ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
เรื่อง แนวทางปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัย
ด้านเทคโนโลยีสารสนเทศ

เพื่อให้ควบคุมการบริหารจัดการ การปฏิบัติงานและการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย เป็นไปได้อย่างมีประสิทธิภาพและมีมาตรฐานมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีจึงได้วางแนวทางในการควบคุมการปฏิบัติงานและการรักษา ความปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้กับหน่วยงานภายในมหาวิทยาลัยฯ โดยแนวทางปฏิบัติฉบับนี้ประกอบด้วย

1. แนวทางข้อที่มีนัยสำคัญ (Mandatory **[ข้อกำหนด]**)
2. แนวทางที่เป็นข้อเสนอแนะเพิ่มเติมที่ควรดำเนินการ (Accredit **[ข้อเสนอแนะ]**)

โดยสาระสำคัญของแนวทางปฏิบัติฉบับนี้ประกอบด้วย

1. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
2. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
4. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
5. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
6. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
7. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
8. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

แนวทางปฏิบัติ

1. <u>การจัดทำนโยบาย</u>
    - ต้องจัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษรและผู้บริหาร เจ้าหน้าที่ฝ่ายคอมพิวเตอร์ และผู้ใช้งานของแต่ละฝ่ายงานต้องมีส่วนร่วมในการจัดทำนโยบาย และอย่างน้อยต้องได้รับอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง(CIO) **[ข้อกำหนด]**
    - ต้องทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ โดยต้องมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง ซึ่งต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง **[ข้อกำหนด]**
    - ต้องมีการเผยแพร่นโยบายที่เป็นลายลักษณ์อักษรให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้โดยง่าย **[ข้อกำหนด]**

2. <u>รายละเอียดของนโยบาย</u>
    - ต้องระบุวัตถุประสงค์และขอบเขตอย่างชัดเจน และมีเนื้อหาครอบคลุมอย่างน้อยในเรื่องต่อไปนี้ **[ข้อกำหนด]**
        - การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
        - การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
        - การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

- การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
- การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
- การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)
- การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

3. <u>การปฏิบัติตามนโยบาย</u>

- ต้องประกาศใช้และสื่อสารนโยบายให้แก่บุคคลที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้สามารถปฏิบัติตามได้ เช่น จัดการฝึกอบรม เป็นต้น **[ข้อกำหนด]**
- ต้องมีระบบติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบาย อย่างเคร่งครัด **[ข้อกำหนด]**
- ต้องมีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละครั้ง ซึ่งอาจเป็นหน่วยงานภายใน หรือผู้ตรวจสอบภายนอก **[ข้อกำหนด]**
- ต้องแจ้งผู้รับผิดชอบทางด้านเทคโนโลยีสารสนเทศโดยเร็ว เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ[1] **[ข้อกำหนด]**
- ต้องมีขั้นตอนหรือวิธีปฏิบัติเพื่อรองรับให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้ **[ข้อกำหนด]**
- ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้อง อย่างชัดเจน เช่น หน้าที่ของผู้ใช้งานในกรณีที่พบว่าเครื่องคอมพิวเตอร์มีการติดไวรัส หน้าที่และความรับผิดชอบของเจ้าหน้าที่รักษาความปลอดภัยระบบเครือข่าย หน้าที่และความรับผิดชอบของลูกจ้างชั่วคราว เป็นต้น **[ข้อกำหนด]**

---

[1] ผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ หมายถึง ผลกระทบที่ส่งผลให้หน่วยงานไม่สามารถดำเนินงานตามภารกิจผ่านระบบเครือข่ายได้อย่างต่อเนื่อง

การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

วัตถุประสงค์

การแบ่งแยกอำนาจหน้าที่มีวัตถุประสงค์เพื่อให้มีการทวนสอบการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure Risk

แนวทางปฏิบัติ

- ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (System Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment) **[ข้อกำหนด]**
- ต้องจัดให้มี Job Description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร **[ข้อกำหนด]**
- ควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น เช่น ผู้บริหารระบบ (System Administrator) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เป็นต้น **[ข้อเสนอแนะ]**

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

การควบคุมการเข้าออกศูนย์คอมพิวเตอร์มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability Risk) ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (Availability Risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทาง การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และระบบป้องกันความเสียหายต่างๆ ที่ควรจัดให้มีภายในศูนย์คอมพิวเตอร์

แนวทางปฏิบัติ

1. <u>การควบคุมศูนย์คอมพิวเตอร์</u>
    - ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ดูแลระบบ (System Administrator) เป็นต้น **[ข้อกำหนด]**
    - ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่ศูนย์คอมพิวเตอร์ควบคุมดูแลการทำงานตลอดเวลา เป็นต้น **[ข้อกำหนด]**
    - ต้องมีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ **[ข้อกำหนด]**
    - ควรจัดศูนย์คอมพิวเตอร์ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) ส่วนเครื่องพิมพ์ (Printer Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น นอกจากนี้ ควรแยกส่วนที่ต้องมีการเข้าถึงโดยเจ้าหน้าที่หลายฝ่ายออกจากศูนย์คอมพิวเตอร์ เป็นต้น **[ข้อเสนอแนะ]**

2. <u>การป้องกันความเสียหาย</u>

2.1 ระบบป้องกันไฟไหม้

- ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา **[ข้อกำหนด]**
- ศูนย์คอมพิวเตอร์หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์คอมพิวเตอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น **[ข้อกำหนด]**

2.2 ระบบป้องกันไฟฟ้าขัดข้อง

- ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ ได้รับความเสียหายจากความไม่คงที่ ของกระแสไฟ **[ข้อกำหนด]**
- ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ เพื่อให้การดำเนินงานมีความต่อเนื่อง **[ข้อกำหนด]**

2.3 ระบบควบคุมอุณหภูมิและความชื้น

- ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม **[ข้อกำหนด]**

2.4 ระบบเตือนภัยน้ำรั่ว

- ในกรณีที่มีการยกระดับพื้นของศูนย์คอมพิวเตอร์ เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและสายเครือข่ายด้านล่าง ก็ควรติดตั้งระบบเตือนภัยน้ำรั่ว บริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา นอกจากนี้ หากศูนย์คอมพิวเตอร์ตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ก็ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่อย่างสม่ำเสมอ **[ข้อเสนอแนะ]**

การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติ

1. <u>การบริหารจัดการข้อมูล</u>

- ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ **[ข้อกำหนด]**
- การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น **[ข้อกำหนด]**
- ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน **[ข้อกำหนด]**
- ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น **[ข้อเสนอแนะ]**

2. <u>การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน[2] (User Privilege)</u>

- ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ **[ข้อกำหนด]**
- ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษ[3] ต้องมีการควบคุมการใช้งานอย่างรัดกุม **[ข้อกำหนด]**

  ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
  - ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
  - ควรควบคุมการใช้งาน User ที่มีสิทธิพิเศษอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งาน User ดังกล่าวในลักษณะ Dual Control โดยให้เจ้าหน้าที่ 2 รายถือรหัสผ่านคนละครึ่ง หรือเก็บซอง Password ไว้ในตู้เซฟ เป็นต้น และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
  - ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
  - ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น
- ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น **[ข้อกำหนด]**
- ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของ

---

[2] ผู้ใช้งาน หมายถึง เจ้าของข้อมูล ผู้บริหารระบบ (System Administrator) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่พัฒนาระบบ (System Developer) และเจ้าหน้าที่อื่นที่ใช้งานระบบคอมพิวเตอร์

[3] User ที่มีสิทธิพิเศษ หมายถึง Root หรือ User อื่นที่มีสิทธิสูงสุด

ข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว **[ข้อกำหนด]**

- ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว **[ข้อกำหนด]**

3. <u>การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)</u>

- ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง **[ข้อกำหนด]**

  ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดา และ การควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

  - ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร
  - ควรใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น
  - สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ (System Sdministrator) และผู้ใช้งานที่ติดมากับระบบ (Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน
  - ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
  - ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “123456” เป็นต้น
  - ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
  - ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 5 ครั้ง
- ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
- ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

○ ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง **[ข้อกำหนด]**

○ ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญ[4] อย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของพนักงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือ เปลี่ยน Password เป็นต้น **[ข้อกำหนด]**

4. <u>การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)</u>

○ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที **[ข้อกำหนด]**

○ ต้องเปิดใช้บริการ (Service) [5] เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม **[ข้อกำหนด]**

○ ต้องดำเนินการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web Server เป็นต้น อย่างสม่ำเสมอ **[ข้อกำหนด]**

---

[4] ระบบงานสำคัญ หมายถึง ระบบที่หน่วยงานใช้ในการดำเนินกิจกรรม และระบบงานตามภารกิจของหน่วยงานโดยผ่านอินเทอร์เน็ต และระบบเครือข่าย

[5] บริการ (service) หมายถึง บริการต่าง ๆ ของเครื่องแม่ข่าย เช่น telnet, ftp, ping เป็นต้น

- ควรทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา **[ข้อเสนอแนะ]**
- ควรมีแนวทางปฏิบัติในการใช้งาน Software Utility เช่น Personal Firewall Password Cracker เป็นต้น และตรวจสอบการใช้งาน Software Utility อย่างสม่ำเสมอ **[ข้อเสนอแนะ]**
- ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน **[ข้อเสนอแนะ]**

5. <u>การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)</u>
   - ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก ส่วน DMZ เป็นต้น **[ข้อกำหนด]**
   - ต้องมีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก **[ข้อกำหนด]**
   - ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ **[ข้อกำหนด]**
     - ความพยายามในการบุกรุกผ่านระบบเครือข่าย
     - การใช้งานในลักษณะที่ผิดปกติ
     - การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
   - ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ **[ข้อกำหนด]**
   - ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า Parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical Disconnect) และจุดเชื่อมต่อ (Disable Port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง **[ข้อกำหนด]**

- ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote Access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ Modem (Dial Out) ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด เช่น การใช้ระบบ Call Back การควบคุมการเปิดปิด Modem การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน การบันทึกรายละเอียดการใช้งาน และในกรณี Dial Out ก็ควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้น รวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว **[ข้อกำหนด]**
- ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ก็ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง**[ข้อเสนอแนะ]**
- การใช้เครื่องมือต่างๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น **[ข้อเสนอแนะ]**

6. <u>การบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ (Configuration Management)</u>
   - ก่อนการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ ควรมีการประเมินผลกระทบที่เกี่ยวข้อง และบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ **[ข้อเสนอแนะ]**
   - ควรติดตั้งซอฟต์แวร์เท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์ **[ข้อเสนอแนะ]**

7. <u>การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (Capacity Planning)</u>
   - ต้องประเมินการใช้งานระบบคอมพิวเตอร์สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต **[ข้อกำหนด]**

8. <u>การป้องกันไวรัส และ Malicious Code</u>
   - ต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น **[ข้อกำหนด]**

- ผู้รับผิดชอบทางด้านระบบ คอมพิวเตอร์ควรจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ รวมทั้งแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ๆ อย่างสม่ำเสมอ **[ข้อเสนอแนะ]**
- ควรควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (Disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส **[ข้อเสนอแนะ]**

9. บันทึกเพื่อการตรวจสอบ (Audit Logs)

- ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (Login-Logout Logs) บันทึกการพยายามเข้าสู่ระบบ (Login Attempts) บันทึกการใช้ Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน **[ข้อกำหนด]**
- ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ **[ข้อเสนอแนะ]**
- ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น **[ข้อกำหนด]**

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการ ของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

แนวทางปฏิบัติ

1. <u>การกำหนดขั้นตอนการปฏิบัติงาน</u>
    - ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน **[ข้อเสนอแนะ]**
    - ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง **[ข้อเสนอแนะ]**
    - ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม **[ข้อเสนอแนะ]**

2. <u>การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน</u>

2.1 การร้องขอ

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น Electronic Transaction เช่น email เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าหน่วยงาน หัวหน้าแผนกคอมพิวเตอร์ หัวหน้าแผนกวิศวกรรมเครือข่าย หัวหน้าแผนกเทคโนโลยีสารสนเทศ เป็นต้น **[ข้อกำหนด]**

- ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง **[ข้อเสนอแนะ]**
- ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ **[ข้อเสนอแนะ]**

2.2 การปฏิบัติงานพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้ **[ข้อกำหนด]**
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ **[ข้อเสนอแนะ]**
- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง **[ข้อเสนอแนะ]**

2.3 การทดสอบ

- ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง **[ข้อกำหนด]**
- ในระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนา และการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง **[ข้อเสนอแนะ]**

2.4 การโอนย้ายระบบงานเพื่อใช้งานจริง

- ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ **[ข้อกำหนด]**

2.5 การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา **[ข้อกำหนด]**
- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน **[ข้อกำหนด]**
- ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้ **[ข้อกำหนด]**

2.6 การทดสอบหลังการใช้งาน (Post- Implementation Test)

- ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน **[ข้อเสนอแนะ]**

2.7 การสื่อสารการเปลี่ยนแปลง

- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง **[ข้อกำหนด]**

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

แนวทางปฏิบัติ

1. <u>การสำรองข้อมูลและระบบคอมพิวเตอร์</u>

1.1 การสำรอง

- ต้องสำรองข้อมูลสำคัญ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง **[ข้อกำหนด]**
- ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้ **[ข้อเสนอแนะ]**
  - ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
  - ประเภทสื่อบันทึก (Media)
  - จำนวนที่ต้องสำรอง (Copy)
  - ขั้นตอนและวิธีการสำรองโดยละเอียด
  - สถานที่และวิธีการเก็บรักษาสื่อบันทึก
- ควรมีการบันทึกการปฏิบัติงาน (Log Book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ **[ข้อเสนอแนะ]**

1.2 การทดสอบ

- ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้ **[ข้อกำหนด]**

- ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน **[ข้อเสนอแนะ]**

1.3 การเก็บรักษา

- ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย **[ข้อกำหนด]**
- ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น **[ข้อกำหนด]**
- ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด **[ข้อเสนอแนะ]**
- การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา **[ข้อเสนอแนะ]**
- ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน Recycle Bin **[ข้อเสนอแนะ]**

2. <u>การเตรียมพร้อมกรณีฉุกเฉิน</u>

- ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้ **[ข้อกำหนด]**
  - ต้องจัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน
  - ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา
  - ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

- ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
- ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ค่า Configuration และอุปกรณ์เครือข่าย เป็นต้น
- ในกรณีที่บริษัทมีศูนย์คอมพิวเตอร์สำรอง ก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น
- ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

- ต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยต้องเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย **[ข้อกำหนด]**
- ควรสื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น **[ข้อเสนอแนะ]**
- ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย **[ข้อเสนอแนะ]**

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

วัตถุประสงค์

การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์มีวัตถุประสงค์เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk และ Availability risk

แนวทางปฏิบัติ

1. <u>การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์</u>
   - ต้องมีขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ **[ข้อกำหนด]**
   - ควรกำหนดให้เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ปฏิบัติงานโดยผ่านเมนู และควรจำกัดการปฏิบัติงานโดยใช้ Command Line เท่าที่จำเป็น **[ข้อเสนอแนะ]**
   - ควรกำหนดให้มีการบันทึก (Log Book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้ **[ข้อเสนอแนะ]**
     - ผู้ปฏิบัติงาน
     - เวลาปฏิบัติงาน
     - รายละเอียดการปฏิบัติงาน
     - ปัญหาที่เกิดขึ้นและการแก้ไข
     - สถานะของระบบ
     - ผู้ตรวจทานการปฏิบัติงาน
2. <u>การติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring)</u>
   - ต้องติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เช่น การรับส่งข้อมูล การใช้งานฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) เป็นต้น เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ (Capacity) ของระบบ **[ข้อกำหนด]**

การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อหน่วยงาน ในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติโดยหน่วยงานเอง เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (Access risk) ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน (Integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้น การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมีวัตถุประสงค์เพื่อให้สามารถใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

แนวทางปฏิบัติ

1. <u>การคัดเลือกผู้ให้บริการ</u>

- ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ **[ข้อเสนอแนะ]**
- ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน**[ข้อเสนอแนะ]**

2. <u>การควบคุมผู้ให้บริการ</u>

- ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้จัดผู้รับผิดชอบควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่หน่วยงาน (onsite service) และตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ Remote Access และปิด Modem ทันทีที่การให้บริการเสร็จสิ้น เป็นต้น **[ข้อกำหนด]**

- ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ **[ข้อเสนอแนะ]**
- ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไขและมีการกำหนดขั้นตอนในการตรวจรับงานของผู้ให้บริการ**[ข้อเสนอแนะ]**

ประกาศ ณ วันที่ มีนาคม พ.ศ. 2549

(ผู้ช่วยศาสตราจารย์นำยุทธ สงค์ธนาพิทักษ์)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี