นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานจัดการทรัพย์สิน จุฬาลงกรณ์มหาวิทยาลัย

Chulalongkorn University Property management office

ส่วนเทคโนโลยีสารสนเทศ

02 มีนาคม 2560

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การจัดทำเอกสารชุดนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศจะช่วยให้ผู้ปฏิบัติงานทราบถึงนโยบายและข้อปฏิบัติเพื่อปกป้องระบบและข้อมูลที่มีความสำคัญต่อการดำเนินงาน ลดปัจจัยเสี่ยง รวมทั้ง เป็นการพัฒนาบุคลากรให้สามารถปฏิบัติงานและใช้งานได้สอดคล้องกับหลักการรักษาความปลอดภัย ประกอบด้วย

1. นโยบายความมั่นคงปลอดภัยด้านกายภาพ ครอบคลุมการรักษาความมั่นคงปลอดภัยทางกายภาพของห้องควบคุม ระบบเครือข่ายคอมพิวเตอร์ การควบคุมการเข้าออก การกำหนดสิทธิผู้ผ่านเข้าออกและความปลอดภัยทางกายภาพของเครือข่ายสื่อสัญญาณภายในสำนักงาน

2. นโยบายการจัดเตรียมระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมมาตรการและแนวปฏิบัติในการดำเนินการติดตั้ง อุปกรณ์เครือข่ายและคอมพิวเตอร์ (Hardware) ระบบปฏิบัติการและระบบงานต่างๆ (Software) เพื่อเชื่อมต่อกับระบบสารสนเทศของสำนักงานฯ

3. นโยบายการจำแนกและการบริหารข้อมูล ครอบคลุมการกำหนดมาตรฐานในการจัดระดับชั้นความลับของข้อมูลและวิธีการจัดการข้อมูล เพื่อให้มีหลักปฏิบัติที่ใช้ในการจัดการกับข้อมูลอย่างถูกต้องเหมาะสม

4. นโยบายการสำรองข้อมูลและกู้คืน ครอบคลุมทั้งในคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคลเพื่อให้มีชุดข้อมูลสำรองกรณีเกิดความเสียหายกับข้อมูลและสามารถกู้กลับคืนมาได้อย่างมีประสิทธิภาพ

5. นโยบายการบริหารความเปลี่ยนแปลง ครอบคลุมการบริหารความเปลี่ยนแปลงในระดับการปรับปรุง (Patch/Upgrade) และระดับการเปลี่ยนแปลง (Change) ระบบงานหรือระบบปฏิบัติการ เพื่อให้มีข้อปฏิบัติก่อน ดำเนินการเปลี่ยนแปลงเพื่อลดความเสี่ยงในการหยุดให้บริการ

6. นโยบายการบริหารระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมการบริหารระบบเครือข่ายทั้งระบบข้อกำหนดเกี่ยวกับการจัดการไอพีแอดเดรส การเข้าถึงระบบจากระยะไกล การตรวจสอบระบบ การซ่อมบำรุงและการดำเนินการเมื่อระบบขัดข้อง

7. นโยบายการเข้าถึงข้อมูลและระบบสารสนเทศ ครอบคลุมการบริหารบัญชีรายชื่อผู้ใช้งานระบบ การกำหนดรหัสผ่าน การกำหนดสิทธิเฉพาะผู้ที่ได้รับอนุญาต

8. นโยบายการใช้อุปกรณ์ไอทีส่วนบุคคล ครอบคลุมการใช้งานคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา และสมาร์ทโฟน (Notebook, Tablet, Mobile computing และ IT gadgets) โดยกำหนดแนวทางการใช้งานข้อกำหนดที่ผู้ใช้งานต้องดำเนินการ เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส

9. นโยบายการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ ครอบคลุมสิ่งที่ผู้ใช้เครือข่ายคอมพิวเตอร์ต้องปฏิบัติตาม

1 นโยบายความมั่นคงปลอดภัยด้านกายภาพ

ให้มีการกำหนดมาตรการและแนวทางในการป้องกันอาคารและอุปกรณ์ในห้องควบคุมระบบคอมพิวเตอร์ และมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์ การควบคุมการเข้า-ออก การแบ่งส่วนพื้นที่และการกำหนดสิทธิผู้ผ่านเข้าออก เพื่อให้มั่นใจได้ว่าห้องควบคุมระบบคอมพิวเตอร์มีความปลอดภัยจากจากการโจรกรรมทรัพย์สินของเครือข่าย รวมถึง การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิในห้องควบคุมที่สูงเกินขีดจำกัด ห้องควบคุมมีความชื้นสูง หรือการกระทำโดยประมาท เช่น การทำน้ำหกลงเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ เป็นต้น

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. สทร. หมายถึง ส่วนเทคโนโลยีสารสนเทศ
2. ห้องควบคุมระบบ หมายถึง ห้องที่ติดตั้งและจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่าย
3. เจ้าหน้าที่ห้องควบคุมระบบ ได้แก่ ผู้ดูแลระบบคอมพิวเตอร์ ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบฐานข้อมูล
4. ผู้บริหาร ได้แก่ ผู้จัดการส่วนเทคโนโลยีสารสนเทศ

ข้อกำหนดการป้องกันทางกายภาพ ประกอบด้วย

1. ข้อกำหนดของห้องควบคุมระบบ
2. ข้อกำหนดการเข้าพื้นที่จำกัดการเข้าถึง (Restricted Area) เป็นห้องที่มีระบบคอมพิวเตอร์และเครือข่ายติดตั้งอยู่ (Data center room)
3. ข้อกำหนดการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

1. ข้อกำหนดของห้องควบคุมระบบ

1.1. แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้ เช่น router, switch และ server ต่างๆ

1.2. จัดหา rack ในการจัดเก็บอุปกรณ์ต่างๆ ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

1.3. ไม่วางอุปกรณ์ต่างๆ ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น หรือวางอุปกรณ์ใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น

1.4. เก็บสายเครือข่าย (Network cable) และสายไฟฟ้าให้เรียบร้อย เพื่อป้องกันการเดินสะดุด

1.5. ติดประกาศบันทึกการบำรุงรักษา การซ่อมแซมและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

1.6. ติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV ระบบการเข้า-ออกห้องโดยระบบ RFID และมีกุญแจเข้าออก

1.7. มีระบบดับเพลิงอัตโนมัติเพื่อป้องกันอัคคีภัย

1.8. มีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ อย่างน้อย 30 นาที

1.9. มีระบบป้องกันไฟฟ้าจากฟ้าผ่า

1.10. มีระบบป้องกันไฟฟ้ารั่ว

1.11. มีระบบปรับอากาศแบบควบคุมอุณหภูมิ (20 - 26.7°C)
1.12. ติดตั้งฉนวนกันไฟไหม้ที่ฝ้าเพดานและผนังกำแพง

2. ข้อกำหนดการเข้าพื้นที่จำกัดการเข้าถึง (Data center room)

2.1 ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ
2.2 ในกรณีมีบุคคลที่มีความจำเป็นต้องเข้าไปปฏิบัติงานในพื้นที่จำกัดการเข้าถึง บุคคลดังกล่าวต้องได้รับอนุญาตจากผู้บริหารและต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย 1 คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง
2.3 กรณีมีบุคคลที่ได้รับคำสั่งจากผู้บริหารให้เข้าปฏิบัติหน้าที่ในพื้นที่จำกัดการเข้าถึง จะต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย 1 คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง
2.4 ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง
2.5 บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชม ต้องได้รับอนุญาตจากผู้บริหาร และจะต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา
2.6 ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของ สทร. บุคคลอื่นสามารถเข้าไปในพื้นที่จำกัดการเข้าถึงได้หากได้รับอนุญาตจากผู้บริหาร

3. ข้อกำหนดการบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

3.1 ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก 6 เดือน
3.2 กำหนดขั้นตอนและแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟไหม้ หรือมีผู้บุกรุก เป็นต้น
3.3 มีตารางกำหนดการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

2 นโยบายการจัดเตรียมระบบเครือข่ายคอมพิวเตอร์

กำหนดให้มีมาตรการและแนวทางในการติดตั้งอุปกรณ์เครือข่ายและเครื่องเซิร์ฟเวอร์ การติดตั้งซอฟต์แวร์ระบบปฏิบัติการ การติดตั้งโปรแกรมประยุกต์สำหรับใช้งานกับอุปกรณ์ รวมถึงการจัดเตรียมระบบเครือข่ายและเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ การทดสอบอุปกรณ์ก่อนทำการติดตั้งในห้องปฏิบัติงานเพื่อให้มีแนวปฏิบัติเป็นมาตรฐานเดียวกันอย่างมีประสิทธิภาพ

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ห้องปฏิบัติงาน หมายถึง ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย
2. อุปกรณ์ หมายถึง อุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์เซิร์ฟเวอร์
3. อุปกรณ์ทดสอบ หมายถึง อุปกรณ์ที่มีลักษณะเหมือนกัน หรือใกล้เคียงกับอุปกรณ์ที่ต้องการติดตั้งอุปกรณ์ต่อพ่วง หรือติดตั้งโปรแกรมประยุกต์เพิ่มเติม โดยที่อุปกรณ์ชุดนี้ต้องไม่ใช่อุปกรณ์ชุดที่ใช้งานอยู่

4. เจ้าหน้าที่ หมายถึง ผู้มีอำนาจในการติดตั้ง และดูแลรักษาอุปกรณ์ภายในห้องปฏิบัติงาน

5. ผู้รับผิดชอบอุปกรณ์ หมายถึง ผู้มีหน้าที่ในการจัดเก็บรายการอุปกรณ์ และเอกสารประกอบอุปกรณ์

ขอบเขต

นโยบายนี้ครอบคลุมถึงอุปกรณ์ทุกชนิดที่เป็นสมบัติของสำนักงานฯ และอุปกรณ์ที่ไม่ใช่สมบัติของสำนักงานแต่มีการติดตั้งและเปิดใช้งานเชื่อมต่อทั้งอย่างถาวรหรือชั่วคราวกับระบบเครือข่ายของสำนักงานฯ และอยู่ในพื้นที่ของสำนักงานฯ

1. ข้อกำหนดการเตรียมเอกสารก่อนการติดตั้ง

1.1 เจ้าหน้าที่ต้องดำเนินการลงทะเบียนอุปกรณ์ทุกชิ้นกับผู้รับผิดชอบอุปกรณ์ โดยระบุ คุณลักษณะที่สำคัญของอุปกรณ์ ระบบปฏิบัติการที่ใช้ พร้อมระบุรุ่น วันที่ติดตั้ง ชื่อผู้ติดตั้ง วัตถุประสงค์การใช้งานของอุปกรณ์รวมถึงรายการโปรแกรมประยุกต์ที่ติดตั้งในอุปกรณ์อย่างชัดเจน

1.2 เจ้าหน้าที่ต้องทำการรวบรวมเอกสารคุณลักษณะของอุปกรณ์ทั้งที่เป็นสิ่งพิมพ์และโปรแกรมที่ใช้กับอุปกรณ์เพื่อนำส่งไปยังผู้รับผิดชอบอุปกรณ์

1.3 เจ้าหน้าที่ต้องจัดเตรียมแผนการติดตั้ง ระยะเวลา ผู้รับผิดชอบ และแผนการรับมือในกรณีฉุกเฉิน

1.4 เจ้าหน้าที่ต้องจัดเตรียมแผนผังทางกายภาพ (Layout) ที่ระบุตำแหน่งของอุปกรณ์ที่จะทำการติดตั้ง

1.5 เจ้าหน้าที่ต้องจัดเตรียมแผนผังทางตรรกะของเครือข่าย (Network Logical Diagram) ที่ระบุการเชื่อมต่อของอุปกรณ์ที่ต้องการจะติดตั้ง

1.6 เจ้าหน้าที่ต้องเตรียมเอกสารการติดตาม (Monitoring Chart) แบบที่เป็นการจดบันทึกและทำการบันทึกด้วยระบบอิเล็กทรอนิกส์

1.7 เจ้าหน้าที่ต้องเตรียมป้ายชื่ออุปกรณ์ ที่ใช้วัสดุและมีรูปแบบการจัดพิมพ์ตามแบบที่ใช้ในห้องปฏิบัติงานติดตั้งให้เห็นชัดเจนบนตัวอุปกรณ์

1.8 ในกรณีต้องทำการใดๆ กับอุปกรณ์ที่กำลังทำหน้าที่ให้บริการอยู่ โดยเฉพาะกับอุปกรณ์ที่มีผลกระทบสูงต่อผู้ใช้งานและหน่วยงาน ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า รวมถึงทราบผลกระทบที่อาจเกิดขึ้น

1.9 ได้รับการอนุมัติในการติดตั้ง และแผนการติดตั้งจากผู้บริหาร ก่อนดำเนินการเคลื่อนย้ายอุปกรณ์เข้าไปในห้องปฏิบัติงาน รวมทั้งก่อนมีการติดตั้งโปรแกรมใดๆ

2. ข้อกำหนดการทดสอบอุปกรณ์และโปรแกรมก่อนการติดตั้ง

2.1 อุปกรณ์ต้องอยู่ในสภาพทางกายภาพสมบูรณ์พร้อมใช้งาน

2.2 อุปกรณ์ทุกชิ้นต้องผ่านการป้อนไฟเพื่อทดสอบว่าใช้งานได้ และไม่เกิดการลัดวงจร หรือ มีความร้อนมากจนอาจเป็นสาเหตุของไฟฟ้าลัดวงจรหรือไฟไหม้

2.3 ในกรณีที่เป็นการติดตั้งอุปกรณ์ใหม่ เจ้าหน้าที่ต้องทำการติดตั้งระบบปฏิบัติการ โปรแกรมต้านไวรัสพร้อมทั้งโปรแกรมประยุกต์ที่จะใช้งานให้เสร็จสิ้น พร้อมทั้งทดสอบการทำงานให้สมบูรณ์ก่อนนำเข้าติดตั้ง

2.4 ในกรณีที่ต้องการติดตั้งโปรแกรมประยุกต์บนอุปกรณ์ที่กำลังใช้งาน

2.4.1 ต้องจัดเตรียมอุปกรณ์ทดสอบที่ติดตั้งระบบปฏิบัติการ รุ่นของระบบปฏิบัติการ และโปรแกรมประยุกต์ทั้งหมดเหมือนกับอุปกรณ์ที่กำลังใช้งาน

2.4.2 ให้เจ้าหน้าที่ทำการทดลองติดตั้งโปรแกรมประยุกต์ดังกล่าวบนอุปกรณ์ทดสอบ เพื่อศึกษาถึงผลกระทบที่เกิดขึ้น

2.4.3 ทำสำเนาข้อมูลของอุปกรณ์ที่กำลังใช้งาน ก่อนการนำโปรแกรมประยุกต์ที่ทดสอบแล้วไปติดตั้ง

3. ข้อกำหนดการทำงานขณะติดตั้งอุปกรณ์และโปรแกรม

3.1 การเคลื่อนย้ายและการติดตั้งอุปกรณ์ต้องเป็นไปตามนโยบายความมั่นคงทางกายภาพของห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

3.2 เจ้าหน้าที่ต้องทำการบันทึก ชื่อบัญชีผู้ใช้ และรหัสผ่านของระบบ (Root User Name และ Password) ไว้ในที่ปลอดภัยตามนโยบายการรักษาความปลอดภัยและจัดเก็บรหัสลับ

3.3 การตั้งค่าทางเครือข่าย (Network Configuration) หมายเลขไอพี การตั้งค่าเครือข่ายเสมือน และการตั้งค่าอื่นๆ ที่เกี่ยวกับเครือข่าย ต้องเป็นไปตามข้อกำหนดการใช้งานเครือข่าย

4. ข้อกำหนดภายหลังการติดตั้ง

4.1 เจ้าหน้าที่ต้องทำการตรวจสอบติดตามการทำงานของอุปกรณ์ หรือโปรแกรมที่ติดตั้ง ทุกช่วงระยะเวลาที่กำหนด

4.2 เจ้าหน้าที่ต้องจัดเตรียมรายงานการติดตั้ง ข้อเสนอแนะในการดูแลรักษา รวมถึงค่าใช้จ่าย ในการดูแลรักษา เพื่อส่งให้กับหัวหน้าและผู้บริหารรับทราบ

3 นโยบายการจำแนกและการบริหารข้อมูล

กำหนดให้มีมาตรฐานในการจำแนก การจัดระดับชั้นความลับของข้อมูลและวิธีการจัดเก็บข้อมูล เพื่อให้มีหลักปฏิบัติที่ใช้ในการจัดการข้อมูลอย่างถูกต้องเหมาะสม

แนวปฏิบัติตามนโยบาย

ขอบเขต

ขั้นตอนการปฏิบัติงานจะใช้กับข้อมูลทั้งที่อยู่ในรูปแบบของเอกสารกระดาษและข้อมูลในรูปแบบอิเล็กทรอนิกส์

1. เอกสารกระดาษ หมายถึง ข้อมูลที่พิมพ์ออกมาในรูปกระดาษ เช่น สัญญา รายงานการประชุม เป็นต้น
2. ข้อมูลในรูปแบบอิเล็กทรอนิกส์ หมายถึง ข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่จัดเก็บอยู่ในเครื่องคอมพิวเตอร์ เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์ต่างๆ
3. สื่อบันทึกข้อมูล หมายถึง สื่อที่ใช้ในการเก็บข้อมูลอิเล็กทรอนิกส์ เช่น แผ่นซีดี แถบแม่เหล็ก แฟลชไดร์ฟ ฮาร์ดไดร์ฟ เป็นต้น

หน้าที่และความรับผิดชอบ

เจ้าของข้อมูล คือ ผู้สร้างข้อมูล โดยเจ้าของข้อมูลมีหน้าที่ดังต่อไปนี้

- กำหนดระดับชั้นความลับของข้อมูลที่ตนเองเป็นเจ้าของ และระบุชั้นความลับให้กับข้อมูลนั้น
- กำหนดสิทธิการเข้าถึงข้อมูลให้ผู้ใช้
- กำหนดมาตรการในการจัดการข้อมูลให้มีความมั่นคงปลอดภัย

ผู้ดูแลข้อมูล คือ ผู้ที่มีหน้าที่ดูแลและจัดการให้ข้อมูลมีความปลอดภัย

ผู้ดูแลข้อมูลมีหน้าที่

- จัดการและบำรุงรักษาให้ข้อมูลอยู่ในระดับชั้นความลับตามที่เจ้าของข้อมูลกำหนดไว้ผู้ใช้ข้อมูล คือ ผู้ที่ได้รับอนุญาตจากเจ้าของข้อมูลให้เข้าถึงข้อมูลได้

ผู้ใช้ข้อมูลมีหน้าที่

- ปฏิบัติและจัดการกับข้อมูลตามระดับชั้นความลับตามที่เจ้าของข้อมูลกำหนดไว้หากมีความจำเป็นต้องส่งผ่านข้อมูลไปยังบุคคลหรือหน่วยงานภายนอกสำนักงานฯ บุคลากรที่รับผิดชอบในการส่งผ่านข้อมูลจะต้องแจ้งให้กับผู้รับข้อมูลทราบถึงระดับชั้นความลับของข้อมูล และวิธีการในการจัดการกับข้อมูลก่อนนำส่งข้อมูล

การจัดระดับข้อมูล

เนื่องจากหากมีการละเมิดการใช้ข้อมูลอย่างไม่เหมาะสม ข้อมูลบางประเภทอาจถูกนำไปใช้และสร้างความเสียหายให้กับสำนักงานฯ ได้ ดังนั้นสำนักงานฯ จึงจำเป็นต้องมีมาตรการในการดูแล ป้องกันให้ข้อมูลมีความปลอดภัย จึงต้องมีการจัดระดับชั้นความลับของข้อมูลขึ้น โดยแบ่ง ออกเป็น 4 ระดับ ได้แก่

- ลับมาก (Secret)
- ลับ (Confidential)
- ใช้เฉพาะภายใน (Internal)
- ใช้ได้ทั่วไป (Public)

นิยาม	ลับมาก (Secret)	ลับ (Confidential)	ใช้เฉพาะภายใน (Internal)	ใช้ได้ทั่วไป (Public)
ประเภทของข้อมูล				
	เป็นข้อมูลที่มีความสำคัญมากต่อสำนักงานฯ จะอนุญาตให้เฉพาะบุคคลที่มีความจำเป็นอย่างแท้จริงสามารถเข้าถึงข้อมูลได้	เป็นข้อมูลที่มีความสำคัญต่อสำนักงานฯ โดยอนุญาตให้เฉพาะผู้ที่มีความจำเป็นในการเข้าถึงข้อมูลสามารถเข้าถึงข้อมูลได้	เป็นข้อมูลที่อนุญาตให้ใช้ได้เฉพาะภายในสำนักงานฯ โดยอนุญาตให้บุคคลที่เกี่ยวข้องสามารถเข้าถึงข้อมูลได้	เป็นข้อมูลที่ต้องการให้มีการเผยแพร่ไปยังภายนอก เช่น ข้อมูลบนเว็บไซต์ และข้อมูลการส่งเสริมการขายกิจกรรมต่างๆ ของสำนักงานฯ เป็นต้น
	หากมีการเปิดเผยโดยไม่ได้รับอนุญาตอาจจะก่อให้เกิดความเสียหายต่อการดำเนินงานและชื่อเสียงของสำนักงานฯ บุคลากร อย่างร้ายแรง	หากมีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะก่อให้เกิดความเสียหายในการดำเนินงานของสำนักงานฯ และอาจส่งผลกระทบไปถึงบุคลากรได้	หากมีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะก่อให้เกิดความเสียหายในวงจำกัด	ไม่มีผลกระทบหากมีการเผยแพร่ไปสู่ภายนอกองค์กร
การติดป้าย				
ชื่อที่ใช้ในการระบุ	เอกสารลับมาก	เอกสารลับ	เอกสารภายใน	ไม่มีข้อกำหนดเป็นพิเศษ
เอกสารกระดาษ	มีการระบุระดับชั้นความลับในทุกๆหน้าของเอกสาร หรืออย่างน้อยที่หน้าแรกของเอกสาร			ไม่มีข้อกำหนดเป็นพิเศษ
ข้อมูลในรูปแบบอิเล็กทรอนิกส์	มีการระบุระดับชั้นความลับในทุกๆหน้าของไฟล์เอกสาร ยกเว้นในกรณีที่มีข้อจำกัดทางเทคนิค			ไม่มีข้อกำหนดเป็นพิเศษ
สื่อบันทึกข้อมูล	ไม่จำเป็นต้องติดป้ายบนสื่อบันทึกข้อมูล แต่กำหนดให้มีวิธีการจัดการที่เทียบเท่าตามระดับชั้นความลับของข้อมูลที่บันทึกในสื่อบันทึกข้อมูลดังกล่าว			ไม่มีข้อกำหนดเป็นพิเศษ
การควบคุมการเข้าถึง				
การยืนยันความถูกต้อง	รหัสผู้ใช้และรหัสผ่าน			ไม่มี
การอนุมัติ	ตามสิทธิของผู้ใช้			ไม่มี

การควบคุมการถ่ายโอนข้อมูล				
แฟกซ์	ใช้ได้เฉพาะในกรณีที่จำ เป็นเท่านั้น ข้อปฏิบัติเช่นเดียวกับข้อมูล “ลับ”	● ต้องอยู่ ณ เครื่องโทรสารในขณะที่ส่งจนแล้วเสร็จ ● ตรวจสอบความถูกต้องของหมายเลขปลายทาง ● ใช้เครื่องโทรสารที่อยู่ในพื้นที่ รับและส่งที่ปลอดภัย ● มีใบปะหน้าที่ระบุถึงผู้ส่ง ผู้รับ และข้อความการปฏิเสธความรับผิดชอบอันเกิดจากการส่งข้อมูลทางโทรสาร	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด
เครื่องพิมพ์	● พิมพ์ที่เครื่องพิมพ์ที่มีความปลอดภัย ● ตรวจสอบเครื่องพิมพ์ปลายทาง	● พิมพ์ที่เครื่องพิมพ์ที่มีความปลอดภัย ● ตรวจสอบเครื่องพิมพ์ปลายทาง	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด
โทรศัพท์มือถือ	ไม่อนุญาต	ไม่อนุญาต	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด
จดหมายอิเล็กทรอนิกส์, อินเตอร์เน็ต, อินทราเน็ต	ไม่อนุญาต เว้น แต่ได้รับอนุญาตจากเจ้าของข้อมูลและต้องใช้ในระบบจดหมายอิเล็กทรอนิกส์และอินเตอร์เน็ตของสำนักงานที่มีความปลอดภัยเท่านั้น รวมถึงให้ส่งข้อมูลที่มีการ encryption จากผู้ส่ง	ไม่อนุญาต เว้น แต่ได้รับอนุญาตจากเจ้าของข้อมูลและต้องใช้ในระบบจดหมายอิเล็กทรอนิกส์และอินเตอร์เน็ตของสำนักงานที่มีความปลอดภัยเท่านั้น รวมถึงให้ส่งข้อมูลที่มีการ encryption จากผู้ส่ง	● ไม่มีข้อกำหนดพิเศษสำหรับการใช้กับจดหมายอิเล็กทรอนิกส์หรืออินทราเน็ต ● ต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อนที่จะส่งไปยังภายนอก	ไม่มีข้อกำหนดพิเศษ

วิธีการจัดเก็บ				
สื่อต่างๆและกระดาษ	• บรรจุในวัสดุห่อหุ้มที่สามารถป้องกันการแก้ไขข้อมูล • ส่งมอบให้ถึงมือผู้รับ หรือบริการการส่งจดหมายที่ไว้ใจได้	บรรจุในซองที่ห่อหุ้มและปิดผนึก	บรรจุในซองที่ปิดผนึก	ไม่มีข้อกำหนดพิเศษ
เอกสารกระดาษหรือสื่อบันทึกข้อมูล	• เก็บในตู้นิรภัยหรือตู้ที่มีกุญแจปิดล็อกและตู้ดังกล่าวจะต้องตั้งอยู่ในพื้นที่ที่มีการวบคุมด้านความมั่นคงปลอดภัย ● หากมีความจำเป็นต้องนำเอกสารออกนอกสำนักงานฯ จะต้องจัดเก็บใส่ซองพร้อมปิดผนึกเพื่อป้องกันการเปิดซองเอกสารโดยที่ไม่ได้รับอนุญาตและต้องนำ เอกสารติดตัวไว้ตลอดเวลา	• เก็บในตู้นิรภัย หรือตู้ที่มีกุญแจปิดล็อกและตู้ดังกล่าวจะต้องตั้งอยู่ในพื้นที่ที่มีการวบคุมด้านความมั่นคงปลอดภัย • หากมีความจำเป็นต้องนำเอกสารออกนอกสำนักงานฯ จะต้องจัดเก็บใส่ซองพร้อมปิดผนึกเพื่อป้องกันการเปิดซองเอกสารโดยที่ไม่ได้รับอนุญาตและต้องนำเอกสารติดตัวไว้ตลอดเวลา	● เก็บในตู้ที่มีกุญแจปิดล็อกเมื่อไม่ใช้งาน • เก็บในแฟ้มเมื่อต้องการนำออกไปใช้ภายนอก	ไม่มีข้อกำหนดพิเศษ
วิธีการจัดเก็บ				
ข้อมูลในรูปแบบอิเล็กทรอนิกส์	●จัดเก็บในดิสก์หรือสื่อบันทึกไว้ในตู้ปิดล็อกที่อยู่ในพื้นที่ที่มีการควบคุมด้านความปลอดภัย ●ห้ามไม่ให้จัดเก็บข้อมูลในพื้นที่เก็บ	●จัดเก็บในดิสก์หรือสื่อบันทึกไว้ในตู้ปิดล็อกที่อยู่ในพื้นที่ที่มีการควบคุมด้านความมั่นคงปลอดภัย • ควรหลีกเลี่ยงไม่จัดเก็บข้อมูลใน	• จัดเก็บในดิสก์หรือสื่อบันทึกไว้ในตู้ปิดล็อกที่อยู่ในพื้นที่ที่มีการควบคุมด้านความมั่นคงปลอดภัย • จัดเก็บข้อมูลในพื้นที่เก็บข้อมูล	ไม่มีข้อกำหนดพิเศษ

	ข้อมูลส่วนกลาง Network Shared Drive	พื้นที่เก็บข้อมูลส่วนกลาง เช่น Network Shared Drive ซึ่งหากจำเป็นจะต้องมีการกำหนดสิทธิในการเข้าถึง (Access Control List)	ข้อมูลส่วนกลาง เช่น Network Shared Drive ซึ่งหากจำเป็นจะต้องมีการกำหนดสิทธิในการเข้าถึง (Access Control List)	
การทำสำเนา				
การทำสำเนาและการพิมพ์งาน	● ห้ามไม่ให้สำเนาหรือพิมพ์ใหม่ ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และผู้บริหารระดับ M1 ของสำนักงานฯ ขึ้นไปเจ้าของข้อมูลควรเป็นผู้ดำเนินการสำเนาข้อมูลด้วยตนเอง ● มีบันทึกการแจกจ่ายข้อมูล ● ให้รอรับเอกสารระหว่างที่เครื่องกำลังพิมพ์งาน ● ห้ามไม่ให้พิมพ์งานโดยใช้เครื่องพิมพ์สาธารณะ เช่นในโรงแรม	● ห้ามไม่ให้สำเนาหรือพิมพ์ใหม่ ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และผู้บริหารระดับส่วนงานขึ้นไป ● มีบันทึกการแจกจ่ายข้อมูล ● ให้เก็บงานที่สั่งพิมพ์ทันทีหลังจากพิมพ์เสร็จ ● ควรหลีกเลี่ยงการพิมพ์งานโดยใช้เครื่องพิมพ์งานสาธารณะ เช่น ในโรงแรม	● อนุญาตให้ทำสำเนา หรือพิมพ์ใหม่ เฉพาะการเผยแพร่ภายในสำนักงานฯ • ให้เก็บงานที่สั่งพิมพ์ทันทีที่ทำได้	ไม่มีข้อห้ามในการทำสำเนา
การทำสำเนาอิเล็กทรอนิกส์ เช่น external drive หรือ thumb drive	ห้ามไม่ให้สำเนา	ห้ามไม่ให้สำเนา	อนุญาตให้ทำสำเนาใหม่เฉพาะการเผยแพร่ภายในสำนักงานฯ	ไม่มีข้อห้ามในการทำสำเนา

วิธีการลบข้อมูล				
สื่อบันทึกข้อมูลแบบแถบแม่เหล็ก	• ให้ลบไฟล์ทันทีโดยไม่ให้เก็บไว้ใน Recycle bin • มีการใช้ซอฟต์แวร์ประเภทยูทิลิตี้เพื่อป้องกันการกู้ข้อมูลคืนได้	ให้ลบไฟล์ทันทีโดยไม่ให้เก็บไว้ใน Recycle bin	อนุญาตให้ลบไฟล์โดยใช้วิธีการปกติ	ไม่มีข้อกำหนดเป็นพิเศษ
วิธีการทำลายข้อมูล				
เอกสารกระดาษ	เจ้าของข้อมูล หรือผู้ใช้จะต้องตัดหรือทำลายเอกสารด้วยตนเองโดยตัดหรือทำ ลายโดยใช้เครื่องทำลายเอกสาร		ตัดหรือทำลายโดยใช้เครื่องทำลายเอกสาร	ไม่มีข้อกำหนดเป็นพิเศษ
สื่อบันทึกข้อมูลประเภทอื่น	การทำลายสื่อบันทึกข้อมูล			ไม่มีข้อกำหนดเป็นพิเศษ

4 นโยบายการสำรองข้อมูลและกู้คืน

ให้กำหนดแนวปฏิบัติในการสำรองข้อมูลและกู้คืนระบบอย่างมีขั้นตอนและลดความเสี่ยงที่อาจเกิดขึ้น เพื่อสร้างความมั่นใจในการเก็บรักษาและใช้งานข้อมูล โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ดูแลระบบคอมพิวเตอร์ หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลจัดการระบบคอมพิวเตอร์
2. ผู้ดูแลระบบเครือข่าย หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลจัดการระบบเครือข่าย
3. ผู้ใช้ ได้แก่ หรือ บุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์
4. การสำรองข้อมูล หมายถึง การทำสำรองข้อมูลทั้งหมด (Full backup) เพื่อให้สามารถกู้คืนข้อมูลภายหลังได้ครบถ้วนสมบูรณ์ ถูกต้อง

การจัดให้มีระบบสำรองข้อมูล

1. ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูล
2. ผู้ดูแลระบบคอมพิวเตอร์ ต้องกำหนดให้มีกระบวนการสร้างความต่อเนื่องให้กับการดำเนินงาน การบริหารจัดการและการปรับปรุงกระบวนการที่ต้องใช้ในการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ
3. การสำรองข้อมูลผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้ โดยการทำสำรองข้อมูล หมายถึง การทำสำรองข้อมูลทั้งหมด ผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้

ตามระยะเวลาที่เหมาะสมและกำหนดไว้ชัดเจน โดยสำนักงานมีการสำรองข้อมูลทุกวันด้วยโปรแกรมสำรองข้อมูลอัตโนมัติ

4. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการทำสำรองข้อมูล รวมทั้งเสนอวิธีการที่ใช้ในการแก้ไขข้อผิดพลาดด้วย

5. ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้ ต้องมีการมอบหมายหน้าที่การสำรองข้อมูลไว้ล่วงหน้าให้กับเจ้าหน้าที่คนอื่น เพื่อให้เจ้าหน้าที่ผู้นั้นสามารถทำหน้าที่สำรองข้อมูลในกรณีที่จำเป็น

6. ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการสำรองข้อมูลอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บริหาร

7. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายมีหน้าที่กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้ในการเก็บข้อมูล โดยตัวอย่างรูปแบบการสำรองข้อมูล อาทิ การสำรองข้อมูลทั้งหมด (Full backup) การสำรองข้อมูลแบบสะสม (Incremental backup) หรืออาจเลือกใช้การสำรองข้อมูลรูปแบบอื่นๆ ตามความเหมาะสม แต่ต้องให้มั่นใจว่ามีการสำรองข้อมูลได้ครบถ้วนตามเป้าหมายที่กำหนดไว้ รวมทั้งสามารถกู้กลับคืนได้ด้วย

8. การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงาน ทั้งนี้เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็วและเพื่อป้องกันระบบจากการถูกโจมตีหรือจากหายนะที่อาจเกิดขึ้น

9. การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองนี้ถูกเปิดเผย

10. นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนการสำรองข้อมูล Backup Procedure โดยเคร่งครัด

การกู้คืนระบบ

1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่าย มีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้บริหารหรือผู้ที่ได้รับมอบหมาย

2. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest update) ที่ได้สำรองไว้เพื่อกู้คืนระบบ

3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

5 นโยบายการบริหารความเปลี่ยนแปลง

ให้มีการกำหนดขั้นตอนและข้อปฏิบัติก่อนดำเนินการเปลี่ยนแปลงเพื่อลดความเสี่ยงในการหยุดให้บริการซึ่งต้องครอบคลุมความเปลี่ยนแปลงที่เกิดขึ้นกับระบบสารสนเทศทั้งในระดับการปรับปรุง (Patch/Upgrade) และระดับการเปลี่ยนแปลง (Change) ระบบงานหรือระบบปฏิบัติการ โดยเฉพาะเครื่องคอมพิวเตอร์ เครื่องแม่ข่าย ระบบงานและโปรแกรมประยุกต์ให้มีการเปลี่ยนแปลงโดยมีเหตุอันควรและเพื่อให้ผู้ดูแลระบบและผู้ใช้ระบบสารสนเทศสามารถวางแผนปฏิบัติงานล่วงหน้าและลดผลกระทบที่เกิดจากการปรับเปลี่ยนได้ความคาดหวังจากการปฏิบัติตามนโยบายนี้ คือ

1. ป้องกันการปรับเปลี่ยนการทำงานของระบบสารสนเทศ โดยผู้ดูแลระบบและผู้ใช้งานไม่ทราบ และมีการเตรียมการรองรับไว้ล่วงหน้า (Announced and scheduled changes)
2. สามารถติดตามและลำดับการปรับเปลี่ยนระบบสารสนเทศ
3. สามารถกู้การทำงานเดิมของระบบสารสนเทศกลับคืนมา

ซึ่งต้องมีการเตรียมการก่อนการปรับเปลี่ยน มีการเฝ้าติดตามและการประเมินผล เพื่อให้การปรับเปลี่ยนเป็นไปด้วยดี ทราบล่วงหน้าและเตรียมการลดผลกระทบต่อการปฏิบัติงาน

แนวปฏิบัติตามนโยบาย

ผู้เกี่ยวข้อง

นโยบายฉบับนี้บังคับให้มีผู้มีอำนาจหน้าที่ และความรับผิดชอบในการติดตั้ง ควบคุมการทำงานของผู้เกี่ยวข้องทุกคนในการดำเนินการเปลี่ยนแปลงระบบสารสนเทศ โดยกำหนดให้มีผู้ที่มีหน้าที่เฉพาะ ดังต่อไปนี้

1. ผู้ร้องขอปรับเปลี่ยนระบบสารสนเทศ มีภาระหน้าที่ คือ
    - 1.1 ยื่นคำร้องขอปรับเปลี่ยนระบบอื่นใดที่มีมา
    - 1.2 เป็นผู้รับผิดชอบให้มีการปรับเปลี่ยนระบบตามที่ร้องขอ โดยดำเนินการตามขั้นตอนการปรับเปลี่ยนระบบ หากระบบใดมีผลต่อระบบที่เป็นสาระสำคัญจะต้องมีการจัดตั้งคณะกรรมการและเสนออนุมัติ
    - 1.3 ร่วมติดตาม ประเมินและจัดทำรายงานแจ้งผลกระทบจริงที่เกิดขึ้นจากการ เปลี่ยนระบบ
2. ผู้ประสานงานการบริหารการปรับเปลี่ยนระบบสารสนเทศ มีภาระหน้าที่ คือ
    - 2.1 ติดตามการปรับเปลี่ยนระบบสารสนเทศที่ยังไม่เสร็จสมบูรณ์ทั้งหมด
    - 2.2 จัดการประชุมคณะกรรมการบริหารการเปลี่ยนแปลงระบบสารสนเทศ (ถ้ามี)
    - 2.3 เวียนปฏิทินการปรับเปลี่ยนระบบสารสนเทศให้กับหน่วยงานที่เกี่ยวข้องทราบ
    - 2.4 แจ้งหน่วยงานและบุคลากรที่เกี่ยวข้องให้ทราบถึงคาดการณ์ ผลกระทบที่อาจเกิดขึ้นจากการปรับเปลี่ยนระบบ
    - 2.5 แจ้งสรุปรายการการปรับเปลี่ยนระบบสารสนเทศที่เสร็จสมบูรณ์แล้ว ส่งให้กับคณะกรรมการที่จัดตั้ง (ถ้ามี)

3 คณะกรรมการบริหารการเปลี่ยนแปลง มีภาระหน้าที่ คือ

- 3.1 ทบทวนคำร้องขอปรับเปลี่ยนระบบและให้ความเห็นชอบในการดำเนินการ โดยคำนึงถึงภารกิจของหน่วยงานที่ร้องขอ และภารกิจภาพรวม
- 3.2 วิเคราะห์และคาดการณ์ผลกระทบที่จะเกิดขึ้นจากการปรับเปลี่ยนระบบ
- 3.3 เสนอทางเลือกและขั้นตอนที่จะลดผลกระทบจากการปรับเปลี่ยนระบบให้มีน้อยที่สุด

3.4 กำหนดขั้นตอนในการปรับเปลี่ยนระบบอย่างละเอียด

3.5 จัดทำแผนการปรับกลับคืน อันได้แก่ ขั้นตอนปฏิบัติเพื่อกู้ระบบสารสนเทศ ให้กลับไปมีการทำงานเป็นดังสภาพเดิมก่อนมีการปรับเปลี่ยน เผื่อใช้สำหรับกรณีที่การปรับเปลี่ยนไม่เกิดสัมฤทธิ์ผล

3.6 กำหนดกระบวนการในการเฝ้าระวังและตรวจสอบความเรียบร้อยของระบบหลังการปรับเปลี่ยน

3.7 กำหนดปฏิทินในการดำเนินการปรับเปลี่ยนระบบ

4 ผู้จัดการส่วนเทคโนโลยีสารสนเทศ (สทร.) มีภาระหน้าที่ คือ

4.1 ทำการอนุมัติการปรับเปลี่ยนระบบ ตามที่เสนอโดยคณะกรรมการบริหารความเปลี่ยนแปลง

4.2 พิจารณารายงานสรุป การปรับเปลี่ยนระบบสารสนเทศของคณะกรรมการบริหารความเปลี่ยนแปลงคณะกรรมการบริหารความเปลี่ยนแปลง

1. องค์ประกอบคณะกรรมการบริหารความเปลี่ยนแปลง

คณะกรรมการการบริหารความเปลี่ยนแปลง คือ คณะบุคคลมีหน้าที่พิจารณาและอนุมัติการปรับเปลี่ยนระบบสารสนเทศ มีองค์ประกอบดังนี้

1) บุคลากรจากหน่วยงานเทคโนโลยีสารสนเทศ ผู้ที่มีความรู้ความสามารถในระบบงานนั้นๆ

2) ผู้ร้องขอปรับเปลี่ยนระบบสารสนเทศ

3) ตัวแทนจากหน่วยงานที่จะได้รับผลกระทบจากการปรับเปลี่ยนระบบสารสนเทศ

2. การดำเนินการของคณะกรรมการการบริหารความเปลี่ยนแปลง

จัดให้มีการประชุมกรรมการ การบริหารความเปลี่ยนแปลง เป็นอย่างน้อยทุกๆ 3 เดือน หรือ จัดประชุมทุกครั้ง ก่อนมีการเปลี่ยนแปลงใหญ่และมีการประกาศ วัน เวลา และสถานที่ชัดเจนหัวข้อการประชุม มาตรฐานสำหรับการประชุมกรรมการบริหารความเปลี่ยนแปลง คือ

1) ทบทวนและรับรองการปรับเปลี่ยนระบบสารสนเทศที่เสร็จสมบูรณ์แล้ว นับจากการประชุมครั้งก่อน

2) การยกเรื่องและนำเสนอคำร้องใหม่ในการปรับเปลี่ยนระบบสารสนเทศ

3) กำหนดตารางเวลาปฏิบัติและจัดทำปฏิทินประกาศตารางเวลาที่จะมีการปรับเปลี่ยนระบบสารสนเทศที่ได้รับการอนุมัติแล้วทั้งหมด

4) ดำเนินการแจ้งล่วงหน้าถึงการปรับเปลี่ยนระบบที่จะเกิดขึ้นแก่หน่วยงานและบุคลากรเพื่อให้ทราบถึงวันเวลา และผลกระทบเป็นระยะเวลาล่วงหน้าอย่างน้อย 30 วันและย้ำเตือนทุกสัปดาห์ จนถึงวันเริ่มดำเนินการผ่านสื่อต่างๆ

5) ติดตาม ประเมิน จัดทำรายงานผลการเปลี่ยนแปลงระบบสารสนเทศ และจัดเก็บเข้าในฐานความรู้

กรณีการปรับเปลี่ยนนอกกำหนดการหรือการปรับเปลี่ยนฉุกเฉินซึ่งต้องได้รับอนุมัติเร่งด่วนจากผู้จัดการส่วนเทคโนโลยีสารสนเทศหรือผู้บริหารระดับสูงขึ้นไป ภายหลังการดำเนินการฉุกเฉินให้ผู้ปฏิบัติที่ทำหน้าที่ปรับเปลี่ยนระบบ จะต้องทำเอกสาร แสดงรายละเอียดการปรับเปลี่ยนทั้งหมด รวมทั้งผลกระทบที่เกิดขึ้นรายงานต่อคณะกรรมการบริหารความเปลี่ยนแปลง ภายใน 30 วันเพื่อรับทราบและจัดเก็บเอกสารเข้าในฐานความรู้ต่อไป นับจากวันที่เสร็จสิ้นการดำเนินการปรับเปลี่ยนฉุกเฉิน

6 นโยบายการบริหารระบบเครือข่ายคอมพิวเตอร์

ให้มีการกำหนดมาตรการและแนวทางในการบริหารระบบเครือข่าย ทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์ ข้อกำหนดเกี่ยวกับการจัดการไอพีแอดเดรส (IP address) การตรวจสอบระบบเครือข่าย การเข้าถึงระบบจากระยะไกล การซ่อมบำรุง และการดำเนินการเมื่อระบบขัดข้อง

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหน้าที่ให้ดูแลรับผิดชอบระบบคอมพิวเตอร์และเครือข่ายของสำนักงานฯ
2. ผู้ตรวจสอบระบบคอมพิวเตอร์และเครือข่าย หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายประจำวัน
3. การหยุดระบบ หมายถึง การปิดระบบและ/หรือการหยุดการให้บริการระบบคอมพิวเตอร์และ/หรือเครือข่าย ทั้งด้านซอฟต์แวร์และ/หรือฮาร์ดแวร์ ซึ่งส่งผลให้การใช้บริการระบบคอมพิวเตอร์ขัดข้องไม่ว่าจะเป็นการชั่วคราว ครั้งคราว หรือตลอดเวลาในทำงานและนอกเวลาการทำงาน

ขอบเขต

นโยบายนี้ครอบคลุมถึงอุปกรณ์เครือข่ายทุกชนิด ทั้งฮาร์ดแวร์และซอฟต์แวร์ การเข้าถึงเครือข่ายและระบบสนับสนุนเครือข่ายที่เป็นสมบัติของสำนักงานฯ และอุปกรณ์ที่ทางสำนักงานฯอนุญาตให้เชื่อมต่อกับเครือข่ายของสำนักงานฯ

1. การจัดการไอพีแอดเดรส (IP address) การจัดสรรไอพีแอดเดรส
    1.1 ส่วนเทคโนโลยีสารสนเทศ มีหน้าที่จัดสรรไอพีแอดเดรสสำหรับหน่วยงานต่างๆ ของสำนักงานฯ
    1.2 ผู้ดูแลระบบมีหน้าที่ประเมินปริมาณความต้องการใช้งานไอพีแอดเดรสและสามารถเสนอแนวทางการลดหรือเพิ่มจำนวนไอพีแอดเดรสตลอดจนระบุ ไอพีแอดเดรส สำหรับการใช้งานในระบบต่างๆ ของสำนักงาน
2. ข้อปฏิบัติสำหรับผู้ดูแลระบบ
    2.1 ผู้ดูแลระบบมีหน้าที่บันทึกข้อมูลการจัดสรรไอพีแอดเดรสในเอกสารข้อมูลการบริหารจัดการไอพีแอดเดรสทันที
3. การตรวจสอบระบบคอมพิวเตอร์และเครือข่าย
    3.1 ข้อปฏิบัติการตรวจสอบประจำวัน
        3.1.1 ผู้ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายมีหน้าที่ตรวจสอบระบบคอมพิวเตอร์และเครือข่าย
        เป็นประจำทุกวันทันทีที่มาปฏิบัติงานตามเวลาทำการ
        3.1.2 ในกรณีที่ตรวจสอบพบปัญหาที่อาจสร้างความเสียหายอย่างรุนแรงทั้งในและนอกเวลาทำการ ให้ผู้ตรวจสอบระบบคอมพิวเตอร์และระบบเครือข่ายแจ้งผู้จัดการส่วนสารสนเทศเพื่อดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกในรายงานการ

3.2 การตรวจสอบระบบคอมพิวเตอร์

3.2.1 ตรวจสอบความคงอยู่และการให้บริการของระบบคอมพิวเตอร์ว่ายังสามารถให้บริการได้ตามปกติหรือไม่ โดยทดลองขอเข้าใช้บริการเสมือนเป็นผู้ขอใช้บริการตามปกติ โดยตรวจสอบระบบคอมพิวเตอร์แม่ข่ายหลักที่ให้บริการ

3.2.2 ตรวจสอบการทำงานของระบบคอมพิวเตอร์ทั้งหมดโดย พิจารณาจากหลักเกณฑ์ต่อไปนี้

- การทำงานของโปรเซสเซอร์
- ภาระงานหน่วยประมวลผลกลาง
- ปริมาณการใช้เนื้อที่ดิสก์ในพาร์ติชัน (partition) ต่างๆ
- ปริมาณการใช้หน่วยความจำหลัก
- แฟ้มบันทึกการทำงาน

3.2.3 ตรวจสอบเซิร์ฟเวอร์และระบบปฏิบัติการในเซิร์ฟเวอร์อื่นๆ ที่มีความสำคัญ

3.3 การตรวจสอบระบบเครือข่าย

3.3.1 ตรวจสอบการเชื่อมโยงเซิร์ฟเวอร์กับเส้นทางเชื่อมโยงการสื่อสารของเครือข่ายว่ายังสามารถใช้งานได้ตามปกติหรือไม่

3.3.2 ตรวจสอบการทำงานของอุปกรณ์เครือข่ายหลักและระบบสนับสนุนการให้บริการ

3.3.3 ตรวจสอบการให้บริการของแอกเซสพอยส์ในเครือข่ายไร้ Property และ Property guest

3.3.4 ตรวจสอบสถิติและ/หรือข้อมูลที่เกี่ยวข้องทางสถิติของการใช้ช่องสัญญาณ เป็นต้น

4. การเข้าใช้ระบบคอมพิวเตอร์จากระยะไกล

ข้อปฏิบัติในการขอเข้าใช้ระบบคอมพิวเตอร์จากระยะไกล

4.1 ผู้ดูแลระบบมีหน้าที่จัดเตรียมระบบที่มีความมั่นคงปลอดภัยเพื่อรองรับการเชื่อมต่อระยะไกล

4.2 ผู้ขอใช้งานต้องยื่นเรื่องขอใช้งาน เพื่อขออนุมัติต่อผู้บริหารส่วนเทคโนโลยีสารสนเทศ

4.3 ผู้ดูแลระบบต้องเตรียมเอกสารบันทึก ข้อมูลชื่อผู้ใช้ และรหัสผ่านที่จำเป็นแก่ผู้ใช้งาน พร้อมกับการแจ้งผลการใช้งาน

4.4 ผู้ขอใช้งานต้องปฏิบัติตามข้อปฏิบัติต่างๆ ที่เกี่ยวข้องกับการใช้งานเครือข่ายอย่างเคร่งครัด

5. ความปลอดภัยการใช้งาน

5.1 ผู้ดูแลระบบมีหน้าที่เตรียมระบบความปลอดภัย ในการรองรับการเชื่อมต่อระยะไกล เช่น การเข้ารหัสการติดตั้งและใช้งานระบบ VPN เป็นต้น

5.2 ผู้ดูแลระบบมีหน้าที่เตรียมเอกสารในการใช้งานและติดตั้งระบบความปลอดภัยให้พร้อมใช้งานได้ตลอดเวลา

5.3 ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนตามประเภทของงานที่ได้รับอนุมัติให้ใช้ระบบจากระยะไกล

6. การซ่อมบำรุง ข้อปฏิบัติการซ่อมบำรุงรักษาระบบ

6.1 ผู้ดูแลระบบมีหน้าที่ซ่อมบำรุงรักษา แก้ไขข้อบกพร่องและจัดทำตารางเวลาแผนบำรุงรักษา เพื่อให้ระบบสามารถให้บริการได้ตามปกติ

6.2 ในกรณีที่ต้องหยุดระบบเพื่อซ่อมบำรุง ผู้ดูแลระบบต้องจัดทำแผนและขั้นตอนการซ่อมบำรุงรักษาระบบ เสนอขออนุมัติจากผู้อำนวยการสำนักงานฯ หรืออย่างน้อยผู้จัดการส่วนเทคโนโลยีสารสนเทศ ก่อนดำเนินการล่วงหน้าโดยมีการจัดทำบันทึกแจ้งวัน เวลา ปิดระบบ โดยแจ้งกับผู้ใช้งานทุกครั้งที่มีผลกระทบต่อผู้ใช้งานของสำนักงานฯ

6.3 ผู้ดูแลระบบต้องวางแผนงานและดำเนินการเพื่อประชาสัมพันธ์ ให้ผู้ใช้งานทราบเป็นเวลาไม่น้อยกว่า 2 วันทำการ นับจากวันประกาศถึงวันที่ต้องหยุดระบบ ยกเว้น ในกรณีฉุกเฉินที่ต้องดำเนินการทันทีเพื่อแก้ปัญหาความมั่นคงปลอดภัย โดยให้มีการประกาศข้อความผ่านทางระบบงานนั้นๆ ก่อนการหยุดระบบ และ/หรือระหว่างการหยุดระบบ

6.4 ผู้ดูแลระบบต้องจัดทำสรุปการดำเนินงานและเสนอต่อผู้บริหารส่วนงานเทคโนโลยีสารสนเทศภายใน 1 วันหลังจากเสร็จสิ้นการหยุดระบบ

7. ข้อปฏิบัติเมื่อระบบคอมพิวเตอร์หรือเครือข่ายขัดข้องการแก้ไขปัญหา

7.1 ให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายวิเคราะห์ผลกระทบเบื้องต้นในกรณีที่ระบบคอมพิวเตอร์และ/หรือเครือข่ายขัดข้อง และรายงานต่อผู้บริหารส่วนงานเทคโนโลยีสารสนเทศ

7.2 ให้เริ่มดำเนินการแก้ไขระบบคอมพิวเตอร์และเครือข่ายที่ขัดข้องหลังจากการวิเคราะห์ผลกระทบทันทีภายใน 1 ชั่วโมง ในกรณีที่มีผลกระทบระดับสูง อนุญาตให้ดำเนินการในเวลาทำการและให้ดำเนินการโดยไม่เว้นวันหยุดราชการและหรือนอกเวลาทำการ

7.3 ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือเครือข่ายกำหนดแนวทางการแก้ปัญหา ขั้นตอนและเวลาการปฏิบัติที่ชัดเจน โดยสรุปลักษณะปัญหา ผลกระทบที่อาจจะเกิดขึ้น หากมีความจำเป็นต้องได้รับความร่วมมือจากผู้มีส่วนเกี่ยวข้อง ให้เรียกประชุมพร้อมกันในคราวเดียว

7.4 ให้เจ้าหน้าที่ปฏิบัติงานแก้ปัญหาตามแนวทางที่กำหนดในข้อก่อนหน้าและรายงานผลการปฏิบัติงานต่อผู้บริหารส่วนงานเทคโนโลยีสารสนเทศ

7.5 หากมีผลกระทบที่จำเป็นต้องแจ้งข่าวสารให้กับผู้ใช้งานทราบ จะต้องตรวจสอบให้แน่ชัดและแจ้งให้ผู้ใช้งานทราบทันที

8. ข้อปฏิบัติเมื่อระบบจ่ายไฟฟ้าขัดข้องการแก้ไขปัญหา

8.1 ให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายวิเคราะห์ผลกระทบ ในกรณีที่ระบบคอมพิวเตอร์และ/หรือเครือข่ายขัดข้องเป็นระยะเวลานานเกินกว่าระบบสำรองไฟฟ้าจะจ่ายไฟฟ้าได้ โดยพิจารณาและรายงานต่อผู้บริหารส่วนงานเทคโนโลยีสารสนเทศ

8.2 ให้ผู้ดูแลระบบเครือข่ายดำเนินการตรวจสอบระบบไฟฟ้าและติดต่อผู้เกี่ยวข้องกับปัญหาด้านไฟฟ้าโดยนำข้อมูลมาวิเคราะห์ว่ามีระบบใดบ้างได้รับผลกระทบ กำหนดแนวทางการแก้ปัญหาด้านเครือข่ายและระบบ คอมพิวเตอร์ ขั้นตอนและตารางเวลาการปฏิบัติ โดยสรุปลักษณะปัญหาและผลกระทบที่อาจจะเกิดขึ้น

8.3 หากมีผลกระทบที่จำเป็นต้องแจ้งข่าวสารให้กับผู้ใช้งานทราบ จะต้องตรวจสอบให้อย่างแน่ชัดและแจ้งให้ผู้ใช้งานทราบทันที

8.4 ให้เจ้าหน้าที่ปฏิบัติงานดำเนินการแก้ปัญหาตามแนวทางที่กำหนดและรายงานผลการปฏิบัติงานต่อผู้บริหารส่วนงานเทคโนโลยีสารสนเทศ

9. ให้มีการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

7 นโยบายการเข้าถึงข้อมูลและระบบสารสนเทศ

ให้มีการกำหนดแนวทางบริหาร และการควบคุมการเข้าถึงข้อมูลเพื่อลดปัญหาในเรื่องความเสี่ยงของระบบสารสนเทศและการดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้มีความมั่นคงปลอดภัยของระบบสารสนเทศและป้องกันความเสียหายอันเกิดจากการกระทำที่ไม่ถูกต้อง และให้เป็นแนวปฏิบัติงานอย่างมีประสิทธิภาพแก่บุคลากร

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย หมายถึง เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลจัดการระบบคอมพิวเตอร์และเครือข่าย

2. ผู้ใช้ หมายถึง บุคลากรได้รับอนุญาตให้ใช้เครือข่ายคอมพิวเตอร์และระบบสารสนเทศของสำนักงานฯ

สาระสำคัญ

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ครอบคลุมการจัดการการเข้าถึงของผู้ใช้ กำหนดขึ้นเพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

1.1 การลงทะเบียนผู้ใช้ใหม่ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้ใหม่เพื่อให้สามารถใช้งานระบบสารสนเทศและต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้ทันที ในกรณีที่มีการยกเลิกการใช้งานเมื่อมีการลาออกของบุคลากร

1.2 การบริหารจัดการรหัสผ่านของผู้ใช้ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องบริหารจัดการรหัสผ่านของผู้ใช้ให้มีความมั่นคงปลอดภัย

1.3 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือ เท่ากับ 6 ตัวอักษร โดยมี การผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

1.4 ผู้ใช้ต้องลงนามสัญญาการใช้งานเครือข่ายว่าจะเก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ และไม่บอกรหัสแก่บุคคลอื่น

1.5 การบริหารสิทธิการเข้าถึงระบบคอมพิวเตอร์และเครือข่ายของผู้ใช้ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายจะกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบตามที่ภาระงานที่ได้รับมอบหมายหรือที่สำนักงานฯ เป็นผู้กำหนด

1.6 ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศของผู้ใช้เมื่อได้รับคำสั่งโดยทันที

1.7 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกสำนักงานฯ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกสำนักงานฯ สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศได้

1.8 การจำกัดเส้นทางบนเครือข่าย ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

2. การควบคุมการเข้าถึงระบบปฏิบัติการ กำหนดขึ้นด้วยวัตถุประสงค์เพื่อป้องกันการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและ/หรือการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต

2.1 การจำกัดระยะเวลาการใช้งาน ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย ต้องจำกัดระยะเวลาการใช้งานสำหรับระบบสารสนเทศที่มีความสำคัญสูงหรือมีความเสี่ยงสูง

2.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้เป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

2.3 การบริหารจัดการรหัสผ่าน ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

2.4 การควบคุมการใช้งานโปรแกรมยูทิลิตี้ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงระบบฯ โดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนเข้าใช้งานต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ใครเป็นผู้ใช้งาน

3. การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ กำหนดขึ้นด้วยวัตถุประสงค์ เพื่อป้องกันการใช้งานระบบสารสนเทศ โดยไม่ได้รับอนุญาต

3.1 การจำกัดการใช้งานสารสนเทศผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย ต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่า สารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

3.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง ต้องแยกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระบบที่เชื่อมต่อระหว่างระบบอินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในสำนักงานออกจากการเชื่อมต่อเพื่อใช้งานระบบ ERP

4. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงาน กำหนดขึ้นด้วยวัตถุประสงค์เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนให้เป็นไปอย่างปลอดภัย

4.1 การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้กลุ่มบุคลากรต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook, Tablet หรือ Smartphone) เช่น เมื่อปฏิบัติงานอยู่นอกสถานที่ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง ต้องใช้กุญแจล็อกเครื่องคอมพิวเตอร์พกพาและต้องเข้ารหัสข้อมูลที่สำคัญไว้ เป็นต้น

4.2 การปฏิบัติงานนอกสำนักงาน ผู้ใช้งานระบบสารสนเทศต้องปฏิบัติงานด้วยความระมัดระวัง เช่น ใช้วิธีการป้องกันสำหรับเครื่องคอมพิวเตอร์พกพา การติดต่อผ่านทางเครือข่ายจากภายนอกต้องได้รับการป้องกันการถูกลักลอบดูข้อมูล เป็นต้น

8 นโยบายการใช้อุปกรณ์ไอทีส่วนบุคคล

ให้กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยของคอมพิวเตอร์ส่วนบุคคล ซึ่งทั้งที่เป็นทรัพย์สินของสำนักงานหรือเป็นทรัพย์สินส่วนตัวของผู้ใช้ที่นำมาใช้งานกับระบบสารสนเทศของสำนักงาน เพื่อให้การจัดการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์เป็นไปอย่างเป็นระบบ มีแบบแผนและสามารถจัดการปัญหาความปลอดภัยที่อาจจะเกิดขึ้นได้อย่างรวดเร็ว เนื่องจากการใช้งานเครื่องคอมพิวเตอร์เชื่อมต่อเครือข่ายภายในและภายนอก (ระบบเครือข่ายอินทราเน็ตและเครือข่ายอินเตอร์เน็ต) ซึ่งอาจมีการติดไวรัสคอมพิวเตอร์ หรือ malware ต่างๆและเครื่องคอมพิวเตอร์เหล่านี้อาจถูกโจมตีและเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ผู้ใช้ (User) ได้แก่ บุคลากรของสำนักงานฯที่มีชื่ออยู่ในบัญชีผู้ได้รับสิทธิการใช้งานระบบคอมพิวเตอร์และเครือข่าย
2. ผู้ดูแลระบบ (System administrator) หมายถึง ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ดูแลระบบคอมพิวเตอร์และเครือข่าย
3. คอมพิวเตอร์ส่วนบุคคล หมายถึง คอมพิวเตอร์ซึ่งเป็นทรัพย์สินของสำนักงานฯซึ่งได้จัดสรรให้บุคลากรคอมพิวเตอร์ประจำตัว และคอมพิวเตอร์ให้บริการ
4. คอมพิวเตอร์ส่วนตัว หมายถึง เครื่องคอมพิวเตอร์พกพา (Notebook, Tablet หรือ Smartphone) ที่ผู้ใช้นำมาเอง

1. การจัดลำดับชั้นความมั่นคงของคอมพิวเตอร์ส่วนบุคคล

คอมพิวเตอร์ส่วนบุคคล ลำดับชั้นความมั่นคงของคอมพิวเตอร์ส่วนบุคคลแบ่งเป็นสามระดับคือ

- ระดับที่ 1(ความมั่นคงสูงมาก)
- ระดับที่ 2 (ความมั่นคงสูง) และ
- ระดับที่ 3 (ความมั่นคงปกติ)

1.1 ระดับที่ 1 (ความมั่นคงสูงมาก) คือ คอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานและมีการจัดเก็บบันทึกข้อมูลที่มีความสำคัญ หากข้อมูลเสียหายจะส่งผลกระทบต่อการดำเนินงานของสำนักงานฯ ได้แก่ คอมพิวเตอร์ด้านการเงิน การบัญชี การลงทะเบียน งานบุคคล งานสารบรรณและงานพัสดุหรืองานอื่นใดที่จะกำหนดเพิ่มเติมในภายหลัง

1.2 ระดับที่ 2 (ความมั่นคงสูง) คือ คอมพิวเตอร์ที่ใช้ดูแลระบบคอมพิวเตอร์และเครือข่าย หรือใช้พัฒนาโปรแกรมของระบบสารสนเทศและคอมพิวเตอร์ของผู้บริหาร

1.3 ระดับที่ 3 (ความมั่นคงปกติ) คือ คอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานทั่วไป และคอมพิวเตอร์

ให้บริการ รวมถึงคอมพิวเตอร์ส่วนตัว

2. ข้อกำหนดด้านความปลอดภัย

2.1 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

2.2 เครื่องคอมพิวเตอร์ทุกเครื่องต้องมีการลงโปรแกรม Antivirus, Antispyware และ Firewall เป็นไปตามข้อกำหนด

2.3 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องที่เป็นทรัพย์สินของสำนักงานต้องมีการป้องกันโดยใช้ Password ในระดับ BIOS เพื่อป้องกันการแก้ไขค่าติดตั้งเบื้องต้นประจำเครื่อง

2.4 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องที่เป็นทรัพย์สินของสำนักงานควรลงโปรแกรมการบริหารการจัดการเครื่องคอมพิวเตอร์เพื่อป้องกันการติดตั้งโปรแกรมหรือการแก้ไขค่าติดตั้งประจำเครื่อง เช่น เปลี่ยนแปลงสิทธิการใช้เครื่อง เป็นต้น

2.5 ห้ามผู้ใช้ที่ไม่ได้รับอนุญาต ใช้งานคอมพิวเตอร์ที่มีความมั่นคงระดับที่ 1 โดยเด็ดขาด หากมีความจำเป็นต้องให้ผู้อื่นใช้ เครื่องคอมพิวเตอร์ในการปฏิบัติงาน ผู้ใช้ประจำเครื่องคอมพิวเตอร์นั้นจะต้องอนุญาตและต้องคอยเฝ้าระวังในระหว่างการใช้งาน

2.6 การเข้าถึงข้อมูลจะถูกจำกัดโดยผู้ดูแลระบบ ห้ามมิให้ผู้ใช้งานเข้าถึงข้อมูลที่ไม่อนุญาต

2.7 การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์เป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์นั้น

2.8 ห้ามนำคอมพิวเตอร์ส่วนตัวมาใช้งานในความมั่นคงระดับที่ 1 และให้ส่วนเทคโนโลยีสารสนเทศเตรียมเครื่องคอมพิวเตอร์ส่วนบุคคลให้กับผู้ว่าจ้างดูแลระบบใช้งาน หรือหากจะยกเว้นให้ผู้ว่าจ้างดูแลระบบใช้คอมพิวเตอร์ส่วนตัวต้องได้รับอนุญาตจากส่วนเทคโนโลยีสารสนเทศ และมีเจ้าหน้าที่นั่งประกบขณะปฏิบัติงาน

3. ข้อกำหนดการใช้งานทั่วไปข้อกำหนดการใช้งานสำหรับผู้ใช้

3.1 ห้ามมิให้มีการเปิดระบบแชร์แฟ้มข้อมูลหรือโฟลเดอร์ระหว่างคอมพิวเตอร์ส่วนบุคคลที่เป็นทรัพย์สินของสำนักงานยกเว้นได้รับอนุญาตจากผู้ดูแลระบบเป็นรายกรณี

3.2 หากคอมพิวเตอร์ส่วนบุคคลที่เป็นทรัพย์สินของสำนักงานฯไม่สามารถทำงานได้ตามปกติ ผู้ใช้งานสามารถแจ้งผู้ดูแลระบบเพื่อแก้ปัญหาได้ ห้ามมิให้ผู้ใช้งานติดตั้ง ปรับแก้ และเปลี่ยนแปลงฮาร์ดแวร์และ/หรือซอฟต์แวร์ด้วยตนเอง ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบเป็นรายกรณี

3.3 ห้ามทำงานอื่นที่ไม่ได้รับมอบหมายในเครื่องคอมพิวเตอร์ที่มีความมั่นคงระดับ 1

3.4 ผู้ใช้งานต้องปฏิบัติตามคำแนะนำเมื่อผู้ดูแลระบบแจ้งให้เปลี่ยนรหัสผ่าน

3.5 ผู้ใช้งานต้องไม่เปิดอ่าน e-mail ที่ไม่มั่นใจว่าผู้ส่งมาเป็นผู้ใดเนื่องจากอาจมีโปรแกรมไวรัสคอมพิวเตอร์และโปรแกรมประเภท malware ต่างๆ ติดมาพร้อม e-mail

3.6 ห้ามไม่ให้ติดตั้งซอฟต์แวร์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานกับเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของสำนักงานฯ

3.7 การติดตั้งซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการทำงานโดยตรงให้ผู้ใช้งานขออนุญาตผ่านผู้บังคับบัญชาโดยแจ้งต่อส่วนเทคโนโลยีสารสนเทศทุกครั้ง

3.8 ผู้ใช้งานต้องตรวจสอบเครื่องว่ามีโปรแกรมไวรัสคอมพิวเตอร์หรือโปรแกรมประเภท malware ในเครื่องหรือไม่

3.9 รายงานสิ่งผิดปกติที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ส่วนบุคคลต่อผู้ดูแลระบบ

4. ข้อกำหนดการใช้งานของผู้ดูแลระบบ

4.1 กำหนดรหัสผ่านให้กับเครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องที่เป็นทรัพย์สินของสำนักงานฯ ผู้ดูแลระบบจะมีรหัสผ่านสองชุดเพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำรองสำหรับการใช้งานในกรณีฉุกเฉิน

4.2 ติดตั้งซอฟต์แวร์ต่างๆ ที่จำเป็นต่อการใช้งานให้เพียงพอต่อการใช้งานในแต่ละระดับ

4.3 ทำการ update โปรแกรมต่าง ๆ เช่น Windows, Antivirus และ Antispyware ทุกสัปดาห์เป็นอย่างน้อยเพื่อให้โปรแกรมที่ใช้งานมีความทันสมัยอยู่เสมอ

4.4 ทำการ update บัญชีรายชื่อไวรัสคอมพิวเตอร์ทุกสัปดาห์ให้คอมพิวเตอร์ทุกเครื่องอยู่ในสภาพพร้อมใช้และปราศจากโปรแกรมที่ไม่พึงประสงค์

4.5 ทำการ scan ไวรัสคอมพิวเตอร์และ malware ทุกสัปดาห์เป็นอย่างน้อย

4.6 ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อผู้บริหารเทคโนโลยีสารสนเทศเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เช่น มีการติดไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์ส่วนบุคคลในระดับความมั่นคงทุกระดับ ทันที ที่เกิดเหตุการณ์ขึ้น

9 นโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ

ให้มีการวางระเบียบแนวทางปฏิบัติทั้งทางด้านจริยธรรม จรรยาบรรณ และความถูกต้องตามกฎหมาย เพื่อป้องกันความเสียหายอันเกิดจากกระทำที่ไม่ถูกต้อง โดยกำหนดเป็นแนวปฏิบัติให้บุคลากรในการใช้งานเครือข่ายสารสนเทศของสำนักงานฯอย่างมีประสิทธิภาพ เพื่อปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้รวมถึงการรักษาข้อมูลที่เป็นสมบัติของสำนักงานฯ ให้มีความมั่นคงปลอดภัยในการนำมาใช้งานและรักษาภาพลักษณ์ของสำนักงานฯ

แนวปฏิบัติตามนโยบาย

คำจำกัดความ

1. ทรัพยากร (Resource) หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของสำนักงานฯ
2. ผู้ใช้ (User) ได้แก่ บุคลากรของสำนักงานฯ หรือบุคคลภายนอกที่มีบัญชีการใช้งานเครือข่ายคอมพิวเตอร์
3. ผู้ดูแลระบบ (System administrator) หมายถึง ผู้ซึ่งได้รับมอบหมายให้ทำหน้าที่ดูแลระบบคอมพิวเตอร์และเครือข่าย

1. ผู้ดูแลระบบ (System administrator)

1.1 ทำหน้าที่เฝ้าระวังการใช้งานผิดวัตถุประสงค์

1.2 มีหน้าที่รายงานเหตุการณ์ผิดปกติให้กับผู้บริหารส่วนเทคโนโลยีสารสนเทศ

1.3 มีหน้าที่ปรับปรุงระบบเครือข่ายและอุปกรณ์คอมพิวเตอร์ให้มีประสิทธิภาพและทันสมัยอยู่เสมอ

1.4 มีหน้าที่ป้องกันภัยจากผู้บุกรุกทั้งภายนอกและภายในสำนักงานฯ รวมถึงการป้องกันภัยไวรัสคอมพิวเตอร์

1.5 มีหน้าที่จัดหาและใช้ระบบบันทึก ระบบตรวจสอบและแก้ไขปัญหาความปลอดภัยของเครือข่าย

1.6 มีสิทธิยุติการทำงานของโปรเซสเซอร์ที่สร้างภาระให้ระบบ และอาจทำให้เกิดปัญหากับการใช้งานต่อผู้ใช้ส่วนรวม

1.7 มีหน้าที่แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบเพื่อบำรุงรักษาปรับปรุงหรือเปลี่ยนแปลงระบบซึ่งส่งผลให้ต้องหยุดบริการในช่วงระยะเวลาหนึ่ง แต่ในกรณีฉุกเฉินผู้ดูแลระบบอาจมีความจำเป็นต้องปิดระบบอย่างเร่งด่วนได้

1.8 มีหน้าที่จัดอบรมและแจ้งให้ผู้ใช้รับทราบถึงวิธีการรักษาความปลอดภัยของเครือข่ายและมีอำนาจที่จะเพิ่ม ลด ยุติหรือเพิกถอนสิทธิการใช้คอมพิวเตอร์และเครือข่ายโดยทันทีหากตรวจพบว่าผู้ใช้ฝ่าฝืน

ระเบียบหรือกระทำการที่อาจสร้างความเสียหายให้กับระบบ

2. ผู้ใช้ (User)

2.1 กำหนดรหัสผ่านที่ปลอดภัยและรักษารหัสให้เป็นความลับอยู่ตลอดเวลา รวมถึงมีการเปลี่ยนแปลงรหัสเมื่อไม่มั่นใจในการรักษาความลับรหัส

2.2 นำเครื่องคอมพิวเตอร์ลูกข่ายส่วนตัวที่ปลอดภัยมาใช้กับระบบคอมพิวเตอร์และเครือข่ายของสำนักงานฯ ตามจำนวนเครื่องที่ได้รับสิทธิที่ทางสำนักงานกำหนด

2.3 รายงานการล่วงละเมิดความปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายให้ผู้ดูแลระบบทราบในทันที

2.4 ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ

2.5 ไม่ปลอมแปลงชื่อผู้ใช้ภายใต้ระบบบัญชี หรือ สร้างรายชื่อผู้ใช้เพื่อให้เข้าใจว่าเป็นบุคคลอื่น

2.6 ไม่เข้าใช้ เรียกดู ลบ สำเนา หรือแก้ไขข้อมูลหรือโปรแกรมของผู้อื่นโดยผู้ใช้ไม่มีสิทธิหรือได้รับอนุญาตโดยเจ้าของ

2.7 ไม่ลักลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้ใช้อื่น หรือการกระทำการอันใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

2.8 ไม่ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ใดๆที่จะตรวจค้นจุดบกพร่องของฮาร์ดแวร์หรือซอฟต์แวร์หรือทำลายกลไกรักษาความปลอดภัยระบบ

2.9 ไม่เผยแพร่ เวอร์ม (Worm, Malware) หรือโปรแกรมประเภทไวรัส

2.10 ไม่ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

2.11 ไม่ใช้คอมพิวเตอร์และเครือข่ายโดยก่อผลกระทบต่อประสิทธิภาพโดยรวม เช่น การสร้างภาระให้กับระบบจนกระทั่งส่งผลกระทบต่อผู้ใช้งานอื่น

2.12 ไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อกระจายข่าวสารที่ไม่พึงประสงค์ หรือส่งจดหมายลูกโซ่ หรือส่งจดหมายขนาดใหญ่ หรือส่งจดหมายจำนวนมาก

2.13 ไม่ส่ง เผยแพร่ หรือประกาศข้อความใดที่จะล่วงละเมิด สร้างความเดือดร้อน รบกวน ข่มขู่ หมิ่นประมาท หรือส่งคำหยาบคายต่อบุคคลหรือกลุ่มบุคคล หรือนิติบุคคลมิว่าในเรื่องเชื้อชาติ ศาสนา เพศ หรืออื่นๆ ผู้ใช้ควรใช้คอมพิวเตอร์และเครือข่ายเพื่อการสื่อสารด้วยมารยาทและจริยธรรมอันดี

2.14 ไม่ใช้เครือข่ายคอมพิวเตอร์ของสำนักงานฯ เข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่น เว็บไซต์การพนัน หรือเว็บไซต์ต้องห้ามต่างๆ

2.15 ไม่เผยแพร่ข้อมูลและซอฟต์แวร์ที่อยู่ภายใต้กฎหมายทรัพย์สินทางปัญญาโดยไม่ได้รับอนุญาตจากเจ้าของ

2.16 ไม่ลักลอบใช้โปรแกรมหรือฮาร์ดแวร์ในการดักจับข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาต

2.17 ไม่ใช้คอมพิวเตอร์เพื่อการกระทำที่ผิดกฎหมาย

3. สิทธิการใช้เครือข่าย

3.1 ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้รายอื่น