

คู่มือการปฏิบัติงาน

กระบวนการ การบริการ ระเบียบปฏิบัติ

สำหรับผู้ดูแลระบบ



โรงพยาบาลเมืองจันทร์

ศูนย์เทคโนโลยีสารสนเทศ

สารบัญ

	หน้า
1. วัตถุประสงค์	1
2. ขอบเขต	1
3. คำจำกัดความ	1
4. หน้าที่ความรับผิดชอบ	2
5. Work Flow กระบวนการการปฏิบัติงานการบริการด้านระบบคอมพิวเตอร์และเครือข่าย	3
5.1 ขั้นตอนการรับบริการขอคำปรึกษาทางโทรศัพท์	3
5.2 ขั้นตอนการรับบริการซ่อมบำรุง	4
6. ขั้นตอนการปฏิบัติงาน	5
6.1 ขั้นตอนการรับบริการขอคำปรึกษาทางโทรศัพท์	5
6.2 ขั้นตอนการรับบริการซ่อมบำรุง ผู้รับบริการ	5
7. มาตรฐานคุณภาพงาน	6
8. ระบบติดตามประเมินผล	7
9. เอกสารอ้างอิง	7
10. แบบฟอร์ม	7
ภาคผนวก	
ภาคผนวก ก พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560	9
ภาคผนวก ข คำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	22
ภาคผนวก ค แบบฟอร์มที่ใช้	25
ภาคผนวก ง ระเบียบปฏิบัติ	27
การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ	28
การจัดการกับเอกสารที่เกี่ยวข้องกับระบบ	29
การจัดการระบบเครือข่าย	30
การจัดการ การลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่	31
การใช้งานห้อง Data Center	32
การจัดการทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย	33
การกำจัดไวรัสคอมพิวเตอร์	34
การสำรองข้อมูล	35
การจัดเก็บข้อมูลตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560	36

สารบัญ (ต่อ)

	หน้า
การลงทะเบียนและควบคุมการเข้าถึงระบบ	37
การพัฒนาระบบงาน.....	38
การปฏิบัติกรณเีรื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์เครือข่ายขัดข้อง	39
การปฏิบัติกรณเีเกิดอัคคีภัย	41
การรักษาความลับของผู้ที่เข้าถึงข้อมูลผู้ป่วย.....	42
การรักษาความปลอดภัย การป้องกันการสูญหายของแฟ้มเวชระเบียนที่จัดเก็บในรูปแบบ Electronic file	43
แนวทางปฏิบัติการแจ้งบัญชีผู้ใช้งาน สำหรับบุคลากรภายนอก ที่ถูกเชิญมาปฏิบัติงานแทนผู้ดูแลระบบ	44
การปฏิบัตินอกเวลาราชการของผู้ดูแลระบบ.....	45



คู่มือการปฏิบัติงาน กระบวนการ การบริการ ICT Service Center

1. วัตถุประสงค์

- 1.1 เพื่อให้จัดมีการจัดคู่มือการปฏิบัติงานที่ชัดเจน อย่างเป็นลายลักษณ์อักษรที่แสดงถึงรายละเอียด ขั้นตอนการปฏิบัติงานของกิจกรรม/กระบวนการต่างๆ ของหน่วยงาน และสร้างมาตรฐาน การปฏิบัติงาน ที่มุ่งไปสู่การบริหารคุณภาพทั่วทั้งองค์กรอย่างมีประสิทธิภาพ เกิดผลงานที่ ได้มาตรฐานเป็นไปตามเป้าหมาย ได้ผลิตผลหรือการบริการที่มีคุณภาพและบรรลุข้อกำหนดที่สำคัญ ของกระบวนการ
- 1.2 เพื่อเป็นหลักฐานแสดงวิธีการทำงานที่สามารถถ่ายทอดให้กับผู้เข้ามาปฏิบัติงานใหม่ พัฒนา ให้การทำงานเป็นมืออาชีพ และใช้ประกอบการประเมินผลการปฏิบัติงานของบุคลากร รวมทั้งแสดง หรือเผยแพร่ให้กับบุคคลภายนอก หรือผู้ใช้บริการ ให้สามารถเข้าใจและใช้ประโยชน์จากกระบวนการ ที่มีอยู่ เพื่อขอการรับบริการที่ตรงกับความต้องการ
- 1.3 เพื่อให้การปฏิบัติงานการบริการด้านระบบคอมพิวเตอร์และเครือข่ายของงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เป็นไปอย่างมีมาตรฐาน มีกำหนดระยะเวลาการให้บริการที่ ชัดเจน และยกระดับการให้บริการของงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ให้มีประสิทธิภาพและสามารถให้บริการได้อย่างต่อเนื่อง

2. ขอบเขต

คู่มือการปฏิบัติงานนี้ครอบคลุมขั้นตอนการบริการด้านระบบคอมพิวเตอร์และเครือข่ายของงาน ประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ตั้งแต่ขั้นตอนการรับบริการขอคำปรึกษาทาง โทรศัพท์ ขั้นตอนการรับบริการซ่อมบำรุง ข้อตกลงระยะเวลาการให้บริการ แผนการดำเนินงานศูนย์บริการ ให้คำปรึกษาแนะนำ และแก้ไขปัญหาทางด้านเทคนิค รวมถึงการรายงานและติดตามประเมินผล

3. คำจำกัดความ

มาตรฐาน หมายถึง สิ่งที่เราเป็นเกณฑ์สำหรับเทียบกำหนด ทั้งในด้านปริมาณและคุณภาพ (พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2542) มาตรฐานการปฏิบัติงาน (Performance standard) เป็นผลการปฏิบัติงานในระดับใดระดับหนึ่ง ซึ่งถือว่าเป็นเกณฑ์ที่น่าพอใจหรืออยู่ในระดับที่ผู้ปฏิบัติงาน ส่วนใหญ่ทำได้ โดยจะมีกรอบในการพิจารณากำหนด มาตรฐานหลายๆ ด้าน อาทิ ด้านปริมาณ คุณภาพ ระยะเวลา ค่าใช้จ่าย หรือพฤติกรรมของผู้ปฏิบัติงาน

IT Help Desk หมายถึง ศูนย์บริการให้ความช่วยเหลือ และแก้ไขปัญหาด้านระบบคอมพิวเตอร์ และเครือข่าย

ผู้รับบริการ หมายถึง ข้าราชการและเจ้าหน้าที่ผู้ปฏิบัติงานของโรงพยาบาลเมืองจันทร์

ผู้ประสานงานด้านเทคนิค หมายถึง เจ้าหน้าที่ผู้ประสานงานด้านการให้ความช่วยเหลือและแก้ไข ปัญหาด้านระบบคอมพิวเตอร์และเครือข่ายของงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

เจ้าหน้าที่ผู้ปฏิบัติงาน หมายถึง เจ้าหน้าที่ผู้รับมอบหมายให้ดำเนินการให้ความช่วยเหลือและแก้ไข ปัญหาด้านระบบคอมพิวเตอร์และเครือข่ายของงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

SLA (Service Level Agreement) หมายถึง ข้อตกลงเพื่อรับประกันการบริการระหว่างผู้ให้บริการกับผู้รับบริการ เพื่อเพิ่มความมั่นใจแก่ผู้รับบริการว่าเจ้าหน้าที่จะสามารถให้บริการได้ตามระยะเวลา แต่ละกระบวนการที่กำหนดไว้ ไม่ถือเป็นข้อผูกพัน อาจมีการเปลี่ยนแปลงได้

ไบเสนอ/ส่งซ่อม/ติดตั้ง หมายถึง แบบบันทึกการรับแจ้งขอความช่วยเหลือและแก้ไขปัญหาด้านระบบคอมพิวเตอร์ และเครือข่าย

4. หน้าที่ความรับผิดชอบ

- 4.1 ผู้อำนวยการงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทำหน้าที่อนุมัติแผนการดำเนินงานพร้อมทั้งมอบหมาย กำกับ ติดตามการปฏิบัติงานของผู้ที่ได้รับมอบหมาย
- 4.2 คณะทำงานบริการและจัดการความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารมีหน้าที่ความรับผิดชอบ ดังต่อไปนี้
 - 4.2.1 จัดทำแผนการดำเนินงานและแนวทางการบริหารจัดการระบบการให้บริการและจัดการความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
 - 4.2.2 บริหารจัดการระบบการให้บริการและจัดการด้านความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารให้สามารถดำเนินการตามแผนและแนวทางได้อย่างมีประสิทธิภาพ
 - 4.2.3 ประสาน ติดตามการดำเนินงาน และรวบรวมข้อมูล รวมถึงรายงานผลการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้บริหาร
 - 4.2.4 ส่งเสริมให้เกิดการถ่ายทอดองค์ความรู้ระดับหน่วยงานและผู้ปฏิบัติงาน ให้สามารถนำความรู้ไปใช้สนับสนุนในการปฏิบัติงาน

5. Work Flow กระบวนการการปฏิบัติงานการบริการด้านระบบคอมพิวเตอร์และเครือข่าย

5.1 ขั้นตอนการรับบริการขอคำปรึกษาทางโทรศัพท์ หมายเลข 112

ลำดับ	กระบวนการ	ระยะเวลา (นาที)	รายละเอียดงาน	ผู้รับผิดชอบ
1	แจ้งปัญหา/ขอรับ ความช่วยเหลือ	6 นาที	ผู้ประสานงานด้านเทคนิครับแจ้งขอรับ บริการ พร้อมแนวทางแก้ไขปัญหาเบื้องต้น (ใบเสนอ/ส่งซ่อม/ติดตั้ง)	ผู้รับบริการ/ ผู้ประสานงาน ด้านเทคนิค
2			ผู้ประสานงานด้านเทคนิค จัดเจ้าหน้าที่เพื่อดำเนินการ	ผู้ประสานงาน ด้านเทคนิค
3			ผู้ประสานงานด้านเทคนิคตัดสินใจ ในการ ตอบคำถามว่าสามารถตอบได้ทันทีหรือไม่	ผู้ประสานงาน ด้านเทคนิค
4			ผู้ประสานงานด้านเทคนิค แจ้งเวลาโทรกลับเพื่อให้คำตอบผู้รับบริการ	ผู้ประสานงาน ด้านเทคนิค
5			ผู้ประสานงานด้านเทคนิค ประสานนักวิชาการ/ผู้เชี่ยวชาญ ให้คำตอบ	ผู้ประสานงาน ด้านเทคนิค
6			ผู้ประสานงานด้านเทคนิค ได้รับคำตอบจากนักวิชาการ/ผู้เชี่ยวชาญ	ผู้ประสานงาน ด้านเทคนิค
7			ผู้รับบริการได้รับคำตอบ/วิธีแก้ไขปัญหา จากเจ้าหน้าที่ประสานงานด้านเทคนิค	ผู้รับบริการ
8			ผู้ประสานงานด้านเทคนิคบันทึกปิดงานใบ เสนอ/ส่งซ่อม/ติดตั้ง)	ผู้ประสานงาน ด้านเทคนิค
9			จบการทำงาน	ผู้ประสานงาน ด้านเทคนิค

5.2 ขั้นตอนการรับบริการซ่อมบำรุง

ลำดับ	กระบวนการ	ระยะเวลา (นาที)	รายละเอียดงาน	ผู้รับผิดชอบ
1	แจ้งปัญหา/ขอรับความช่วยเหลือ	6 นาที	ผู้ประสานงานด้านเทคนิค รับแจ้งขอรับบริการ พร้อมแนวทางแก้ไขปัญหาเบื้องต้น (ใบเสนอ/ส่งซ่อม/ติดตั้ง)	ผู้รับบริการ/ ผู้ประสานงานด้านเทคนิค
2		20 นาที	ผู้ประสานงานด้านเทคนิค จัดเจ้าหน้าที่เพื่อดำเนินการ (ใบเสนอ/ส่งซ่อม/ติดตั้ง)	ผู้ประสานงานด้านเทคนิค
3			เจ้าหน้าที่ผู้ปฏิบัติงาน รับมอบหมายงาน (JOB) และวิเคราะห์ปัญหา หาวิธีแก้ไข	เจ้าหน้าที่ผู้ปฏิบัติงาน
4		ตามข้อตกลงระยะเวลาการให้บริการ SLA	เจ้าหน้าที่ผู้ปฏิบัติงานดำเนินการแล้วเสร็จหรือไม่	เจ้าหน้าที่ผู้ปฏิบัติงาน
5			กรณีเจ้าหน้าที่ผู้ปฏิบัติงานไม่สามารถดำเนินการแล้วเสร็จ ให้แจ้งเวลาการมาให้บริการครั้งที่ 2 (Follow up)	เจ้าหน้าที่ผู้ปฏิบัติงาน
6			เจ้าหน้าที่ผู้ปฏิบัติงาน ศึกษาค้นหาวิธีแก้ไข	เจ้าหน้าที่ผู้ปฏิบัติงาน
7			เจ้าหน้าที่ผู้ปฏิบัติงาน บันทึกการดำเนินการ (Resolution) (ใบเสนอ/ส่งซ่อม/ติดตั้ง)	
8			ผู้รับบริการประเมินผล การให้บริการ	ผู้รับบริการ
9			ผู้ประสานงานด้านเทคนิคบันทึกงาน (ใบเสนอ/ส่งซ่อม/ติดตั้ง)	ผู้ประสานงานด้านเทคนิค
10			จบการทำงาน	ผู้ประสานงานด้านเทคนิค

6. ขั้นตอนการปฏิบัติงาน

6.1 ขั้นตอนการรับบริการขอคำปรึกษาทางโทรศัพท์

ผู้รับบริการ

1. แจ้งปัญหา/ ขอรับบริการ ขอความช่วยเหลือผ่านทางโทรศัพท์หมายเลข 112
2. รับคำตอบหรือวิธีการแก้ไขปัญหา ผู้ประสานงานด้านเทคนิค
 - 2.1 เมื่อผู้รับบริการแจ้งขอรับความช่วยเหลือ ผู้ประสานงานด้านเทคนิคต้องทำการบันทึกคำแจ้งลงใบเสนอ/ส่งซ่อม/ติดตั้ง
 - 2.2 ทำการวิเคราะห์ปัญหาที่รับแจ้ง
3. ทำการตอบคำถามหรือแนะนำวิธีการแก้ปัญหา
 - 3.1 ในกรณีที่สามารถตอบได้ทันที ผู้ประสานงานด้านเทคนิคจะทำการแนะนำวิธีการแก้ไขปัญหาให้ผู้รับบริการทราบทันที
 - 3.2 ในกรณีที่ไม่สามารถตอบได้ทันที ผู้ประสานงานด้านเทคนิคจะต้องดำเนินการ ดังนี้
 - ทำการแจ้งเวลาโทรกลับให้ผู้รับบริการทราบ
 - ประสานนักวิชาการหรือผู้เชี่ยวชาญให้คำตอบหรือวิธีการแก้ไขปัญหาทำการแจ้งวิธีการแก้ไขปัญหาให้ผู้รับบริการทราบ
4. ทำการบันทึกใบแบบบันทึกข้อมูลและปิดงาน

6.2 ขั้นตอนการรับบริการซ่อมบำรุง ผู้รับบริการ

1. แจ้งปัญหา/ขอรับบริการขอความช่วยเหลือผ่านทางโทรศัพท์หมายเลข 112
2. รอเจ้าหน้าที่ผู้ปฏิบัติงานมาดำเนินการแก้ไขตามเวลาที่แจ้งไว้
3. เมื่อเจ้าหน้าที่ผู้ปฏิบัติงานทำการแก้ไขปัญหาแล้วเสร็จ ให้ลงชื่อผู้ขอรับบริการ ผู้ประสานงานด้านเทคนิค
 1. เมื่อผู้รับบริการแจ้งขอรับความช่วยเหลือ ผู้ประสานงานด้านเทคนิคต้องทำการบันทึกคำแจ้งลงใบเสนอ/ส่งซ่อม/ติดตั้ง
 2. ทำการจัดเจ้าหน้าที่เพื่อดำเนินการ พร้อมทั้งบันทึกลงใบเสนอ/ส่งซ่อม/ติดตั้ง
 3. ทำการบันทึกหลักฐานข้อมูลและปิดงานลงใบเสนอ/ส่งซ่อม/ติดตั้ง เมื่อเจ้าหน้าที่ผู้ปฏิบัติงานดำเนินการแล้วเสร็จ

เจ้าหน้าที่ผู้ปฏิบัติงาน

1. รับมอบหมายงานจากผู้ประสานงานด้านเทคนิค และทำการวิเคราะห์ปัญหาเพื่อหาวิธีการแก้ไข
2. ดำเนินการแก้ไขปัญหา
 - 2.1 กรณีแก้ไขปัญหาแล้วเสร็จ ทำการบันทึกการดำเนินการลงในใบเสนอ/ส่งซ่อม/ติดตั้ง
 - 2.2 กรณีไม่สามารถแก้ไขปัญหาให้แล้วเสร็จ จะต้องดำเนินการดังนี้
 - ทำการแจ้งกำหนดการมาดำเนินการครั้งที่ 2
 - ทำการค้นหาวิธีการแก้ไขปัญหา
 - ดำเนินการแก้ไขปัญหา และทำการบันทึกการดำเนินการลงในใบเสนอ/ส่งซ่อม/ติดตั้ง
3. ให้ผู้รับบริการลงชื่อ พร้อมทั้งนำใบเสนอ/ส่งซ่อม/ติดตั้ง ส่งคืนผู้ประสานงานด้านเทคนิค เพื่อทำการบันทึกหลักฐานข้อมูลและปิดงาน

7. มาตรฐานคุณภาพงาน

ข้อตกลงระยะเวลาการให้บริการ SLA (Service Level Agreement)

ลำดับ	กระบวนการ	ระยะเวลา	หมายเหตุ
1	ตอบปัญหาทางโทรศัพท์	6 นาที	
2	Hardware		ถ้ามี Drive พร้อมติดตั้ง
	• Format + ติดตั้งระบบปฏิบัติการ	1 ชั่วโมง	
	• ติดตั้ง Driver - Printer, Accessories	20 นาที	
3	Software		ระยะเวลาต่อ 1 โปรแกรม
	• Setup Microsoft Office	45 นาที	
	• Setup Antivirus	20 นาที	
	• Setup Program (HIS)	20 นาที	
4	Network		
	• ติดตั้ง IP address	20 นาที	
	• ติดตั้งสายสัญญาณพร้อมอุปกรณ์	2 วัน	เพิ่มจุดเครือข่าย

หมายเหตุ :

1. SLA (Service Level Agreement) หมายถึง ข้อตกลงเพื่อรับประกันการบริการระหว่างผู้ให้บริการ กับผู้รับบริการ เพื่อเพิ่มความมั่นใจแก่ผู้รับบริการว่าเจ้าหน้าที่จะสามารถให้บริการได้ตามระยะเวลาแต่ละกระบวนการที่กำหนดไว้ไม่ถือเป็นข้อผูกพัน อาจมีการเปลี่ยนแปลงได้
2. ระยะเวลาตาม SLA หมายถึง ระยะเวลาการให้บริการ กรณีพื้นฐานปกติของปัญหาในแต่ละด้านทางเทคนิค โดยดูลยพินิจของเจ้าหน้าที่เท่านั้น

* เจ็อนไขการดำเนินงาน หลังจากงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ได้รับแจ้งจะจัดส่งเจ้าหน้าที่ดำเนินการในทันที ในกรณีที่เจ้าหน้าที่ผู้ปฏิบัติงานพร้อมให้บริการ แต่หากเจ้าหน้าที่ผู้ปฏิบัติงาน ติดงานให้บริการอื่นอยู่ คาดว่าจะเข้าดำเนินการให้ภายใน 30 นาทีเป็นอย่างน้อย

8. ระบบติดตามประเมินผล

8.1 การรายงานผล

ทีมดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จะต้องจัดทำรายงานสรุปผลการปฏิบัติงานที่เกี่ยวข้อง ได้แก่ การรับแจ้งปัญหา สาเหตุของปัญหา การแก้ไขปัญหา ประเภทของปัญหาตามความเหมาะสมเป็นรายเดือน และเสนอผู้บังคับบัญชาทราบ

8.2 การติดตามประเมินผล

ทีมดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จะดำเนินการติดตามประเมินผลจากการสำรวจความพึงพอใจ ในการรับบริการให้ความช่วยเหลือและแก้ไขปัญหาด้านระบบคอมพิวเตอร์และเครือข่ายอย่างน้อยปีละ 1 ครั้ง

9. เอกสารอ้างอิง

9.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) พ.ศ.2560

9.2 คำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

10. แบบฟอร์มที่ใช้

10.1 ระบบบริหารงาน IT





ภาคผนวก



ภาคผนวก ก

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

หน้า ๒๔

เล่ม ๑๓๔ ตอนที่ ๑๐ ก

ราชกิจจานุเบกษา

๒๔ มกราคม ๒๕๖๐



พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)

พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร

ให้ไว้ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐

เป็นปีที่ ๒ ในรัชกาลปัจจุบัน

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร มีพระราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของ สภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่ที่ออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้”

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๑๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

หน้า ๒๕

เล่ม ๑๓๔ ตอนที่ ๑๐ ก

ราชกิจจานุเบกษา

๒๔ มกราคม ๒๕๖๐

“ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ และลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย”

มาตรา ๕ ให้ยกเลิกความในมาตรา ๑๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

มาตรา ๖ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๒/๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

มาตรา ๗ ให้เพิ่มความต่อไปนี้เป็นวรรคสอง วรรคสาม วรรคสี่ และวรรคห้าของมาตรา ๑๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญา ตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่ง หรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่าย หรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสาม หรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทางเดียว”

มาตรา ๘ ให้ยกเลิกความในมาตรา ๑๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิด ความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใด บุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้”

มาตรา ๙ ให้ยกเลิกความในมาตรา ๑๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ”

มาตรา ๑๐ ให้ยกเลิกความในมาตรา ๑๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการดีชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

มาตรา ๑๑ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๖/๑ และมาตรา ๑๖/๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้รู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี”

มาตรา ๑๒ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๗/๑ ในหมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๑๗/๑ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่ง มาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗ ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งมีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่ นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว”

มาตรา ๑๓ ให้ยกเลิกความในมาตรา ๑๘ และมาตรา ๑๙ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสอง ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

หน้า ๒๙

เล่ม ๑๓๔ ตอนที่ ๑๐ ก

ราชกิจจานุเบกษา

๒๔ มกราคม ๒๕๖๐

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจากรายทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจากรายทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจากรายทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจากรายทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๑) (๒) และ (๓) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงาน

หน้า ๓๐

เล่ม ๑๓๔ ตอนที่ ๑๐ ก

ราชกิจจานุเบกษา

๒๔ มกราคม ๒๕๖๐

เจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณา คำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรืออายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง”

มาตรา ๑๔ ให้ยกเลิกความในมาตรา ๒๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

หน้า ๓๑

เล่ม ๑๓๔ ตอนที่ ๑๐ ก

ราชกิจจานุเบกษา

๒๔ มกราคม ๒๕๖๐

“มาตรา ๒๐ ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้ พนักงานเจ้าหน้าที่ โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้ มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

(๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกฤษฎีกาข้อมูลคอมพิวเตอร์ จะมอบหมายให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้ มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ ทั้งนี้ ให้นำบทบัญญัติ ว่าด้วยคณะกรรมการที่มีอำนาจดำเนินการพิจารณาทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการ ทางปกครองมาใช้บังคับกับการประชุมของคณะกรรมการกฤษฎีกาข้อมูลคอมพิวเตอร์โดยอนุโลม

ให้รัฐมนตรีแต่งตั้งคณะกรรมการกฤษฎีกาข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่ง หรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคนซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชน ด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการ ได้รับคำตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

การดำเนินการของศาลตามวรรคหนึ่งและวรรคสอง ให้นำประมวลกฎหมายวิธีพิจารณาความอาญา มาใช้บังคับโดยอนุโลม ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตามวรรคหนึ่งหรือวรรคสอง พนักงานเจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ นั้นเองหรือจะสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรี ประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือ ลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการ ทางเทคโนโลยีที่เปลี่ยนแปลงไป เว้นแต่ศาลจะมีคำสั่งเป็นอย่างอื่น

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับความ เห็นชอบจากรัฐมนตรี หรือพนักงานเจ้าหน้าที่โดยความเห็นชอบของคณะกรรมการกฤษฎีกาข้อมูล คอมพิวเตอร์จะยื่นคำร้องตามวรรคสองไปก่อนที่รัฐมนตรีจะมอบหมายก็ได้ แต่ทั้งนี้ต้องรายงาน ให้รัฐมนตรีทราบโดยเร็ว”

มาตรา ๑๕ ให้ยกเลิกความในวรรคสองของมาตรา ๒๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง เว้นแต่เป็นชุดคำสั่งไม่พึงประสงค์ที่อาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่งไม่พึงประสงค์ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์ก็ได้”

มาตรา ๑๖ ให้ยกเลิกความในมาตรา ๒๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสองเปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นในกรณีตามมาตรา ๑๘ วรรคสอง หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบหรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่ตามมาตรา ๑๘ วรรคสอง โดยมิชอบหรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา ๑๘ วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วย

การสืบพยานได้ แต่ต้องเป็นชนิดที่มีได้เกิดขึ้นจากการจงใจ มีค้ำมั่นสัญญา ชูเชื้อ หลอกลวง หรือโดยมิชอบ ประการอื่น”

มาตรา ๑๗ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่มีข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้”

มาตรา ๑๘ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษ ตามที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในการกำหนดให้ได้รับค่าตอบแทนพิเศษต้องคำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมาก คุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่น ในกระบวนการยุติธรรมด้วย”

มาตรา ๑๙ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๓๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“มาตรา ๓๑ ค่าใช้จ่ายในเรื่องดังต่อไปนี้ รวมทั้งวิธีการเบิกจ่ายให้เป็นไปตามระเบียบที่รัฐมนตรี กำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

- (๑) การสืบสวน การแสวงหาข้อมูล และรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัตินี้
- (๒) การดำเนินการตามมาตรา ๑๘ วรรคหนึ่ง (๔) (๕) (๖) (๗) และ (๘) และมาตรา ๒๐
- (๓) การดำเนินการอื่นใดอันจำเป็นแก่การป้องกันและปราบปรามการกระทำความผิดตามพระราชบัญญัตินี้”

มาตรา ๒๐ บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ ใช้บังคับ

หน้า ๓๔

เล่ม ๑๓๔ ตอนที่ ๑๐ ก

ราชกิจจานุเบกษา

๒๔ มกราคม ๒๕๖๐

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จภายในหกสิบวัน นับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

มาตรา ๒๑ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้

ผู้รับสนองพระราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

หน้า ๓๕

เล่ม ๑๓๔ ตอนที่ ๑๐ ก

ราชกิจจานุเบกษา

๒๔ มกราคม ๒๕๖๐

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็วและโดยที่มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศสมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวข้องกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดขึ้นใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้



ภาคผนวก ข

คำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ



คำสั่งโรงพยาบาลเมืองจันทร์

ที่ ๕๗ / ๒๕๖๓

เรื่อง แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลเมืองจันทร์ ตระหนัก และมองเห็นความสำคัญและความจำเป็นอย่างยิ่งในการพัฒนาระบบข้อมูลทางด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดระบบสารสนเทศและข้อมูลสารสนเทศที่มีความถูกต้อง ครบถ้วนและรวดเร็ว ทันต่อการใช้งาน ทั้งทางด้านของการพัฒนาศักยภาพในการรักษา และการบริหารงานโรงพยาบาลด้วยข้อมูลสารสนเทศที่มีความถูกต้อง และครอบคลุมทุกด้าน ประกอบกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลเมืองจันทร์ จะมีการดำเนินการจัดทำแผนแม่บทด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาลเมืองจันทร์ ในระยะ ๕ ปี เพื่อให้เกิดการพัฒนาของระบบสารสนเทศของโรงพยาบาลที่ครอบคลุม ทุกส่วนงาน และมีประโยชน์สูงสุด และเพื่อให้การดำเนินงานดังกล่าวเป็นไปด้วยความเรียบร้อยและบรรลุวัตถุประสงค์ จึงมีคำสั่งดังต่อไปนี้

๑. นายจิระวัตร วิเศษสังข์	ผู้อำนวยการ	ประธาน
๒. นางสาวธิดา มุลลา	นักจัดการงานทั่วไปปฏิบัติการ	รองประธาน
๓. นางสาวธัญยจิรา ปัญญาพิพัฒน์	นักวิชาการสาธารณสุขชำนาญการ	กรรมการ
๔. นายธีระยุทธ ท้าวนิล	นายช่างเทคนิค	กรรมการ
๕. นางสาวจุฑารัตน์ โอวาท	นักวิชาการคอมพิวเตอร์	กรรมการ/เลขานุการ
๖. นายทวีรัชต์ งามหอม	นักวิชาการคอมพิวเตอร์	กรรมการ/ผู้ช่วยเลขานุการ

มีบทบาทและหน้าที่

- ๑) จัดทำแผนแม่บทด้านสารสนเทศของแต่ละหน่วยงานและในภาพรวมระดับโรงพยาบาล
- ๒) วางระบบ กำหนดแนวทาง นโยบายในการพัฒนาระบบสารสนเทศในการพัฒนาคุณภาพของโรงพยาบาล เพื่อให้สามารถตอบสนองความต้องการของผู้ให้บริการ และผู้รับบริการ
- ๓) สำรวจความต้องการใช้ข้อมูลของหน่วยงาน ทั้งบุคลากรผู้บริหาร ผู้ป่วย และองค์กรภายนอก นำไปสู่การออกแบบ การจัดการ และการตอบสนองความต้องการอย่างเหมาะสม
- ๔) ดำเนินการรวบรวม เชื่อมโยงข้อมูลสารสนเทศให้ไปในทิศทางเดียวกัน เพื่อใช้ในการติดตามผลการปฏิบัติงานประจำวัน ติดตามผลงานของโรงพยาบาลโดยรวม รวมถึงติดตามความก้าวหน้า ตามวัตถุประสงค์เชิงกลยุทธ์และแผนปฏิบัติการของโรงพยาบาล
- ๕) วิเคราะห์ แผลผลข้อมูลหรือสารสนเทศ เพื่อประโยชน์ในการบริหาร การดูแลผู้ป่วย และการพัฒนาคุณภาพข้อมูลด้านสารสนเทศให้ดียิ่งขึ้น
- ๖) กระจายข่าวสาร ข้อมูลด้านสารสนเทศที่เหมาะสม ถูกต้อง ทันเวลา ให้กับผู้ร่วมปฏิบัติงาน ผู้ปฏิบัติงานได้บังคับบัญชา ประชาชนผู้รับบริการ เพื่อความถูกต้อง และเกิดความเข้าใจไปในทิศทางเดียวกัน

/๗) ดำเนิน...

๗) ดำเนินการประสานงาน กลุ่มงาน ฝ่ายงาน และทีมงานต่างๆ เพื่อให้เกิดกิจกรรม ทบทวนคุณภาพและ ความสมบูรณ์ของระบบงานสารสนเทศ

๘) กำหนดแนวทาง มาตรการ ข้อตกลงและข้อปฏิบัติในการใช้งานระบบเทคโนโลยี สารสนเทศของ โรงพยาบาล

๙) ประชุม ติดตามผลการดำเนินงาน และรายงานคณะกรรมการบริหารโรงพยาบาลเมืองจันทร์ตามสมควร

๑๐) บริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑๑) ควบคุมการเข้าถึงระบบคอมพิวเตอร์และเครือข่าย

๑๒) จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์

๑๓) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

สั่ง ณ วันที่ ๑ เดือนตุลาคม พ.ศ.๒๕๖๓



(นายแพทย์จรัสวัตร วิเศษสังข์)

ผู้อำนวยการโรงพยาบาลเมืองจันทร์



192.168.111.32:81/it/application/index.php?r=site%2Fregister

ระบบบริหารงาน IT

ลงทะเบียนเข้าใช้งานระบบ

เข้าสู่ระบบ

ลงทะเบียนเข้าใช้งานระบบ

ชื่อ - นามสกุล

ตำแหน่ง

เบอร์ติดต่อ

อีเมล

Username

Password

หน่วยงาน / แผนก

หน่วยงาน / แผนก

บันทึก ยกเลิก

192.168.111.32:81/it/application/index.php?r=user-request%2Fform-request

ระบบบริหารงาน IT

แจ้งปัญหา / งานซ่อม

User (น.ส.จุฑารัตน์ โอภาส)

บันทึกข้อมูลการแจ้งปัญหา / งานซ่อม

แจ้งปัญหา / งานซ่อม

วันที่แจ้ง

2022-05-27 11:24:26

ประเภทงานซ่อม

เลือกประเภทงานซ่อม

ชื่ออุปกรณ์

ชื่ออุปกรณ์

ปัญหา

เบอร์ติดต่อ

** รองรับเฉพาะ ไฟล์ภาพ jpg, jpeg, png หรือ ไฟล์เอกสาร word excel Pdf เท่านั้น
ไฟล์แนบ

เลือกไฟล์


ไม่ได้เลือกไฟล์ใด

บันทึก ยกเลิก

ภาคผนวก ง


ระเบียบปฏิบัติ

1. การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
2. การจัดการกับเอกสารที่เกี่ยวข้องกับระบบ
3. การจัดการระบบเครือข่าย
4. การจัดการ การลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่
5. การใช้งานห้อง Data Center
6. การจัดการทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย
7. การกำจัดไวรัส
8. การสำรองข้อมูล
9. การจัดเก็บข้อมูลตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560
10. การลงทะเบียนและควบคุมการเข้าถึงระบบ
11. การพัฒนาระบบงาน
12. การปฏิบัติกรณีเครื่องคอมพิวเตอร์ลูกและข่ายอุปกรณ์เครือข่ายขัดข้อง
13. การปฏิบัติกรณีเกิดอัคคีภัย
14. การรักษาความลับของผู้ที่เข้าถึงข้อมูลผู้ป่วย
15. การรักษาความปลอดภัย การป้องกันการสูญหายของแฟ้มเวชระเบียน ที่จัดเก็บในรูปแบบ Electronic files
16. แนวทางปฏิบัติการแจ้งบัญชีผู้ใช้งานสำหรับบุคลากรภายนอก ที่ถูกเชิญมาปฏิบัติงานแทนผู้ดูแลระบบ
17. การปฏิบัติงานนอกเวลาราชการของผู้ดูแลระบบ

	MCH – IT - 001	หน้าที่ 1/1
	เรื่อง การบริหารจัดการด้านความมั่นคง ปลอดภัยสำหรับสารสนเทศ	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. จัดให้มีการทำและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
2. แสดงเจตนาธรรมณ์ หรือสื่อสารให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศขององค์กร โดยเคร่งครัด อย่างสม่ำเสมอ
3. จัดให้มีการประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดให้มีวาระการประชุมที่ต้องหารือกันอย่างน้อยดังนี้
 - การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยฯ และผลการตรวจสอบ
 - แผนการดำเนินการเชิงป้องกัน/แก้ไข จากผลการตรวจสอบดังกล่าว
 - การปรับปรุงนโยบายความมั่นคงปลอดภัยฯ สำหรับปีถัดไป
 - การประเมินความเสี่ยงและแผนลดความเสี่ยง จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการและวัตถุดิบที่เพียงพอต่อการจัดการดังกล่าว
4. จัดให้มีการสร้างความตระหนักรู้ทางด้านการความมั่นคงปลอดภัยเพื่อให้เจ้าหน้าที่ขององค์กร มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ 1 ครั้ง
5. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อลด ความเสี่ยง หรือปัญหาที่พบ
6. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยฯ โดยผู้ตรวจสอบภายในด้านสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุง หรือแก้ไขปัญหาที่พบ
7. จัดให้มีการแจ้งเวียนให้เจ้าหน้าที่ทั้งหมดได้ระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน เพื่อป้องกันการสูญหาย อย่างน้อยปีละ 1 ครั้ง
8. กำหนดนโยบายการใช้งานระบบเครือข่ายอย่างชัดเจน ว่าบริการใดที่อนุญาตให้ใช้งาน และบริการใดไม่อนุญาตให้ใช้งาน เช่น การใช้งานไลน์ ดูหนังผ่านทางอินเทอร์เน็ต เป็นต้น รวมทั้งปรับปรุงนโยบายตามความจำเป็น
9. ห้ามเข้าเว็บไซต์ที่อยู่ในประเภท ดังต่อไปนี้
 - วิกิพีเดียที่เกี่ยวกับชาติ ศาสนา และพระมหากษัตริย์
 - การพนัน
 - ลามก อนาจาร
 - อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม
 - งดเว้นการเล่นเกมส์ ดูภาพยนตร์ ผ่านทางอินเทอร์เน็ตในเวลาทำงาน

	MCH – IT - 002	หน้าที่ 1/1
	เรื่อง การจัดการกับเอกสารที่เกี่ยวข้องกับระบบ	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. จัดทำและปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัย อย่างน้อยให้ครอบคลุมระบบงาน เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ที่มีความสำคัญ ดังนี้
 - คู่มือระบบงานต่างๆ ทั้งในส่วนของผู้ใช้งาน และผู้ดูแลระบบ
 - คู่มือการตรวจสอบสถานะของเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย
 - คู่มือการตรวจสอบระบบและอุปกรณ์ต่างๆ ในห้อง Data Center
 - คู่มือการสำรองข้อมูล
 - คู่มือการตรวจสอบทรัพยากรของระบบ
2. ให้จำกัดการเข้าถึงคู่มือการปฏิบัติงานเฉพาะทีมงานที่มีความเกี่ยวข้องเท่านั้น
3. หากมีการจัดเก็บคู่มือการปฏิบัติงานไว้บนระบบเครือข่าย จัดให้มีการป้องกันการเข้าถึงเพื่อให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น

	MCH – IT - 003	หน้าที่ 1/1
	เรื่อง การจัดการระบบเครือข่าย	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์

ระเบียบปฏิบัติ


1. ปรับปรุงผังเครือข่ายให้มีความทันสมัย อย่างน้อยปีละ 1 ครั้ง
2. จัดแบ่ง และปรับปรุงระบบเครือข่ายออกเป็นกลุ่มๆ ตามลักษณะการใช้งาน เช่น แบ่งตามกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย เครื่องลูกข่าย และระบบงานที่มีความสำคัญ
3. จำกัดการเชื่อมต่อไปยังเครื่องคอมพิวเตอร์แม่ข่าย ระบบงานหรืออุปกรณ์ที่มีความสำคัญ โดยจะต้องกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อได้จะต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบเท่านั้น
4. ปิดบริการบนเครื่องคอมพิวเตอร์แม่ข่ายที่ไม่มีความจำเป็นในการใช้งาน
5. กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจากภายในเครือข่ายเพื่อเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่าย
6. กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูล ที่ใช้สำหรับการเชื่อมต่อจากระยะไกลภายนอกองค์กร เข้ามาสู่เครือข่ายภายในองค์กร
7. ปรับแต่งไฟร์วอลล์ เพื่อให้เป็นไปตามนโยบายการใช้งานระบบเครือข่ายที่กรมการสารสนเทศได้กำหนดไว้

	MCH - IT - 004	หน้าที่ 1/1
	เรื่อง การจัดการ การลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์

ระเบียบปฏิบัติ


1. ถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายออกจากระบบต่างๆ ทั้งหมดโดยทันทีที่ได้รับแจ้งจากงานบริหาร
2. จัดให้มีตรวจสอบความถูกต้องของข้อมูลผู้ใช้สิทธิในระบบต่างๆ ทุก 1 เดือน



	MCH – IT - 005	หน้าที่ 1/1
	เรื่อง การใช้งานห้อง Data Center	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. ห้ามนำบุคคลภายนอกเข้าไปในห้อง Data Center โดยไม่มีกิจที่จำเป็นหากจำเป็นต้องได้รับอนุญาตจากผู้ดูแลระบบ โดยมีบันทึกการเข้าห้องไว้เป็นลายลักษณ์อักษร ทุกครั้ง
2. ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้อง Data Center
3. ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้อง Data Center ให้ปิดล็อกอยู่เสมอ
4. ตรวจสอบสภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ ได้แก่
 - ระบบกระแสไฟ
 - ระบบควบคุมอุณหภูมิ
 - ระบบเครื่องสำรองไฟ
5. จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัยระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย
6. ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ 1 ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่
7. ให้อุณหภูมิและความชื้นและความเป็นระเบียบเรียบร้อยของห้อง Data Center อย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษ หรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้อง
8. ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย
9. ตรวจสอบสายสัญญาณสื่อสารให้มีการปิดล็อกอยู่เสมอ
10. จัดทำหรือต่อสัญญาการบำรุงรักษาระบบงานสำคัญ ไฟรอลล์ เราท์เตอร์ อุปกรณ์ เครื่องสำรองไฟ สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องให้ครบถ้วน
11. จัดให้ระบบงานสำคัญ เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์ เครื่องสำรองไฟ และระบบกระแสไฟฟ้าสำรอง (electricity power generator) เพื่อสนับสนุนการทำงานอย่างครบถ้วน

	MCH - IT - 006	หน้าที่ 1/1
	เรื่อง การจัดการทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. ดำเนินการตรวจสอบทรัพยากรของ เครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบงานสำคัญอย่างน้อย สัปดาห์ละ 1 ครั้ง สิ่งที่ต้องตรวจสอบ ประกอบด้วย ปริมาณการใช้ CPU ปริมาณการใช้ฮาร์ดดิสก์ ปริมาณการใช้หน่วยความจำ และปริมาณการใช้เครือข่าย รวมทั้งควรมีการตรวจสอบการใช้งาน เครือข่ายโดยภาพรวม
2. บันทึกข้อมูลการใช้ทรัพยากรดังกล่าวไว้ด้วย (เพื่อใช้ในการตรวจสอบแนวโน้มการใช้ทรัพยากร รวมทั้งวางแผน จัดซื้อเพิ่มเติมตามความจำเป็นในอนาคต)
3. ตั้งค่าและหมั่นตรวจสอบสัญญาณนาฬิกาของ เครื่องคอมพิวเตอร์แม่ข่ายตามที่ พ.ร.บ.ว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ได้ระบุไว้และของระบบงานสำคัญให้มีความถูกต้องอยู่เสมอ (โดยสามารถอ้างอิงเวลาได้จาก “dock.thaicert.org”)

	MCH - IT - 007	หน้าที่ 1/1
	เรื่อง การกำจัดไวรัสคอมพิวเตอร์	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. ตรวจสอบว่าเครื่องคอมพิวเตอร์แม่ข่ายป้องกันไวรัสยังทำงานตามปกติ และมีการปรับปรุงฐานข้อมูลไวรัส (Virus signature) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยสัปดาห์ละ 1 ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบดำเนินการแก้ไข (ข้อนี้จะใช้ได้กับองค์กรที่มีการใช้งานโปรแกรมป้องกันไวรัสแบบ Client/server เท่านั้น)
2. ทำการติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งานเพื่อให้ทำงานในลักษณะ Real-time Scan เมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน
3. ทำการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัย กับเครื่องลูกข่ายทั้งหมด เครื่องคอมพิวเตอร์แม่ข่าย สำหรับระบบงานสำคัญ และเครื่องแม่ข่ายคอมพิวเตอร์แม่ข่าย

	MCH – IT - 008	หน้าที่ 1/1
	เรื่อง การสำรองข้อมูล	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. กำหนดรายชื่อของระบบงานสำคัญทั้งหมด
2. กำหนดรายชื่อของเครื่องคอมพิวเตอร์แม่ข่ายตามที่ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2560 ได้กำหนดไว้ เช่น เว็บเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น
3. กำหนดผู้รับผิดชอบในการสำรองข้อมูล
4. กำหนดชนิดของข้อมูลบนระบบงานหรือบนเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย
 - ข้อมูลในฐานข้อมูลของระบบงาน HIS โรงพยาบาล และเวชระเบียน Electronic file
 - ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น
 - ข้อมูลบัญชีผู้ใช้งานระบบอินเทอร์เน็ต
5. กำหนดความถี่ในการสำรองข้อมูลของระบบงานหรือเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าว
6. ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

	MCH - IT - 009	หน้าที่ 1/1
	เรื่อง การจัดเก็บข้อมูลตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2560	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

- จัดเก็บข้อมูลล็อกดังต่อไปนี้อย่างน้อยเป็นระยะเวลา 90 วัน
 - เครื่องคอมพิวเตอร์แม่ข่าย FTP (FTP.log)
 - Mail (SMTP.log)
 - Firewall/Proxy/Gateway (เช่น FW.log)
 - Web (Access.log)
 - RADIUS (RADIUS.log) Vils TACACS + (TACACS.log)
- จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์
- จำกัดการเข้าถึงข้อมูลล็อกดังกล่าวโดยกำหนดให้เฉพาะผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถเข้าถึงได้

	MCH – IT - 010	หน้าที่ 1/1
	เรื่อง การลงทะเบียนและควบคุมการเข้าถึงระบบ	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้งานใหม่ตาม “แบบฟอร์ม” และกำหนดสิทธิของผู้ใช้งานตามสิทธิความจำเป็นในการใช้งานเท่านั้น
2. ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน สำหรับเจ้าหน้าที่ของโรงพยาบาลเมืองจันทร์อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
3. ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน สำหรับหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง

	MCH – IT - 011	หน้าที่ 1/1
	เรื่อง การพัฒนาระบบงาน	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. จัดให้มีการตรวจรับและทดสอบระบบงานใหม่ โดยผู้ใช้งานที่เกี่ยวข้องให้ครอบคลุมตามข้อกำหนดที่ระบุ จนกระทั่งสามารถใช้งานได้ตรงตามความต้องการของหน่วยงาน จึงจะเปิดให้บริการระบบงานนั้นได้
2. สำหรับระบบงานสำคัญ ให้กำหนดมาตรฐานการเข้ารหัสข้อมูลที่มีการรับ-ส่งระหว่างเครื่องลูกข่ายกับเครื่องคอมพิวเตอร์แม่ข่าย และกำหนดให้พัฒนาระบบตามมาตรฐานนี้
3. การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้น จึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบอาจมีการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม
4. ทำการทดสอบระบบงาน และบันทึกผลการทดสอบเก็บไว้เป็นลายลักษณ์อักษรตามแนวทางในการตรวจสอบ
5. พัฒนาระบบงานเพื่อให้สามารถกำหนดรหัสผ่านที่มีความเข้มแข็งตามระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน และมีการกำหนดให้รหัสผ่านมีอายุการใช้งาน 90 วัน เมื่อใช้งานครบกำหนดจะต้องทำการกำหนดรหัสผ่านใหม่เพื่อเข้าใช้งานระบบต่อไป
6. จัดให้มีการอบรมสำหรับระบบงานใหม่ให้แก่ผู้ใช้งานทั้งหมดที่เกี่ยวข้อง
7. จัดทำคู่มือการใช้งานสำหรับระบบงานใหม่ สำหรับผู้ใช้งาน และผู้ดูแลระบบ

	MCH - IT - 012	หน้าที่ 1/2
	เรื่อง การปฏิบัติกรณีเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์เครือข่ายขัดข้อง	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. เครื่องคอมพิวเตอร์ลูกข่าย (Client) มีปัญหามากกว่า 5 เครื่องพร้อมกัน
 - หัวหน้า/รองหัวหน้า เจ้าหน้าที่งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ตรวจสอบเพื่อค้นหาสาเหตุของปัญหา หากไม่สามารถแก้ไขได้ภายใน 20 นาที ดำเนินการเปลี่ยนเครื่องคอมพิวเตอร์สำรอง เปลี่ยนตามจุดบริการต่างๆ ที่มีปัญหาโดยให้มุ่งเน้น หน่วยงาน OPD เป็นหน่วยงานแรก โดยพิจารณาใช้เครื่องคอมพิวเตอร์สำรองจากงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์
 - งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ดำเนินการแก้ไขให้แล้วเสร็จ ภายใน 24 ชั่วโมง
 - บันทึกรายงานการซ่อมลงในระบบและลงบันทึกความเสี่ยงต่อไป
2. อุปกรณ์เครือข่ายสำรอง มีดังนี้
 - 2.1 กรณี Switch Layer 3 (Core Switch) มีปัญหา
 - 1) เจ้าหน้าที่ตรวจสอบหาสาเหตุของปัญหาอย่างรวดเร็ว หากไม่สามารถแก้ไขได้ภายใน 20 นาที ให้แจ้งหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทราบในเบื้องต้น ทำการเปลี่ยนทดแทน Switch Layer 3 สำรองที่กำหนดค่าอุปกรณ์ไว้เรียบร้อยแล้วเปลี่ยนทดแทน
 - 2) ทำการแก้ไขอุปกรณ์เพื่อทำเป็นอุปกรณ์สำรอง เพื่อเก็บไว้ยังงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์
 - กรณีแก้ไขได้เองภายใน 7 วัน ให้ทำแก้ไขและกำหนดค่าเพื่อใช้เป็นอุปกรณ์สำรอง ต่อไป
 - กรณีแก้ไขไม่ได้ต้องส่งเคลม หรือส่งซ่อม กรณีแก้ไขได้ภายใน 30 วัน ให้ทำการส่ง หลังจากได้รับอุปกรณ์คืนให้ทำการกำหนดค่าเพื่อใช้งานเป็นอุปกรณ์สำรองต่อไป
 - กรณีเกิน 30 วัน ให้ดำเนินการจัดเตรียมสั่งซื้ออุปกรณ์ทดแทนอุปกรณ์ตัวเดิมและทำการกำหนดค่าเพื่อใช้เป็นอุปกรณ์สำรองต่อไป

	MCH – IT - 012	หน้าที่ 2/2
	เรื่อง การปฏิบัติกรณีเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์เครือข่ายขัดข้อง	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


2.2 กรณี Switch Layer 2 มีปัญหา

- 1) เจ้าหน้าที่ตรวจสอบหาสาเหตุของปัญหาชั่วคราว หากไม่สามารถแก้ไขได้ภายใน 20 นาที ให้แจ้งหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทราบในเบื้องต้น ทำการเปลี่ยน Switch Layer 2 โดยพิจารณาใช้อุปกรณ์สำรองจากศูนย์คอมพิวเตอร์ ตามลำดับต่อไปนี้
 - กรณี Switch Layer 2 - 24 Port สำรองมีจำนวนเพียงพอ
 - ดำเนินการเปลี่ยนอุปกรณ์ให้นำอุปกรณ์ Switch Layer 2 - 24 Port สำรองจำนวน 1 เครื่องมาใช้ทดแทน ทำการกำหนด VLAN ตามค่าเดิมของอุปกรณ์ ดังกล่าว
 - ดำเนินการแก้ไขให้เสร็จภายใน 30 วันเพื่อนำกลับมากำหนดค่าอุปกรณ์เพื่อใช้เป็นอุปกรณ์สำรองต่อไป หากไม่สามารถดำเนินการแก้ไขได้ให้ทำการจัดหาอุปกรณ์ตัวใหม่มาทดแทนและทำการกำหนดค่าเพื่อใช้งานเป็นอุปกรณ์สำรองต่อไป
 - กรณี Switch Layer 2 - 24 Port สำรองมีจำนวนไม่เพียงพอ
 - ดำเนินการเปลี่ยนอุปกรณ์ให้นำอุปกรณ์ Switch HUB - 24 Port สำรอง จำนวน 1 เครื่องมาใช้ทดแทน
 - ดำเนินการแก้ไขให้เสร็จภายใน 3 วันเพื่อนำกลับมากำหนดค่าอุปกรณ์เพื่อนำมาเปลี่ยนกลับคืน หรือทำการหาอุปกรณ์สำรองที่ดำเนินการเสร็จสิ้นมาเปลี่ยน
 - หากไม่สามารถดำเนินการแก้ไขได้ ให้ทำการจัดหาอุปกรณ์ตัวใหม่มาทดแทนหรือทำการกำหนดค่าเพื่อใช้งานเป็นอุปกรณ์สำรองต่อไป

	MCH – IT - 013	หน้าที่ 1/1
	เรื่อง การปฏิบัติกรณีเกิดอัคคีภัย	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์


ระเบียบปฏิบัติ

1. กรณีเกิดอัคคีภัย เจ้าหน้าที่งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ดำเนินการขนย้ายอุปกรณ์ตามลำดับความสำคัญตามแผนอัคคีภัย ดังนี้
 - 1.1 ขนย้ายอุปกรณ์ในห้อง Server ดังนี้
 - Computer Server
 - อุปกรณ์เครือข่าย
 - เครื่องสำรองไฟฟ้า
 - ตู้จัดเก็บอุปกรณ์เครือข่าย ขนย้ายเป็นกรณีท้ายสุดเนื่องจากมีน้ำหนักมากยากแก่การขนย้าย
 - 1.2 ขนย้ายอุปกรณ์ในห้องคอมพิวเตอร์ ดังนี้
 - Computer PC ของแต่ละคน หลังจากมีการจัดการตามหน้าที่ในการจัดการตามแผนอัคคีภัยของโรงพยาบาลเมืองจันทร์
 - Computer Notebook
 - อุปกรณ์เครือข่ายคอมพิวเตอร์และอุปกรณ์สำนักงานที่มีราคาสูง และมีความสำคัญ
 - วัสดุอุปกรณ์ในห้องเก็บของห้องคลัง
 - 1.3 เมื่อสามารถควบคุมอัคคีภัยได้แล้ว ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่าย, ระบบไฟฟ้า และติดตั้งอุปกรณ์ให้พร้อมใช้งาน
 - 1.4 ตรวจสอบความพร้อมใช้ของเครื่องลูกข่าย หากยังไม่พร้อมใช้งานให้ดำเนินการตามระเบียบปฏิบัติกรณีไฟฟ้าดับ หรือกรณีเครื่อง Server/Database มีปัญหาหากเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศไม่อยู่ เจ้าหน้าที่อื่นสามารถดำเนินการได้ดังนี้
 - ให้เปิดประตูห้อง Server หรือพังประตูเพื่อเข้าไปในห้อง Server
 - ทำการถอดสาย LAN ออกให้หมด
 - ทำการถอดสายไฟที่อยู่ภายนอกตู้ Server ออกให้หมด
 - ทำการเคลื่อนย้ายตามแผนป้องกันอัคคีภัย

	MCH – IT - 014	หน้าที่ 1/1
	เรื่อง การรักษาความลับของผู้ที่เข้าถึงข้อมูลผู้ป่วย	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์

ระเบียบปฏิบัติ

1. การบันทึกข้อมูลประวัติและการเข้ารับบริการของผู้ป่วย
 - ไม่บันทึกข้อมูลที่ไม่เป็นจริง (untrue information)
 - ไม่ควรบันทึกข้อมูลที่เป็นจริงแต่เป็นข้อมูลที่ไม่สมควรบันทึกไว้เป็นหลักฐาน
 - ก่อนการบันทึกข้อมูลใดๆ ลงในแฟ้มประวัติเวชระเบียนของผู้ป่วย หรือในคอมพิวเตอร์ต้องพิจารณาเนื้อหาที่จะบันทึกให้รอบคอบ
2. การนำข้อมูลของผู้ป่วยหรือตัวผู้ป่วยไปเผยแพร่ให้ความรู้ จัดทำรายการตีพิมพ์เอกสารทางวิชาการต่างๆ
 - ให้เก็บเอกสารหรือรายงานเกี่ยวกับข้อมูลของผู้ป่วยไว้เป็นความลับ เมื่อนำไปใช้ในการสอนหรือใช้ประกอบในการเขียนรายงานต่าง ๆ
 - การเปิดเผยข้อมูลจะต้องได้รับหลักฐานเป็นลายลักษณ์อักษร ที่แสดงถึงความยินยอมให้เปิดเผยข้อมูล
 - หลีกเลี่ยงการตีพิมพ์ หรือแสดงรูปผู้ป่วยที่เห็นใบหน้าชัดเจน ถ้าจำเป็นต้องปิดส่วนหนึ่งของใบหน้า
 - การนำเรื่องผู้ป่วยเข้าประชุมปรึกษาหารือกับกลุ่มบุคคลอื่น ที่อยู่นอกวิชาชีพทางการแพทย์ไม่ควรเปิดเผย ชื่อ - นามสกุลผู้ป่วย


	MCH – IT - 015	หน้าที่ 1/1
	เรื่อง การรักษาความปลอดภัย การป้องกันการสูญหายของแฟ้มเวชระเบียนที่จัดเก็บในรูปแบบ Electronic file	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์

ระเบียบปฏิบัติ

1. การ Backup ข้อมูลที่จัดเก็บในรูปแบบ Electronic files ให้ปฏิบัติดังนี้
 - 1.1 จัดเก็บข้อมูลใน Server สำรอง ในรูปแบบ SAS story Raid จัดทำเป็น RAIDS-5 ร่วมกับ Hot Spare โดยมี Hard disk สำหรับ บันทึกข้อมูลที่เหมือนกันจำนวน 6 ลูก
 - 1.2 การ Copy ข้อมูล Back up เก็บไว้ใน Hard disk External อาทิตย์ละ 1 ครั้ง
2. แนวทางการพิทักษ์สิทธิผู้ป่วยในการเปิดเผยข้อมูล ดังนี้


กรณีที่ไม่สามารถตามเจ้าหน้าที่ของศูนย์เทคโนโลยีฯ ได้หรือมีปัญหาอื่นๆ เกี่ยวกับบุคลากรที่จะแก้ไข ปัญหาโปรแกรม HIMPro และระบบเครือข่ายอื่นๆ ให้คณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแจ้ง ผู้อำนวยการโรงพยาบาลเมืองจันทร์ทราบ และพิจารณาเชิญบุคลากรดังต่อไปนี้

 - นายเกรียงศักดิ์ บุญรอด โรงพยาบาลกันทรารมย์ โทร. 081-069-9783
 - นายประยูร หาญเสมอ โรงพยาบาลศรีสะเกษ โทร. 085-025-5522

	MCH - IT - 016	หน้าที่ 1/1
	เรื่อง แนวทางปฏิบัติการแจ้งบัญชีผู้ใช้งาน สำหรับบุคลากรภายนอก ที่ถูกเชิญมาปฏิบัติงานแทนผู้ดูแลระบบ	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์

ระเบียบปฏิบัติ

1. เมื่อเกิดปัญหาผู้ดูแลระบบ ไม่สามารถมาปฏิบัติงานได้ด้วย เหตุผลดังต่อไปนี้คือ
 - 1.1 หลบหนี
 - 1.2 ลาออกแบบไม่ได้คาคหมาย
 - 1.3 ทูพพลภาพ
 - 1.4 เสียชีวิต
2. ให้คณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดำเนินการตามระเบียบปฏิบัติดังต่อไปนี้
 - 2.1 ให้คณะกรรมการสารสนเทศแจ้ง ผู้อำนวยการโรงพยาบาลเมืองจันทร์ ทราบและพิจารณาเชิญบุคลากรดังต่อไปนี้ ตามลำดับดังต่อไปนี้
 - นายเกรียงศักดิ์ บุณอรอด โรงพยาบาลกันทรารมย์ โทร. 081-069-9783
 - นายประยูร หาญเสมอ โรงพยาบาลศรีสะเกษ โทร. 085-025-5522
 - 2.2 ให้คณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทำเอกสารบันทึกข้อความถึงผู้อำนวยการโรงพยาบาลเมืองจันทร์พิจารณา เพื่อเปิดเผยบัญชีผู้ใช้งานระดับสูงสุด ในระบบโปรแกรมต่างๆ เท่าที่จำเป็น หรือบัญชีผู้ใช้งานระดับสูงสุด ในระบบโปรแกรมต่างๆ ที่บุคลากรที่ได้รับเชิญ
 - 2.3 ให้คณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ทำเอกสารบันทึกข้อความขอเปิดเผยเอกสารบัญชีผู้ใช้งานระดับ สูงสุด ที่ ผู้อำนวยการโรงพยาบาลเมืองจันทร์ ลงลายมือชื่อแล้วยื่นต่อหัวหน้าฝ่ายบริหารทั่วไป เพื่อนำเอกสารบัญชีผู้ใช้งานระดับ สูงสุดออกจากตู้নিরภัยของโรงพยาบาล
 - 2.4 ให้คณะกรรมการสารสนเทศนำเอกสารบัญชีผู้ใช้งานระดับสูงสุดที่ได้จากหัวหน้าฝ่ายบริหารแล้วให้นำเอกสารบัญชีผู้ใช้งานระดับสูงสุด ผู้อำนวยการโรงพยาบาลเมืองจันทร์ เพื่อพิจารณาเปิดเผยแก่ บุคลากรที่ได้รับเชิญ นำไปแก้ไขปัญหาที่เกิดขึ้นต่อไปตามความเหมาะสม

	MCH - IT - 017	หน้าที่ 1/1
	เรื่อง การปฏิบัติงานนอกเวลาราชการของผู้ดูแลระบบ	
	กลุ่มงานที่เกี่ยวข้อง : งานประกันสุขภาพ ฯ	
	ผู้จัดทำ : งานประกันสุขภาพ ฯ	ผู้อนุมัติ : นพ.จิระวัตร วิเศษสังข์

ระเบียบปฏิบัติ

1. วันราชการมีการจัดเวรปฏิบัติงานนอกเวลาราชการ เวิร์ลละ 1 คน โดยปฏิบัติงานตั้งแต่เวลา 16.00 น. - 08.00 น.
2. วันเสาร์-อาทิตย์ และวันหยุดนักขัตฤกษ์มีการจัดเวรปฏิบัติงานเวิร์ลละ 1 คนโดยปฏิบัติงานตั้งแต่เวลา 08.00 น. - 16.00 น. และเวลา 16.00 น. - 08.00 น.
3. การขึ้นปฏิบัติงานนอกเวลาอาจมีการเปลี่ยนแปลงตามสถานการณ์หากมีเหตุฉุกเฉินหรือเหตุจำเป็นที่ต้องการเจ้าหน้าที่ขึ้นปฏิบัติงานเพิ่มเติมให้ทำบันทึกการขึ้นปฏิบัติงานทุกครั้ง
4. หากผู้รับบริการมีปัญหาด้านเทคนิคที่ไม่สามารถแก้ไขได้นอกเวลาการปฏิบัติงานของเจ้าหน้าที่งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ให้ติดต่อทางโทรศัพท์หรือพิจารณาเชิญเจ้าหน้าที่ ดังนี้

ด้าน Soft ware / ด้าน Hard ware

- นายเกรียงศักดิ์ บุญรอด โรงพยาบาลกันทรารมย์ โทร. 081-069-9783
- นายประยูร หาญเสมอ โรงพยาบาลศรีสะเกษ โทร. 085-025-5522

