

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

โรงพยาบาลบ้านด่าน

อำเภอบ้านด่าน จังหวัดบุรีรัมย์

บทที่ ๑ บทนำ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดีโดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กรทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อ การดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการ ความเสี่ยงโดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ โรงพยาบาลบ้านด่าน
๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

โรงพยาบาลบ้านด่านมีระบบบริหารจัดการข้อมูลสารสนเทศ และได้นำระบบบริการผู้ป่วยโดยใช้ฐานข้อมูลตั้งแต่ปี ๒๕๕๗ โดย เริ่มต้นด้วยโปรแกรม HOSXP ซึ่งเป็นโปรแกรมที่พัฒนาโดยบริษัทบางกอกเมดิคอลซอฟต์แวร์

นิยาม ความเสี่ยงของระบบสารสนเทศ

คือ เหตุการณ์หรือการกระทำใดๆที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบต่อหรือสร้างความเสียหายหรือความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบริหารงานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลของข้อมูลทั้งภายในและภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

๑. **Hardware** หมายถึง อุปกรณ์ต่างๆที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช้คอมพิวเตอร์

๒. **Software** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

๓. **บุคลากร** หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำ จัดการข้อมูลและนำผลลัพธ์ออกจากระบบคอมพิวเตอร์

๔. **ข้อมูลและแฟ้มข้อมูล** หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

๕. **หน้าที่การปฏิบัติงาน** หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็ฝ่ายต่างๆขององค์กร

บุคลากร บุคลากรที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)
๒. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan)
๓. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล
๔. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพ ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance)

หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๑. การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่เกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมีได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

๒. การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่ทางศูนย์คอมพิวเตอร์ ออกให้แล้ว อาจจะบอกให้ผู้ได้บังคับบัญชาของตนทราบ User/Password ดังกล่าว และเมื่อผู้ได้บังคับบัญชาทราบ User/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย ซึ่งทางศูนย์คอมพิวเตอร์ต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น และกำหนด User/Password ใหม่ ให้กับหัวหน้างาน เป็นต้น

๓. การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสียหายลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความเสียหายเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้นการควบคุมขนาดของความเสียหาย เป็นวิธีการที่พยายามจะลดความรุนแรงของความเสียหายเมื่อเกิดความเสียหายขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควันเครื่องตรวจจับความร้อน หรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความเสียหายของอุปกรณ์ภายในห้อง Server ให้มีความเสียหายน้อยที่สุดหรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

๔.การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงานองค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายเป็นการเพิ่มเติม

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกรมการแพทย์ ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server) จากการเคลื่อนย้าย หรืออื่นๆ

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ชัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ

๒.๓ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก(Hacker)โดย

ไม่ได้รับอนุญาต

การประเมินความเสียหาย

๑. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒. ความเสียหายที่เกิดผลเสียหายจะต้องหยุดระบบชั่วคราว ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์โรงพยาบาลบ้านด่าน มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ซอฟต์แวร์ เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่ายโดยใช้โปรแกรมป้องกันไวรัสและFirewall เพื่อให้คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของโรงพยาบาล เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของ โรงพยาบาลบ้านด่าน มีการกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วย การวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

การประเมินความเสี่ยง

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน

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

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน(ต่อ)

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๔.	ความเสี่ยงด้านข้อมูล		
	๔.๑ ข้อมูลถูกทำลาย / สูญหาย	- Hardware เสีย - การปฏิบัติงานผิดพลาด - ผู้ไม่หวังดี	ไม่มีข้อมูลเพื่อนำไปใช้งาน
	๔.๒ ข้อมูลผิดพลาด	- เนื่องจากการปฏิบัติงานผิดพลาด - โปรแกรมทำงานผิดพลาด	ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้
	๔.๓ ความปลอดภัยของข้อมูล	- ขาดอุปกรณ์ป้องกันข้อมูลที่ดี - ขาดการตรวจสอบ - ขาดบุคลากรที่มีความรู้ อย่างแท้จริง	อาจทำให้ข้อมูลเสียหาย ข้อมูลรั่วไหล
๕.	ความเสี่ยงด้านหน้าที่การปฏิบัติ		
	๕.๑ ปฏิบัติหน้าที่ไม่ถูกต้อง	- ไม่เข้าใจในขั้นตอนปฏิบัติ	ไม่สามารถทำงานได้หรือ งานมีความผิดพลาด
	๕.๒ ละเลยการปฏิบัติ	- ไม่เอาใจใส่ในงาน	งานไม่มีประสิทธิภาพ

ตารางที่ ๒ 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.	
๓.๔ ขาดเครื่องมือป้องกันหรือ ตรวจจับไวรัส ๔. ความเสี่ยงด้านสิทธิการใช้งาน ของผู้ใช้งานในแต่ละระดับ ๔.๑ การเข้าใช้ระบบเครือข่าย คอมพิวเตอร์ภายในองค์กรโดย ไม่ได้รับอนุญาต ๕. อุปกรณ์คอมพิวเตอร์เสียหาย ๕.๑ คอมพิวเตอร์ไม่สามารถใช้ งานได้	- มีโปรแกรมป้องกันไวรัสและ Update ฐานข้อมูลไวรัส - กำหนดสิทธิในการเข้าถึงข้อมูล - บำรุงรักษาคอมพิวเตอร์ เช่น เป่าฝุ่น สแกนฮาร์ดดิสก์ disk cleanup และ disk defragmenter	- สัปดาห์ละ ๑ ครั้ง - เมื่อแต่งตั้ง/โยกย้าย /ลาออก / เกษียณอายุราชการ - สัปดาห์ละ ๑ ครั้ง												

ส่วนงานย่อย ศูนย์คอมพิวเตอร์ กลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์ โรงพยาบาลบ้านด่าน

รายงานการประเมินผลการควบคุมภายใน

สำหรับระยะเวลาการดำเนินงานสิ้นสุด ณ วันที่ ๓๐ เดือน เมษายน พ.ศ. ๒๕๖๙

ภารกิจตามกฎหมายที่ จัดตั้งหน่วยงานของรัฐ หรือภารกิจตามแผนการ ดำเนินการหรือภารกิจอื่นๆ ที่สำคัญของหน่วยงานของ รัฐ/วัตถุประสงค์	ความเสี่ยง	การควบคุมภายในที่มีอยู่	การ ประเมินผล การควบคุม ภายใน	ความเสี่ยงที่ยังมีอยู่	การปรับปรุงการ ควบคุมภายใน	กำหนดเสร็จ/ หน่วยงาน ผู้รับผิดชอบ
การควบคุมด้าน Hardware Software และ application_ - วัตถุประสงค์ ๑.เพื่อสำรวจความต้องการ คอมพิวเตอร์ในการพัฒนา ระบบงาน ๒.เพื่อให้เข้าใจถึงการใช้ คอมพิวเตอร์ ที่ถูกต้อง เหมาะสม	๑.การจัดซื้ออุปกรณ์ คอมพิวเตอร์ ไม่เพียงพอ ๒.คอมพิวเตอร์และอุปกรณ์ ถูกใช้งานอย่างไม่เหมาะสม และไม่ถูกวิธี ๓.คอมพิวเตอร์ล้าสมัย ๔.ไม่มีระบบบำรุงรักษาที่ ต่อเนื่องเหมาะสม ๕.คอมพิวเตอร์และอุปกรณ์ เสียหาย ๖.ความเสียหายที่เกิดจาก ไวรัสและโปรแกรมไม่พึงประ สงค์ต่างๆ	๑.พรบ.ว่าด้วยการกระทำความ ผิดทางคอมพิวเตอร์พ.ศ.๒๕๖๐ ๒.ประเมินความเหมาะสมของ วิธีการและมาตรการในการใช้ ทรัพยากรด้าน IT ๓.ประเมินและตรวจสอบความ เพียงพอและความทันสมัยของ อุปกรณ์คอมพิวเตอร์ ๔.ติดตั้งระบบป้องกันไวรัสยังไม่ ครบทุกเครื่อง ๕.มาตรฐานการรักษาความมั่น คงปลอดภัยของระบบ สารสนเทศ	การควบคุม ที่มีอยู่ไม่ เพียงพอ	๑.การจัดซื้ออุปกรณ์ คอมพิวเตอร์ ไม่เพียงพอ ๒.คอมพิวเตอร์และ อุปกรณ์ถูกใช้งานอย่างไม่ เหมาะสมและไม่ถูกวิธี ๓.คอมพิวเตอร์ล้าสมัย ๔.จัดให้มีระบบบำรุงรักษา ที่ต่อเนื่องเหมาะสม ๕.คอมพิวเตอร์และ อุปกรณ์เสียหาย ๖.ติดตั้งระบบป้องกันไว รัสให้ครบทุกเครื่อง	-แผนจัดซื้อปีงบประมาณ ๒๕๖๘ -ป้ายคำแนะนำ แสดงระยะเวลาการ บำรุงรักษาที่ติดอยู่ ข้างเครื่อง คอมพิวเตอร์ -ปรับเปลี่ยน/เพิ่ม คุณสมบัติของ เครื่องคอมพิวเตอร์ ให้เหมาะสมกับการ ใช้งานของ ระบบงาน เช่น เพิ่ม RAM เป็น SSD	๓๐ เมษายน ๒๕๖๙ ศูนย์คอมพิวเตอร์

ชื่อผู้รายงาน.....

(นางสาวดวงจันทร์ ชะงักรมย์)

ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

วันที่ ๓๐ เดือน เมษายน พ.ศ. ๒๕๖๙