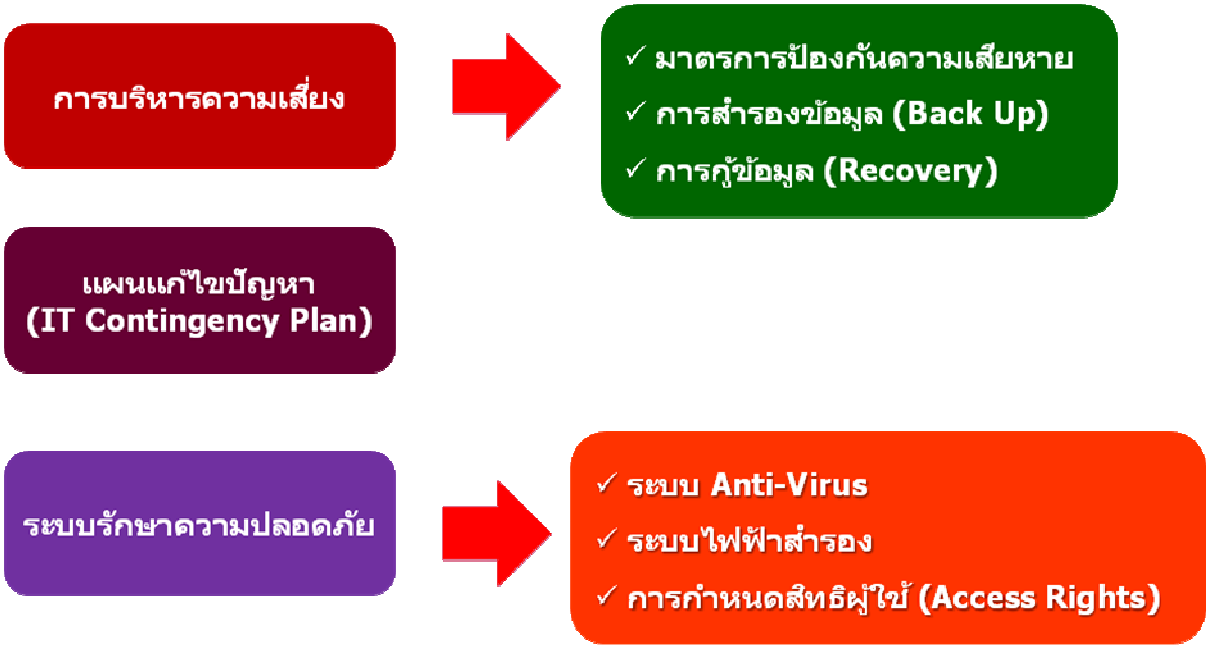
**ระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ**




**ระเบียบปฏิบัติสำหรับการใช้งานห้องเครื่อง**

**ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย**

| ที่ | ระเบียบปฏิบัติ | วิธีตรวจสอบ | ตัวอย่าง หลักฐานการปฏิบัติ |
|---|---|---|---|
| 1 | ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น | สังเกตการณ์เพื่อดูว่ามีคนนอกเข้ามาในห้องเครื่องโดยมีกิจที่ต้องทำหรือไม่ โดยปกติบุคคลเหล่านั้นต้องลงชื่อไว้พร้อมกิจที่ต้องการปฏิบัติ | สมุดบันทึกลงนามบุคคลภายนอก วันเวลาการเข้า และกิจที่ต้องการปฏิบัติ |
| 2 | ห้ามใส่รองเท้าเข้าห้องเครื่อง | สังเกตการณ์เพื่อดูว่ามีการใส่รองเท้าเข้าไปในห้องเครื่องหรือไม่ | ไม่สังเกตพบว่ามีการใส่รองเท้าเข้าไปในห้องเครื่อง |
| 3 | ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง | สังเกตการณ์เพื่อดูว่ามีการนำอาหารหรือเครื่องดื่มเข้าไปในห้องเครื่องหรือไม่ | ไม่สังเกตพบว่ามีการนำอาหารหรือเครื่องดื่มเข้าไปในห้องเครื่อง |
| 4 | ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องให้ปิดล็อคอยู่เสมอ | สังเกตการณ์เพื่อดูว่ามีการล็อกประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องหรือไม่ | ไม่สังเกตพบว่ามีการเปิดประตูทางเข้า-ออก และหน้าต่างทิ้งไว้ |
| 5 | ตรวจสอบสภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ ได้แก่<br>▪ ระบบกระแสไฟฟ้า<br>▪ ระบบการควบคุมความชื้น<br>▪ ระบบการระบายอากาศ<br>▪ ระบบการปรับอุณหภูมิ<br>▪ ระบบกระแสไฟฟ้าสำรอง<br>▪ ระบบ UPS<br>ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ | ตรวจสอบว่ามีการลงบันทึกการตรวจสอบระบบดังกล่าวหรือไม่ | มีการลงบันทึกการตรวจสอบอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ดังกล่าวทุกวัน |

| ที่ | ระเบียบปฏิบัติ | วิธีตรวจสอบ | ตัวอย่าง หลักฐานการปฏิบัติ |
|---|---|---|---|
| | อย่างน้อยวันละ 1 ครั้ง ยกเว้นการตรวจสอบระบบกระแสไฟฟ้าสำรองให้ตรวจสอบเดือนละ 1 ครั้ง | | |
| 6 | จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย | ตรวจสอบการจัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ในห้องเครื่อง | ไม่พบว่ามีเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่จัดวางอยู่ในสภาพที่เสี่ยงต่อการล้มหรือเสียหาย |
| 7 | ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพิ่มเติมตามความจำเป็น เช่น ในกรณีที่เป็นมุมอับ รวมทั้งตรวจสอบการทำงานของกล้องให้มีการทำงานอย่างถูกต้อง ต่อเนื่อง และให้สามารถเก็บภาพได้ในมุมกว้าง และไม่มีสิ่งกีดขวาง โดยบันทึกภาพล่าสุดไว้อย่างน้อย 1 เดือน | ตรวจสอบตำแหน่งติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อให้ครอบคลุมพื้นที่โดยรอบ | - มีการติดตั้งกล้องโทรทัศน์วงจรปิดอย่างเพียงพอ<br>- มีการเก็บภาพบันทึกไว้ในสื่อบันทึกข้อมูลไว้อย่างน้อย 1 เดือน |
| 8 | ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ 1 ครั้ง ว่ายังใช้งานได้เป็นปกติ หรือไม่ | - ตรวจสอบจากป้ายที่ติดอยู่บนอุปกรณ์ดับเพลิงว่ามีการตรวจสอบครั้งล่าสุดเมื่อใด<br>- ตรวจสอบแรงดันในถังดับเพลิง | -พบว่าป้ายได้รับการปรับปรุงตามวันและเวลาที่ตรวจสอบล่าสุด<br>-เข็มหน้าปัทม์แสดงแรงดันในถังดับเพลิงจะต้องแสดงว่ามีแรงดันอย่างเพียงพอ |
| 9 | ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องเครื่องอย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษหรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้องเครื่อง | ตรวจสอบความสะอาดและเป็นระเบียบเรียบร้อย รวมทั้งการไม่เก็บกล่องกระดาษต่างๆ ไว้ในห้องเครื่อง | ไม่พบว่าห้องเครื่องมีการเก็บกล่องกระดาษต่างๆ และห้องเครื่องมีความสะอาดและเป็นระเบียบเรียบร้อย |
| 10 | ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย | ตรวจสอบการจัดเก็บสายสัญญาณสื่อสารว่าอยู่ในสภาพเรียบร้อยหรือไม่ | ไม่พบการเดินสายสัญญาณที่เกะกะขวางทาง หรือรกรุงรัง |
| 11 | ตรวจสอบห้องสายสัญญาณสื่อสารให้มีการปิดล็อกอยู่เสมอ | สังเกตการณ์เพื่อดูว่ามีการล็อกประตูทางเข้า-ออกของห้องสายสัญญาณสื่อสารหรือไม่ | ไม่สังเกตพบว่ามีการเปิดประตูทางเข้า-ออกทิ้งไว้ |
| 12 | จัดทำหรือต่อสัญญาการบำรุงรักษาระบบงานสำคัญ<br>ไฟร์วอลล์ เราท์เตอร์ อุปกรณ์ UPS สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องเครื่อง ให้ครบถ้วน | ตรวจสอบว่าระบบเหล่านั้นได้รับการต่อสัญญาการบำรุงรักษาอย่างครบถ้วนหรือไม่ | สัญญาการบำรุงรักษาระบบเหล่านั้นมีการต่อสัญญาสำหรับปีปัจจุบัน |
| 13 | จัดให้ระบบงานสำคัญ เครื่องเซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์ UPS และระบบกระแสไฟฟ้าสำรอง (electricity power generator) เพื่อสนับสนุนการทำงานอย่างครบถ้วน | ตรวจสอบว่ามีระบบกระแสไฟฟ้าสำรองจ่ายให้กับระบบเหล่านั้นครบถ้วนหรือไม่ | -ในกรณีที่มีระบบงานใหม่เกิดขึ้นต้องพบว่าได้มีการหารือเรื่องการคำนวณโหลดการจ่ายกระแสไฟฟ้าสำรองเพิ่มเติมสำหรับระบบงานใหม่ที่เกิดขึ้น<br>-แผนการเตรียมอุปกรณ์ UPS และระบบกระแสไฟฟ้าสำรอง |

| ที่ | ระเบียบปฏิบัติ | วิธีตรวจสอบ | ตัวอย่าง หลักฐานการปฏิบัติ |
|---|---|---|---|
| | | | ให้เพียงพอกับระบบทั้งหมดเหล่านั้น |

**ระเบียบปฏิบัติในการลงทะเบียนและควบคุมการเข้าถึงระบบ**

**ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย และ ผู้พัฒนาระบบงาน**

| ที่ | ระเบียบปฏิบัติ | วิธีตรวจสอบ | ตัวอย่าง หลักฐานการปฏิบัติ |
|---|---|---|---|
| 1 | กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้งานใหม่ตาม "**แบบฟอร์มสำหรับลงทะเบียนผู้ใช้งาน**" และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์มฯ แต่ควรให้สิทธิความจำเป็นในการใช้งานเท่านั้น | ตรวจสอบความสอดคล้องระหว่างแบบฟอร์มลงทะเบียนกับบัญชีผู้ใช้งานของระบบ | บัญชีผู้ใช้งานในระบบสอดคล้องกับแบบฟอร์มลงทะเบียน |
| 2 | ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน สำหรับเจ้าหน้าที่ของกรม อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าวและจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง | -ตรวจสอบรายการชื่อผู้ที่ลาออก หรือย้ายแผนก<br>-ตรวจสอบว่ารายชื่อดังกล่าวต้องไม่สามารถเข้าถึงระบบได้<br><br>(กองการเจ้าหน้าที่จะต้องแจ้งภายในระยะเวลาอันสมควรเกี่ยวกับการลาออกหรือย้ายแผนกของเจ้าหน้าที่ เช่น ภายใน 1 เดือน) | -หนังสือที่เกี่ยวข้องกับแจ้งเวียนการลาออก หรือย้ายแผนก (ต้องจัดเก็บและแยกเอกสารดังกล่าวไว้ต่างหากเพื่อง่ายในการตรวจสอบในภายหลัง)<br>-ไม่พบบัญชีผู้ใช้งานของผู้ที่ลาออก หรือย้ายแผนก ยังคงค้างอยู่ในระบบงาน |
| 3 | ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน สำหรับหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าวและจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง | -ตรวจสอบบัญชีผู้เข้าถึงระบบจากหน่วยงานภายนอก<br>-ตรวจสอบว่าบัญชีดังกล่าวต้องไม่สามารถเข้าถึงระบบได้ เมื่อหมดสัญญาการจ้างงานแล้ว หรือไม่มีความจำเป็นต้องใช้งานอีกต่อไป และบันทึกผลการตรวจสอบไว้ใน แบบฟอร์มตรวจสอบการเข้าถึงระบบจากหน่วยงานภายนอก | -บัญชีผู้เข้าถึงระบบจากหน่วยงานภายนอก<br>-แบบฟอร์มตรวจสอบการเข้าถึงระบบจากหน่วยงานภายนอก<br>-ไม่พบบัญชีผู้ใช้งานจากหน่วยงานภายนอก- ดังกล่าวยังคงค้างอยู่บนระบบงานเมื่อหมดความจำเป็นแล้ว |
| 4 | ให้ทำการจัดส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยใส่ซองปิดผนึก และประทับตรา "ลับ" และ ส่งไปยังผู้ใช้งาน และแนบเอกสาร "**ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์ และ ระบบเครือข่าย**" รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด | สังเกตการณ์วิธีการจัดส่งบัญชีผู้ใช้งาน | ไม่สังเกตพบว่ามีผู้ใช้งานที่ได้บัญชีผู้ใช้โดยไม่เป็นไปตามระเบียบปฏิบัติดังกล่าว |