แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

สำนักงานสาธารณสุขอำเภออู่ทอง

บทที่ ๑ บทนำ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสนใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การ ติดตามควบคุม และวัดผลการปฏิบัติงานตลอดจนการใช้ทรัพยากรต่างๆอย่างเหมาะสมและมี ประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่ง ในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการ ปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มี ความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบโดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยง ใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและ ผลกระทบที่เกิดขึ้นจัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูล สารสนเทศ

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศมีความเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้ อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

สำนักงานสาธารณสุขอำเภออู่ทองและโรงพยาบาลส่งเสริมสุขภาพตำบลในสังกัดมีระบบ บริหารจัดการข้อมูลสารสนเทศ และได้นำระบบบริการผู้ป่วยโดยใช้ฐานข้อมูลตั้งแต่ปี ๒๕๕๔ โดย เริ่มต้นด้วยโปรแกรม HOSxP_PCU ซึ่งเป็นโปรแกรมที่พัฒนาโดยบริษัทบางกอกเมดิคอลซอฟแวร์ และสำนักงานสาธารณสุขจังหวัดร้อยเอ็ดและปัจจุบัน ใช้โปรแกรม MyPCU โดยบริษัท อินไซด์เดต้าคอนซัลแตนท์ จำกัดเป็นผู้พัฒนา

นิยาม ความเสี่ยงของระบบสารสนเทศ

คือ เหตุการณ์หรือการกระทำใดๆที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผล กระทบหรือสร้างความเสียหายหรือความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบริหาร งานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลขอมูลทั้งภายในและ ภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

๑. Hardware หมายถึงอุปกรณ์ต่างๆที่กระทำกับข้อมูลเอกสารทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์

๒. Software หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

๓. บุคลากร หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำจัดการข้อมูลและนำผลลัพธ์ออกจากระบบคอมพิวเตอร์

๔. ข้อมูลและแฟ้มข้อมูล หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

๕. หน้าที่ปฏิบัติงาน หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

องค์กรโครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานของ องค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆขององค์กร

บุคลากร บุคลาการที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกันบุคลากร ที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งตอไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศเพื่อส่งต่อไปยังบุคลากรที่ใช้ ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดย ต้องดำเนินการดังต่อไปนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒. มีการจัดทาแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับ ระบบสารสนเทศ (IT Contingency Plan)

๓. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล

๔. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการ ความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการ ดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance)

หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๑. การหลีกเลี่ยง (Terminate)

เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การ เลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความ เสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกบสิ่งที่จะเกิดขึ้นจึง หลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงาน เลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาส ของหน่วยงานได้

๒. การยอมรับ(Take)

เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิด ความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการ จัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้User/Password ที่

ทางศูนย์คอมฯ ออกให้แล้ว อาจจะบอกให้ผู้ใต้บังคับบัญชาของตนทราบUser/Passwordดังกล่าวและเมื่อผู้ใต้บังคับบัญชาทราบ User/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งใน กรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย ซึ่ง ทางศูนย์คอมฯ ต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นและกำหนด User/Password ใหม่ให้กับหัวหน้างาน เป็นต้น

๓. การควบคุม(Treat)

เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรง ของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการ ควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบ ป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้า สู่ระบบเครือข่ายเป็นการป้องกันบุคคลไวรัส มิให้เขาถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการ ทำงานของระบบคอมพิวเตอร์ เป็นต้น การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิงอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควันเครื่องตรวจจับความร้อน หรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายใน ห้อง Server ให้มีความเสียหายน้อยที่สุด หรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของ ระบบเครือข่าย เป็นต้น

๔. การถ่ายโอน (Transfer)

การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์ เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกันหรอสัญญาการบำรุงรักษาหลังการขายเป็นการ เพิ่มเติม

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกรมการแพทย์ ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักภัยพิบัติหรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ข้อมูล

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวม

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)จากการเคลื่อนย้าย หรืออื่นๆ

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสยหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ

๒.๓ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก(Hacker)โดยไม่ได้รับอนุญาต

การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒. ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบ ฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแล ทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถ ดำเนินการได้ในทุกกรณีตามที่ระบุ

ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์ สำนักงานสาธารณสุขอำเภออู่ทองและโรงพยาบาลส่งเสริมสุขภาพตำบลในสังกัด มีการกำหนด นโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ซอฟต์แวร์ เพื่อป้องกันการ โจมตีและบุกรกเข้ามายังเครือข่ายโดยใช้โปรแกรมป้องกันไวรัสและFirewall เพื่อให้คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของ รพ.สต. เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหาย ที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของ รพ.สต.ในอำเภออู่ทอง มีการกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การ ประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยง เพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

การประเมินความเสี่ยง

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๑	**ความเสี่ยงด้าน Hardware**		
	๑.๑ อุปกรณ์คอมพิวเตอร์เสียหาย	- หมดอายุการใช้งาน - มีการใช้งานหนัก - สภาวะแวดล้อม (ไฟฟ้า,อากาศ)	ไม่สามารถทำงานต่อไปได้
	๑.๒ ระบบเครือข่ายมีปัญหา	- อุปกรณ์เครือข่ายเสียหาย - ผู้ให้บริการเครือข่ายขัดข้อง	ไม่สามารถใช้บริการผ่านเครือข่ายได้
๒	**ความเสี่ยงด้าน Software**		
	๒.๑Software ไม่สามารถทำงานได้	- ระบบปฏิบัติการเสียหาย - Software มีการทำงานผิดพลาด - Virus /Hacker /Spyware	ไม่สามารถให้บริการได้
๓	**ความเสี่ยงดานบุคลากร**		
	๓.๑ ขาดทักษะในการทำงาน	-ไม่เข้าใจระบบงานนั้นๆ อย่างถี่ถ้วน -ปรับเปลี่ยนตำแหน่ง	งานที่ได้ไม่มี ประสิทธิภาพเท่าที่ควร
	๓.๒ ไม่ใช่หน้าที่หลักที่รับผิดชอบ	-ทำงานที่ไม่ใช่หน้าที่ของตน	งานอาจผิดพลาด

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน(ต่อ)

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๔	**ความเสี่ยงด้านข้อมูล**		
	๔.๑ ข้อมลถูกทำลาย / สูญหาย	- Hardware เสีย - การปฏิบัติงานผิดพลาด - ผู้ไมหวังดี	ไม่มีข้อมูลเพื่อนำไปใช้งาน
	๔.๒ ข้อมลผิดพลาด	-เนื่องจากการปฏิบัติงานผิดพลาด -โปรแกรมทำงานผิดพลาด	ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้
	๔.๓ ความปลอดภัยของข้อมูล	-ขาดอุปกรณ์ป้องกันข้อมูลที่ดี -ขาดการตรวจสอบ -ขาดบุคลากรที่มีความรู้อย่างแท้จริง	- อาจทำให้ข้อมูลเสียหาย - ข้อมูลรั่วไหล
๕	**ความเสี่ยงด้านหน้าที่การปฏิบัติ**		
	๕.๑ปฏิบัติหน้าที่ไม่ถูกต้อง	ไม่เข้าใจในขั้นตอนปฏิบัติ	ไม่สามารถทำงานได้หรืองานมีความผิดพลาด
	๕.๒ ละเลยการปฏิบัติ	ไม่เอาใจใส่ในงาน	งานไม่มีประสิทธิภาพ

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ตารางที่ ๒ แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ประเภทความเสี่ยง	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.	
๑. ความเสี่ยงด้านความ เสียหายของระบบสารสนเทศและข้อมูล สารสนเทศ															
๑.๑ ระบบฐานข้อมูล/ โปรแกรมที่ให้บริการเกิด ความเสียหาย	๑จัดทำการสำรองข้อมูลแบบอัตโนมัติ	ทุกวัน/ทุกสัปดาห์													
	๒จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	ทุกสัปดาห์เดือนละ ๔ ครั้ง	←											→	
	๓ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	ทุกสัปดาห์เดือนละ ๔ ครั้ง													
๑.๒ ข้อมูลเสียหายเกิดจาก อุปกรณ์ บันทึกข้อมูล (Hard disk) ชำรุด	๑ จัดทำการสำรองข้อมูลแบบอัตโนมัติ	ทุกวัน/ทุกสัปดาห์													
	๒ จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	ทุกสัปดาห์เดือนละ ๔ ครั้ง	←											→	
	๓ทดสอบการกู้คืนฐานข้อมูลและระบบสารสนเทศ	ทุกสัปดาห์เดือนละ ๔ ครั้ง													
๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ															
๒.๑ ไฟไหม้ห้อง Server	ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ ดับเพลิง	ทุกวันที่ ๓๐ ก.ย. ของทุกปี												☐	
๒.๒ ระบบเครือข่ายสื่อสารหลัก เสียหาย/ขัดข้อง	ตรวจสอบระบบ เครือข่ายสื่อสารหลัก	ทุก ๓ เดือน			☐			☐			☐			☐	
๓. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล														☐	
๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้า ดับ	ตรวจสอบระบบ สำรองไฟฟ้า (UPS)	ทุกวันที่ ๓๐ ก.ย. ของทุกปี													
๓.๒ การถูกเจาะหรือลักลอบ(Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	ตรวจสอบระบบ ป้องกันการบุกรุก ระบบเครือข่าย (Firewall)	ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน	←											→	

๓.๓ การถูกเจาะหรือลักลอบ(Hack) ระบบฐานข้อมูล	ตรวจสอบระบบ ป้องกันการบุกรุก ระบบเครือข่าย (Firewall)	ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน														
๓.๔ ขาดเครื่องมือป้องกันหรือตรวจจับ ไวรัส	มีโปรแกรมป้องกันไวรัสและUpdateฐานข้อมูลไวรัส	สัปดาห์ละ ๑ ครั้ง														
๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ																
๔.๑ การเข้าใช้ระบบเครือข่าย คอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับ อนุญาต	กำหนดสิทธิ์ในการ เข้าถึงข้อมูล	เมื่อแต่งตั้ง/โยกย้าย / ลาออก / เกษียณอายุราชการ														
๕. อุปกรณ์คอมพิวเตอร์เสียหาย																
๕.๑ คอมพิวเตอร์ไม่สามารถใช้งานได้	บำรุงรักษา คอมพิวเตอร์ เช่น เป่าฝุ่น สแกนฮาร์ดดิสค์ disk cleanup และ disk defragmenter	สัปดาห์ละ ๑ ครั้ง														