ใบขอขึ้นทะเบียน/ปรับปรุงแก้ไข/สำเนา/ยกเลิก เอกสารคุณภาพ

ส่วนที่ 1 ผู้เสนอขอ

วันที่เสนอ 6 มค. 2563

คณะกรรมการฯ/หน่วยงาน งานนวัตกรรมเทคโนโลยีสารสนเทศ

เรื่อง
- ☑ การขอขึ้นทะเบียนเอกสารคุณภาพ
- ☐ การขอปรับปรุงแก้ไขข้อความในเอกสารคุณภาพ
- ☐ การขอสำเนาเอกสารคุณภาพ
- ☐ การยกเลิกเอกสารคุณภาพ

ประเภทเอกสารคุณภาพ
- ☑ นโยบายคุณภาพ (Quality Manual)
- ☐ ระเบียบปฏิบัติ (System Procedure)
- ☐ วิธีปฏิบัติงาน (Work Instruction)
- ☐ เอกสารสนับสนุน (Supporting Document)
- ☐ แนวทางการดูแลผู้ป่วย (Clinical Practice Guideline)

เอกสารคุณภาพเรื่อง นโยบายด้านเทคโนโลยีสารสนเทศ

รหัสเอกสารคุณภาพ QM-IT-001-018-00

เหตุผลการจัดทำ _____

☐ กรณีที่เป็นเอกสารคุณภาพขึ้นทะเบียนใหม่ ได้ส่งเอกสารคุณภาพใหม่ พร้อมไฟล์ข้อมูลมาด้วย

☐ กรณีที่เป็นการแก้ไข/ยกเลิกเอกสารคุณภาพที่เคยทำแล้ว ได้ส่งเอกสารเดิมพร้อมกับเอกสารที่จัดทำขึ้นใหม่ มาด้วย

ลงชื่อ _____ ผู้เสนอขอ
(เภสัชกร พศวีร์ รัตนพยุงสกุล)
ตำแหน่ง ผู้ช่วยคณบดีฝ่ายบริหารเทคโนโลยีสารสนเทศ
วันที่ 6 มค. 2563

ส่วนที่ 2 ผู้ตรวจสอบ

☑ เห็นชอบให้จัดทำเอกสาร ดำเนินการขออนุมัติ

☐ ไม่เห็นชอบ ส่งคืนผู้จัดทำ

เหตุผลและข้อเสนอแนะ _____

ลงชื่อ _____ ผู้ตรวจสอบ
(นายแพทย์บดินทร์ บุตรธรรม)
ตำแหน่ง รองคณบดีฝ่ายบริหารและพัฒนาวัฒกรรม
วันที่ 6 มค. 2563

ส่วนที่ 3 ผู้อนุมัติ

☑ อนุมัติ

☐ ไม่อนุมัติ

เหตุผลและข้อแนะ _____

เห็นควรให้งานพัฒนาคุณภาพดำเนินการต่อไป

ลงชื่อ _____ ผู้อนุมัติ
(รองศาสตราจารย์นายแพทย์ศิริเกษม ศิริลักษณ์)
ตำแหน่ง คณบดีคณะแพทยศาสตร์
วันที่ 8 ม.ค. 2563

คณะแพทยศาสตร์ **มหาวิทยาลัยนเรศวร**	หน้าที่ 1/2 วันที่อนุมัติใช้: 8 มี.ค. 2563 รหัสเอกสาร: QM-IT-001-018-00
เรื่อง: นโยบายด้านเทคโนโลยีสารสนเทศ	**ผู้จัดทำ :** ฝ่ายบริหารเทคโนโลยีสารสนเทศ
ระดับเอกสาร: นโยบาย	**ผู้ตรวจสอบ :** ..... (นพ.บดินทร์ บุตรธรรม) รองคณบดีฝ่ายบริหารและพัฒนานวัตกรรม
หน่วยงานที่เกี่ยวข้อง: หน่วยงานภายในคณะแพทยศาสตร์	**ผู้อนุมัติ :** ..... (รองศาสตราจารย์นายแพทย์ศิริเกษม ศิริลักษณ์) คณบดีคณะแพทยศาสตร์

การควบคุมเอกสาร

ประวัติการแก้ไข:

ครั้งที่	วันที่ประกาศใช้	รายละเอียด	แผ่นที่
-	-	-	-

1. วัตถุประสงค์

1.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 เพื่อให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2. ขอบเขต

คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร

3. นิยามศัพท์

3.1 **องค์กร** หมายถึง คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร

3.2 **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของคณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร

3.3 **กลุ่มสารสนเทศและเทคโนโลยี** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในคณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร

3. นิยามศัพท์ (ต่อ)

3.4 **รองคณบดีฝ่ายบริหารและพัฒนานวัตกรรม** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร

3.5 **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร

3.6 **มาตรฐาน** (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

3.7 **วิธีการปฏิบัติ** (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

3.8 **แนวทางปฏิบัติ** (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

3.9 **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท(Role) ซึ่งองค์กรกำหนดไว้

3.10 **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์กร เช่น คณบดี รองคณบดี ผู้ช่วยคณบดี เป็นต้น

3.11 **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

3.12 **เจ้าหน้าที่** หมายถึง พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการขององค์กร

3.13 **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลมหาวิทยาลัยนเรศวรอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

3.14 **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

4. แนวทางปฏิบัติ

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัยซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด โดยสามารถแบ่งออกเป็นส่วน ๆ ดังต่อไปนี้

1. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
2. การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์
3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
4. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
5. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
6. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
7. การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์
8. การใช้งานจดหมายอิเล็กทรอนิกส์
9. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
10. การจัดทำระบบสำรองสารสนเทศ

5. ภาคผนวก

- นโยบายนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร

ส่วนที่ 1
การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and environment security)

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. แนวทางปฏิบัติ

2.1 คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร จำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศ โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2.2 คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งได้จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

2.3 คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร กำหนดสิทธิ์ให้กับเจ้าหน้าที่ สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

2.3.1 ดำเนินจัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่ คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร ” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

2.3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่ คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร”

2.3.3 จัดให้มีเจ้าหน้าที่งานบริหารเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยนเรศวร ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 2
การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์
(Computer Center Entry Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

2. แนวทางปฏิบัติการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

2.1 ผู้ดูแลระบบ กลุ่มสารสนเทศและเทคโนโลยี และเจ้าหน้าที่ องค์กร มีแนวทางปฏิบัติ ดังนี้

2.1.1 ผู้ดูแลระบบจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วน เพื่อสะดวกในกาปฏิบัติงาน และยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้นได้แก่

2.1.1.1.1 ส่วนระบบเครือข่าย(Network Zone)

2.1.1.1.2 ส่วนเครื่องแม่ข่าย(Server Zone)

2.1.1.1.3 ส่วนเครื่องพิมพ์(Printer Zone) เป็นต้น

2.1.2 ผู้ดูแลระบบกำหนดสิทธิ์การเข้าออกกลุ่มสารสนเทศและเทคโนโลยี โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่”

2.1.3 ผู้ดูแลจัดทำระบบเก็บบันทึกการเข้าออกกลุ่มสารสนเทศและเทคโนโลยี ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

2.1.4 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยี ทบทวนสิทธิ์ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้ง

2.2 ผู้ใช้งานจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

2.2.1 ผู้ใช้งานแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” และติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลา

2.2.2 ผู้ใช้งานบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”และเจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยี ต้องตรวจสอบว่าบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว ทุกเดือน

2.2.3 ผู้ใช้งานที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร ต้องบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

2.2.4 ผู้ใช้งานปฏิบัติงาน ณ บริเวณที่กลุ่มงานเทคโนโลยีสารสนเทศกำหนดไว้ในแบบฟอร์มการขออนุญาตเข้าออก ภายใต้การดูแลโดยเจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ

ส่วนที่ 3
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างถูกต้อง

2. แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 ผู้ดูแลระบบกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบ หรือได้รับมอบหมาย มีสิทธิ์แก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

2.4 ผู้ดูแลระบบ ติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรและตรวจสอบการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

2.5 ผู้ดูแลระบบบันทึกข้อมูลการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. แนวทางปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน

3.1 ผู้ดูแลระบบ ตรวจสอบสิทธิ์และอนุมัติการผ่านเข้าสู่ระบบ ได้แก่ผู้ใช้งานขออนุญาตเข้าระบบงานนั้น

3.2 ผู้ใช้งานต้องทำเอกสารเป็นลายลักษณ์อักษรเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

3.3 ผู้ดูแลระบบกำหนดสิทธิ์ในการเข้าถึงระบบงานเทคโนโลยีสารสนเทศของผู้ใช้งานตามความจำเป็นเท่านั้น อีกทั้งเจ้าของข้อมูล และ “เจ้าของระบบงาน” อนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น

3.4 การลงทะเบียนเจ้าหน้าที่ใหม่ของกลุ่มสารสนเทศและเทคโนโลยี ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน

3.5 ผู้ดูแลกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

3.6 ผู้ใช้งานต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

3.7 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password)

3.7.1 ผู้ดูแลระบบ กำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”โดยการกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.7.2 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุด มีหลักการพิจารณาและปฏิบัติดังนี้

3.7.2.1 ผู้ดูแลระบบควบคุมการใช้งานของผู้ใช้งานอย่างเข้มงวด

3.7.2.2 ผู้ดูแลระบบกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวและแจ้งให้ผู้ใช้งานทราบ

3.7.2.3 ผู้ใช้งานได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานก่อนเข้าถึงข้อมูลเสมอ

3.7.2.4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัดตามที่ผู้ดูแลระบบแจ้ง

3.7.2.5 ผู้ใช้งานต้องรับผิดชอบและปกป้องข้อมูลตามสิทธิ์ที่ได้รับอย่างเคร่งครัด

3.8 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

3.8.1 ผู้ดูแลระบบกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

3.8.2 ผู้ดูแลระบบสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 4 ครั้ง

3.8.3 ผู้ดูแลระบบกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูลวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

3.8.4 ผู้ดูแลระบบทำการเข้ารหัส(Encryption) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะที่เป็นมาตรฐานสากล ก่อนดำเนินการการรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ

3.8.5 ผู้ดูแลระบบมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

3.8.6 ผู้ดูแลระบบมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

4. แนวทางปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่าย

4.1 ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กรต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

4.2 ระบบเครือข่ายทั้งหมดขององค์กรต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

4.3 ผู้ดูแลระบบออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน(Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

4.4 ผู้ดูแลระบบกำหนดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

4.5 ผู้ดูแลระบบกำหนดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

4.6 ผู้ดูแลระบบกำหนดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

4.7 กลุ่มงานสารสนเทศและเทคโนโลยีกำหนดบุคลากรกลุ่มงานสารสนเทศที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

4.8 ผู้ใช้งานเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

4.9 ผู้ดูแลระบบจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

4.10 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

4.11 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีเท่านั้นเป็นผู้มีสิทธิ์ดำเนินการหรือควบคุมการติดตั้งและเชื่อมต่ออุปกรณ์เครือข่าย

5. แนวทางปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

5.1 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software)

5.2 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

5.3 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีติดตั้งอัพเดทระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software)

5.4 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

5.5 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีเท่านั้นเป็นผู้มีสิทธิ์ดำเนินการติดตั้งและเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย

6. แนวทางปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

6.1 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของ

ระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

6.2 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

6.3 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

7. แนวทางปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก

กลุ่มสารสนเทศและเทคโนโลยี กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

7.1 การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

7.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากรองคณบดีฝ่ายบริหารและพัฒนานวัตกรรมก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

7.3 ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล

7.4 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

8. แนวทางปฏิบัติการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

กลุ่มสารสนเทศและเทคโนโลยีควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

8.1 ผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

8.1.1 การแสดงตัวตน(Identification) คือขั้นตอนที่ผู้ใช้งานแสดงชื่อผู้ใช้งาน (Username)

8.1.2 การพิสูจน์ยืนยันตัวตน(Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน(Password)

8.2 การเข้าสู่ระบบสารสนเทศขององค์กร จะต้องตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี

ส่วนที่ 4
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Third party access control)

1. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัย

2. แนวทางปฏิบัติ

2.1 รองคณบดีฝ่ายบริหารและพัฒนานวัตกรรม ประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

2.2.1 บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากรองคณบดีฝ่ายบริหารและพัฒนานวัตกรรม

2.2.2 กลุ่มงานสารสนเทศและเทคโนโลยีจัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

2.2.2.1 เหตุผลในการขอใช้

2.2.2.2 ระยะเวลาในการใช้

2.2.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

2.2.2.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

2.2.2.5 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

2.2.3 หน่วยงานภายนอก ที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

2.2.4 องค์กรประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก โดยพิจารณาจากความสำคัญของระบบเทคโนโลยีสารสนเทศที่เข้าไปปฏิบัติงาน

2.2.5 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

2.2.6 หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2.2.7 องค์กรมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจว่า องค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.2.8 ผู้ให้บริการหน่วยงานภายนอกต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ ร่วมกับกลุ่มงานสารสนเทศและเทคโนโลยี

ส่วนที่ 5
การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Use of Personal Computer)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้งานควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

2. แนวทางปฏิบัติการใช้งานทั่วไป

2.1 ผู้ดูแลระบบหรือเจ้าหน้าที่กลุ่มงานสารสนเทศเท่านั้นเป็นผู้มีสิทธิ์ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร โดยโปรแกรมบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

2.2 ผู้ดูแลระบบหรือเจ้าหน้าที่กลุ่มงานสารสนเทศเท่านั้นเป็นผู้มีสิทธิ์กำหนดเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลขององค์กร

2.3 ผู้ดูแลระบบหรือเจ้าหน้าที่กลุ่มงานสารสนเทศเท่านั้นเป็นผู้มีสิทธิ์เคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม

2.4 ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ดังนี้

2.4.1 ผู้ใช้งานใช้เครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพและตระหนักว่าเครื่องคอมพิวเตอร์เป็นทรัพย์สินขององค์กร

2.4.2 ผู้ใช้งานไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

2.4.3 ผู้ใช้งานไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

2.4.4 ผู้ใช้งานไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

2.4.5 ผู้ใช้งานตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ

2.4.6 ผู้ใช้งานแจ้งปัญหาปัญหาเกี่ยวกับเครื่องคอมพิวเตอร์แก่ผู้ดูแลระบบหรือเจ้าหน้าที่กลุ่มงานสารสนเทศ

2.4.7 ผู้ใช้งานดูแลรักษาเครื่องคอมพิวเตอร์เมื่อเปิดและปิดเครื่องตามคำแนะนำของกลุ่มงานสารสนเทศ

2.4.8 ผู้ใช้งานต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆออกนอกสำนักงาน ต้องขออนุมัติจากทางฝ่ายบริหารทรัพยากรคณะฯ หรือผู้มีอำนาจ

2.4.9 ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดก่อนใช้งานเครื่องคอมพิวเตอร์

2.4.10 ผู้ใช้งานไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิมหรือเปลี่ยนไปจากที่องค์กรกำหนด

2.4.11 ผู้ใช้งานระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์และระบบเครือข่าย เหมือนเช่น บุคคลทั่วไปพึงปฏิบัติในการใช้งานทรัพย์สินของตนเอง

2.4.12 ผู้ใช้งานหลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แตกเสียหายได้

2.4.13 ผู้ใช้งานไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

2.4.14 ผู้ใช้งานเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจำทำให้หน้าจอมีรอยขีดข่วนได้

2.4.15 ผู้ใช้งานเครื่องคอมพิวเตอร์ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น ในกรณีที่ทำเครื่องชำรุดหรือสูญหายไปโดยประมาท

3. แนวทางปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้งานกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

3.2 ผู้ใช้งานตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นผู้ใช้งานต้องใส่รหัสผ่านเมื่อต้องการใช้งาน

3.3 ผู้ใช้งานไม่ให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.4 ผู้ใช้งาน Log-out ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver เมื่อไม่ใช้งานเครื่องคอมพิวเตอร์

4. แนวทางปฏิบัติในการใช้รหัสผ่าน

4.1 ผู้ใช้งานต้องปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

5. แนวทางปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศและเทคโนโลยีต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ เพื่อปิดช่องโหว่ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

5.2 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศและเทคโนโลยีติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

5.3 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

5.4 ผู้ใช้งานตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.5 กรณีที่พบไวรัสหรือมัลแวร์ ที่โปรแกรม Anti Virus ไม่สามารถกำจัดได้ รีบแจ้งเจ้าหน้าที่งานบริหารเทคโนโลยีสารสนเทศสารสนเทศ ให้ดำเนินการทันที

5.6 ผู้ใช้งานตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

5.7 ผู้ใช้งานตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

5.8 ผู้ใช้งานระมัดระวังในการใช้อินเทอร์เน็ต เพื่อหลีกเลี่ยงการติดมัลแวร์โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับ E-mail แนบจากคนที่ไม่รู้จัก, ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชทต่างๆ หรือช่องทาง Social Network

6. แนวทางปฏิบัติการสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

6.2 ผู้ใช้งานเก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.3 ผู้ใช้งานตระหนักความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

6.4 ผู้ใช้งานทดสอบแผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้สำหรับการกู้คืนอย่างสม่ำเสมอ

6.5 ผู้ใช้งานควรทำลายแผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานหรือไม่สามารถใช้งานได้แล้ว

ส่วนที่ 6
การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้งานจึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. แนวทางปฏิบัติการใช้งานทั่วไป

2.1 ผู้ดูแลระบบหรือเจ้าหน้าที่กลุ่มงานสารสนเทศเท่านั้นเป็นผู้มีสิทธิ์ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร โดยโปรแกรมบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

2.2 ผู้ดูแลระบบหรือเจ้าหน้าที่กลุ่มงานสารสนเทศเท่านั้นเป็นผู้มีสิทธิ์กำหนดเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลขององค์กร

2.3 ผู้ดูแลระบบหรือเจ้าหน้าที่กลุ่มงานสารสนเทศเท่านั้นเป็นผู้มีสิทธิ์เคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม

2.4 ผู้ใช้งานต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆออกนอกสำนักงาน ต้องขออนุมัติจากทางฝ่ายบริหารทรัพยากรคณะฯ หรือผู้มีอำนาจ ในกรณีที่

2.5 ผู้ใช้งานใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กรและตระหนักเป็นทรัพย์สินขององค์กร

2.6 ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดก่อนใช้งานเครื่องคอมพิวเตอร์

2.7 ผู้ใช้งานไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิมหรือเปลี่ยนไปจากที่องค์กรกำหนด

2.8 ผู้ใช้งานต้องใส่เครื่องคอมพิวเตอร์ในกระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา

2.9 ผู้ใช้งานไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

2.10 ผู้ใช้งานปิดเครื่องคอมพิวเตอร์แบบพกพาที่ครอบครองการใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 3 ชั่วโมง

2.11 ผู้ใช้งานระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์แบบพกพา และระบบเครือข่าย เหมือนเช่น บุคคลทั่วไปพึงปฏิบัติในการใช้งานทรัพย์สินของตนเอง

2.12 ผู้ใช้งานหลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

2.13 ผู้ใช้งานไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.14 ผู้ใช้งานทำการยกจากฐานภายใต้แป้นพิมพ์เพื่อการเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

2.15 ผู้ใช้งานไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

2.16 ผู้ใช้งานไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

2.17 ผู้ใช้งานไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.18 ผู้ใช้งานไม่วางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.19 ผู้ใช้งานไม่ติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

2.20 ผู้ใช้งานเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจำทำให้หน้าจอมีรอยขีดข่วนได้

2.21 ผู้ใช้งานเครื่องคอมพิวเตอร์แบบพกพาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น ในกรณีที่ทำเครื่องชำรุดหรือสูญหายไปโดยประมาท

3. แนวทางปฏิบัติการความปลอดภัยทางด้านกายภาพ

3.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2 ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

3.3 ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

4. แนวทางปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้งานกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพาและกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

4.2 ผู้ใช้งานตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นผู้ใช้งานต้องใส่รหัสผ่านเมื่อต้องการใช้งาน

4.3 ผู้ใช้งาน Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

5. แนวทางปฏิบัติในการใช้รหัสผ่าน

5.1 ผู้ใช้งานต้องปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใชงาน ระบบและรหัสผ่าน"

6. แนวทางปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

6.1 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศและเทคโนโลยีต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ เพื่อปิดช่องโหว่ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

6.2 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศและเทคโนโลยีติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

6.3 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

6.4 ผู้ใช้งานตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.5 ผู้ใช้งานพบไวรัสหรือมัลแวร์ ที่โปรแกรม Anti Virus ไม่สามารถกำจัดได้ รีบแจ้งเจ้าหน้าที่งานบริหารเทคโนโลยีสารสนเทศสารสนเทศ ให้ดำเนินการทันที

6.6 ผู้ใช้งานตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

6.7 ผู้ใช้งานตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6.8 ผู้ใช้งานไม่ใช้อินเทอร์เน็ต เพื่อหลีกเลี่ยงการติดมัลแวร์โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับจดหมายอิเล็กทรอนิกส์แนบจากคนที่ไม่รู้จัก, ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชทต่างๆ หรือช่องทาง Social Network

7. แนวทางปฏิบัติการสำรองข้อมูลและการกู้คืน

7.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

7.2 ผู้ใช้งานเก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.3 ผู้ใช้งานตระหนักความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

7.4 ผู้ใช้งานทดสอบแผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้สำหรับการกู้คืนอย่างสม่ำเสมอ

7.5 ผู้ใช้งานทำลายแผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานหรือไม่สามารถใช้งานได้

ส่วนที่ 7
การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน
(Use of the Internet and social media)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์อย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น

2.2 ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากรองคณบดีฝ่ายบริหารและพัฒนานวัตกรรม เป็นลายลักษณ์อักษรแล้ว

2.3 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์(Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

2.4 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

2.5 ผู้ใช้งานไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.6 ผู้ใช้งานเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบและตามสิทธิ์ที่กำหนดไว้ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

2.7 ผู้ใช้งานไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

2.8 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

2.9 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.10 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.11 ผู้ใช้งานตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.12 ผู้ใช้งานไม่ดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.13 ผู้ใช้งานปิดเว็บบราวเซอร์หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วทุกครั้ง

3. แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์

3.1 ผู้ใช้งานไม่เผยแพร่ ส่งต่อข้อความ รูปภาพ วีดิโอที่อาจทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง ถูกคุกคาม หรือถูกกลั่นแกลง หรือการเผยแพรเนื้อหาที่ละเมิดศักดิ์ศรีความเป็นมนุษย์ การเผยแพรข้อมูลเท็จ (false claims) หรือข้อมูลที่มีเจตนาชี้นำโดยมิชอบ (misleading claims) และไม่ใช้ถ้อยคำหยาบคาย ถ้อยคำลามก อนาจาร ดูหมิ่น ส่อเสียด เสียดสี ให้ร้ายผู้อื่นในทางเสียหาย หรือสร้างความแตกแยกในสังคม ทั้งนี้ผู้เผยแพร่ต้องรับผิดชอบ ทั้งด้านสังคมและกฎหมาย รวมถึงชื่อเสียของตนเองและองค์กร

3.2 ผู้ใช้งานคำนึงประโยชนของผู้ป่วยเป็นสำคัญ ไมวากรณีใด การใช้งานสื่อสังคมออนไลน์จะต้องไมกระทบกระเทือนหรือเป็นอุปสรรคต่อการให้บริการสุขภาพแกผู้ป่วย หรือทำให้ผู้ป่วยไม่ไดรับบริการสุขภาพด้วยมาตรฐานในระดับที่ดีที่สุดในสถานการณนั้นๆ ภายใต้ความสามารถและข้อจำกัด ตามภาวะ วิสัย และพฤติการณ์ที่มีอยู่

3.3 ผู้ใช้งานปฏิบัติตามหลักจริยธรรม และข้อบังคับว่าด้วยการรักษาจริยธรรมแห่งวิชาชีพ ตลอดจนข้อบังคับ ระเบียบ และประกาศที่เกี่ยวข้องของสภาวิชาชีพที่ตนเป็นสมาชิกอย่างเคร่งครัด

3.4 ผู้ใช้งานระวังในการเผยแพรภาพหรือเนื้อหาในขณะปฏิบัติหน้าที่ในวิชาชีพ ในลักษณะไม่เหมาะสมหรือไมมีความเป็นวิชาชีพได้

3.5 ผู้ใช้งานระวังการแสดงความเห็นบนสื่อสังคมออนไลน์ที่เป็นข้อถกเถียงหรือสุ่มเสี่ยงอย่างมากในสังคม เช่น ชาติ ศาสนา พระมหากษัตริย์ การเมืองการปกครอง

3.6 ผู้ใช้งานศึกษาและตั้งค่าความเป็นส่วนตัว (privacy settings) ของสื่อสังคมออนไลน์ที่ใช้งานอยู่อย่างเหมาะสม เพื่อจำกัดการเข้าถึงเนื้อหาที่เป็นเรื่องส่วนตัวจากบุคคลภายนอก และพิจารณา

แยกบัญชีผู้ใช้งาน (user account) หรือเนื้อหาที่เป็นเรื่องส่วนตัว กับเรื่องทางวิชาชีพออกจากกัน

3.7 ผู้ใช้งานรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลสารสนเทศ (information security) อยู่เสมอ ไม่ส่งผลกระทบสำคัญต่อความมั่นคงปลอดภัยหรือละเมิดความเป็นส่วนตัวของข้อมูลผู้ป่วย และระวังไม่ให้ผู้อื่นล่วงรู้ข้อมูลผู้ป่วยจากการใช้งานสื่อสังคมออนไลน์โดยไม่มีความจำเป็นและสมควร ตลอดจนไม่เปิดเผยข้อมูลส่วนบุคคลที่เป็นความลับของผู้อื่น

3.8 ผู้ใช้งานปกปิดข้อมูลส่วนบุคคลของผู้ป่วยในลักษณะที่สามารถระบุตัวตนของผู้ป่วยได้ เว้นแต่จะได้รับความยินยอมจากผู้ป่วยหรือผู้แทนโดยชอบธรรม และแม้จะได้รับความยินยอมแล้วก็ตาม ผู้ปฏิบัติงานควรพิจารณาข้อดีข้อเสียของการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวอย่างรอบคอบ

3.9 ผู้ใช้งานไม่ใช้ชื่อ เครื่องหมาย หรือสัญลักษณ์ขององค์กรในการที่อาจทำให้ผู้อื่นเข้าใจผิดว่าตนเป็นผู้แทนขององค์กรนั้นได

3.10 ผู้ใช้งานพิจารณาผลดีและผลเสียของการให้คำปรึกษาออนไลน์อย่างรอบคอบ และงดการให้คำปรึกษาในลักษณะที่แสดงถึงความมั่นใจ โดยขาดการคำนึงถึงโอกาสเกิดปัญหาหรือภาวะแทรกซ้อนที่รุนแรงหรือกรณีฉุกเฉิน

3.11 ผู้ใช้งานรักษาความลับของชื่อบัญชีผู้ใช้งาน (User Account) ของตนเอง ไม่เผยแพร่หรือแจ้งให้กับผู้อื่นใช้ร่วมด้วย

3.12 ผู้ใช้งานลงชื่อออกจากระบบ (Log out) หลังจากเลิกใช้งานทุกครั้ง

3.13 ผู้ใช้งานระวัง การเข้าใช้เว็บไซต์ ควรพิมพ์ที่อยู่ URL ของเว็บไซต์นั้นๆ โดยตรง ให้หลีกเลี่ยงการเข้าเครือข่ายทางสังคมผ่านทางคลิกลิงก์จากผลแสดงการค้นหา หรือจากอีเมล เพราะอาจเป็น URL ปลอมที่นำเราไปยังเว็บไซต์ปลอม เพื่อหลอกเอาบัญชีผู้ใช้งานและ Password ได้

ส่วนที่ 8
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

2.1 ผู้ดูแลระบบกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ

2.2 ผู้ดูแลระบบกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

2.3 ผู้ดูแลระบบกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง

2.4 ผู้ดูแลระบบกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ Logout ออกจากหน้าจอตัดการใช้งานผู้ใช้งานเมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

2.5 ผู้ใช้งานรายใหม่รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรก ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่โดยทันทีตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน” รวมทั้งรหัสจดหมายอิเล็กทรอนิกส์ ใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” ในการพิมพ์แต่ละตัวอักษร

2.6 ผู้ใช้งานไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

2.7 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด และเปลี่ยนรหัสผ่านทุก 3-6 เดือน

2.8 ผู้ใช้งานไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

2.9 ผู้ใช้งานไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.10 ผู้ใช้งานใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

2.11 ผู้ใช้งาน Logout ออกจากระบบทุกครั้ง หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นทุกครั้ง

2.12 ผู้ใช้งานตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

2.13 ผู้ใช้งานไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

2.14 ผู้ใช้งานไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

2.15 ผู้ใช้งานไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ที่เป็นความลับ

2.16 ผู้ใช้งานตรวจสอบกล่องเก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

2.17 ผู้ใช้งานลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

2.18 ผู้ใช้งานไม่โอนย้ายจดหมายอิเล็กทรอนิกส์ที่ใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตนเพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในกล่องเก็บจดหมายอิเล็กทรอนิกส์

ส่วนที่ 9
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 ผู้ดูแลระบบกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

2.2 ผู้ดูแลระบบเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

2.3 ผู้ดูแลระบบเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

2.4 ผู้ดูแลระบบเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบโดยเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.5 ผู้ดูแลระบบกำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP

2.6 ผู้ดูแลระบบเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งานรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

2.7 ผู้ดูแลระบบติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

2.8 ผู้ดูแลระบบกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

2.9 ผู้ดูแลระบบใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ 10
การจัดทำระบบสำรองสารสนเทศ
(Information Backup Systems)

1. วัตถุประสงค์

เพื่อให้ระบบสารสนเทศขององค์กรมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง และกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่ สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

2. ระบบสำรองข้อมูล

2.1 ผู้ดูแลระบบ จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชี อย่างน้อยปีละ 1 ครั้ง

2.2 ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

2.2.1 มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

2.2.2 มีระบบไฟฟ้าสำรอง

2.2.3 มีระบบปรับอากาศและความชื้นที่เหมาะสม

2.2.4 มีระบบป้องกันอัคคีภัย

2.2.5 มีระบบส่องสว่างที่เหมาะสม

2.2.6 มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

2.2.7 มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

2.3 มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

3. แนวทางปฏิบัติการสำรองข้อมูล(Data Backup)

3.1 ผู้ดูแลระบบจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูลและทบทวนบัญชีอย่างน้อยปีละ 1 ครั้ง

3.2 ผู้ดูแลระบบกำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

3.3 ผู้ดูแลระบบกำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

3.4 ผู้ดูแลระบบบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

3.5 ผู้ดูแลระบบตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น

3.6 ผู้ดูแลระบบจัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

3.7 ผู้ดูแลระบบเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

3.7.1 ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

3.7.2 ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุม ประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

3.7.3 ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

3.7.4 ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

3.7.5 ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

4. แนวทางปฏิบัติการกู้คืนข้อมูล(Data Recovery)

4.1 ผู้ดูแลระบบจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอน ปฏิบัติอย่างสม่ำเสมอ

4.2 ผู้ดูแลระบบตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ ตามปกติ

4.3 ผู้ดูแลระบบใช้ข้อมูลทันสมัยที่สุด(Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

4.4 ผู้ดูแลระบบทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

5. แนวทางปฏิบัติการทดสอบสภาพพร้อมใช้งาน

5.1 ผู้ดูแลระบบ ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง