หัวข้อ

หน่วยงาน	กรมสุขภาพจิต
หน่วยงานที่เกี่ยวข้อง	สำนัก/กอง/สถาบัน/โรงพยาบาล/ศูนย์/ศูนย์สุขภาพจิต ในสังกัดกรมสุขภาพจิต
ผู้จัดทำ	คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ผู้ทบทวน	คณะกรรมการพัฒนาระบบบริหารคุณภาพ
ผู้อนุมัติ	อธิบดีกรมสุขภาพจิต

บันทึกการแก้ไขนับตั้งแต่เริ่มใช้

ฉบับที่	แก้ไขครั้งที่	ประกาศใช้	รายละเอียด
00	00	1 มิถุนายน 2548	เริ่มใช้ฉบับร่าง
01	00	1 กรกฎาคม 2548	ประกาศใช้
01	01	26 สิงหาคม 2548	แก้ไขครั้งที่ 1 หัวข้อหน่วยงานที่เกี่ยวข้อง/2 ขอบเขต/3 คำจำกัดความ/4 ผู้รับผิดชอบ/5 ข้อกำหนดที่เกี่ยวข้อง/6 ขั้นตอนปฏิบัติงาน/7 เอกสารที่เกี่ยวข้อง
01	02	1 ธันวาคม 2548	แก้ไขครั้งที่ 2 การค้นหาความเสี่ยงฯ การประเมินความเสี่ยง การประเมินผล ขั้นตอนการปฏิบัติงาน/7 การควบคุมการบันทึก/8
01	03	1 เมษายน 2549	แก้ไขครั้งที่ 3 หน้า 5, ขั้นตอนปฏิบัติงาน 7.2.4 และภาคผนวก
01	04	1 กรกฎาคม 2549	- แก้ไขเลขรหัสระเบียบปฏิบัติเป็นของกรมสุขภาพจิต - 6.2 การค้นหาความเสี่ยง เพิ่มเติมข้อ 6.2.1.4 - แก้ไขข้อ 7.1.1 และ 7.3.2 - 7.2.4 การบันทึกข้อมูลที่สำคัญลงใน Databank เพิ่มเติม กรณี ศูนย์สุขภาพจิต หน้า 7-8

ฉบับที่	แก้ไขครั้งที่	ประกาศใช้	รายละเอียด
			- แก้ไขแผนการดำเนินงานฯ (0804-402-009) - 8. การควบคุมเอกสาร เพิ่มข้อ 8. แบบฟอร์มฯ
01	05	1 มกราคม 2550	- แก้ไขแผนงานการบริหารความเสี่ยงในภาคผนวก
01	06	1 กรกฎาคม 2550	- 6.2.1 หน้า 4 แก้เป็น ทุก 3 เดือน - 6.4.3 หน้า 5 แก้หัวข้อการแบ่งแยกความเสี่ยงฯ - 6.5.2 หน้า 5 แก้ค้นหาความเสี่ยงทุก 3 เดือน
01	07	1 มกราคม 2551	- แก้ไขตั้งแต่ 3.คำจำกัดความ - หัวข้อ 7.3.2.2 , 8. การควบคุมเอกสาร
01	08	1 กรกฎาคม 2551	- หน่วยงานที่เกี่ยวข้อง, ขอบเขต, กรควบคุมเอกสารหน้า 10
01	09	1 ธันวาคม 2551	- เพิ่มเติมหัวข้อที่ 7.2.2.2.5 กรณีเครื่องคอมพิวเตอร์กระเป๋าหิ้ว
01	10	1 มกราคม 2552	- หัวข้อ 5.1 แก้ไข ISO 9001:2000 เป็น ISO 9001:2008 - หัวข้อ 6.1.1 เพิ่มข้อความ “ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกรม”
01	11	1 มกราคม 2553	- แก้ไขแผนงานการบริหารความเสี่ยงในภาคผนวก
01	12	1 มกราคม 2554	- แก้ไขคำจำกัดความ - 6.2 แก้ไขรายละเอียดการค้นหาความเสี่ยง - 6.3 แก้ไขรายละเอียดการประเมินความเสี่ยง - 6.4 แก้ไขรายละเอียดการจัดการความเสี่ยง (Action to Manage Risk) - 6.5 แก้ไขรายละเอียดการประเมินผล (Evaluation) - 7.2.2.2.2 แก้ไขรายละเอียดการตรวจจับ Virus Computer - 7.2.2.2.5 กรณี เครื่องคอมพิวเตอร์กระเป๋าหิ้ว - 7.2.4 การบันทึกข้อมูลที่สำคัญ(ตามภารกิจ) ลงใน Databank - แก้ไขแผนงานการบริหารความเสี่ยงในภาคผนวก
01	13	23 ธันวาคม 2554	แก้ไขหัวข้อที่ - 6.3.1 การควบคุมความเสียหาย 6.3.1.1 ดำเนินการนิเทศหรือประชุมชี้แจง 6.3.1.2 การเข้าถึง Data Center และ Logout เมื่อเลิกใช้งานระบบเครือข่ายคอมพิวเตอร์ - แก้ไข 7.2.2.4 การบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Databank เป็น Data Center - แก้ไขแผนงานการบริหารความเสี่ยงในภาคผนวก
01	14	23 ธันวาคม 2554	เพิ่มเติมหัวข้อที่

ฉบับที่	แก้ไขครั้งที่	ประกาศใช้	รายละเอียด
			5.2 กฎระเบียบ 5.2.1 พระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2540 5.2.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 6.2 การค้นหาความเสี่ยง - 6.2.5 ด้านการสำรวจและจัดทำคำขอครุภัณฑ์คอมพิวเตอร์ - 6.2.6 การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer - 6.2.7 การบริหารเครือข่ายคอมพิวเตอร์ของหน่วยงาน - 6.3.1 การควบคุมความเสียหาย 6.3.1.6 ตรวจสอบว่าคณะทำงานบริหารความเสี่ยงฯของแต่ละหน่วยงาน ได้มีการสำรวจและจัดทำคำของบประมาณ 6.3.1.7 ตรวจสอบว่าผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานได้มีการติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer 6.3.1.8 ตรวจสอบว่าผู้รับผิดชอบในการดูแลระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานได้ปฏิบัติตามวิธีการบริหารเครือข่ายคอมพิวเตอร์ของหน่วยงาน 6.5 การประเมินผล (Evaluation) คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมจะดำเนินการจัดการประเมินผลการบริหารความเสี่ยงฯ ปีละ 1 ครั้ง 7.2 วิธีปฏิบัติ - 7.2.2.1.3 กรณีเจ้าหน้าที่นำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้ปฏิบัติงานภายในหน่วยงาน - 7.2.2.5 การบริหารเครือข่ายคอมพิวเตอร์ของหน่วยงาน หัวข้อ 7.2.2.5.1 การควบคุมห้อง Server 7.2.2.5.2 การควบคุม ดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server) 7.2.2.5.3 การควบคุมการสำรองข้อมูลสำหรับเครื่อง Server 7.2.2.5.4 การควบคุมผู้ใช้บริการ 7.2.2.5.5 การยกเลิกการเข้าใช้งานในระบบเครือข่าย

ฉบับที่	แก้ไขครั้งที่	ประกาศใช้	รายละเอียด
			7.2.2.5.6 การวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ - 7.2.2.6 การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer
01	15	11 มีนาคม 2556	เพิ่มเติมหัวข้อที่ **กลุ่มผู้ดูแลระบบเครือข่ายคอมพิวเตอร์** 7.2.1.1.1 ประเภทของงานการควบคุมห้อง Server 7.2.1.1.2 วิธีปฏิบัติ 7.2.1.1.3 ความถี่ในการปฏิบัติ 7.2.1.1.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.1.5 การบันทึกผลการปฏิบัติ 7.2.1.2.1 ประเภทของการควบคุมดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์(Server) 7.2.1.2.2 วิธีปฏิบัติ 7.2.1.2.3 ความถี่ในการปฏิบัติ 7.2.1.2.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.2.5 แบบฟอร์มการบันทึกผลการปฏิบัติ **กลุ่มสำนัก/กอง/ศูนย์สุขภาพจิต** 7.2.1.2.6 ประเภทของเครื่องคอมพิวเตอร์แม่ข่าย 7.2.1.2.7 วิธีปฏิบัติ 7.2.1.2.8 ความถี่ในการปฏิบัติ 7.2.1.2.9 ช่วงเวลาที่ปฏิบัติ 7.2.1.2.10 แบบฟอร์มการบันทึกผลการปฏิบัติ 7.2.1.3.1 ประเภทของข้อมูลการควบคุมการสำรองข้อมูลสำหรับเครื่อง Server 7.2.1.3.2 วิธีปฏิบัติ 7.2.1.3.3 ความถี่ในการปฏิบัติ 7.2.1.3.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.3.5 แบบฟอร์มการบันทึกผลการปฏิบัติ 7.2.1.3.6 วิธีการ Backup โดยใช้โปรแกรม 7.2.1.3.7 อุปกรณ์ที่ใช้ Backup 7.2.1.3.8 สถานที่จัดเก็บ กลุ่มสำนัก/กอง/ศูนย์สุขภาพจิต

ฉบับที่	แก้ไขครั้งที่	ประกาศใช้	รายละเอียด
			7.2.1.3.9 ประเภทของข้อมูล 7.2.1.3.10 ประเภทของ Server 7.2.1.3.11 วิธีปฏิบัติ 7.2.1.3.12 ช่วงเวลาที่ปฏิบัติ 7.2.1.3.13 วิธีการ Backup 7.2.1.3.14 อุปกรณ์ที่ใช้ Backup 7.2.1.3.15 สถานที่จัดเก็บ 7.2.1.4.1 วิธีปฏิบัติในการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ 7.2.1.4.2 ความถี่ในการปฏิบัติ 7.2.1.4.3 ช่วงเวลาที่ปฏิบัติ 7.2.1.4.4 แบบฟอร์มการบันทึกผลการปฏิบัติ 7.2.1.5.1 ประเภทของผู้ใช้คอมพิวเตอร์ 7.2.1.5.2 วิธีปฏิบัติในการควบคุมผู้ใช้คอมพิวเตอร์ 7.2.1.5.3 ความถี่ในการปฏิบัติ 7.2.1.5.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.7.1 ประเภทของการยกเลิกการเข้าใช้งานระบบเครือข่าย 7.2.1.7.2 วิธีปฏิบัติ 7.2.1.7.3 ความถี่ในการปฏิบัติ 7.2.1.7.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.7.5 การบันทึกผลการปฏิบัติ 7.2.1.8.1 การปรับปรุงทะเบียนผู้ใช้บริการ 7.2.1.8.2 วิธีปฏิบัติ 7.2.1.8.3 ความถี่ในการปฏิบัติ 7.2.1.8.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.8.5 การบันทึกผลการปฏิบัติ 7.2.1.9.1 ประเภทของเครื่องคอมพิวเตอร์ในการบำรุงรักษา 7.2.1.9.2 วิธีปฏิบัติ 7.2.1.9.2.1 การทำความสะอาด 7.2.1.9.3 ความถี่ในการปฏิบัติ 7.2.1.9.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.10.1 ประเภทของการติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus computer

ฉบับที่	แก้ไขครั้งที่	ประกาศใช้	รายละเอียด
			7.2.1.10.2 วิธีปฏิบัติ 7.2.1.10.3 ความถี่ในการปฏิบัติ 7.2.1.10.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.11.1 ประเภทของการบันทึกข้อมูลที่สำคัญ 7.2.1.11.2 วิธีปฏิบัติ 7.2.1.11.3 ความถี่ในการปฏิบัติ 7.2.1.11.4 ช่วงเวลาที่ปฏิบัติ 7.2.1.11.5 การบันทึกผลการปฏิบัติ
01	16	12 มีนาคม 2556	- แก้ไขแผนงานการบริหารความเสี่ยงในภาคผนวก
01	17	12 มีนาคม 2556	ประกาศใช้
01	18	3 มีนาคม 2557	แก้ไขรายชื่อ - ศูนย์สารสนเทศ เป็น กลุ่มพัฒนาข้อมูลและสารสนเทศ - กองแผนงาน เป็น สำนักยุทธศาสตร์สุขภาพจิต เพิ่มเติมหัวข้อที่ 7.2.1.1.2 วิธีปฏิบัติ (4) Administrator ประจำวันหรือผู้ที่ Administrator มอบหมาย 7.2.1.2.2 วิธีปฏิบัติ (4) ตรวจสอบการทำงานของอุปกรณ์ที่เกี่ยวข้อง เช่น สายเชื่อมต่อ, อุปกรณ์เครือข่าย เช่น Switch, Hub, Access Point 7.2.1.2.5 แบบฟอร์มการบันทึกผลการปฏิบัติ : แบบบันทึกการดูแลบำรุงเครื่องคอมพิวเตอร์แม่ข่ายของกรมสุขภาพจิตหรือตามที่หน่วยงานกำหนด 7.2.1.3.2 วิธีปฏิบัติ (1) หรือผู้ที่ได้รับการแต่งตั้งให้มีหน้าที่ดูแลและสำรองฐานข้อมูล 7.2.1.3.6 วิธีการ Backup โดยใช้โปรแกรม (2) Tools อื่นตามความเหมาะสม 7.2.1.4.1 วิธีปฏิบัติ (5) ตรวจสอบสถานะของ System Resource CPU Usage ใช้ไปแล้วร้อยละเท่าไร หรือแสดงลักษณะอื่นที่บ่งบอกสถานะและระดับการใช้งาน 7.2.1.6.1. ผู้ขอใช้บริการบันทึกขอมี User Name และ Password เพื่อเสนอต่อผู้อำนวยการฯ เป็นผู้ลงนามอนุญาต 7.2.1.7.4 ช่วงเวลาที่ปฏิบัติ ประมาณเดือนกันยายน

ฉบับที่	แก้ไขครั้งที่	ประกาศใช้	รายละเอียด
			7.2.1.10.5.2 ในวิธีปฏิบัติ เรื่อง การตรวจจับ Virus computer เมื่อดำเนินการ Scan virus ให้เลือกกด View หรือ Capture ผลไว้
01	19	1 มิถุนายน 2557	ประกาศใช้

1 วัตถุประสงค์

เพื่อควบคุมกระบวนงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

2 ขอบเขต

2.1 ครอบคลุมถึง ทุกหน่วยงานที่อยู่ในขอบเขตของระบบบริหารคุณภาพของกรมสุขภาพจิต ตามที่ระบุในคู่มือคุณภาพ

2.2 ครอบคลุมการค้นหาความเสี่ยง การประเมินความเสี่ยง การจัดการความเสี่ยง (Action to Manage Risk) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร และการประเมินผล (Evaluation)

3 คำจำกัดความ

3.1 ความเสี่ยง (Risk) หมายถึง โอกาสที่จะประสบกับความสูญเสียหรือสิ่งที่ไม่พึงประสงค์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

3.2 บุคลากรทุกคน หมายถึง ผู้ใช้งานคอมพิวเตอร์ในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานกรมสุขภาพจิต

3.3 คณะทำงานของหน่วยงาน หมายถึง คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารประจำหน่วยงาน

3.4 กลุ่มพัฒนาข้อมูลและสารสนเทศ หมายถึง หน่วยงานของกอง/สำนัก/สถาบัน/ โรงพยาบาล/ศูนย์ ในสังกัดกรมสุขภาพจิตที่ทำหน้าที่ในการดูแลระบบข้อมูลและ/หรือระบบเทคโนโลยีสารสนเทศของแต่ละหน่วยงาน

3.5 ระบบเครือข่ายคอมพิวเตอร์ หมายถึง ระบบงานซึ่งเชื่อมโยงคอมพิวเตอร์ต่าง ๆ ในองค์กรเข้าด้วยกัน เพื่อประโยชน์ในการใช้ทรัพยากรร่วมกัน ซึ่งประกอบด้วย คอมพิวเตอร์แม่ข่าย ลูกข่าย ระบบเชื่อมต่อสัญญาณ และระบบปฏิบัติการที่ใช้ในตึกสำนักงานกรมสุขภาพจิตหรือหน่วยงานสังกัดกรมสุขภาพจิต

3.6 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ หมายถึง ผู้ปฏิบัติงานในกลุ่มพัฒนาข้อมูลและสารสนเทศ ที่มีหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงาน

3.7 Hardware หมายถึง อุปกรณ์ต่าง ๆ ที่นำมารวมกันเข้าให้กลายเป็นครุภัณฑ์คอมพิวเตอร์ ซึ่งแบ่งเป็น 3 หน่วยใหญ่ ๆ ได้แก่ หน่วยรับข้อมูล เช่น แป้นพิมพ์ (Key board) หน่วยความจำ เช่น Chip จานบันทึก (Hard disk) และหน่วยแสดงผล เช่น จอภาพ (Monitor) เครื่องพิมพ์ (Printer) ฯลฯ นอกนี้ยังมีอุปกรณ์ประกอบอื่น ๆ เช่น Modem Switch เป็นต้น

3.8 Software หมายถึง โปรแกรมคอมพิวเตอร์ หรือชุดคำสั่งต่าง ๆ ที่ทำให้คอมพิวเตอร์ทำงานได้ ซึ่งนำมาใช้ให้เหมาะสมกับแต่ละหน่วยงานในสังกัดกรมสุขภาพจิต

3.9 อุปกรณ์ต่อพ่วง หมายถึง เครื่องมือหรืออุปกรณ์ที่ใช้ทำงานร่วมกับเครื่องคอมพิวเตอร์ ได้แก่ UPS (เครื่องควบคุม และสำรองไฟฟ้าสำหรับคอมพิวเตอร์) SCANNER อุปกรณ์รักษาความปลอดภัยแก่ระบบ ฯลฯ

3.10 เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ หมายถึง บุคลากรที่ปฏิบัติงานประจำศูนย์คอมพิวเตอร์ หรือศูนย์ข้อมูล เช่น หัวหน้าศูนย์คอมพิวเตอร์ หรือหัวหน้าศูนย์ข้อมูล ผู้ดูแลระบบเครือข่าย ผู้ช่วยผู้ดูแลระบบอื่นๆ และบุคลากรที่ปฏิบัติงานด้านข้อมูล ตามคำสั่งแต่งตั้งของสำนัก กอง โรงพยาบาล สถาบันศูนย์สุขภาพจิตในสังกัดกรมสุขภาพจิต

3.11 การบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center หมายถึง การนำข้อมูลที่สำคัญตามภารกิจของแต่ละหน่วยงานไปจัดเก็บไว้ในเครื่อง Server กลางของหน่วยงาน เช่น กรณี กรมสุขภาพจิต การบันทึกข้อมูลที่สำคัญ ลงใน Data bank , โรงพยาบาล/สถาบัน การบันทึกข้อมูลที่เกี่ยวกับการให้บริการแก่ผู้ป่วยจิตเวช, ศูนย์สุขภาพจิต การบันทึกข้อมูลที่สำคัญตามภารกิจ ลงใน เครื่องคอมพิวเตอร์กลาง

4. ผู้รับผิดชอบ

4.1 อธิบดีกรมสุขภาพจิต

4.2 ผู้แทนฝ่ายบริหารคุณภาพ (QMR)

4.3 คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4.4 คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

5. ข้อกำหนดที่เกี่ยวข้อง

5.1 มาตรฐาน ได้แก่ ISO 9001:2008 ข้อกำหนด 8.5.3

5.2 กฎระเบียบ

5.2.1 พระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2540

5.2.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

6. ขั้นตอนการปฏิบัติ

6.1 อธิบดีกรมสุขภาพจิตหรือผู้แทนฝ่ายบริหารคุณภาพของแต่ละหน่วยงาน ลงนามในเอกสาร ดังนี้

6.1.1 คำสั่งแต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกรมหรือประจำของแต่ละหน่วยงานเป็นผู้จัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

6.1.2 คำสั่งแต่งตั้งคณะกรรมการและคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของแต่ละหน่วยงาน

6.1.3 อนุมัติแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

6.2 การค้นหาความเสี่ยง

ผู้แทนคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของแต่ละหน่วยงาน ดำเนินการค้นหาความเสี่ยงในหน่วยงานของตนเอง ทุก 6 เดือน ดังนี้

6.2.1 **ด้านการมีตัวตนในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน**

6.2.1.1 ตรวจสอบการมีตัวตนในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน หมายถึง เจ้าหน้าที่ในหน่วยงานที่เป็นผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์จะต้องมี Username และ Password ของตนเอง ในการ Logon เข้าสู่ระบบเครือข่าย และ Logout เมื่อเลิกใช้งานระบบเครือข่ายคอมพิวเตอร์

6.2.2 **ด้านการบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center**

6.2.2.1 ผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ จะต้องมีการบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center ตามคู่มือการบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center

6.2.2.2 ผู้แทนคณะทำงานของแต่ละหน่วยงาน จะต้องรายงานผลการตรวจสอบและประเมินการบันทึกข้อมูลที่สำคัญ(ข้อ 7.2.1.11) ในแบบรายงานการประเมินความเสี่ยงการบันทึกข้อมูลที่สำคัญลงใน Data Center (0804-402-011) โดยให้ผู้แทนคณะทำงานของแต่ละหน่วยงาน เขียนผลสรุปในตอนท้ายของเอกสาร ว่า ทำการค้นหาความเสี่ยงตรวจจำนวนกี่คน ผ่านเกณฑ์การประเมินจำนวนกี่คน คิดเป็นร้อยละเท่าไร และเมื่อเปรียบเทียบกับดัชนีชี้วัดและเป้าหมายแล้วผ่านเกณฑ์การประเมินตามที่กำหนดในดัชนีชี้วัดและเป้าหมายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ข้อ 9.2) หรือไม่

6.2.3 ด้านการกำหนดชื่อผู้รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

6.2.3.1 ตรวจสอบรายชื่อผู้รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์แต่ละเครื่องให้ตรงกับความเป็นจริงในปัจจุบัน ทั้งชื่อหนังสือแต่งตั้งหรือมอบหมายซึ่งลงนามโดยหัวหน้าส่วนราชการ

6.2.4 ด้านการดูแลและบำรุงรักษาคอมพิวเตอร์

6.2.4.1 ตรวจสอบผู้รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์ได้มีการปฏิบัติตามวิธีปฏิบัติในงานบำรุงรักษาอุปกรณ์คอมพิวเตอร์และรายงานผลการปฏิบัติตาม ข้อ 7.2.1.9

6.2.4.2 รายงานผลการตรวจสอบและประเมินในแบบรายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต (0804-402-014) โดยให้ผู้แทนคณะทำงานของแต่ละหน่วยงาน เขียนผลสรุปในตอนท้ายของเอกสาร ว่า ทำการค้นหาความเสี่ยงจำนวนทั้งหมดกี่เครื่อง ผ่านเกณฑ์การประเมินจำนวนกี่เครื่อง คิดเป็นร้อยละเท่าไร และเมื่อเปรียบเทียบกับดัชนีชี้วัดและเป้าหมายแล้ว ผ่านเกณฑ์การประเมินตามที่กำหนดในดัชนีชี้วัดและเป้าหมายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ข้อ 9.2) หรือไม่

6.2.5 ด้านการสำรวจและจัดทำคำขอครุภัณฑ์คอมพิวเตอร์

6.2.5.1 ตรวจสอบว่าคณะทำงานบริหารความเสี่ยงฯของแต่ละหน่วยงาน ได้มีการสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแบบสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารหน่วยงานสังกัดกรมสุขภาพจิต

6.2.5.2 ตรวจสอบว่าได้มีการจัดทำคำของบประมาณจากแหล่งเงินต่างๆเพื่อการจัดหาครุภัณฑ์ด้านเทคโนโลยีสารสนเทศ (โดยเฉพาะครุภัณฑ์ที่มีอายุการใช้งานเกิน 5 ปี) เสนอต่อผู้อำนวยการของแต่ละหน่วยงาน

6.2.6 การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer

6.2.6.1 ตรวจสอบว่าผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานได้มีการติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer ตลอดจนมีการบันทึกผลการติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer ตามข้อ 7.2.1.10

6.2.7 การบริหารเครือข่ายคอมพิวเตอร์ของหน่วยงาน

6.2.7.1 ตรวจสอบว่าผู้รับผิดชอบในการดูแลระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานได้ปฏิบัติตามวิธีการบริหารเครือข่ายคอมพิวเตอร์ของหน่วยงาน (ข้อ 7.2.2.5) การควบคุมห้อง Server, การควบคุม ดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server), การควบคุมการสำรองข้อมูลสำหรับเครื่อง Server, การควบคุมผู้ใช้บริการ, การวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์)

6.2.7.2 ได้มีการรายงานผลการปฏิบัติงานในรายการกิจกรรมที่ปฏิบัติภายในห้อง Server ในแบบบันทึกขอเข้าห้อง Server 0804-401-028 หรือแบบบันทึกอื่นๆ ที่หน่วยงานกำหนด

ผู้แทนคณะทำงานบริหารความเสี่ยงฯของแต่ละหน่วยงาน จัดทำบัญชีความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสารของกรมสุขภาพจิต (0804-402-015) และจัดส่งเอกสารรหัส 0804-402-011, 0804-402-014 และ 0804-402-015 ที่ดำเนินการเรียบร้อยแล้ว ให้กลุ่มพัฒนาข้อมูลและสารสนเทศ กรมสุขภาพจิต และผู้จัดการความเสี่ยงฯของแต่ละหน่วยงาน

6.3 การประเมินความเสี่ยง

คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรม ทำการนิเทศงานหรือประชุมด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานสังกัดกรม อย่างน้อยปีละ 1 ครั้ง ดังนี้

6.3.1 การควบคุมความเสียหาย

6.3.1.1 ดำเนินการนิเทศงานหรือประชุมชี้แจงข้อมูล/คำแนะนำการใช้งานระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานที่เหมาะสมในขณะเวลานั้นๆ ให้แก่ผู้แทนคณะทำงานบริหารความเสี่ยงฯของแต่ละหน่วยงาน รวมถึงเจ้าหน้าที่ในหน่วยงานรับทราบและถือปฏิบัติในแนวทางเดียวกัน

6.3.1.2 ตรวจสอบการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์และการเข้าถึง Data Center ของเจ้าหน้าที่ในแต่ละหน่วยงาน โดยให้ทำการ Logon เข้าสู่ระบบเครือข่าย และ Logout เมื่อเลิกใช้งานระบบเครือข่ายคอมพิวเตอร์

6.3.1.3 ให้แสดงการจัดเก็บข้อมูลที่สำคัญ(ตามภารกิจ)ใน Data Center ตามวิธีปฏิบัติในการบันทึกข้อมูลที่สำคัญ (ข้อ 7.2.2.4) จากนั้นบันทึกการตรวจสอบในรายงานการประเมินความเสี่ยงการบันทึกข้อมูลที่สำคัญลงใน Databank (0804-402-011) ของแต่ละหน่วยงาน

6.3.1.4 ตรวจสอบการบำรุงรักษาฯและบันทึกการปฏิบัติตามวิธีปฏิบัติในงานบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (ข้อ 7.2.2.2)

6.3.1.5 ตรวจสอบรายชื่อผู้รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์แต่ละเครื่องให้ตรงกับความเป็นจริงในปัจจุบัน ทั้งชื่อหนังสือแต่งตั้งหรือมอบหมายซึ่งลงนามโดยหัวหน้าส่วนราชการ และชื่อที่ติดไว้แต่ละเครื่องคอมพิวเตอร์ โดยใช้วิธีสุ่มเลือกเครื่องคอมพิวเตอร์และอุปกรณ์ประมาณ 3 – 5 เครื่องในแต่ละหน่วยงาน จากนั้นบันทึกการตรวจสอบในรายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต (0804-402-014) ของแต่ละหน่วยงาน

6.3.1.6 ตรวจสอบว่าคณะทำงานบริหารความเสี่ยงฯของแต่ละหน่วยงาน ได้มีการสำรวจและจัดทำคำของบประมาณด้านเทคโนโลยีสารสนเทศและการสื่อสารจากแหล่งเงินต่างๆ ตามแบบสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารหน่วยงานสังกัดกรมสุขภาพจิต

6.3.1.7 ตรวจสอบว่าผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานได้มีการติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer ตลอดจนมีการบันทึกผลการป้องกัน Virus Computer ตามข้อ 7.2.2.6

6.3.1.8 ตรวจสอบว่าผู้รับผิดชอบในการดูแลระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานได้ปฏิบัติตามวิธีการบริหารเครือข่ายคอมพิวเตอร์ของหน่วยงาน (ข้อ 7.2.1.1 การควบคุมห้อง Server, ข้อ 7.2.1.2 การควบคุม ดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server), ข้อ 7.2.1.3 การควบคุมการสำรองข้อมูลสำหรับเครื่อง Server, ข้อ 7.2.1.6 การควบคุมผู้ใช้บริการ, ข้อ 7.2.1.4 การวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์)

6.3.2 **จัดทำบัญชีความเสี่ยง (Risk profile)** เมื่อคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรม ดำเนินการตรวจประเมินความเสี่ยงของแต่ละหน่วยงานเรียบร้อยแล้ว จะรายงาน

6.3.2.1 รายงานผลการตรวจประเมินในบัญชีความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสารของกรมสุขภาพจิต (0804-402-015) ของแต่ละหน่วยงาน

6.3.2.2 จัดทำรายงานการค้นหาความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต (0804-402-013)

6.3.2.3 เสนอประธานคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรม เพื่อลงนามกำกับในรายงานการค้นหาความเสี่ยงฯ (0804-402-013)

6.4 การจัดการความเสี่ยง (Action to Manage Risk)

เมื่อคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานรายงานผลการตรวจประเมินในบัญชีความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานให้แก่คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานจะเสนอให้ผู้จัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศฯแจ้งให้แต่ละหน่วยงาน ทราบและพิจารณาหาทางเลือกในการจัดการกับความเสี่ยง ดังนี้

6.4.1 การหลีกเลี่ยงความเสี่ยง (Risk avoidance) โดยชี้แจงให้แก่ผู้แทนคณะทำงานบริหารความเสี่ยงฯ และบุคลากรในฝ่าย / กลุ่มงานที่ค้นพบความเสี่ยงฯ ให้ดำเนินการแก้ไขโดยด่วน

6.4.2 การป้องกันความเสี่ยง (Risk prevention) ผู้แทนคณะทำงานบริหารความเสี่ยงฯ ของแต่ละหน่วยงานจะดำเนินการชี้แจงและฝึกปฏิบัติให้แก่บุคลากรทุกคนที่มีส่วนเกี่ยวข้องของแต่ละหน่วยงาน โดยดำเนินการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามวิธีปฏิบัติ ข้อ 7.2

6.4.3 การแบ่งแยกความเสี่ยง (Risk segregation) เมื่อแต่ละหน่วยงานมีการค้นพบความเสี่ยงฯ จะดำเนินการแบ่งแยกความเสี่ยงฯ ตามบัญชีความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ การควบคุมผู้ใช้คอมพิวเตอร์, การบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center, การบำรุงรักษาอุปกรณ์คอมพิวเตอร์, การสำรวจและจัดทำคำขอครุภัณฑ์คอมพิวเตอร์, การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer, การบริหารเครือข่ายคอมพิวเตอร์ของหน่วยงาน

6.4.4 คณะทำงานบริหารความเสี่ยงฯของแต่ละหน่วยงาน จัดทำหนังสือเวียนเรื่อง ขอให้ดำเนินการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยแจ้งหน่วยงานที่พบประเด็นความเสี่ยงที่สำคัญในรายงานการค้นหาความเสี่ยงฯ (0804-402-013) และแนบสำเนารายงานการค้นหาความเสี่ยงฯ (0804-402-013) ที่ประธานคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ลงนามแล้ว ไปพร้อมด้วย

6.5 การประเมินผล (Evaluation)

คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมจะดำเนินการจัดการประเมินผลการบริหารความเสี่ยงฯ ปีละ 1 ครั้ง โดยเชิญประชุม คณะกรรมการบริหารความเสี่ยงฯ และคณะทำงานบริหารความเสี่ยงฯของกรม ดำเนินการวิเคราะห์และประเมินความเสี่ยง ดังนี้

6.5.1 รับทราบผลการดำเนินงานที่ผ่านมา พร้อมทั้งร่วมกันหาแนวทางแก้ไขปัญหา/ความเสี่ยงที่พบ

6.5.2 ทบทวนและปรับปรุงระเบียบปฏิบัติ ให้สามารถปฏิบัติได้จริงและเหมาะสมกับปัจจัยสิ่งแวดล้อม และสถานการณ์ในช่วงเวลานั้นๆ

6.5.3 ให้ผู้แทนคณะทำงานฯของแต่ละหน่วยงาน เสนอข้อคิดเห็นในการพัฒนาระบบบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานให้มีประสิทธิภาพยิ่งขึ้น พร้อมทั้งเสนอเปลี่ยนแปลงแก้ไขวิธีปฏิบัติ การกำหนดดัชนีชี้วัด เป้าหมาย และ/หรือ รายชื่อคณะทำงาน ทั้งนี้เพื่อให้เหมาะสมกับแต่ละหน่วยงานในช่วงเวลานั้นๆ

7. เอกสารที่เกี่ยวข้อง

7.1 ระเบียบปฏิบัติ ได้แก่ ที่ 0804-301-004 เรื่อง งานเทคโนโลยีสารสนเทศ

7.2 วิธีปฏิบัติ ได้แก่

7.2.1 วิธีปฏิบัติงานควบคุมความเสี่ยงในระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมสุขภาพจิต ดังนี้

กลุ่มผู้ดูแลระบบเครือข่ายคอมพิวเตอร์

7.2.1.1 การควบคุมห้อง Server

7.2.1.1.1 ประเภทของงาน การควบคุมห้อง Server แบ่งออกเป็น 2 ลักษณะ คือ

(1) ห้องศูนย์ปฏิบัติการคอมพิวเตอร์

(2) จัดกั้นพื้นที่เป็นการเฉพาะ

7.2.1.1.2 วิธีปฏิบัติ

(1) ผู้อำนวยการของแต่ละหน่วยงาน ลงนามในเอกสารมอบหมายหรือคำสั่งแต่งตั้งหรือกำหนดตารางการปฏิบัติงานของ Administrator ประจำวัน ให้มีหน้าที่ควบคุมดูแลห้อง Server ตลอดจนการปฏิบัติการดูแลเครื่อง Server

(2) กลุ่มพัฒนาข้อมูลและสารสนเทศ ของแต่ละหน่วยงานประกาศเขตพื้นที่ห้ามบุคคลภายนอกที่ไม่มีส่วนเกี่ยวข้องเข้าไปในบริเวณห้อง Server ให้ชัดเจน เช่น การขีดเส้นสีแสดงสัญลักษณ์ไว้หน้าประตูเข้าห้อง หรือมีกุญแจ Key card ในการเข้าออกห้อง Server หรือสัญลักษณ์อย่างอื่นเช่น นำตู้มากั้น ฯลฯ

(3) กรณีบุคคลภายนอกหรือบุคคลอื่นนอกเหนือจาก Administrator ที่มีหน้าที่รับผิดชอบในแต่ละวัน มีความจำเป็นต้องเข้าไปภายในห้อง Server จะต้องขออนุญาตจาก Administrator ประจำวัน และจะต้องลงชื่อในรายการกิจกรรมที่ปฏิบัติภายในห้อง Server ในแบบบันทึกขอเข้าห้อง Server 0804-401-028 หรือแบบบันทึกอื่นๆ ที่หน่วยงานกำหนด

(4) Administrator ประจำวันหรือผู้ที่ Administrator มอบหมายจะต้องเข้าไปพร้อมกับบุคคลภายนอกในการเข้าปฏิบัติงานภายในห้อง Server ด้วยทุกครั้ง

(5) กรณีที่ต้องอนุญาตให้บุคคลภายนอกเข้าห้อง Server เช่น ทำความสะอาดห้อง , ตรวจเช็คและ Maintenance ระบบงานที่ห้อง Server เช่น ซ่อม/ปรับปรุงระบบไฟฟ้า เครื่องปรับอากาศ เพิ่มเติมอุปกรณ์ระบบเครือข่าย

เช่น Fiber Optic,สาย UTP, Switching, Router, Modem เป็นต้น จะต้องลงชื่อในแบบบันทึก 0804-401-028 หรือแบบบันทึกอื่นๆ ที่หน่วยงานกำหนด

7.2.1.1.3 ความถี่ในการปฏิบัติ ทุกวันทำการ หรือทุกครั้งที่เข้าไปปฏิบัติงานภายในห้อง Server

7.2.1.1.4 ช่วงเวลาที่ปฏิบัติ ช่วงเช้าของวันทำการ

7.2.1.1.5 การบันทึกผลการปฏิบัติ แบบบันทึก 0804-401-028 หรือแบบบันทึกอื่นๆ ที่หน่วยงานกำหนด

7.2.1.2 การควบคุม ดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server) โดยแบ่งออกเป็น 2 กลุ่มหน่วยงาน คือ

- <u>กรมสุขภาพจิต / สถาบัน / โรงพยาบาลในสังกัดกรมสุขภาพจิต</u>

7.2.1.2.1 ประเภทของ Server แบ่งออกเป็น 2 ประเภท คือ

(1) Server ที่สำคัญ

(2) Server ทั่วไป

7.2.1.2.2 วิธีปฏิบัติ

(1) Administrator ประจำวัน มีหน้าที่ปฏิบัติการดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่แต่ละหน่วยงานมีอยู่ (เช่น Data Center, Proxy Server, 1667, Web Server, Database Server, Mail Server ฯลฯ) และอุปกรณ์บริหารจัดการเครือข่าย

(2) ตรวจสอบการทำงานของเครื่อง ดูไฟแจ้งเตือนสถานะทำงานทุกวันทำการ

(3) ทำความสะอาดภายนอกสัปดาห์ละครั้ง อาจใช้ไม้ขนไก่ปัดฝุ่น

(4) ตรวจสอบการทำงานของอุปกรณ์ที่เกี่ยวข้อง เช่น สายเชื่อมต่อ, อุปกรณ์เครือข่าย เช่น Switch, Hub, Access Point, UPS ฯลฯ (UPS ต้องทดสอบปิดไฟ ซ่อมแซมเปลี่ยนแบตเตอรี่)

(5) ตรวจสอบสถานการณ์ทำงานของเครื่อง Server ผ่านระบบเครือข่าย โดยทดสอบการเชื่อมต่อจากเครื่องลูกข่ายเข้ามาที่เครื่อง Server และ ทดสอบการเชื่อมต่อจาก Server ไปยัง Web site อื่นๆ ที่ไม่ได้อยู่ภายใต้การดูแลของ Web Server หน่วยงาน

(6) ทดสอบสถานการณ์ทำงานของเครื่อง Server จากต่างเครือข่าย (กรณีที่มีมากกว่า 1 เครือข่าย)

(7) ตรวจสอบ/ปรับปรุงโปรแกรมป้องกัน Virus ทุกสัปดาห์ หากเป็นระบบปฏิบัติการ Linux ให้อัพเดตแพตช์ใหม่อย่างน้อยเดือนละ 1 ครั้ง

(8) ปรับปรุงโปรแกรมอุดช่องโหว่ของระบบปฏิบัติการ ทุก 1 เดือน

(9) เมื่อพบข้อผิดพลาดในแต่ละ Server หรือ Server หยุดให้บริการ(ล่ม) ให้ดำเนินการแก้ไขเบื้องต้น หากไม่แล้วเสร็จให้รีบแจ้งหัวหน้ากลุ่มพัฒนาข้อมูลและสารสนเทศ (ผู้รับผิดชอบ) เพื่อหาแนวทางจัดการปัญหาต่อไป พร้อมบันทึกไว้เป็นหลักฐานในแบบบันทึกขอเข้าห้อง Server (0804-401-028) หรือแบบบันทึกอื่นๆ ที่หน่วยงานกำหนด

(10) กรณีปัญหาที่เกิดกับ Server หรือ อุปกรณ์เครือข่าย เช่น Switch, Router, Modem, สาย UTP เป็นปัญหาความเสี่ยงที่เกินความสามารถของเจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ ให้ทำตามระเบียบพัสดุ โดยจัดจ้างช่างหรือผู้เชี่ยวชาญจากภายนอกเพื่อแก้ไขปัญหาให้แล้วเสร็จ

7.2.1.2.3 ความถี่ในการปฏิบัติ

(1) ทุกวันทำการ ได้แก่ ตรวจสอบการทำงานของเครื่อง

(2) สัปดาห์ละครั้ง ได้แก่ การทำความสะอาดภายนอก ตรวจสอบ/ปรับปรุงโปรแกรมป้องกัน Virus

(3) ทุกเดือน ได้แก่ ปรับปรุงโปรแกรมอุดช่องโหว่ของระบบปฏิบัติการ, ตรวจสอบ Event Viewer

7.2.1.2.4 ช่วงเวลาที่ปฏิบัติ

(1) วันหยุด

(2) ช่วงที่มีการใช้งานน้อยที่สุด

7.2.1.2.5 แบบฟอร์มการบันทึกผลการปฏิบัติ : แบบบันทึกการดูแลบำรุงเครื่องคอมพิวเตอร์แม่ข่ายของกรมสุขภาพจิตหรือตามที่หน่วยงานกำหนด

- **<u>กลุ่ม สำนัก/กอง/ศูนย์สุขภาพจิต</u>**

7.2.1.2.6 ประเภทของเครื่องคอมพิวเตอร์แม่ข่าย แบ่งออกเป็น 2 ประเภท คือ

(1) Server ที่สำคัญ

(2) Server ทั่วไป

7.2.1.2.7 วิธีปฏิบัติ

(1) Administrator ของแต่ละหน่วยงาน มีหน้าที่ปฏิบัติการดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย(Server) ที่แต่ละหน่วยงานมีอยู่

(2) ทำความสะอาดภายนอก 6 เดือนครั้ง

(3) ตรวจสอบสถานการณ์ทำงานของเครื่อง Server ผ่านเครือข่าย โดยทดสอบการเชื่อมต่อจากเครื่องลูกข่ายเข้ามาที่เครื่อง Server และทดสอบการเชื่อมต่อจาก Server ไปยัง Web site อื่นๆ ที่ไม่ได้อยู่ภายใต้การดูแลของ Web Server หน่วยงาน

(4) ตรวจสอบ/ปรับปรุงโปรแกรมป้องกัน Virus ทุกสัปดาห์ เฉพาะ Windows

(5) เมื่อพบข้อผิดพลาดในแต่ละ Server หรือ Server หยุดให้บริการ(ล่ม)ให้ดำเนินการแก้ไขเบื้องต้น หากไม่แล้วเสร็จให้รีบแจ้งหัวหน้ากลุ่มพัฒนาข้อมูลและสารสนเทศ เพื่อหาแนวทางจัดการปัญหาต่อไป

7.2.1.2.8 ความถี่ในการปฏิบัติ

(1) เดือนละครั้ง ได้แก่ การทำความสะอาดภายนอก

(2) ตรวจสอบ/ปรับปรุงโปรแกรมป้องกัน Virus สัปดาห์ละ 1 ครั้ง

7.2.1.2.9 ช่วงเวลาที่ปฏิบัติ

(1) วันหยุด

(2) ช่วงเวลาที่การใช้งานน้อยที่สุด

7.2.1.2.10 แบบฟอร์มการบันทึกผลการปฏิบัติ : แบบบันทึกการดูแลบำรุงเครื่องคอมพิวเตอร์แม่ข่ายของกรมสุขภาพจิตหรือตามที่หน่วยงานกำหนด

7.2.1.3 การควบคุมการสำรองข้อมูลสำหรับเครื่อง Server โดยแบ่งออกเป็น 2 กลุ่มหน่วยงาน คือ

- <u>กรมสุขภาพจิต / สถาบัน / โรงพยาบาลในสังกัดกรมสุขภาพจิต</u>

7.2.1.3.1 ประเภทของข้อมูล

(1) ข้อมูลที่เป็น Database

(2) ข้อมูลของ Web Server

7.2.1.3.2 วิธีปฏิบัติ

(1) มีหนังสือแต่งตั้งผู้มีหน้าที่สำรองข้อมูลและมีคู่มือปฏิบัติโดยเจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ ปฏิบัติตามคู่มือการควบคุมการสำรองข้อมูลสำหรับเครื่อง Server ของหน่วยงาน (0804-306-002) โดย ผู้มีสิทธิ์จะทำการสำรองข้อมูลจะต้องมีรายชื่อเป็น Administrator ตามตารางการดูแลและปฏิบัติหน้าที่ในห้อง Serve ในแต่ละเดือนหรือผู้ที่ได้รับการแต่งตั้งให้มีหน้าที่ดูแลและสำรองฐานข้อมูล

(2) ผู้มีหน้าที่ในการสำรองข้อมูลจะต้องทำการสำรอง (Backup) ข้อมูลใน Server ที่แต่ละหน่วยงานมีอยู่ (เช่น Data Center, Proxy Server, 1667, Web Server, Database Server, Mail Server ฯลฯ)

(3) ก่อนการสำรองในแต่ละครั้ง จะต้องตรวจสอบข้อมูลให้ดีก่อนว่า ข้อมูลสมบูรณ์ดี และต้องรอให้ผู้ใช้งานฐานข้อมูล ได้ทำการ Update เรียบร้อยก่อนและฐานข้อมูลไม่มีการเปิดใช้งาน

(4) กรณีที่เป็น Database เช่น MySQL, SQL Server, Access, Oracle, ฯลฯ ให้ทำการสำรอง (Backup) ข้อมูลทุกวันทำการ และทำการจดบันทึกการปฏิบัติงานไว้เป็นหลักฐานทุกครั้ง ตามแบบบันทึกการสำรองข้อมูลของหน่วยงาน (0804-401-010)

(5) กรณี Web Server ให้ทำการสำรอง (Backup) ข้อมูล 2 สัปดาห์ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลง และทำการ Manual Update เดือนละครั้ง และจดบันทึกการปฏิบัติงานไว้เป็นหลักฐานทุกครั้ง ตามแบบบันทึกการสำรองข้อมูล (0804-401-010) หรือตามแบบฟอร์มที่หน่วยงานกำหนด

(6) สื่อที่ใช้ในการ Backup ข้อมูลใน Server ได้แก่ แผ่น CD, แผ่น DVD, Tape Backup , External Hard disk หรือเครื่องคอมพิวเตอร์เครื่องอื่นๆ จะต้องถูกจัดเก็บไว้ในที่ปลอดภัย และสามารถนำข้อมูลกลับมา Restore ใช้งานได้ทันทีเมื่อเกิดความเสี่ยงหรือภาวะวิกฤต เช่น ถูกโจรกรรมข้อมูล , อัคคีภัย และมีการทดสอบ Restore อย่างน้อย 6 เดือนต่อครั้ง

7.2.1.3.3 ความถี่ในการปฏิบัติ

(1) ทุกวันทำการ ได้แก่ การสำรอง (Backup) ข้อมูลที่เป็น Database ถ้าเป็นฐานข้อมูลคนไข้ควร Backup ทุกวัน

(2) สัปดาห์ครั้ง ได้แก่ ข้อมูลของ Web Server หรือทุกครั้งที่มีการเปลี่ยนแปลง

(3) ทุกเดือน ได้แก่ ข้อมูลของ Web Server ในลักษณะ Manual Update

7.2.1.3.4 ช่วงเวลาที่ปฏิบัติ

(1) วันหยุด

(2) ช่วงที่มีการใช้งานน้อยที่สุด

7.2.1.3.5 แบบฟอร์มการบันทึกผลการปฏิบัติ : แบบบันทึกการสำรองข้อมูล (0804-401-010)

7.2.1.3.6 วิธีการ Backup โดยใช้โปรแกรม

(1) Schedule

(2) Tools อื่นตามความเหมาะสม

(3) Manual

7.2.1.3.7 อุปกรณ์ที่ใช้ Backup

(1) External Hard disk

(2) Tape

(3) DVD

(4) เครื่องคอมพิวเตอร์

7.2.1.3.8 สถานที่จัดเก็บ : จะต้องจัดเก็บไว้ในที่ปลอดภัย และสามารถนำข้อมูลกลับมา Restore ใช้งานได้ทันทีเมื่อเกิดความเสี่ยงหรือภาวะวิกฤต เช่น ถูกโจรกรรมข้อมูล , อัคคีภัย

- **<u>กลุ่ม สำนัก/กอง/ศูนย์สุขภาพจิต</u>**

7.2.1.3.9 ประเภทของข้อมูล

(1) Application

(2) ข้อมูลที่เป็น Database

(3) ข้อมูลของ Web Server

7.2.1.3.10 ประเภทของ Server

(1) Server ที่หน่วยงานใช้ของกรมฯ

(2) Sever ของหน่วยงานที่ฝากกรมฯดูแล

7.2.1.3.11 วิธีปฏิบัติ

(1) Administrator ของแต่ละหน่วยงานปฏิบัติการสำรองข้อมูล Application, Database, Web Server ของแต่ละหน่วยงาน

(2) กรณีเป็น Application ให้ทำการสำรองข้อมูลไว้ 2 สำเนา ไว้ที่สื่อที่ใช้ในการ Backup ได้แก่ แผ่น CD , แผ่น DVD, Tape Backup, External Hard disk ฯลฯ

(3) กรณี Database เช่น MySQL, SQL Server, Access, Oracle, ฯลฯ ให้ทำการสำรอง(Backup)ข้อมูล ไว้ที่สื่อที่ใช้ในการ Backup ได้แก่ แผ่น CD , แผ่น DVD, Tape Backup, External Hard disk ฯลฯ

(4) กรณี Web Server สำรอง(Backup)ข้อมูลไว้ที่สื่อที่ใช้ในการ Backup ได้แก่ แผ่น CD , แผ่น DVD, Tape Backup, External Hard disk ฯลฯ

(5) สื่อที่ใช้ในการ (Backup)ข้อมูลใน Server ได้แก่ แผ่น CD , แผ่น DVD, Tape Backup, External Hard disk ฯลฯ จะต้องถูกจัดเก็บไว้ที่ปลอดภัยและสามารถนำข้อมูลกลับมา Restore ใช้งานได้ทันที่เมื่อเกิดความเสี่ยงหรือภาวะวิกฤต เช่นถูกโจรกรรมข้อมูล, อัคคีภัย

7.2.1.3.12 ช่วงเวลาที่ปฏิบัติ

(1) วันหยุด

(2) ช่วงที่มีการใช้งานน้อยที่สุด

7.2.1.3.13 วิธีการ Backup

(1) Map Drive

(2) Manual

7.2.1.3.14 อุปกรณ์ที่ใช้ Backup

(1) External Hard disk

(2) Tape

(3) DVD

7.2.1.3.15 สถานที่จัดเก็บ : จะต้องจัดเก็บไว้ในที่ปลอดภัย และสามารถนำข้อมูลกลับมา Restore ใช้งานได้ทันทีเมื่อเกิดความเสี่ยงหรือภาวะวิกฤต เช่น ถูกโจรกรรมข้อมูล , อัคคีภัย

7.2.1.4 การวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์

7.2.1.4.1 วิธีปฏิบัติ

(1) ดำเนินการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ โดยใช้เครื่องคอมพิวเตอร์ชนิด Client ที่มีการ Fix IP Address

(2) ใช้โปรแกรม Internet Browser ในการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ โดยเข้าไปที่ Address ตามที่หน่วยงานกำหนด

(3) ใส่ User Name และ Password ตามที่กำหนด

(4) ที่หน้าจอของโปรแกรม ตรวจสอบสถานะของอุปกรณ์ว่าเข้าสู่ระบบได้หรือไม่ และระบบช้าหรือไม่

(5) ตรวจสอบสถานะของ System Resource CPU Usage ใช้ไปแล้วร้อยละเท่าไร หรือดูจาก Gauge (Meter) ว่าชี้ในช่วงใด (สีเขียว หรือ สีเหลือง หรือ สีแดง) หรือแสดงลักษณะอื่นที่บ่งบอกสถานะและระดับการใช้งาน

- Memory Usage ใช้ไปแล้วร้อยละเท่าไร หรือดูจาก Gauge (Meter) ว่าชี้ในช่วงใด (สีเขียว หรือ สีเหลือง หรือ สีแดง) หรือแสดงลักษณะอื่นที่บ่งบอกสถานะและระดับการใช้งาน
- Fortianalyser Usage ใช้ไปแล้วร้อยละเท่าไร หรือดูจาก Gauge (Meter) ว่าชี้ในช่วงใด (สีเขียว หรือ สีเหลือง หรือ สีแดง)

(6) ตรวจสอบสถานะของ Top Session จะแสดง Bar chart เลือกกด Bar chart ที่สูงสุดหรือที่สนใจ จะได้ report และพิมพ์ผลของ report

(7) ตรวจสอบสถานะของ Usage จะแสดง Bar chart เลือกกด Bar chart ที่สูงสุดหรือที่สนใจ จะได้ report และพิมพ์ผลของ report

(8) ตรวจสอบสถานะของ Alert Message Console เพื่อดู Message ที่ผิดปกติ เลือกกด Detail จะได้ report และพิมพ์ผลของ report

(9) ตรวจสอบสถานะของ Log and Architecture เพื่อดู Protocol ที่สนใจ เช่น Http, Https, E-mail, FTP, Log-Average, IPS- Intension Prevention System, Event Occur เลือกกด Detail จะได้ report และพิมพ์ผลของ report

(10) ดำเนินการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ ตามผลจาก Report ที่ได้รับเสนอให้ผู้อำนวยการทราบและพิจารณาเป็นประจำทุกสัปดาห์หรือตามความเหมาะสม

7.2.1.4.2 ความถี่ในการปฏิบัติ

(1) สัปดาห์ครั้ง

7.2.1.4.3 ช่วงเวลาที่ปฏิบัติ

(1) วันหยุด

(2) ตามความเหมาะสมของแต่ละหน่วยงาน

7.2.1.4.4 แบบฟอร์มการบันทึกผลการปฏิบัติ : รายงานผลการวิเคราะห์

7.2.1.4.4.1 วิธีการวิเคราะห์ โดยใช้โปรแกรม

(1) Schedule

(2) Manual

7.2.1.4.4.2 สถานที่จัดเก็บ : แฟ้มรวบรวมผลการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์

<u>กรณี โรงพยาบาล/สถาบัน/ศูนย์สุขภาพจิต</u> การวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์อาจใช้ Hardware หรือ Software ตามบริบทที่แต่ละหน่วยงานมีอยู่ โดยดำเนินการวิเคราะห์ตรวจสอบสถานะของ System Resource, Top Session, สถานะของ Usage, สถานะของ Log และจัดทำ Report เสนอให้ผู้อำนวยการทราบและพิจารณาเป็นประจำทุกสัปดาห์หรือตามความเหมาะสม

7.2.1.5 การควบคุมผู้ใช้คอมพิวเตอร์

7.2.1.5.1 ประเภทของผู้ใช้คอมพิวเตอร์ แบ่งออกเป็น 2 กลุ่ม คือ

(1) บุคลากรของหน่วยงาน

(2) บุคลากรที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้รับผิดชอบในการดูแลเครื่องคอมพิวเตอร์และอุปกรณ์

7.2.1.5.2 วิธีปฏิบัติในการควบคุมผู้ใช้คอมพิวเตอร์

(1) หัวหน้าส่วนราชการ/ผู้อำนวยการของแต่ละหน่วยงาน ลงนามในหนังสือมอบหมาย/กำหนด/คำสั่งแต่งตั้งผู้รับผิดชอบหลักและรอง (ควรมี

ข้าราชการ 1 คน) ดูแลเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงภายในหน่วยงาน

(2) หัวหน้าฝ่าย/หัวหน้ากลุ่มงาน ภายในแต่ละหน่วยงานมีหน้าที่ดูแลและควบคุมกำกับ ผู้รับผิดชอบดูแลเครื่องคอมพิวเตอร์นั้น ให้ปฏิบัติตามวิธีปฏิบัติงานบำรุงรักษาเครื่องคอมพิวเตอร์ อย่างสม่ำเสมอ ตามกำหนดเวลา

(3) กรณีเจ้าหน้าที่นำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้ปฏิบัติงานภายในหน่วยงาน/ในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน กำหนดให้ดำเนินการตามระเบียบปฏิบัติที่ : 0800-301-004 เรื่อง การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เช่นเดียวกับเครื่องคอมพิวเตอร์ภายในหน่วยงาน

7.2.1.5.3 ความถี่ในการปฏิบัติ ทุกแห่ง

7.2.1.5.4 ช่วงเวลาที่ปฏิบัติ หลังจากที่ได้รับการจัดสรรครุภัณฑ์คอมพิวเตอร์

7.2.1.6 การควบคุมผู้ใช้บริการ

7.2.1.6.1. ผู้ขอใช้บริการบันทึกขอมี User Name และ Password เพื่อเสนอต่อผู้อำนวยการฯ เป็นผู้ลงนามอนุญาต โดยใช้แบบฟอร์มการขอเข้าระบบเครือข่ายและการเข้าใช้งานในระบบคอมพิวเตอร์(0804-401-022) หรือแบบฟอร์มตามที่หน่วยงานกำหนด

7.2.1.6.2. ผู้อำนวยการ มอบหมายให้หัวหน้ากลุ่มพัฒนาข้อมูลและสารสนเทศ เพื่อพิจารณาอนุญาต

7.2.1.6.3. กรณีไม่อนุญาต หัวหน้ากลุ่มพัฒนาข้อมูลและสารสนเทศ แจ้งกลับผู้ขอใช้บริการทราบ

7.2.1.6.4. กรณีอนุญาต เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ ดำเนินการ Add user ให้บันทึกลงในรายชื่อผู้ขอใช้ระบบโดยใช้แบบฟอร์มจากเครื่องคอมพิวเตอร์แม่ข่ายเรียงตามลำดับตัวอักษร

7.2.1.6.5. จัดส่ง Username และ Password ที่เป็นความลับของแต่ละบุคคลที่สามารถเข้าระบบเครือข่ายและซักซ้อมความเข้าใจเรื่องการใช้บริการระบบเครือข่ายท้องถิ่น (LAN) ของหน่วยงาน

7.2.1.7 การยกเลิกการเข้าใช้งานในระบบเครือข่าย

7.2.1.7.1 ประเภทของงาน การยกเลิกการเข้าใช้งานในระบบเครือข่าย แบ่งออกเป็น 2 ประเภท คือ

(1) บุคลากรของหน่วยงานมีการลาออก ย้ายหน่วยงาน เสียชีวิต ฯลฯ

(2) บุคลากรที่ไม่ปฏิบัติตามข้อกำหนด

7.2.1.7.2 วิธีปฏิบัติในการยกเลิกการเข้าใช้งานในระบบเครือข่าย

(1) กลุ่มพัฒนาข้อมูลและสารสนเทศ ของแต่ละหน่วยงาน สำรวจรายชื่อสมาชิก โดยส่งรายชื่อสมาชิกที่เข้าระบบเครือข่ายฯให้แต่ละหน่วยงานตรวจสอบรายชื่อผู้ที่ปฏิบัติงานจริงปีละ 1 ครั้ง ประมาณเดือนกันยายน

(2) กรณีสมาชิกฯในแต่ละหน่วยงานมีการลาออก ย้ายหน่วยงาน เสียชีวิต ฯลฯ ให้แจ้งหัวหน้าฝ่าย/กลุ่มพัฒนาข้อมูลและสารสนเทศ ทราบ และดำเนินการคัดชื่อออกหรือปิดการให้บริการ

(3) กำหนดระเบียบปฏิบัติเมื่อสมาชิกไม่ปฏิบัติตามข้อกำหนด

- กลุ่มพัฒนาข้อมูลและสารสนเทศ แจ้งรายชื่อผู้ที่ไม่ปฏิบัติตามข้อกำหนดให้แก่ผู้บังคับบัญชาได้รับทราบ
- กลุ่มพัฒนาข้อมูลและสารสนเทศ ทบทวนเรื่องกฎ ระเบียบ บทลงโทษ และดำเนินการตามขั้นตอนที่กำหนดไว้ในระเบียบ
- ตรวจสอบการไม่ปฏิบัติตามข้อกำหนดของสมาชิก
- หากไม่เป็นไปตามข้อกำหนดให้ปฏิบัติตามที่ระเบียบกำหนด
- หากปฏิบัติตามตามข้อกำหนด สามารถเข้าใช้ระบบได้ตามระเบียบ

7.2.1.7.3 ความถี่ในการปฏิบัติ

(1) ตรวจสอบรายชื่อผู้ที่ปฏิบัติงานจริงปีละ 1 ครั้ง

(2) เมื่อมีสมาชิกฯในแต่ละหน่วยงานมีการลาออก ย้ายหน่วยงาน เสียชีวิต ฯลฯ

7.2.1.7.4 ช่วงเวลาที่ปฏิบัติ ประมาณเดือนกันยายน หรือเมื่อมีสมาชิกฯในแต่ละหน่วยงานมีการลาออก ย้ายหน่วยงาน เสียชีวิต ฯลฯ

7.2.1.7.5 การบันทึกผลการปฏิบัติ แบบสำรวจรายชื่อสมาชิก

7.2.1.8 การปรับปรุงทะเบียนผู้ใช้บริการในระบบเครือข่ายคอมพิวเตอร์ (User)

7.2.1.8.1 การปรับปรุงทะเบียนผู้ใช้บริการ ให้แก่บุคลากรในหน่วยงาน

7.2.1.8.2 วิธีปฏิบัติ

(1) คณะทำงานบริหารความเสี่ยงฯของแต่ละหน่วยงาน ทำการสำรวจ/ตรวจสอบรายชื่อบุคลากรทุกคนในหน่วยงานปีละ 1 ครั้ง ประมาณเดือนกันยายน และแจ้งผลการสำรวจ/ตรวจสอบ ไปยังกลุ่มพัฒนาข้อมูลและสารสนเทศ ของแต่ละหน่วยงาน เพื่อ Update ฐานข้อมูลผู้ใช้ระบบเครือข่ายคอมพิวเตอร์

(2) กรณี User คนใดไม่ได้อยู่ปฏิบัติงานในหน่วยงาน(ลาออก, ย้ายหน่วยงาน, เสียชีวิต ฯลฯ) คณะทำงานฯ ของหน่วยงาน จะต้องแจ้ง ชื่อ-สกุลของ User นั้นๆ ให้ชัดเจนพร้อมผลการสำรวจ/ตรวจสอบ

(3) กรณี เพิ่ม User ให้คณะทำงานฯของหน่วยงาน รวบรวมแบบฟอร์มการขอเข้าใช้งานในระบบเครือข่ายและเข้าใช้งานใน Data Bank (0804-401-022) ของเจ้าหน้าที่ ที่ประสงค์ขอเข้าใช้บริการระบบเครือข่ายฯ (รายใหม่) และทำหนังสือจากหน่วยงาน เรียนผู้อำนวยการฯ เพื่อพิจารณาดำเนินการสมัคร/อนุญาตสิทธิ์การเข้าใช้บริการระบบเครือข่ายฯ ต่อไป

(4) ผู้ใช้บริการในระบบเครือข่ายคอมพิวเตอร์ (User) ทุกคน ต้อง Logon เข้าสู่ระบบเครือข่ายฯ / ระบบ Data Center ของหน่วยงาน ด้วย Username และ Password ของตนเองเท่านั้น และเมื่อเสร็จสิ้นภารกิจ ต้องทำการ Logout ทุกครั้ง เพื่อป้องกันผู้อื่นแอบอ้างชื่อ User ใช้กระทำความผิดใดๆ ในระบบเครือข่ายทั้งภายในและภายนอก (Internet)

7.2.1.8.3 ความถี่ในการปฏิบัติ ปีละ 1 ครั้ง

7.2.1.8.4 ช่วงเวลาที่ปฏิบัติ ประมาณเดือนกันยายน

7.2.1.8.5 การบันทึกผลการปฏิบัติ ตามแบบสำรวจ/ตรวจสอบรายชื่อบุคลากร

กลุ่มผู้รับผิดชอบดูแลระบบคอมพิวเตอร์

7.2.1.9 งานบำรุงรักษาเครื่องคอมพิวเตอร์

7.2.1.9.1 ประเภทของเครื่องคอมพิวเตอร์

(1) เครื่องคอมพิวเตอร์ของหน่วยงานราชการ

(2) เครื่องคอมพิวเตอร์ที่เช่า

7.2.1.9.2 วิธีปฏิบัติ

7.2.1.9.2.1 การทำความสะอาด กำหนดให้

7.2.1.9.2.1.1 ทำความสะอาด อุปกรณ์ภายนอก

(1) ตัวเครื่องและจอภาพ : ใช้ผ้าแห้งหรือใช้น้ำยาเฉพาะจอภาพ เช็ดทำความสะอาด อย่างน้อยเดือนละ 1 ครั้ง

(2) อุปกรณ์ต่อพ่วงต่างๆ เช่น Mouse Keyboard (มีการเคาะฝุ่นด้วย) UPS Printer Scanner ใช้ผ้าแห้งทำความสะอาด หรือใช้น้ำยาเฉพาะ โดยทำความสะอาดอย่างน้อยเดือนละ 1 ครั้ง

7.2.1.9.2.1.2 ทำความสะอาดอุปกรณ์ภายใน

(1) ใช้วิธีการเป่าอย่างน้อยปีละ 1 ครั้ง โดยเจ้าหน้าที่ IT หรือจ้างหน่วยงานภายนอก

7.2.1.9.2.2 การบำรุงรักษา Hard Disk

7.2.1.9.2.2.1 กำหนดให้ลบไฟล์ที่เป็นไฟล์ขยะ เช่น Temporary Files, Temporary Internet Files, Cookies Files และทำการ Empty ไฟล์ใน Recycle Bin เพื่อลบอย่างถาวร อย่างน้อยเดือนละ 1 ครั้ง

7.2.1.9.2.2.2 กำหนดให้ ทำการตรวจสอบ/จัดระเบียบ Hard Disk ด้วยโปรแกรม Scandisk / Disk Defragmenter ใน System tools อย่างน้อยเดือนละ 1 ครั้ง ทั้งนี้เพื่อรักษาประสิทธิภาพในการจัดเก็บ/เข้าถึงข้อมูล

7.2.1.9.3 ความถี่ในการปฏิบัติ

7.2.1.9.3.1 ทำความสะอาดอุปกรณ์ภายนอก และ ภายใน อย่างน้อยเดือนละ 1 ครั้ง

7.2.1.9.3.2 การบำรุงรักษา Hard Disk อย่างน้อยเดือนละ 1 ครั้ง

7.2.1.9.4 ช่วงเวลาที่ปฏิบัติ ตามความเหมาะสมของแต่ละหน่วยงาน

7.2.1.9.5 การบันทึกผลการปฏิบัติ

7.2.1.9.5.1 สร้าง Folder ใหม่ขึ้นที่ Desktop ของเครื่องคอมพิวเตอร์ ชื่อ “Maintenance” และภายใน Maintenance สร้าง Folder เพิ่มเติมชื่อ “Defragmenter” แต่ในกรณี window ใหม่ ให้ capture ไว้ที่ Desktop เพื่อป้องกัน Drive C มีปัญหา

7.2.1.9.5.2 ในวิธีปฏิบัติ เรื่อง การบำรุงรักษา Hard Disk เมื่อดำเนินการ Defragmenter เสร็จเรียบร้อยแล้ว ให้เลือกกด View เพื่อดูผลของการ จัดระเบียบ Hard Disk ด้วยโปรแกรม Disk Defragmenter กด Save ไปเก็บไว้ที่ Folder Maintenance/ Defragmenter ที่สร้างไว้ โดยตั้งชื่อ File ว่า “ DDMMYYYY.txt “ ตามวันเดือนปี ที่ดำเนินการ แต่ในกรณี window ใหม่ ให้ capture ไว้ที่ Desktop

7.2.1.10 การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer

7.2.1.10.1 ประเภทของงาน การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer

7.2.1.10.1.1 เครื่องคอมพิวเตอร์ของหน่วยงาน

7.2.1.10.1.2 เครื่องคอมพิวเตอร์ที่เช่า

7.2.1.10.1.3 เครื่องคอมพิวเตอร์ส่วนตัวที่นำมาใช้ในหน่วยงาน ยกเว้น เครื่องคอมพิวเตอร์ที่ไม่ได้ต่อเข้ากับระบบ LAN ของหน่วยงาน

7.2.1.10.2 วิธีปฏิบัติ

7.2.1.10.2.1 คอมพิวเตอร์ที่นำมาใช้งานในระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานจะต้องมีการติดตั้งโปรแกรมป้องกัน Virus Computer

7.2.1.10.2.2 การตรวจจับ Virus Computer กำหนดให้

(1) Update / ตรวจสอบการ Update รายชื่อ Virus computer (Definition Antivirus Table Files) อย่างน้อยสัปดาห์ละ 1 ครั้ง

(2) Scan Virus แบบ Full System อย่างน้อยสัปดาห์ละ 1 ครั้ง

7.2.1.10.3 ความถี่ในการปฏิบัติ

7.2.1.10.3.1 ติดตั้งโปรแกรมป้องกัน Virus Computer เมื่อได้รับเครื่องคอมพิวเตอร์

7.2.1.10.3.2 การตรวจจับ Virus Computer อย่างน้อยสัปดาห์ละ 1 ครั้ง

7.2.1.10.4 ช่วงเวลาที่ปฏิบัติ ตามความเหมาะสมของแต่ละหน่วยงาน

7.2.1.10.5 การบันทึกผลการปฏิบัติ โดยดำเนินการ

7.2.1.10.5.1 สร้าง Folder ใหม่ขึ้นที่ Desktop ของเครื่องคอมพิวเตอร์ ชื่อ “Maintenance” และภายใน Maintenance สร้าง Folder เพิ่มเติมชื่อ “Scan Virus”

7.2.1.10.5.2 ในวิธีปฏิบัติ เรื่อง การตรวจจับ Virus computer เมื่อดำเนินการ Scan virus ให้เลือกกด View หรือ Capture ผลไว้ เพื่อดูผลของการ Scan Virus แบบ Full System กด Save ไปเก็บไว้ที่ Folder Maintenance/Scan Virus ที่สร้างไว้ โดยตั้งชื่อ File ว่า “ DDMMYYYY.txt “ ตามวันเดือนปี ที่ดำเนินการ

7.2.1.11 การบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center

7.2.1.11.1 ประเภทของ การบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) กรณี

7.2.1.11.1.1 สำนัก/กอง/กลุ่ม และศูนย์สุขภาพจิตที่มีสำนักงานตั้งอยู่ในอาคารกรมสุขภาพจิต

7.2.1.11.1.2 ศูนย์สุขภาพจิตที่มีสำนักงานตั้งอยู่นอกอาคารกรมสุขภาพจิต

7.2.1.11.1.3 สถาบัน/โรงพยาบาลในสังกัดกรมสุขภาพจิต

7.2.1.11.2 วิธีปฏิบัติ

7.2.1.11.2.1 กรณี สำนัก/กอง/กลุ่ม และศูนย์สุขภาพจิตที่มีสำนักงานตั้งอยู่ในอาคารกรมสุขภาพจิต

(1) ผู้ใช้บริการในระบบเครือข่ายคอมพิวเตอร์จะต้อง Logon เข้าสู่ระบบด้วย User name ของตนเอง

(2) Map Network Drive ของเครื่องคอมพิวเตอร์ที่ใช้งานไปยัง path: \\dmh_data1\databank ตามคู่มือการใช้งาน Data Center

(3) นำข้อมูลที่สำคัญตามภารกิจของแต่ละหน่วยงานบันทึกเก็บรวมกันไว้เป็น Folder ใน Data Bank จำแนกตามระดับของหน่วยงาน เช่น ฝ่าย/กลุ่มงาน ภายใต้กอง/ สำนัก/กลุ่ม/ศูนย์ ทั้งนี้ขึ้นอยู่กับภารกิจที่อยู่ในความรับผิดชอบของแต่ละบุคคล

7.2.1.11.2.2 กรณีศูนย์สุขภาพจิตที่มีสำนักงานตั้งอยู่นอกอาคารกรมสุขภาพจิต

(1) ผู้ดูแลระบบ ICT ของหน่วยงาน จัดหาเครื่องคอมพิวเตอร์ 1 เครื่อง และตั้งค่าระบบปฏิบัติการให้ทำหน้าที่เป็น File Sharing Server หรือ Data Bank และรองรับการ Access เข้าใช้งานข้อมูลที่จัดเก็บอยู่ภายใน (Map Drive) จากเครื่องลูกข่ายในระบบเครือข่ายคอมพิวเตอร์ภายใน (LAN) ของหน่วยงานได้

(2) ผู้ดูแลระบบ ICT ของหน่วยงาน ควรสร้าง Folder ที่ใช้ในการจัดเก็บข้อมูลที่สำคัญตามระเบียบปฏิบัติของศูนย์สุขภาพจิต เช่น

(2.1) งานบริหารทั่วไป ประกอบด้วย

- งานธุรการ
- งานการเจ้าหน้าที่
- งานการเงินและบัญชี
- งานพัสดุ
- งานยานพาหนะ
- งานโครงสร้างพื้นฐาน
- งานดูแลสภาพแวดล้อมในการทำงาน
- งานควบคุมเอกสาร
- การตรวจประเมินภายใน

(2.2) งานพัฒนาวิชาการ ประกอบด้วย

- การรับนโยบายหรือความต้องการ
- การวางแผน
- การดำเนินงาน
- การประเมินผล
- การรายงานผล
- งานโครงการพิเศษ

(2.3) การบริหารความเสี่ยง

- การบริหารความเสี่ยง
- การควบคุมความไม่สอดคล้อง

(3) ผู้ดูแลระบบ ICT ของหน่วยงาน กำหนดระยะเวลาที่ชัดเจนในแต่ละวัน ให้บุคลากรทุกคน นำข้อมูลสำคัญที่อยู่ในความรับผิดชอบ บันทึก/จัดเก็บ ลงใน Folder ที่สร้างไว้

(4) ผู้ดูแลระบบ ICT ของหน่วยงาน กำหนดระยะเวลาในการ Scan Virus Computer และการสำรองข้อมูล (Back up) ในเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Data Bank เพื่อความปลอดภัยของข้อมูล เช่น กำหนดให้จัดเก็บในแผ่น CD หรือ External Hard disk ทุกวันพุธ และศุกร์ เวลา 17.00 น. เป็นต้น

7.2.1.11.2.3 กรณี สถาบัน/โรงพยาบาลในสังกัดกรมสุขภาพจิต

(1) ให้มีการจัดทำ Data Center ตามบริบทของหน่วยงาน

(2) กำหนดภารกิจที่สำคัญเพื่อนำข้อมูลเข้าสู่ Data Center

(3) กำหนดสิทธิ์การเข้าถึง

7.2.1.11.3 ความถี่ในการปฏิบัติ ทุกครั้งที่มีการบันทึกข้อมูลที่สำคัญ (ตามภารกิจ)

7.2.1.11.4 ช่วงเวลาที่ปฏิบัติ ตามความเหมาะสมของแต่ละหน่วยงาน

7.2.1.11.5 การบันทึกผลการปฏิบัติ ตามความเหมาะสมของแต่ละหน่วยงาน

7.3 แบบฟอร์ม ได้แก่

7.3.1 แบบฟอร์มการขอเข้าระบบเครือข่ายและเข้าใช้งานใน Data Bank (0804-401-022)

7.3.2 แผนการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารกรมสุขภาพจิต ปีงบประมาณ 2551 (0804-402-009)

7.3.3 รายงานการประเมินความเสี่ยงการบันทึกข้อมูลที่สำคัญลงใน Databank (0804-402-011)

7.3.4 รายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต (0804-402-014)

7.3.5 รายงานการค้นหาความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต (0804-402-013)

7.3.6 บัญชีความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสารของกรมสุขภาพจิต (0804-402-015)

7.3.7 แบบบันทึกการดูแลบำรุงเครื่องคอมพิวเตอร์แม่ข่ายของกรมสุขภาพจิต

7.4 เอกสารอื่น ๆ

7.4.1 คู่มือการบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center

8. การควบคุมเอกสาร

ลำดับ	ชื่อเอกสาร	รหัส	สถานที่จัดเก็บ	ผู้รับผิดชอบ	การจัดเก็บ	ระยะเวลา	ผู้เข้าถึง
1	แผนการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารกรมสุขภาพจิต	0804-402-009	กลุ่มพัฒนาข้อมูลและสารสนเทศ	เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ	เรียงลำดับวัน/เดือน/ปี	อย่างน้อยปีละ 1 ครั้ง	เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ
2	รายงานการประเมินความเสี่ยงการบันทึกข้อมูลที่สำคัญลงใน Databank	0804-402-011	กลุ่มพัฒนาข้อมูลและสารสนเทศ	เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แต่ละเครื่อง	เรียงลำดับวัน/เดือน/ปี	ทุกครั้งที่ปฏิบัติงาน	เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ
3	รายงานการค้นหาความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต	0804-402-013	กลุ่มพัฒนาข้อมูลและสารสนเทศ	คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร	เรียงลำดับวัน/เดือน/ปี	ปีละ 2 ครั้ง	คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
4	รายงานการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต	0804-402-014	กลุ่มพัฒนาข้อมูลและสารสนเทศ	เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ	เรียงลำดับวัน/เดือน/ปี	ปีละ 1 ครั้ง	เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ
5	บัญชีความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต	0804-402-015	กลุ่มพัฒนาข้อมูลและสารสนเทศ	คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร	เรียงลำดับวัน/เดือน/ปี	ทุกครั้งที่ปฏิบัติงาน	คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
6	แบบฟอร์มการขอเข้าระบบเครือข่ายและเข้าใช้งานใน Databank	0804-401-022	กลุ่มพัฒนาข้อมูลและสารสนเทศ	เจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ	เรียงลำดับวัน/เดือน/ปี	ทุกครั้งที่ปฏิบัติงาน	ผู้ใช้บริการในระบบเครือข่ายคอมพิวเตอร์ (User)

9. ภาคผนวก

9.1 ผังกระบวนงาน (Flowchart) ไม่มี

9.2 ดัชนีชี้วัดและเป้าหมายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ดัชนีชี้วัด	เป้าหมาย	ผู้รับผิดชอบ
1	ผู้ใช้บริการในระบบเครือข่ายคอมพิวเตอร์ของกรมสุขภาพจิตต้องมี Username และ Password ในการ Logon เข้าสู่ระบบ	ร้อยละ 85	คณะทำงานบริหารความเสี่ยงด้าน ICT ของแต่ละหน่วยงาน
2	มีรายชื่อผู้รับผิดชอบในการดูแลและบำรุงรักษาคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์	ร้อยละ 100	คณะทำงานบริหารความเสี่ยงด้าน ICTของแต่ละหน่วยงาน
3	เครื่องคอมพิวเตอร์ได้รับการดูแลและบำรุงรักษาตามวิธีปฏิบัติที่กำหนด	ร้อยละ 85	ผู้ได้รับมอบหมายให้รับผิดชอบในการดูแลคอมพิวเตอร์
4	มีการนำข้อมูลตามภารกิจของแต่ละหน่วยงานจัดเก็บไว้ใน Data Center	ร้อยละ 80	ผู้ปฏิบัติงานตามภารกิจของหน่วยงาน
5	เครื่องคอมพิวเตอร์แม่ข่ายได้รับการดูแลและบำรุงรักษาตามเกณฑ์ที่กำหนดการควบคุม Server	ร้อยละ 100	ผู้ได้รับมอบหมายให้รับผิดชอบในการดูแลระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงาน

แผนการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารกรมสุขภาพจิต (0804-402-009)

กิจกรรม	ตค	พย	ธค	มค	กพ	มีค	เมย	พค	มิย	กค	สค	กย	ผู้รับผิดชอบ
1. นิเทศงานหรือประชุมชี้แจงการดูแลและบำรุงรักษาคอมพิวเตอร์			↔										คณะทำงานบริหารความเสี่ยงฯของกรม
2. การค้นหาความเสี่ยงด้านเทคโนโลยี สารสนเทศ และการสื่อสาร						↔						↔	คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการสื่อสารของแต่ละหน่วยงาน
3. การประเมินความเสี่ยงด้านเทคโนโลยี สารสนเทศ และการสื่อสาร												↔	คณะทำงานบริหารความเสี่ยงฯของกรม
4. การจัดการความเสี่ยงด้านเทคโนโลยี สารสนเทศ และการสื่อสาร						↔						↔	คณะทำงานบริหารความเสี่ยงฯของกรม
5. การประเมินผล			↔										คณะทำงานบริหารความเสี่ยงฯของกรม