แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กร ล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูล สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้
2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
3. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

งานเทคโนโลยีสารสรเทศเป็นหน่วยงานดูแลระบบ สนับสนุนพัฒนาระบบเทคโนโลยีสารสนเทศ ดูแลระบบคอมพิวเตอร์ทั้งด้าน Hardware Software และ ฐานข้อมูล ให้ระบบสามารถทำงานได้ตลอด 24 ชั่วโมง โดย มีวัตถุประสงค์เพื่อตอบสนองความต้องการของหน่วยงานในสถาบันฯและผู้มีส่วนได้เสียเพื่อให้ได้ข้อมูลที่ครบถ้วน ถูกต้องรวดเร็ว ตรวจสอบได้ และลดขั้นตอนการทำงาน มีการนำข้อมูลที่ได้มา ใช้ในการวางแผนการดำเนินงาน การแก้ปัญหาต่าง ๆ เพิ่มช่องทางการสื่อสารและการเรียนรู้ภายในองค์กร โดยด้านโครงสร้างพื้นฐานหรือ Infrastructure มีการเชื่อมโยงเครือข่าย LAN ครอบคลุมหน่วยงานทั้งสถาบันฯ มีการแบ่งระบบเครือข่ายออกเป็น 5 ระบบ คือ ระบบเครือข่ายการให้บริการผู้ป่วย jHos , ระบบเครือข่าย Internet, ระบบเครือข่ายให้บริการ WIFI ฟรี, ระบบเครือข่ายโทรศัพท์ และระบบเครือข่ายกล้องวงจรปิด

ก.หน้าที่และเป้าหมาย

หน้าที่

เป็นหน่วยงานสนับสนุนที่ตั้งขึ้นมาเพื่อให้บริการระบบเทคโนโลยีสารสนเทศของสถาบันฯในงานดูแลผู้ป่วยงานบริหารและบริการเครือข่ายฯ เพื่อตอบสนองความต้องการของผู้บริหาร ผู้ให้บริการและผู้รับบริการอย่างถูกต้องทันเวลาและสามารถนำไปใช้ประโยชน์ได้จริง

เป้าหมาย

- สถาบันฯมีระบบสารสนเทศและคอมพิวเตอร์ต้องมีความถูกต้อง เพียงพอ พร้อมใช้ ปลอดภัย และได้รับความพึงพอใจ
- มีการจัดเก็บข้อมูลที่สามารถสืบค้นได้ง่าย มีความถูกต้องและทันเวลา
- มีระบบการรักษาความลับและความปลอดภัยของข้อมูล
- มีการเชื่อมโยงข้อมูลเพื่อการบริหาร บริการดูแลผู้ป่วยและการพัฒนาคุณภาพ

ข.ขอบเขตการให้บริการ (Scope of Service)

1 ดูแลระบบให้พร้อมใช้งาน ตลอด 24 ชั่วโมง

2 สำรวจและจัดหาคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

3 บำรุงรักษาดูแลและรักษาความปลอดภัยของระบบเครือข่าย

4 วางแผนและออกแบบระบบรายงานสารสนเทศเพื่อตอบสนองความต้องการตามคำร้องขอข้อมูล

5 พัฒนาคุณภาพ ประเมิน ทบทวน ความสมบูรณ์ของเวชระเบียนปรับปรุงฐานข้อมูลให้ถูกต้องครบถ้วนก่อนส่งออก

6 เชื่อมโยงข้อมูลสารสนเทศ เพื่อการพัฒนาคุณภาพ

7 ให้คำปรึกษา แนะนำอบรมงานด้านสารสนเทศและการใช้คอมพิวเตอร์ให้สอดคล้องกับสถานการณ์ปัจจุบัน

8 รวบรวมข้อมูล วิเคราะห์ และนำเสนอข้อมูลต่อทีมนำหน่วยงาน

นิยามความเสี่ยง

ความเสี่ยง คือ ความไม่แน่นอนที่อาจนำไปสู่ความสูญเสียทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เป็นความเสี่ยงที่มีโดยธรรมชาติ และความเสี่ยงที่เกิดจากการเก็งกำไร ความหมายของความเสี่ยงอาจมีการตีความแตกต่างกันไปหลายอย่างตามแต่ความเชี่ยวชาญ และอาชีพของผู้ให้คำจำกัดความ

การบริหารความเสี่ยง เป็นการบริหารปัจจัย และควบคุมกิจกรรม หรือกระบวนการต่าง ๆ เพื่อลดโอกาสที่จะทำให้เกิดความเสียหาย หรือล้มเหลว ดังนั้นเพื่อควบคุมให้ระดับความเสียหาย และผลกระทบที่อาจจะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และสามารถตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตาม

แผนปฏิบัติราชการ ประจำปีงบประมาณของส่วนราชการและเป้าหมายตามแผนปฏิบัติราชการประจำปีของส่วนราชการ

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

1***. Hardware*** หมายถึง อุปกรณ์ต่างๆที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์

2***. Software*** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

3***. บุคลากร*** หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำจัดการข้อมูลและนำผลลัพธ์ออกจากระบบคอมพิวเตอร์

4. ***ข้อมูลและแฟ้มข้อมูล*** หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

5. ***หน้าที่การปฏิบัติงาน*** หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆขององค์กร

บุคลากร บุคลาการที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เ***ทคโนโลยี*** อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

1. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกัน หรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)
2. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)
3. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล
4. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) ***หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ***

1.การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงาน เลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

2.การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่ทางงานเทคโนโลยีสารสนเทศ ออกให้แล้ว อาจจะบอกให้ผู้ใต้บังคับบัญชาของตนทราบ User/Password ดังกล่าว และเมื่อผู้ใต้บังคับบัญชาทราบ User/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย ซึ่งทางงานเทคโนโลยีสารสนเทศ ต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น และกำหนด User/Password ใหม่ ให้กับหัวหน้างาน เป็นต้น

3.การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสียและการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้น

การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้น

การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควันเครื่อง

ตรวจจับความร้อน หรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้อง Server ให้มีความเสียหายน้อยที่สุด หรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

4.การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายเป็นการเพิ่มเติม

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศ ได้แก่

1. ปัจจัยภายนอก ได้แก่

1.1 ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

1.2 การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

1.3 การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server) จากการเคลื่อนย้าย หรืออื่นๆ

1.4 ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ขัดข้อง

1.5 ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

2. ปัจจัยภายใน ได้แก่

2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.2 การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ

2.3 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

การประเมินความเสียหาย

1.ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลาย เสียหายจากไวรัส

2.ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณี

ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ซอฟต์แวร์และอุปกรณ์เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่ายโดยใช้โปรแกรมป้องกันไวรัส และ Firewall เพื่อให้คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

การประเมินความเสี่ยง

ตารางที่ 1 การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง 5 ด้าน

ลำดับ	*ความเสี่ยง*	*สาเหตุ*	*ผลกระทบ*
1	***ความเสี่ยงด้าน Hardware***		
	1.1 อุปกรณ์คอมพิวเตอร์เสียหาย หมดอายุการใช้งาน Hang หรือค้าง	- มีการใช้งานหนัก - เปิดใช้งานอุปกรณ์เป็นเวลานาน - สภาวะแวดล้อม (ไฟฟ้า,อากาศ)	- ไม่สามารถทำงานต่อไปได้ - อุปกรณ์ไม่ตอบสนองการใช้งาน
	1.2 ระบบเครือข่ายมีปัญหา	- อุปกรณ์เครือข่ายเสียหาย - อุปกรณ์เครือข่ายค้างหรือขัดข้อง - ผู้ให้บริการเครือข่ายขัดข้อง	ไม่สามารถใช้บริการผ่านระบบเครือข่ายคอมพิวเตอร์ได้ ไม่ว่าจะเป็นระบบอินเตอร์เน็ต อุปกรณ์ หรือโปรแกรมต่างๆที่อยู่ในระบบเครือข่ายคอมพิวเตอร์
	1.3 การเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตขัดข้อง	- การดำเนินการของหน่วยงานภายนอกที่มีผลกระทบต่อระบบอินเตอร์เน็ต - การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - สัตว์กัดแทะสายสัญญาณ เช่น กระรอก, หรือหนู - อุปกรณ์เสื่อมสภาพ	- ไม่สามารถใช้งานระบบงานของหน่วยงานผ่านเครือข่ายอินเตอร์เน็ตได้ - ไม่สามารถเชื่อมต่อระบบงานภายนอกผ่านเครือข่ายอินเตอร์เน็ตได้
	1.4 เกิดระบบกระแสไฟฟ้าขัดข้อง	- ไฟฟ้าลัดวงจร - ภัยธรรมชาติ - น้ำรั่ว และความชื้นในอากาศ - กิจกรรมต่างๆของมนุษย์ - สัตว์กัดแทะ เช่น งู, หนู หรือแมลง - อุปกรณ์เสื่อมสภาพ	- เกิดความเสียหายของระบบอุปกรณ์ภายใน Hardware - เกิดความเสียหายกับระบบข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์
	1.5 เกิด อัคคีภัย อุทกภัย	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ - น้ำรั่ว และความชื้นในอากาศ - สัตว์กัดแทะ เช่น หนูหรือแมลง - อุปกรณ์เสื่อมสภาพ	- เกิดความเสียหายของระบบอุปกรณ์ภายใน Hardware - เกิดความเสียหายกับระบบข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์ - เกิดความเสียหายของระบบอุปกรณ์เครือข่าย ทำให้หน่วยงานใช้งานระบบ หรืออุปกรณ์ไม่ได้

ลำดับ	***ความเสี่ยง***	***สาเหตุ***	***ผลกระทบ***
2	***ความเสี่ยงด้าน Software***		
	2.1 Software ไม่สามารถทำงานได้ ติดไวรัสคอมพิวเตอร์ Malware หรือการโจมตีจากภายนอก	- ระบบปฏิบัติการเสียหาย - Software มีการทำงาน ผิดพลาด - Virus /Hacker /Spyware - การถูกโจมตีระบบจากภายนอก	- โปรแกรมหรือข้อมูลถูกทำลาย - ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ
3	***ความเสี่ยงด้านบุคลากร***		
	3.1 ขาดทักษะในการทำงาน	-ไม่เข้าใจระบบงานนั้นๆอย่างถี่ถ้วน -ปรับเปลี่ยนตำแหน่ง	งานที่ได้ไม่มี ประสิทธิภาพเท่าที่ควร
	3.2 ไม่ใช่หน้าที่หลักที่รับผิดชอบ	-ทำงานที่ไม่ใช่หน้าที่ของตน	งานอาจผิดพลาด
4	***ความเสี่ยงด้านข้อมูล***		
	4.1 ข้อมูลถูกทำลาย / สูญหาย	- Hardware เสีย - การปฏิบัติงานผิดพลาด - ผู้ไม่หวังดี - ไวรัสเรียกค่าไถ่ (Ransomware) - ไวรัส/เวิร์ม -ขาดอุปกรณ์ป้องกันข้อมูลที่ดี	ไม่มีข้อมูลเพื่อนำไปใช้งาน
	4.2 ข้อมูลผิดพลาด	-เนื่องจากการปฏิบัติงานผิดพลาด -โปรแกรมทำงานผิดพลาด	ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้
	4.3 ความปลอดภัยของข้อมูล	- ถูกโจรกรรมข้อมูลของผู้ป่วย - ไวรัสเรียกค่าไถ่ (Ransomware) - ถูกเผยแพร่สาธารณะบนอินเตอร์เน็ต - ไวรัส/เวิร์ม -ขาดอุปกรณ์ป้องกันข้อมูลที่ดี -ขาดการตรวจสอบ -ขาดบุคลากรที่มีความรู้อย่างแท้จริง	- โปรแกรมหรือข้อมูลเสียหาย - ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ - ข้อมูลสำคัญของหน่วยงานเสียหาย - ข้อมูลเสียหาย - ข้อมูลรั่วไหล
5	***ความเสี่ยงด้านหน้าที่การปฏิบัติ***		
	5.1 ปฏิบัติหน้าที่ไม่ถูกต้อง	ไม่เข้าใจในขั้นตอนปฏิบัติ	ไม่สามารถทำงานได้หรืองานมีความผิดพลาด
	5.2 ละเลยการปฏิบัติ	ไม่เอาใจใส่ในงาน	งานไม่มีประสิทธิภาพ

การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

พิจารณาจาก การประเมินระดับโอกาสในการเกิดเหตุการณ์ (Likelihood) และความรุนแรงของผลกระทบ จากเหตุการณ์ความเสี่ยง (Impact) โดยใช้ตาราง risk matrix

Likelihood / ระดับโอกาสในการเกิดเหตุการณ์

ระดับ	***โอกาสที่จะเกิด***	***ผลกระทบ***
1	น้อยมาก	5 ปีต่อครั้ง
2	น้อย	2 – 5 ปีต่อครั้ง
3	ปานกลาง	1 ปีต่อครั้ง
4	สูง	2 – 6 เดือนไม่เกิน 5 ครั้ง
5	สูงมาก	1 เดือนต่อครั้ง หรือมากกว่า

ระดับความรุนแรงของผลกระทบ (Impact)

1. ระดับผลกระทบความเสี่ยงทางคลินิก (Clinical risk) * ดัดแปลงจาก NCC MERP Index for Categorizing Medication Errors

ระดับ ความสำคัญ	ระดับ ความรุนแรง	ผลกระทบ
1 / น้อยมาก	A No error	เหตุการณ์ซึ่งมีโอกาสเกิดความคลาดเคลื่อน/เหตุการณ์เกือบพลาด แต่ตรวจพบหรือแก้ไขทันก่อนเกิดเหตุ ดักจับได้ก่อนที่จะถึงผู้ป่วย
2 / น้อย	B Error no harm	เกิดความคลาดเคลื่อนแล้ว แต่ถูกตรวจพบก่อน ยังไม่ถึงผู้ป่วย
	C Error no harm	เกิดความคลาดเคลื่อนกับผู้ป่วยแต่ไม่เกิดอันตราย
	D Error no harm	เกิดความคลาดเคลื่อน กับผู้ป่วยส่งผลให้ต้องเฝ้าระวัง (to observe or record relevant physiological or psychological signs) เพื่อมั่นใจว่าไม่เกิดอันตราย
3 / ปานกลาง	E Error no harm	เกิดความคลาดเคลื่อนต่อผู้ป่วย ส่งผลให้เกิดความเสียหายต่อผู้ป่วยเป็นการชั่วคราวต้องมีการบำบัดรักษาเพิ่มเติม (may include change in therapy or active medical/surgical treatment)
	F Error no harm	เกิดความคลาดเคลื่อนต่อ ผู้ป่วย ส่งผลให้เกิดความเสียหายต่อผู้ป่วยเป็นการชั่วคราวต้องรับไว้ใน รพ หรือต้องรักษานานกว่ากำหนด
4 / สูง	G Error no harm	เกิดความคลาดเคลื่อนต่อ ผู้ป่วย ส่งผลให้เกิดความเสียหายต่อ ผู้ป่วยเป็นการถาวร
	H Error no harm	เกิดความคลาดเคลื่อนต่อ ผู้ป่วย ส่งผลให้เกิดความเสียหายต่อ ผู้ป่วยต้องช่วยชีวิตหรือเกือบเสียชีวิต(includes cardiovascular and respiratory support e,g, CPR, intubation, etc.)
5 / สูงมาก	I Error no death	เกิดความคลาดเคลื่อนต่อ ผู้ป่วย ส่งผลให้ ผู้ป่วย เสียชีวิต

ตารางแสดงระยะเวลาและระดับดำเนินการแบ่งตามระดับความรุนแรงของอุบัติการณ์

ระดับความรุนแรงของผลกระทบ		***ระยะเวลารายงาน RMC ภายใน (วัน)***	***ระดับดำเนินการ***
ความเสี่ยงทั่วไป	***ความเสี่ยงทางคลินิก***		
1	A	3	- เจ้าหน้าที่ประสบเหตุแก้ไขปัญหาเฉพาะหน้า - รายงานหัวหน้าหน่วยงาน ภายใน 3 วัน
2	B,C,D	3	- เจ้าหน้าที่ประสบเหตุแก้ไขปัญหาเฉพาะหน้า - รายงานหัวหน้าหน่วยงาน ภายใน 3 วัน เพื่อร่วมวางแนวทางแก้ไขระดับหน่วยงาน
3	E,F	2	- เจ้าหน้าที่ประสบเหตุแก้ไขปัญหาเฉพาะหน้า - รายงานหัวหน้าหน่วยงานทันที - หน่วยงานทำ RCA และตอบกลับทีมความเสี่ยงใน 7 วัน
4	G,H	1	- เจ้าหน้าที่ประสบเหตุแก้ไขปัญหาเฉพาะหน้า - รายงานหัวหน้าหน่วยงานทันที - หน่วยงานทำ RCA และตอบกลับทีมความเสี่ยงใน 7 วัน
5 Sentinel event	I Sentinel event	ด้วยวาจาทันที	- เจ้าหน้าที่ประสบเหตุแก้ไขปัญหาเฉพาะหน้า - และรายงานหัวหน้าหน่วยงานทันทีเพื่อรายงาน - ผู้บังคับบัญชาตามลำดับด้วยวาจาทันที กรณีเร่งด่วน/ sentinel event ผู้อำนวยการมอบทีมที่ได้รับมอบหมายดำเนินการเร่งด่วน - หน่วยงานร่วมกับทีมความเสี่ยงทำ RCA วางมาตรการป้องกันภายใน 7 วัน

Risk Matrix คือ การนำระดับโอกาสในการเกิดเหตุการณ์ (Likelihood) และความรุนแรงของผลกระทบ จากเหตุการณ์ความเสี่ยง (Impact) มาวิเคราะห์และจัดลำดับความสำคัญของเหตุการณ์เพื่อใช้ประกอบการตัดสินใจดำเนินการแก้ไข

ตารางแสดง Risk Matrix สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

โอกาสที่จะเกิด Likelihood	***ระดับความรุนแรงของผลกระทบ (Impact)***				
	1	2	3	4	5
5	Low	Significant	High	High	High
4	Low	Significant	Significant	High	High
3	Low	Low	Significant	High	High
2	Very Low	Low	Significant	Significant	Significant
1	Very Low	Very Low	Low	Low	Significant

จากตาราง risk matrix สามารถแบ่งระดับความสำคัญของความเสี่ยงเป็น 4 ระดับ จากระดับความสำคัญจากน้อยไปมาก ดังนี้

1. Very low risk level หมายถึง ระดับความเสี่ยงที่โรงพยาบาลสามารถยอมรับได้เนื่องจากมีมาตรการควบคุมแล้ว
2. Low risk level หมายถึง ระดับความเสี่ยงที่โรงพยาบาลสามารถยอมรับได้แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ
3. Significant risk level หมายถึง ระดับความเสี่ยงไม่สามารถยอมรับได้ หน่วยงานต้องวางแผนบริหารจัดการ
4. High risk level หมายถึง ระดับความเสี่ยงที่โรงพยาบาลไม่สามารถยอมรับได้ จำเป็นต้องบริหารจัดการระดับโรงพยาบาลเพื่อลดระดับความสำคัญลงให้ต่ำกว่า high risk level

ประเด็นความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

ลำดับ	***ความเสี่ยง***	***โอกาสที่จะเกิด***	***ผลกระทบ***	***คะแนน***
1	***ความเสี่ยงด้าน Hardware***			
	1.1 อุปกรณ์คอมพิวเตอร์เสียหาย หมดอายุการใช้งาน Hang หรือค้าง	3	1	3
	1.2 ระบบเครือข่ายมีปัญหา	3	3	9
	1.3 การเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตขัดข้อง	3	3	9
	1.4 เกิดระบบกระแสไฟฟ้าขัดข้อง	4	2	8
	1.5 เกิด อัคคีภัย อุทกภัย	2	2	4
2	***ความเสี่ยงด้าน Software***			
	2.1 Software ไม่สามารถทำงานได้ ติดไวรัสคอมพิวเตอร์ Malware หรือการโจมตีจากภายนอก	3	3	9
3	***ความเสี่ยงด้านบุคลากร***			
	3.1 ขาดทักษะในการทำงาน	4	2	8
	3.2 ไม่ใช่หน้าที่หลักที่รับผิดชอบ	2	2	4
4	***ความเสี่ยงด้านข้อมูล***			
	4.1 ข้อมูลถูกทำลาย / สูญหาย	1	2	2
	4.2 ข้อมูลผิดพลาด	4	2	8
	4.3 ความปลอดภัยของข้อมูล	1	3	3
5	***ความเสี่ยงด้านหน้าที่การปฏิบัติ***			
	5.1 ปฏิบัติหน้าที่ไม่ถูกต้อง	4	2	8
	5.2 ละเลยการปฏิบัติ	1	2	2

การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณา จัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและ ผลกระทบที่เกิดขึ้นและขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ (ความถี่) X ความรุนแรงของเหตุการณ์ต่างๆ (ผลกระทบ)

ซึ่งใช้เกณฑ์ในการจัดแบ่ง ดังนี้

ระดับคะแนนความเสี่ยง	***จัดระดับความเสี่ยง***	***กลยุทธ์ในการจัดการความเสี่ยง***	***พื้นที่สี***
1 – 7	ต่ำ	สามารถยอมรับความเสี่ยง (มีมาตรการควบคุมแล้ว)	เขียว
8 – 14	ปานกลาง	ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	เหลือง
15 – 20	สูง	ความเสี่ยงไม่สามารถยอมรับได้ (หน่วยงานต้องวางแผนบริหารจัดการ)	ส้ม
20 - 25	สูงมาก	ไม่สามารถยอมรับได้ (บริหารจัดการระดับโรงพยาบาล)	แดง

ลำดับ	*ความเสี่ยง*	*ค่าระดับความเสี่ยง*	*กลยุทธ์การจัดการความเสี่ยง*	*แนวทางการดำเนินการจัดการความเสี่ยง*
1	***ความเสี่ยงด้าน Hardware***			
	1.1 อุปกรณ์คอมพิวเตอร์เสียหาย หมดอายุการใช้งาน Hang หรือค้าง		สามารถยอมรับความเสี่ยง (มีมาตรการควบคุมแล้ว)	- มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ - มีการปิดอุปกรณ์คอมพิวเตอร์ในเวลาที่ไม่มีการใช้งาน เพื่อยืดอายุการใช้งานของอุปกรณ์ - มีการใช้งานเครื่องสำรองไฟฟ้า เพื่อป้องกันปริมาณไฟฟ้าไม่คงที่
	1.2 ระบบเครือข่ายมีปัญหา		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- มีการตรวจเช็คการทำงานของอุปกรณ์ในระบบเครือข่าย (Monitor) อย่างสม่ำเสมอ - มีการปิดอุปกรณ์ของระบบเครือข่ายในเวลาที่ไม่มีการใช้งาน เพื่อยืดอายุการใช้งานของอุปกรณ์
	1.3 การเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตขัดข้อง		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- สลับไปใช้งานสายสัญญาณอินเตอร์เน็ตสำรอง - ประสานผู้ให้บริการอินเตอร์เน็ตทำการแก้ไข - มีการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ - มีการตรวจเช็คการทำงานของอุปกรณ์ (Monitor) และปริมาณการใช้งานอินเตอร์เน็ตเป็นประจำ
	1.4 เกิดระบบกระแสไฟฟ้าขัดข้อง		สามารถยอมรับความเสี่ยง (มีมาตรการควบคุมแล้ว)	- มีการติดตั้งระบบสำรองไฟฟ้าให้มีความครอบคลุมกับระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และตรวจสอบประสิทธิภาพของระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์ตามระยะเวลาที่กำหนด - มีเครื่องกำเนิดไฟฟ้า (Generator) ของทางโรงพยาบาลสวนสราญรมย์ ซึ่งสามารถจ่ายไฟฟ้าให้ใช้งานหลังเกิดไฟฟ้าดับภายใน 30 วินาที
	1.5 เกิด อัคคีภัย อุทกภัย		สามารถยอมรับความเสี่ยง (มีมาตรการควบคุมแล้ว)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง - มีการตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - มีการสำรองข้อมูลที่สำคัญเก็บไว้

ลำดับ	*ความเสี่ยง*	*ค่าระดับความเสี่ยง*	*กลยุทธ์การจัดการความเสี่ยง*	*แนวทางการดำเนินการจัดการความเสี่ยง*
2	***ความเสี่ยงด้าน Software***			
	2.1 Software ไม่สามารถทำงานได้ ติดไวรัสคอมพิวเตอร์ Malware หรือการโจมตีจากภายนอก		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- มีการติดตั้งอุปกรณ์ Firewall เพื่อป้องกันการโจมตีระบบจากภายนอก - มีการตรวจเช็คการทำงานของอุปกรณ์ (Firewall) การฝ้าระวัง (Monitor) การโจมตีจากภายนอกอย่างสม่ำเสมอ - มีการปรับปรุงโปรแกรมของอุปกรณ์ (Firewall) ให้เป็นปัจจุบัน - มีการติดตั้งระบบปฏิบัติการ Windows ถูกลิขสิทธิ์ และและปรับปรุงระบบปฏิบัติการ Windows ให้เป็นปัจจุบัน - มีการติดตั้งโปรแกรมสแกนไวรัส และปรับปรุงระบบฐานข้อมูลของระบบสแกนไวรัสคอมพิวเตอร์ให้เป็นปัจจุบัน
3	***ความเสี่ยงด้านบุคลากร***			
	3.1 ขาดทักษะในการทำงาน		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- แจ้งหัวหน้างานที่รับผิดชอบให้ทราบ เพื่อให้แนะนำวิธีการทำงานให้ถูกต้องครบถ้วน
	3.2 ไม่ใช่หน้าที่หลักที่รับผิดชอบ		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- แจ้งหัวหน้างานที่รับผิดชอบให้ทราบ เพื่อแก้ไขให้ถูกต้อง
4	***ความเสี่ยงด้านข้อมูล***			
	4.1 ข้อมูลถูกทำลาย / สูญหาย		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- มีการสำรองข้อมูลเก็บไว้ - มีการติดตั้งอุปกรณ์ Firewall เพื่อป้องกันการโจมตีระบบจากภายนอก - มีการตรวจเช็คการทำงานของอุปกรณ์ (Firewall) การฝ้าระวัง (Monitor) การโจมตีจากภายนอกอย่างสม่ำเสมอ - มีการปรับปรุงโปรแกรมของอุปกรณ์ (Firewall) ให้เป็นปัจจุบัน

ลำดับ	*ความเสี่ยง*	*ค่าระดับความเสี่ยง*	*กลยุทธ์การจัดการความเสี่ยง*	*แนวทางการดำเนินการจัดการความเสี่ยง*
				- มีการติดตั้งระบบปฏิบัติการ Windows ถูกลิขสิทธิ์ และและปรับปรุงระบบปฏิบัติการ Windows ให้เป็นปัจจุบัน - มีการติดตั้งโปรแกรมสแกนไวรัส และปรับปรุงระบบฐานข้อมูลของระบบสแกนไวรัสคอมพิวเตอร์ให้เป็นปัจจุบัน
	4.2 ข้อมูลผิดพลาด		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- มีการตรวจเช็คความถูกต้องและความครบถ้วนของข้อมูลอยู่อย่างสม่ำเสมอ - มีการรายงานข้อมูลที่ผิดพลาดให้ผู้ที่รับผิดชอบแก้ไขข้อมูลให้ถูกต้อง
	4.3 ความปลอดภัยของข้อมูล		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- มีการติดตั้งอุปกรณ์ Firewall เพื่อป้องกันการโจมตีระบบจากภายนอก - มีการตรวจเช็คการทำงานของอุปกรณ์ (Firewall) การฝ้าระวัง (Monitor) การโจมตีจากภายนอกอย่างสม่ำเสมอ - มีการปรับปรุงโปรแกรมของอุปกรณ์ (Firewall) ให้เป็นปัจจุบัน - มีการสำรองข้อมูลที่สำคัญเก็บไว้
5	***ความเสี่ยงด้านหน้าที่การปฏิบัติ***			
	5.1 ปฏิบัติหน้าที่ไม่ถูกต้อง		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- แจ้งหัวหน้างานที่รับผิดชอบให้ทราบ เพื่อให้แนะนำวิธีการทำงานให้ถูกต้องครบถ้วน
	5.2 ละเลยการปฏิบัติ		ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- แจ้งหัวหน้างานที่รับผิดชอบให้ทราบ เพื่อแก้ไขให้ถูกต้อง

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ตารางที่ 2 แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ประเภทความเสี่ยง/กิจกรรม	*แนวทางการควบคุม*	*ระยะเวลาเริ่มต้น/สิ้นสุด*	*ปีงบประมาณ*												*หมายเหตุ*
			ต.ค.	*พ.ย.*	*ธ.ค.*	*ม.ค.*	*ก.พ.*	*มี.ค.*	*เม.ย.*	*พ.ค.*	*มิ.ย.*	*ก.ค.*	*ส.ค.*	*ก.ย.*	
1. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ															
1.1 ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ - ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	- ทุกวัน/ทุกสัปดาห์ - ทุกเดือน - ทุกเดือน													
1.2 ข้อมูลเสียหายเกิดจากอุปกรณ์	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ -ทดสอบการกู้คืนฐานข้อมูลและระบบสารสนเทศ	- ทุกวัน/ทุกสัปดาห์ - ทุกเดือน - ทุกเดือน													

ตารางที่ 2 แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ (ต่อ)

ประเภทความเสี่ยง/กิจกรรม	*แนวทางการควบคุม*	*ระยะเวลาเริ่มต้น/สิ้นสุด*	*ปีงบประมาณ*												*หมายเหตุ*
			ต.ค.	*พ.ย.*	*ธ.ค.*	*ม.ค.*	*ก.พ.*	*มี.ค.*	*เม.ย.*	*พ.ค.*	*มิ.ย.*	*ก.ค.*	*ส.ค.*	*ก.ย.*	
2. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ															
2.1 ไฟไหม้ห้อง Server	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	- ทุกเดือน													
2.2 ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก	- ทุกเดือน													
3. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล															
3.1 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบระบบสำรองไฟฟ้า (UPS)	- ทุกเดือน													
3.2 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกเดือน													
3.3 การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกเดือน													

ตารางที่ 2 แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ (ต่อ)

ประเภทความเสี่ยง/กิจกรรม	*แนวทางการควบคุม*	*ระยะเวลาเริ่มต้น/สิ้นสุด*	*ปีงบประมาณ*												*หมายเหตุ*
			ต.ค.	*พ.ย.*	*ธ.ค.*	*ม.ค.*	*ก.พ.*	*มี.ค.*	*เม.ย.*	*พ.ค.*	*มิ.ย.*	*ก.ค.*	*ส.ค.*	*ก.ย.*	
4. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ															
4.1 การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต	- กำหนดสิทธิ์ในการเข้าถึงข้อมูล	- เมื่อแต่งตั้ง /โยกย้าย / ลาออก / เกษียณอายุราชการ													
5. อุปกรณ์คอมพิวเตอร์เสียหาย															
5.1 คอมพิวเตอร์ไม่สามารถใช้งานได้	- บำรุงรักษาคอมพิวเตอร์ เช่น เป่าฝุ่น สแกนฮาร์ดดิสค์ disk cleanup และ disk defragmenter	-ทุก 3 เดือน			✓			✓			✓			✓	