สรุปข้อสั่งการในการประชุม คณะกรรมการสารสนเทศ ครั้งที่ ๒/๒๕๕๙
วัน จันทร์ ที่ ๑๕ มิถุนายน ๒๕๕๙ ณ ห้องประชุม ๓
ประธาน นายกรีฑา ต่อสุวรรณ นายแพทย์ชำนาญการพิเศษ (ด้านเวชกรรม)

ผู้สั่งการ	ข้อสั่งการ	ผู้รับผิดชอบ
นายกรีฑา ต่อสุวรรณ นายแพทย์ชำนาญการพิเศษ (ด้านเวชกรรม)	**๑. มาตรฐานการรักษาความปลอดภัยพื้นที่ห้อง Server** ๑.๑. ต้องปิดล็อกประตูหรือหน้าต่างของห้องตลอดเวลา ๑.๒. ต้องมีระบบควบคุมการเข้าออก (Access Control) ๑.๓. กรณีบุคคลภายนอกมีความจำเป็นต้องเข้าออกพื้นที่ฯ จะต้องมีเจ้าหน้าที่คอยควบคุมติดตามอยู่ด้วยตลอดเวลา และหากต้องการ Access อุปกรณ์ใด จะต้องได้รับอนุญาตจากเจ้าของระบบหรือผู้มีสิทธิ์อนุญาตก่อน ๑.๔. ต้องจัดวางตำแหน่งของอุปกรณ์อย่างเหมาะสม ป้องกันความเสี่ยงจากความร้อนจากแสงแดดฝุ่นละออง และความชื้น ๑.๕. ต้องมีการบันทึกตรวจสอบสภาพความพร้อมของระบบUPS เก็บบันทึกการตรวจสอบไว้เป็นหลักฐาน ๑.๖. ไม่นำอาหารและเครื่องดื่มเข้ามารับประทานในห้อง Server **๒. มาตรฐานการรักษาความปลอดภัยของ Server** ๒.๑. ต้องกำหนดสิทธิ์การเข้าถึงแบบชั่วคราวแก่บุคคลภายนอกที่ต้องการเข้าถึง Server นั้น และต้องมอบหมายให้มีผู้ควบคุมตรวจสอบบันทึกรายการ และลบสิทธิ์ทันทีที่ปฏิบัติงานเสร็จ ๒.๒. ต้องมีบันทึกรายการของ OS,Service Patch,Application ที่ติดตั้งบน Server นั้นๆ ๒.๓. ต้องตรวจสอบ Security Log ๒.๔. ต้องมีคู่มือการจัดการ server ๒.๕. ต้องมีบันทึกการ Backup data และ OS เป็นประจำ (Dairy Backup และ monthly Full Backup) ๒.๖. ต้องทำการ Synchronize clock ของ Server และ Network Device ให้มีเวลาตรงกันทั้งหมด ๒.๗. ต้องตั้งค่า Administrator account/Password ให้ยากต่อการคาด ๒.๘. ต้องกำหนดค่า Limit time to access ๒.๙. ต้อง Log off System ทุกครั้งเมื่อเลิกใช้ Management console ๒.๑๐. กรณีที่มี System Administrator โยกย้ายหรือเปลี่ยนแปลงหน้าที่ให้ หัวหน้าหน่วยยกเลิกสิทธิ์การเข้าถึงอุปกรณ์ดังกล่าวทันที ๒.๑๑. ต้อง Update Security Patch อย่างสม่ำเสมอ ๒.๑๒. ต้องมีบันทึกสรุปการเกิดปัญหาของอุปกรณ์ และการแก้ไขระบบ ๒.๑๓. ต้องมีขั้นตอนการทำลาย Computer media เช่น Disk, Tape, Print out Report	๑. นักวิชาการคอมพิวเตอร์ ๒.พนักงานเครื่องคอมพิวเตอร์

(นายกรีฑา ต่อสุวรรณ)
นายแพทย์ชำนาญการพิเศษ (ด้านเวชกรรม) รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชฉวาง

นโยบายและมาตรฐานด้านเทคโนโลยีสารสนเทศ คณะกรรมการสารสนเทศ โรงพยาบาลสมเด็จพระยุพราชฉวาง

นโยบายด้านเทคโนโลยีสารสนเทศ

นโยบายเพื่อพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อการดูแลรักษา การบริหารจัดการ และการสร้างเสริมการเรียนรู้ เพื่อตอบสนองต่อวิสัยทัศน์และพันธกิจของโรงพยาบาล ดังนี้

๑. การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อการบริการและการดูแลรักษา

๑.๑. เพื่อจัดบริการผู้ป่วยอย่างมีประสิทธิภาพ โดยเชื่อมโยงข้อมูลทั้งระบบ

๑.๒. พัฒนาระบบข้อมูลผู้ป่วยโดยคำนึงถึงสิทธิผู้ป่วย ความลับและความปลอดภัยของข้อมูลควบคู่กับความสะดวกในการใช้ข้อมูล

๑.๓. พัฒนาระบบสารสนเทศให้ตอบสนองต่อภารกิจหลักของโรงพยาบาล ในการดูแลผู้ป่วยระดับทุติยภูมิและการรับส่งต่อ ผู้ป่วยจากหน่วยงานอื่น

๒. การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อการบริหารจัดการ

๒.๑. พัฒนาระบบศูนย์ข้อมูลเพื่อการบริหารจัดการ เพื่อสนับสนุนการพัฒนาคุณภาพและประสิทธิภาพในการทำงานของโรงพยาบาล ผ่านทางระบบ Local Area Network (LAN)

๒.๒. พัฒนาระบบการตรวจสอบความถูกต้องของข้อมูล โดยมีการประมวลผลเป็นระยะๆ เพื่อการบริหารจัดการที่มีประสิทธิภาพ

๓. การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อเสริมสร้างการเรียนรู้

๓.๑. พัฒนาระบบสารสนเทศเพื่อสนับสนุนวิชาการ ทั้งการวิจัย การสร้างองค์ความรู้ การศึกษาอบรมและการเผยแพร่วิชาการ โดยสนับสนุนการค้นคว้าข้อมูลทาง internet

๓.๒. สนับสนุนกลุ่มงาน/หน่วยงานต่างๆ ให้พัฒนาสารสนเทศเพื่อการสื่อสารและการประชาสัมพันธ์

๓.๓. ฝึกอบรมเพิ่มพูนความรู้ด้านสารสนเทศแก่เจ้าหน้าที่โรงพยาบาล กระตุ้นให้เกิดความสนใจในการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้พัฒนางานอย่างมีประสิทธิภาพ

มาตรฐานด้านเทคโนโลยีสารสนเทศ

การกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศ เพื่อเป็นกรอบกติกาและการจัดการเพื่อใช้ในงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชฉวาง เพื่อเป็นแนวทางในการให้บริการและจัดอุปกรณ์ต่างๆให้กับบุคลากรในองค์กร เพื่อให้บุคลากรในองค์กรมีทักษะ และเพื่อเป็นแนวทางในการจัดทำงบประมาณด้านเทคโนโลยีสารสนเทศ

คณะกรรมการสารสนเทศได้แบ่งมาตรฐานเทคโนโลยีสารสนเทศเป็น ๔ หมวดดังนี้

หมวดที่ ๑ มาตรฐานด้านครุภัณฑ์คอมพิวเตอร์ (Hardware)

ในการจัดซื้อครุภัณฑ์คอมพิวเตอร์(Hardware) ใหม่นั้น จะต้องพิจารณา Specification ของอุปกรณ์ที่เหมาะสมกับซอฟแวร์ที่ใช้งานและพิจารณาจากเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

หมวดที่ ๒ มาตรฐานโปรแกรมที่ติดตั้งใน PC และ Notebook

การใช้ติดตั้ง Software บนเครื่อง PC และ Notebook ในองค์กร มีข้อกำหนด ดังนี้

๑. ฝ่ายคอมพิวเตอร์จะเป็นผู้รับผิดชอบการจัดหา ให้บริการติดตั้งและการให้คำแนะนำช่วยเหลือสำหรับ Software ที่กำหนดเป็นมาตรฐานของ Office Desktop และ Software ตามภาระหน้าที่ของหน่วยงาน

๒. Software ที่นอกเหนือจากรายการที่ระบุ ถือเป็น Software ที่ใช้เฉพาะหน่วยงาน ซึ่งผู้ใช้จะต้องแจ้งคณะกรรมการสารสนเทศเพื่อขอรับความเห็นชอบในการนำมาใช้งาน

๓. ห้ามผู้ใช้ติดตั้ง Software นอกเหนือจากรายการที่ระบุในเครื่องคอมพิวเตอร์ขององค์กร

๔. กำหนดมาตรฐาน Font งานเอกสารที่ใช้สื่อสารในองค์กร รูปแบบของเอกสารที่ใช้เป็นไปตามรูปแบบเอกสารที่กำหนดเป็นเอกลักษณ์ขององค์กร

หมวดที่ ๓ มาตรฐานการจัดเก็บเอกสารแบบอิเลคทรอนิกส์เพื่อสำรองข้อมูล

มาตรฐานต่างๆที่เกี่ยวข้องกับการจัดเก็บเอกสารแบบอิเล็กทรอนิกส์ โดยพิจารณาแยกเป็นเอกสารจากภายนอกองค์กรและเอกสารภายในองค์กร โดยมีข้อกำหนดดังนี้

๑. มาตรฐานการจัดการ Hard disk สำหรับจัดเก็บข้อมูลในเครื่อง PC และ notebook มีดังนี้- *Drive C: สำหรับติดตั้งระบบปฏิบัติการและโปรแกรมต่างๆ-Drive D: สำหรับเก็บ*

๒. มาตรฐานการจัดเก็บข้อมูลบน File Server ผู้ใช้งานจะต้องเก็บไฟล์ในโฟล์เดอร์ที่เป็นชื่อของหน่วยงานตนเองเท่านั้น

๓. มาตรฐานการสำรองข้อมูลจากฐานข้อมูล Hosxp จะทำการสำรองข้อมูลทุกวัน

หมวดที่ ๔ มาตรฐานการรักษาความปลอดภัย

มาตรฐานการรักษาความปลอดภัยของโรงพยาบาลสมเด็จพระยุพราชฉวาง มีรายละเอียดดังนี้

๑. มาตรฐานการรักษาความปลอดภัยพื้นที่ห้อง Server

- ปิดล็อกประตูหรือหน้าต่างของห้องตลอดเวลา
- กรณีบุคคลภายนอกมีความจำเป็นต้องเข้าออกพื้นที่ฯ จะต้องมีเจ้าหน้าที่คอยควบคุมติดตามอยู่ด้วยตลอดเวลา และหากต้องการ Access อุปกรณ์ใด จะต้องได้รับอนุญาตจากเจ้าของระบบหรือผู้มีสิทธิ์อนุญาตก่อน
- จัดวางตำแหน่งของอุปกรณ์อย่างเหมาะสม ป้องกันความเสี่ยงจากความร้อนจากแสงแดดฝุ่นละออง และความชื้น
- ไม่นำอาหารและเครื่องดื่มเข้ามารับประทานในห้อง Server

๒. มาตรฐานการรักษาความปลอดภัยของ Server

- กำหนดสิทธิ์การเข้าถึงแบบชั่วคราวแก่บุคคลภายนอกที่ต้องการเข้าถึง Server นั้น และมอบหมายให้มีผู้ควบคุมตรวจสอบบันทึกรายการ และลบสิทธิ์ทันที่ที่ปฏิบัติงานเสร็จ
- มีบันทึกรายการของ OS,Service Patch,Application ที่ติดตั้งบน Server นั้นๆ
- มีบันทึกการ Backup data และ OS เป็นประจำ (Dairy Backup และ monthly Full Backup)
- ทำการ Synchronize clock ของ Server และ Network Device ให้มีเวลาตรงกันทั้งหมด
- ตั้งค่า Administrator account/Passwordให้ยากต่อการคาดเดา(ไม่ต่ำกว่า๘ ตัวอักษร) และต้องไม่ใช้คำ Default
- Update Security Patch อย่างสม่ำเสมอ
- มีบันทึกสรุปการเกิดปัญหาของอุปกรณ์ และการแก้ไขระบบ

๓. มาตรฐานการรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์และสื่อสาร

- กำหนด Network Service ที่ไม่อนุญาตให้รับ-ส่งได้บนเครือข่าย
- ทำ Secure Authenticate ทุกครั้งที่ต้องการ access อุปกรณ์เพื่อการ Administration และต้องกำหนดสิทธิ์การเข้าถึงแบบชั่วคราวแก่บุคคลภายนอกที่ต้องการเข้าถึงอุปกรณ์นั่น พร้อมมอบหมายให้มีผู้ควบคุม ตรวจสอบและลบสิทธิ์ทันที่ปฏิบัติงานเสร็จ
- ตั้งค่า Network Administrator Account/Password ให้ยากต่อการคาดเดา (ไม่ต่ำกว่า ๘ Characters) และต้องไม่ใช้คำ Default
- ป้องกัน Unauthorized access สู่ Remote Access diagnostic port และต้องใช้ Secure Port ในการทำ Remote Administration เท่านั้น

๔. มาตรฐานการรักษาความปลอดภัยเคลื่อนย้ายและทำลายข้อมูลของอุปกรณ์ ICT

ทำการ Clear ข้อมูลที่บันทึกอยู่ในอุปกรณ์ HD, Backup หรือสื่อที่ใช้เก็บข้อมูลก่อนทำการเปลี่ยนทดแทนอุปกรณ์ รวมทั้งลบข้อมูลที่บันทึกในอุปกรณ์ที่ต้องการทำลายหรือแทงจำหน่ายต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการเคลื่อนย้ายอุปกรณ์ออกไปบำรุงรักษาภายนอกสถานที่

มาตรการรักษาความปลอดภัยของข้อมูลผู้รับบริการโรงพยาบาลสมเด็จพระยุพราชฉวาง

กำหนดให้มีมาตรการรักษาความปลอดภัยของฐานข้อมูลผู้รับบริการ ดังต่อไปนี้

๑. กำหนดให้บุคคลที่ได้รับรหัสผู้ใช้งานและรหัสผ่าน เพื่อเข้าใช้ฐานข้อมูลของโรงพยาบาล ต้องรับผิดชอบ เก็บรักษารหัสผู้ใช้งานและรหัสผ่านไว้เป็นความลับ และปกป้องมิให้บุคคลอื่นใช้รหัสผู้ใช้งานและรหัสผ่าน เช่น ต้องไม่เขียนรหัสผ่าน หรือจดบันทึกไว้ที่มองเห็นได้

๒. ห้ามมิให้ผู้ได้รับรหัสผู้ใช้งานและรหัสผ่าน บอกหรือกระทำการใดๆที่ประสงค์ต่อผล เพื่อให้บุคคลอื่นทราบรหัสผ่านของตน

๓. ในการเข้าใช้ฐานข้อมูลผู้รับบริการของโรงพยาบาล ให้เข้าใช้ได้ตามหน้าที่รับผิดชอบและที่ได้รับมอบหมายจากทางโรงพยาบาล เท่านั้น

๔. กรณีตรวจพบว่าผู้ได้รับรับรหัสผู้ใช้งานและรหัสผ่าน มีการเข้าใช้งานฐานข้อมูลผู้รับบริการของโรงพยาบาลที่ไม่เหมาะสม คณะกรรมการสารสนเทศขอสงวนสิทธิการใช้งานของรหัสผู้ใช้และรหัสผ่าน

๕. ห้ามมิให้เข้าใช้ฐานข้อมูลผู้รับบริการ เพื่อประโยชน์ทางธุรกิจ หรือเรื่องอื่นที่ไม่เกี่ยวกับทางราชการ

แผนการดูแลบำรุงรักษาระบบงานเทคโนโลยีสารสนเทศ
โรงพยาบาลสมเด็จพระยุพราชฉวาง

---

๑. หลักการและเหตุผล

โรงพยาบาลสมเด็จพระยุพราชฉวาง ได้ใช้เทคโนโลยีสารสนเทศในการดำเนินงาน และการให้บริการผู้ผู้มารับบริการ เพื่อให้ได้รับความสะดวก รวดเร็วขึ้น ระบบเทคโนโลยีสารสนเทศภายในโรงพยาบาลอาจจะได้รับความเสียหายจากปัจจัยทั้งภายในและภายนอกต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ บุคคล ปัญหาไฟฟ้าขัดข้อง อัคคีภัย ซึ่งอาจจะทำให้ระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย ส่งผลกระทบต่อระบบฐานข้อมูล ฮาร์ดแวร์ การปฏิบัติงาน และการให้บริการผู้มารับบริการทางด้านต่างๆของโรงพยาบาลสมเด็จพระยุพราชฉวางได้

เพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว ทางโรงพยาบาลจึงได้จัดทำแผนการดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศเพื่อใช้เป็นแนวทางในการปฏิบัติงาน

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลสารสนเทศ เครื่องคอมพิวเตอร์ ระบบอินเทอร์เน็ต และอุปกรณ์ต่อพ่วง ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสี่ยงและความเสียหายที่จะอาจเกิดกับระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ

๓. เป้าหมาย

เพื่อให้ระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาลสมเด็จพระยุพราชฉวาง ใช้งานอย่างเป็นระบบและมีประสิทธิภาพ และสามารถใช้ได้ในกรณีที่มีภาวะฉุกเฉิน เช่น ไฟดับ อินเตอร์เน็ตขัดข้อง ระบบเครือข่ายใช้งานไม่ได้โดยระบบเทคโนโลยีสารสนเทศ ต้องสามารถกลับมาดำเนินการได้ในระยะเวลา ดังนี้

๓.๑ ระบบสำรองไฟฟ้า สามารถสำรองไฟฟ้า ให้ระบบไม่น้อยกว่า ๑๕ นาที และเครื่อง Server สามารถใช้ไฟสำรองได้ ไม่น้อยกว่า ๔๕ นาที

๓.๒ ระบบ Network (เครือข่าย) เมื่อขัดข้องจะต้องกลับสู่สภาวะปกติภายในระยะเวลา ๒ ชั่วโมง

๓.๓ ระบบ Internet เมื่อขัดข้องจะต้องกลับสู่สภาวะปกติภายในระยะเวลา ๖ ชั่วโมง ทั้งนี้ขึ้นอยู่กับเครือข่ายผู้ให้บริการ ถ้าแก้ไขไม่ได้ในเวลา ต้องใช้ระบบ Internet สำรอง

๔. การประเมินสถานการณ์ความเสี่ยง

การตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ พบว่าสาเหตุของความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ เกิดขึ้นได้จากปัจจัยเสี่ยง ดังนี้

๔.๑ เจ้าหน้าที่หรือบุคลากร ของหน่วยงาน (Human error) ซึ่งขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ทำให้ระบบเทคโนโลยีสารสนเทศ เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน ส่งผลให้ไม่สามารถ ใช้งานระบบเทคโนโลยี สารสนเทศได้อย่างเต็มประสิทธิภาพ

๔.๒ ภัยไซเบอร์คุกคาม มัลแวร์ ไวรัสคอมพิวเตอร์ (Computer virus) อาจสร้างความเสียหายให้แก่เครื่อง คอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์ถึงขั้นใช้งานไม่ได้

๔.๓ ระบบไฟฟ้าขัดข้อง หรือความเสียหายจากความร้อนหรือเพลิงไหม้

๔.๔ การขโมยอุปกรณ์คอมพิวเตอร์ในห้องคอมพิวเตอร์แม่ข่าย

๔.๕ ปัจจัยภายนอก เช่น ระบบ Internet ไม่สามารถใช้งานได้หรืออาจเกิดจากการบุกรุกโจมตีจากภายนอก

๕. ข้อปฏิบัติในการป้องกัน แก้ไขปัญหาสถานการณ์ความเสี่ยงและภัยพิบัติ

๕.๑ จัดฝึกอบรม สัมมนา หรือแนะนำแนวทางใช้งาน เสริมสร้างความรู้ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศ ทั้งด้าน Hardware และ Software เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด

๕.๒ การสำรองข้อมูล (Backup) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายโดยไวรัสคอมพิวเตอร์หรือมีผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูลให้สามารถนำข้อมูลดังกล่าวกลับมาใช้งานได้โดยมีแนวทางดำเนินการ ดังนี้

๕.๒.๑ การตั้งค่าระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ให้มีการสำรองข้อมูลโดยอัตโนมัติเป็นประจำทุกวัน

๕.๒.๒ การสำรองข้อมูลไว้ใน อุปกรณ์บันทึกหรือคอมพิวเตอร์เครื่องอื่นๆ

๕.๓ การป้องกันมัลแวร์ ไวรัสคอมพิวเตอร์มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยมีวิธีการดังนี้

๕.๓.๑ ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง (Update) ข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัส
- Update ข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูล ต่างๆ

๕.๓.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น Flash drive/Thumb drive เป็นต้น

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จักหรือน่าสงสัย เช่น .pif ,.inf เป็นต้น
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๕.๓.๓ ใช้ความระมัดระวังในการเปิด e-Mail

- อย่าเปิดไฟล์e-Mail ถ้าไม่ทราบแหล่งที่มา
- ลบ e-Mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๕.๓.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จักที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น Facebook, Twitter และ Skype เป็นต้น หรือสอบถามคนที่ส่งไฟล์มาให้ก่อนกดรับ

- ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง e-Mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลด ไฟล์จาก Website ที่ไม่น่าเชื่อถือ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๕.๔ เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครือข่าย Internet ขัดข้อง ดำเนินการดังนี้

๕.๔.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๕.๔.๒ ตรวจสอบแผนผังเครือข่ายอุปกรณ์เพื่อหาสาเหตุการขัดข้อง และดำเนินการแก้ไข หากเครือข่ายอินเทอร์เน็ต แจ้งผู้ให้บริการ

๕.๔.๓ กรณีไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพ ของ เครื่องสำรองไฟฟ้า

๕.๔.๔ กรณีเกิดเหตุไฟไหม้เครื่องคอมพิวเตอร์และเครือข่าย ให้ตัดระบบ จ่ายไฟและใช้ถังดับเพลิงฉีดควบคุมเพลิงโดยเร็วรีบขนย้ายเครื่องคอมพิวเตอร์และเครือข่ายไปไว้ในที่ปลอดภัย

๕.๔.๕ กรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง และซ่อมให้สามารถใช้งานได้ให้เร็วที่สุดถ้าเกินขีดความสามารถในการ ดูแล ติดต่อร้านซ่อมหรือผู้เชี่ยวชาญมาดูแลให้เป็นปกติ

๕.๕ ซอฟแวร์ หรือโปรแกรม เสียหาย ให้ดำเนินการติดตั้งซอฟแวร์ หรือโปรแกรมใหม่เพื่อกลับมาใช้งานได้ตามปกติภายใน ๑-๒ วัน

๕.๖ กู้ระบบคอมพิวเตอร์กลับสู่สภาพปกติตามเดิม

การกู้ระบบเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์กระจายสัญญาณ (System recovery) โดยปกติระบบเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์กระจายสัญญาณจะต้องอยู่ในสภาพพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องดำเนินการกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้โดยแผนการกู้ระบบคอมพิวเตอร์นี้เป็นวิธีการที่จะทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และฐานข้อมูลสารสนเทศ กลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยให้ดำเนินการดังนี้

๕.๖.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๕.๖.๒ เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๕.๖.๓ กรณีเครื่อง Server เสียหาย ใช้คอมพิวเตอร์เครื่องอื่นทดแทนชั่วคราว

๕.๖.๔ นำ Backup ที่ได้สำรองข้อมูลไว้กลับมา

๕.๖.๕ ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูลสารสนเทศ และความถูกต้อง ของข้อมูล รวมทั้งระบบเครือข่ายคอมพิวเตอร์อื่น ๆ ที่เกี่ยวข้อง

๕.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ที่ซึ่งอาจสร้าง ความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

๕.๗.๑ ติดตั้งเครื่องสำรองไฟฟ้า (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับ อุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนของเครื่อง

คอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าได้นาน ประมาณ ๑๕ - ๒๐ นาที

๕.๗.๒ เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๕.๗.๓ เมื่อเกิดกระแสไฟฟ้าดับ หากมีเครื่องสำรองไฟฟ้าใช้งานอยู่ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ด้วย

๕.๘ ติดตั้งระบบป้องกันไฟไหม้โดยติดตั้งอุปกรณ์ดับเพลิงทุกชั้นของอาคารเพื่อการควบคุมเพลิงในเบื้องต้น

๕.๙ การนำมาตรการความปลอดภัยด้วยรหัสผ่าน เพื่อการเข้าใช้งานเครื่อง Server รหัสผ่านการเข้าโปรแกรม และรหัสผ่านการใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ภายในบริเวณอาคาร