช้ค่าเสียหาย ไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน
   4.4 ทรัพย์สินและระบบสารสนเทศต่างๆ ที่บริษัท จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของบริษัทเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สิน และระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัท ความเสียหายใดๆ ที่เกิดขึ้นให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
   4.5 มีการจัดหาคอมพิวเตอร์ให้เหมาะสมตามตำแหน่งงาน ซึ่งมีนโยบายการจัดซื้ออย่างชัดเจน (อ้างอิงเอกสาร QP-PUR-02 การจัดซื้อทรัพย์สิน) โดยที่ฝ่ายไอทีเป็นผู้ตรวจสอบคุณลักษณะ (Spec) ตามความเหมาะสม
5. การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)
   5.1 บริษัทได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทอนุญาตให้ใช้งานหรือที่บริษัทมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัทห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว
   5.2 หากผู้ใช้มีความจำเป็นต้องใช้งานโปรแกรมที่นอกเหนือจากที่ฝ่ายไอทีเตรียมไว้ให้ ให้แจ้งความประสงค์มายังฝ่ายไอที เพื่อจัดหาลิขสิทธิ์ซอฟต์แวร์มาให้ใช้งานตามความเหมาะสม ซึ่งมีนโยบายการจัดซื้ออย่างชัดเจน (อ้างอิงเอกสาร QP-PUR-02 การจัดซื้อทรัพย์สิน)
6. การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)
   6.1 ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูลรวมทั้งห้ามเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อบริษัท
   6.2 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทเพื่อประโยชน์ทางการค้าหรือประโยชน์ส่วนบุคคล
   6.3 ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัทโดยเด็ดขาดไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม
   6.4 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัทต้องหยุดชะงัก
   6.5 ห้ามใช้ระบบสารสนเทศของบริษัทเพื่อการควบคุมคอมพิวเตอร์ (Remote) หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากฝ่ายไอที
   6.6 ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

6.7 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัทโดยไม่ได้รับอนุญาตจากฝ่ายไอที

7. การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)
   7.1 ควรมีการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า parameter ที่ผิดปกติไป จะต้องเร่งทำการแก้ไขและมีการรายงานโดยทันที
   7.2 ต้องดำเนินการอัพเดต patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ของระบบอย่างสม่ำเสมอ
   7.3 ควรทำการทดสอบ system software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนการติดตั้ง และหลังจากมีการแก้ไข หรือบำรุงรักษา
   7.4 ควรกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข เปลี่ยนแปลง parameter ของระบบไว้อย่างชัดเจน
8. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (network)
   8.1 ต้องมีระบบป้องกันและตรวจสอบการบุกรุก (firewall) ระหว่างเครือข่ายภายในกับภายนอก เพื่อควบคุมการใช้งานที่ผิดปกติผ่านระบบเครือข่าย
   8.2 ต้องจัดทำแผนผังระบบเครือข่าย (network diagram) ซึ่งมีรายละเอียดขอบเขตของเครือข่าย และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
   8.3 กรณีที่มีการเข้าถึงระบบเครือข่ายจากภายนอก ในลักษณะของการ remote control จะต้องมีการควบคุมอย่างเข้มงวด
   8.4 ควรมีการทบทวนการกำหนดค่า parameter ต่างๆ และสำรองค่าไว้อย่างน้อยปีละ 1 ครั้ง นอกจากนี้เมื่อมีการเปลี่ยนแปลง แก้ไขค่า parameter ต้องแจ้งให้ผู้ที่เกี่ยวข้องทุกคนรับทราบทุกครั้ง
9. การบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ (Configuration Management)
   9.1 ควรมีการประเมินผลกระทบที่เกี่ยวข้องก่อนที่จะมีการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ อีกทั้งควรบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ
   9.2 ควรติดตั้งซอฟต์แวร์เท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์
10. การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (Capacity Planning)
   10.1 ต้องมีการประเมินการใช้งานระบบคอมพิวเตอร์ที่สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต
11. การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)
   11.1 ต้องติดตั้งโปรแกรมป้องกันคอมพิวเตอร์ (Antivirus) ทั้งเครื่องแม่ข่ายและเครื่องของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เว้นแต่เครื่องนั้นเป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกัน
   11.2 มีการปรับปรุงระบบป้องกันไวรัสให้เป็นปัจจุบันอยู่เสมอ
   11.3 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อเห็นสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งผู้ดูแลระบบเสมอ
   11.4 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจนำความเสียหายมาสู่ทรัพย์สินของบริษัท
   11.5 ผู้ใช้งานต้องพึงระวังในการเปิดไฟล์ที่ไม่รู้จัก จากอีเมล์ หรือลิ้งจากเว็บไซต์ภายนอก เพื่อป้องกันไวรัสคอมพิวเตอร์ประเภท Advance, Malware

12. บันทึกเพื่อการตรวจสอบ (Audit Log)
    12.1 ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) เช่น บันทึกการเข้าออกระบบ (login-logout logs) บันทึกการเปลี่ยนแปลงข้อมูล เป็นต้น เพื่อประโยชน์ในการตรวจสอบ
    12.2 ต้องมีการจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
13. นโยบายการสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและคอมพิวเตอร์
    13.1 จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางช่องทางสื่อสารขององค์กร
    13.2 ประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวัง ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

บทที่ 5 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(Use of Personal Computer)

วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

แนวปฏิบัติ

1. การใช้งานทั่วไป
   - 1.1 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง
   - 1.2 เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร
   - 1.3 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องส่วนตัว หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
   - 1.4 ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร
   - 1.5 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
   - 1.6 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร
   - 1.7 ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัท ความเสียหายใดๆที่เกิดขึ้นให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
2. การควบคุมการเข้าถึงระบบปฏิบัติการ
   - 2.1 ผู้ใช้ควรกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการระบบปฏิบัติการ
   - 2.2 ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน
3. แนวทางปฏิบัติในการใช้รหัสผ่าน
   - 3.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน โดยแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน
   - 3.2 ผู้ใช้งานควรตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านที่ดีควรประกอบด้วยตัวอักษรผสมกับตัวเลข และมีความยาวไม่น้อยกว่า 6 ตัว
   - 3.3 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำที่เกิดจากบัญชีของผู้ใช้งาน (Username) ของตน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

4. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

4.1 ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

4.2 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อเห็นสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งผู้ดูแลระบบเสมอ

4.3 ผู้ใช้งานต้องพึงระวังในการเปิดไฟล์ที่ไม่รู้จักจากอีเมล์ หรือลิ้งจากเว็บไซต์ภายนอก เพื่อป้องกันไวรัสคอมพิวเตอร์ทุกประเภท

บทที่ 6 การใช้งานจดหมายอิเล็กทรอนิกส์

(Use of Electronic Mail)

วัตถุประสงค์

การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวปฏิบัติ

1. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์
   - 1.1 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) เมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
   - 1.2 ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
   - 1.3 ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ หรือสร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร
   - 1.4 ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
   - 1.5 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น
   - 1.6 ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร
   - 1.7 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
   - 1.8 ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
   - 1.9 ผู้ใช้ควรตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด ไม่ควรเปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากที่อยู่ที่ต้องสงสัยว่าจะไม่ปลอดภัย

บทที่ 7 การสำรองข้อมูลและระบบคอมพิวเตอร์ (Backup)

วัตถุประสงค์

เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และทันเวลาที่ต้องการ (availability risk)

แนวปฏิบัติ

1. การสำรองข้อมูล
   1.1 ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ในการทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยมีการสำรองข้อมูลระบบ ได้แก่ ระบบ HR, ระบบบัญชี, ข้อมูลอีเมล์, ระบบ PPS Drive ซึ่งจะทำการสำรองข้อมูลอย่างน้อยสัปดาห์ละ 1 ครั้ง
      1) ระบบ HR
         ทำการสำรองข้อมูลอัตโนมัติแบบ Snapshot ขึ้นไปเก็บไว้บน Cloud Storage
      2) ระบบบัญชี
         ทำการสำรองข้อมูลอัตโนมัติแบบ Snapshot ขึ้นไปเก็บไว้บน Cloud Storage
      3) อีเมล์
         ฝ่ายไอทีจะทำการสำรองข้อมูลของพนักงานที่ลาออกไว้ในอุปกรณ์จัดเก็บข้อมูล (External Storage) ภายหลังจากที่พนักงานพ้นสภาพแล้ว 1 เดือน ก่อนที่จะทำการลบบัญชีอีเมล์ออกจากระบบ
      4) ระบบ PPS Drive
         ทำการสำรองข้อมูลอัตโนมัติแบบ Snapshot ขึ้นไปเก็บไว้บน Cloud Storage
   1.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน
2. การบำรุงรักษา
   2.1 ต้องหมั่นตรวจเช็คการทำงานของอุปกรณ์ที่สำคัญ ให้มีประสิทธิภาพที่ดีในการทำงานอยู่เสมอ

บทที่ 8 การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk

แนวปฏิบัติ

1. การกำหนดขั้นตอนการปฏิบัติงาน
   - 1.1 มีขั้นตอนหรือวิธีปฏิบัติในการพัฒนา แก้ไข หรือเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร
   - 1.2 สื่อสารรายละเอียดขั้นตอนให้ผู้ใช้งาน หรือบุคคลที่เกี่ยวข้องรับทราบ พร้อมทั้งควบคุมให้มีการปฏิบัติตาม รวมทั้งมีการติดตามอย่างต่อเนื่อง
2. การควบคุมการพัฒนา หรือแก้ไข เปลี่ยนแปลงระบบ
   - 2.1 ต้องมีการร้องขอให้พัฒนาระบบอย่างเป็นลายลักษณ์อักษร และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หัวหน้าฝ่ายไอที
3. การประเมินความเป็นไปได้ของโครงการ
   - 3.1 ต้องมีการจัดทำงบประมาณก่อนเริ่มต้นโครงการเสมอ เพื่อประเมินต้นทุนและประเมินความคุ้มค่าในการลงทุน
   - 3.2 พิจารณาระบบที่มีอยู่ในตลาดที่สามารถตอบสนองต่อ requirement ได้ เพื่อประเมินเปรียบเทียบความคุ้มค่าระหว่างการพัฒนาขึ้นเอง กับการซื้อผลิตภัณฑ์ที่มีอยู่แล้วมาใช้งาน
4. การปฏิบัติงานพัฒนาระบบ
   - 4.1 ต้องแบ่งแยกคอมพิวเตอร์ที่ใช้สำหรับส่วนงานพัฒนาระบบ (Development Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น
   - 4.2 ตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงานของระบบตั้งแต่เริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง
5. การทดสอบระบบ
   - 5.1 ผู้ที่ร้องขอและฝ่ายไอที รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้อง ต้องมีส่วนร่วมในการทดสอบระบบที่พัฒนา หรือทำการเปลี่ยนแปลงแก้ไข ให้มีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้อง ครบถ้วน และตรงตามความต้องการก่อนใช้งานจริง.
6. การโอนย้ายระบบเพื่อใช้งานจริง จะต้องตรวจสอบการโอนย้ายให้มีความถูกต้อง
7. การทดสอบหลังการใช้งาน (Post-Implementation Test)
   - 7.1 ควรกำหนดให้มีการทดสอบระบบที่พัฒนา หรือเปลี่ยนแปลง แก้ไข หลังจากที่มีการใช้งานไปแล้วระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้อง ครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน
8. การสื่อสารการเปลี่ยนแปลง
   - 8.1 ต้องสื่อสารการเปลี่ยนแปลงระบบให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

บทที่ 9 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์
(Computer Operation)

วัตถุประสงค์

เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ มีแนวทางในการควบคุม ได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk และ availability risk

แนวปฏิบัติ

1. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์
   1.1 ต้องมีขั้นตอนหรือวิธีปฏิบัติงานในด้านต่างๆที่สำคัญเป็นลายลักษณ์อักษร (Manual) เพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติงาน (Computer Operation) และปรับปรุงขั้นตอนหรือวิธีปฏิบัติให้เป็นปัจจุบันอยู่เสมอ
2. การติดตามการทำงานของระบบคอมพิวเตอร์
   2.1 ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้สามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพของระบบ
   2.2 ควรบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์ต่างๆให้อยู่ในสภาพที่ดี และพร้อมใช้งานอยู่เสมอ
3. การจัดการปัญหาต่างๆ
   3.1 ต้องกำหนดผู้มีหน้าที่และรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน รวมถึงช่องทางติดต่อในกรณีที่มีปัญหา

บทที่ 10 การควบคุมการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

เพื่อให้บริษัทใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (access risk) ความเสี่ยงเกี่ยวกับความถูกต้อง ครบถ้วนของข้อมูล และการประมวลผลของระบบงาน (integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น

แนวปฏิบัติ

1. การคัดเลือกผู้ให้บริการ
   - 1.1 มีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ ดังนี้
     1) คำนึงถึงความลับของข้อมูลของบริษัทที่ผู้ให้บริการ Outsource จะเข้าถึง
     2) ควรเป็นบริษัทที่มีความชำนาญและมีประสบการณ์ในการให้บริการด้าน Outsource ที่เป็นมาตรฐานสากล
     3) ความสามารถของผู้ให้บริการด้าน Outsource ตรงกับความต้องการของเนื้องาน
     4) ระยะเวลาในการใช้บริการด้าน Outsource
     5) ค่าใช้จ่ายในการใช้บริการด้าน Outsource
   - 1.2 ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขการให้บริการ (service level agreement) อย่างชัดเจน
   - 1.3 ควรพิจารณาเงื่อนไขในการยกเลิกสัญญา หากเกิดกรณีที่มีความจำเป็นที่ต้องยกเลิกการใช้บริการ
2. การควบคุมผู้ให้บริการ
   - 2.1 ต้องกำหนดผู้ทำหน้าที่ Project Leader / Project Manager เพื่อรับผิดชอบ ควบคุม และติดตามการดำเนินงาน
   - 2.2 กรณีที่ใช้บริการด้านการพัฒนาระบบงาน กำหนดให้ผู้ให้บริการเข้าถึงได้เฉพาะส่วน ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น
   - 2.3 หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้
     1) กรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่บริษัท (Onsite Service) ให้เจ้าหน้าที่บริษัทควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิด
     2) กรณีที่เป็นการให้บริการในลักษณะ Remote Access ให้เจ้าหน้าที่บริษัทตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียด และปิดการเชื่อมต่อทันทีที่การให้บริการเสร็จสิ้น
   - 2.4 ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไขเป็นระยะ
   - 2.5 ควรให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

บทที่ 11 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้บริษัทฯ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สำหรับเป็นแนวทางในการป้องกัน และลดระดับความเสี่ยงที่อาจเกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้

แนวปฏิบัติ

1. การตรวจสอบและประเมินความเสี่ยง (Risk Assessment)
   - 1.1 มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ1 ครั้ง โดยประเมินถึงโอกาสที่ควาเสี่ยงด้านสารสนเทศนั้นจะเกิดและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อหาแนวทางในการจัดการ
   - 1.2 กำหนดแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านสารสนเทศที่เหมาะสมและสอดคล้องกับผลประเมินความเสี่ยง เพื่อให้ความเสี่ยงที่เหลืออยู่ในระดับที่ยอมรับได้
   - 1.3 มีการตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายในองค์กร (Internal Audit) หรือผู้ตรวจสอบจากองค์กรภายนอก (External Audit) เพื่อให้องค์กรได้ทราบถึงระดับความเสี่ยงและความมั่นคงปลอดภัยของระบบสารสนเทศ
2. แนวทางในการตรวจสอบและประเมินความเสี่ยง (Risk Management)
   - 2.1 มีการทบทวนกระบวนการบริหารความเสี่ยง อย่างน้อยปีละ 1 ครั้ง
   - 2.2 มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
   - 2.3 มีการตรวจสอบและประเมินความเสี่ยง และให้จัดทำรายงานพร้อมข้อเสนอแนะ ให้ผู้บริหารพิจารณาระดับความเสี่ยงที่เป็นอยู่ กำหนดแนวทางการปรับปรุง และแจ้งให้ผู้ที่เกี่ยวข้องทราบ เพื่อนำไปปฏิบัติ
   - 2.4 มีมาตรการในการตรวจประเมินระบบสารสนเทศ ดังนี้
     1) กำหนดสิทธิให้ผู้ตรวจสอบมีสิทธิเข้าถึงข้อมูลที่จะตรวจสอบได้ในลักษณะอ่านข้อมูลได้อย่างเดียว
     2) มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสอบเข้าถึงข้อมูลที่เขียนหรือบันทึกได้
     3) มีการสร้างสำเนาสำหรับข้อมูล เพื่อให้ผู้ตรวจสอบใช้งาน และทำลายหรือลบทันทีที่ตรวจสอบเสร็จ หรือจัดเก็บไว้โดยมีการป้องกันอย่างรัดกุม
     4) มีวิธีการที่ปลอดภัยสำหรับการเก็บหลักฐานที่ใช้อ้างอิงในการตรวจสอบ
     5) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบสารสนเทศ
     6) มีการบันทึกข้อมูล Log เพื่อแสดงถึงการเข้าถึงข้อมูล ซึ่งรวมถึงวันและเวลาที่เข้าถึงข้อมูลในระบบสำคัญต่างๆ
     7) เครื่องมือที่ใช้ในการตรวจสอบระบบทั้งหมดต้องได้รับการป้องกันในการเข้าถึง และควบคุม จำกัดให้เข้าใช้งานได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น
3. การติดตามและทบทวนความเสี่ยง (Risk Monitoring)
   - 3.1 กำหนดให้มีกระบวนการติดตามความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง และทบทวนความเสี่ยงให้อยู่ในระดับที่ยอมรับได้