มาตรการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ
สำนักงานปลัดกระทรวงสาธารณสุข

ความเสี่ยง (Risk) เป็นสิ่งที่เกิดจากการรวมตัวกันของข้อจำกัด (Constraint) และความไม่แน่นอน (Uncertainly) การบริหารความเสี่ยง (Risk Management) เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่าง ๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงว่าเป็นไปได้มากน้อยเพียงใด สำนักงานปลัดกระทรวงสาธารณสุข จึงมีมาตรการในการบริหารความเสี่ยงเพื่อลดโอกาสที่จะเกิดความเสี่ยง ดังนี้

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
1	**การสร้างความปลอดภัยทางกายภาพ** เพื่อป้องกันผู้ที่ไม่เกี่ยวข้องเข้ามาในบริเวณซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์	1.ห้ามบุคคลผู้ที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหรือห้องที่มีความสำคัญต่าง ๆ หากจำเป็นให้เจ้าหน้าที่ที่เป็นผู้รับผิดชอบในการนำพาเข้าไป และเฝ้าดูตลอดเวลาที่บุคคลนั้นอยู่ในห้องดังกล่าว และนำกลับออกมาเมื่อเสร็จสิ้นภารกิจ 2.การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ของเจ้าหน้าที่จะต้องทำการใส่บัญชีผู้ใช้ (User name) และ/หรือรหัสผ่าน (Password)	1. มีการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Server) ห้องที่มีความสำคัญต่าง ๆ รวมทั้งการควบคุมและจำกัดการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ ให้เป็นไปตามระเบียบของทางราชการ	1.ปรับปรุงห้องเครื่องคอมพิวเตอร์แม่ข่าย และห้องที่มีความสำคัญต่าง ๆ ให้มีความมั่นคงมากยิ่งขึ้น	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
2	**การป้องกันและแก้ไขปัญหากระแสไฟฟ้าขัดข้อง** เพื่อป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์	1. เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล	1.การติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply:UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล(PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 20-30 นาที	1.บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ	
		2. หากกระแสไฟฟ้าดับนานเกิน 1 ชั่วโมง (โดยทราบล่วงหน้า)สำนักงานปลัดกระทรวงสาธารณสุขมีการเช่าเครื่องปั่นไฟฟ้ามาใช้ในการให้บริการเครือข่าย	เช่าเครื่องปั่นไฟฟ้ามาใช้ในการให้บริการเครือข่ายเป็นรายครั้ง	1. ให้ความรู้และความเข้าใจแก่บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุขในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
2	**การป้องกันและแก้ไขปัญหากระแสไฟฟ้าขัดข้อง** (ต่อ)	2.เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในหน่วยงานด้วย 1.ผู้ใช้งานจะต้องตั้งค่าให้ระบบปฏิบัติการ ทำการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ (Patch Update) 2. ผู้ใช้งานจะต้องเปิดใช้งานไฟร์วอลล์ (Firewall) การกู้คืนข้อมูล (Recovery) ของระบบปฏิบัติการตลอดเวลา	1.มีการควบคุมการติดตั้งระบบปฏิบัติการ และมีการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอและใช้ความสามารถของระบบปฏิบัติการในการสร้างความปลอดภัยให้กับระบบคอมพิวเตอร์ ได้แก่ การควบคุมและจำกัดสิทธิของผู้ใช้ได้		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
3	**การสร้างความปลอดภัยให้กับระบบปฏิบัติการ** เพื่อเป็นการสร้างพื้นฐานความปลอดภัยและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์แก่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และคอมพิวเตอร์ส่วนบุคคล	1.ผู้ใช้งานจะต้องตั้งค่าให้ระบบปฏิบัติการ ทำการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ (Patch Update) 2. ผู้ใช้งานจะต้องเปิดใช้งานไฟร์วอลล์ (Firewall) การกู้คืนข้อมูล (Recovery) ของระบบปฏิบัติการตลอดเวลา	1.มีการควบคุมการติดตั้งระบบปฏิบัติการ และมีการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอและใช้ความสามารถของระบบปฏิบัติการในการสร้างความปลอดภัยให้กับระบบคอมพิวเตอร์ ได้แก่ การควบคุมและจำกัดสิทธิของผู้ใช้ได้ตามอำนาจหน้าที่และความรับผิดชอบ การเปิดใช้งานไฟร์วอลล์ (Firewall) การกู้คืนข้อมูล เป็นต้น		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
4	**การสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์แม่ข่าย** (Server) เพื่อเป็นการสร้างพื้นฐานความปลอดภัยและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์แก่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	1. ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่าย จะต้องเฝ้าระวังภัยคุกคามทางคอมพิวเตอร์ที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายอย่างต่อเนื่อง 2.เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการใส่บัญชีผู้ใช้ (Username) และ/หรือ รหัสผ่าน (password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายเสมอ 3. เจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่าย จะต้องทำการตั้งค่าและเปิดใช้งานบริการ (Service) ต่าง ๆของระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย ที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบตลอดเวลา	1.มีการติดตั้งระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นระบบปฏิบัติการที่มีความสามารถในการบริหารจัดการความปลอดภัยสูง และใช้ความสามารถของระบบปฏิบัติการ ในการสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์แม่ข่าย ได้แก่ การควบคุมและจำกัดสิทธิของผู้ใช้ได้ตามอำนาจหน้าที่และความรับผิดชอบ การเปิดใช้งานไฟล์วอลล์ การกู้คืนข้อมูล การสำรองข้อมูลเป็นต้น รวมทั้ง การใช้โปรโตคอล Secure Shell (SSH) ในการติดต่อกับ Web Server เพื่อเพิ่มความปลอดภัยให้สูงกว่าการ FTP หรือ Telnet		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
5	**การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์** เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์	1.เจ้าหน้าที่ผู้รับผิดชอบจะต้องเปิดใช้งานไฟล์วอลล์และระบบป้องกันไวรัสคอมพิวเตอร์ตลอดเวลา 2.ผู้ดูแลระบบ Proxy Server จะต้องมีการกำหนดค่า (Configuration) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ 3. เจ้าหน้าที่ดูแลระบบเครือข่ายจะต้องทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตอย่างสม่ำเสมอ 4. เจ้าหน้าที่ผู้รับผิดชอบจะต้องตั้งค่า (Setup) ให้ซอฟท์แวร์สามารถ Update โปรแกรมสำหรับการอุดช่องโหว่โดยอัตโนมัติ หรือการลงซอฟท์แวร์ที่มีเวอร์ชั่นใหม่กว่าตามความเหมาะสม 5. ผู้ใช้จะต้องบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน	1. การติดตั้งไฟล์วอลล์ (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคลของสำนักงานปลัดกระทรวงสาธารณสุขได้ 2. การติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายสำหรับโปรแกรมป้องกันไวรัสคอมพิวเตอร์ทั่วทั้งสำนักงานปลัดกระทรวงสาธารณสุขทั้งเครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ส่วนบุคคลโดย	1. พัฒนาและปรับปรุงระบบให้มีความพร้อมใช้งานอยู่ตลอดเวลา อย่างต่อเนื่อง 2. การให้ความรู้อย่างต่อเนื่องแก่บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุขในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างปลอดภัย	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
5	**การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์**(ต่อ)	(Password) เพื่อเป็นการแสดงตนก่อนอนุญาตให้เข้าสู่ระบบต่าง ๆ ตามอำนาจหน้าที่และความรับผิดชอบ 6. ห้ามไม่ให้ผู้ที่มีอำนาจหน้าที่เข้ามาใช้งานซอฟท์แวร์ระบบหรือซอฟท์แวร์บางประเภทที่มีผลต่อการควบคุมการทำงานของซอฟท์แวร์อื่น หรือเป็นตัวกลางในการแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง	ใช้โปรแกรม Trend Micro Office Scan ซึ่งกำหนดให้มีการ Update โปรแกรมอัตโนมัติและทำการ Scan ไวรัสทุกวันศุกร์ของสัปดาห์ 3. การติดตั้ง Proxy Sever เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของสำนักงานปลัดกระทรวงสาธารณสุข และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศ 4. มีระบบการตรวจสอบปริมาณข้อมูลการใช้งานเครือข่ายอินเตอร์เน็ตผ่านซอฟท์แวร์ของสำนักงานปลัดกระทรวงสาธารณสุข 5. มีระบบการตรวจสอบปริมาณข้อมูลการใช้งานเครือข่ายอินเตอร์เน็ตผ่านซอฟท์แวร์ของผู้ให้บริการอินเตอร์เน็ต(ISP) ซึ่งใช้บริการวงจรสื่อสารเช่า (Leased Line)		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
5	**การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์**(ต่อ)		6.มีการเฝ้าดูการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย และใช้ความสามารถของซอฟท์แวร์ในการนำข้อมูลเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย เพื่อบันทึกกิจกรรม วัน เวลาที่มีการนำเข้าข้อมูล หรือ การปรับปรุงแก้ไขข้อมูล 7. มีการอุดช่องโหว่ของซอฟท์แวร์คอมพิวเตอร์ทั้งซอฟท์แวร์ระบบปฏิบัติการและซอฟท์แวร์ประยุกต์ โดยการตั้งค่า (Setup) ให้ซอฟท์แวร์สามารถ Update โปรแกรมสำหรับการอุดช่องโหว่โดยอัตโนมัติ หรือการลงซอฟท์แวร์ที่มีเวอร์ชั่นใหม่กว่าตามความ		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
5	**การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์**(ต่อ)		เหมาะสม 8.มีระบบสารสนเทศซึ่งบังคับให้ผู้ใช้จะต้องบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นการแสดงตนก่อนอนุญาตให้เข้าสู่ระบบ 9.มีการควบคุมและป้องกันไม่ให้ผู้ที่ไม่มีอำนาจหน้าที่เข้ามาใช้งานซอฟท์แวร์ระบบหรือซอฟท์แวร์บางประเภทที่มีผลต่อการควบคุมการทำงานของซอฟท์แวร์อื่น หรือเป็นตัวกลางในการแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
6	**การพัฒนานโยบายการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์** เพื่อให้การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงสาธารณสุขเป็นไปอย่างมีประสิทธิภาพและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์	1. มีหลักเกณฑ์หรือแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ สำนักงานปลัดกระทรวงสาธารณสุข 2. มีการมอบหมายเจ้าหน้าที่ดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์	1.ออกระเบียบหรือแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ สำนักงานปลัดกระทรวงสาธารณสุข พ.ศ.2552 2. ออกบันทึกมอบหมายเจ้าหน้าที่ดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์	1. กำกับการดำเนินการให้เป็นไปตามระเบียบฯว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ สำนักงานปลัดกระทรวงสาธารณสุขอย่างต่อเนื่อง	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
7	**การสร้างความตระหนักให้กับผู้ใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์** เพื่อให้การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพและสัมฤทธิผลตามนโยบายการใช้งานดังกล่าว	1. ประชาสัมพันธ์ให้บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุขตระหนักและเห็นความจำเป็นของการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์	1. ประชาสัมพันธ์ให้มีการดำเนินการตามระเบียบหรือแนวปฏิบัติว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ สำนักงานปลัดกระทรวงสาธารณสุข พ.ศ.2552 2.การประชาสัมพันธ์ให้ผู้ใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้รับทราบและปฏิบัติตามมาตรการบริหารความเสี่ยง 3.การเผยแพร่ความรู้และคู่มือการใช้ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างปลอดภัยแก่ผู้ใช้งานโดยผ่านทางหนังสือเวียน อินทราเน็ตและเว็บไซต์	1. การประชาสัมพันธ์ให้มีการดำเนินการตามระเบียบหรือแนวปฏิบัติว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศ พ.ศ.2552 อย่างต่อเนื่อง 2. การให้ความรู้แก่บุคลากรของสำนักงานปลัดกระทรวงสาธารณสุขอย่างต่อเนื่องในด้านการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างปลอดภัย	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
8	**การฟื้นฟูระบบ / ข้อมูลจากความเสียหาย (Recovery)** เพื่อให้การฟื้นฟูระบบ/ ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งอาจส่งผลให้เครื่องคอมพิวเตอร์หรือการประมวลผลของคอมพิวเตอร์หยุดชะงัก	1. ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืนข้อมูล (Recovery) ของระบบปฏิบัติการตลอดเวลา 2.เจ้าหน้าที่ผู้รับผิดชอบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟท์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหายไป 3.เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการบำรุงรักษาระบบเครื่องคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ	1.มีการตั้งค่าให้ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ทำการฟื้นฟูระบบ/ข้อมูลจากความเสียหาย โดยอัตโนมัติหรือการดำเนินการโดยผู้ใช้งานในการฟื้นฟูระบบ/ข้อมูลจากความเสียหาย 2. มีการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์และการติดตั้งซอฟท์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหาย 3. มีการบำรุงรักษาระบบเครื่องคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ	1. การดำเนินการตามมาตรการดังกล่าวอย่างต่อเนื่อง	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
9	**การสำรองข้อมูล** (Back up) เพื่อลดความเสี่ยงจากที่อาจเกิดขึ้นกับข้อมูลและสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ฮาร์ดิสก์เสียหาย ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูล โดยผู้ใช้งานเอง	1.เจ้าหน้าที่ผู้รับผิดชอบจะต้องตั้งค่าระบบให้มีสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบ แต่ไม่ต่ำกว่า 1 ครั้ง / เดือน 2.เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server) จะต้องตั้งค่าระบบให้มีสำรองข้อมูลโดยอัตโนมัติ 3. ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม แต่ไม่ต่ำกว่า 1 ครั้งต่อเดือน 4. เมื่อสำนักงานปลัดกระทรวงสาธารณสุขประกาศให้มีการสำรองข้อมูล เนื่องจากจะได้มีการ	1.การติดตั้งระบบสำรองข้อมูลสำหรับเครื่องคอมพิวเตอร์แม่ข่าย 2.การสำรองข้อมูลไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้โดยการบันทึกไว้คนละ Drive 3. การสำรองข้อมูลไว้ในแผ่น CD 4. การสำรองข้อมูลโดยการพิมพ์ (Print) ออกมาเก็บไว้ในกระดาษสำหรับข้อมูลที่สำคัญ	1. มีการกำหนดมาตรการและแนวทางในการสำรองข้อมูลที่เป็นระบบมากยิ่งขึ้น 2. มีการทดสอบและเรียกใช้งานข้อมูล สำรองตามระยะเวลาที่เหมาะสม	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
9	**การสำรองข้อมูล** (Back up) (ต่อ)	ดำเนินการที่อาจส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าวภายในระยะเวลาที่กำหนด 5.หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บไว้ในรูปของเอกสารกระดาษ (Hard Copy) 6.เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่าย และผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไปจะต้องมีการทดสอบความถูกต้องของข้อมูลสำรองและการรายงานผลตรวจสอบเป็นครั้งคราว ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูลในแต่ละระบบฐานข้อมูล หรือของผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ	5. มีการทดสอบความถูกต้องของข้อมูลสำรองและการรายงานผลการตรวจสอบเป็นครั้งคราว ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูลในแต่ละระบบฐานข้อมูล หรือของผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ		

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
10	**การป้องกันและแก้ไขปัญหาจากภัยพิบัติ** (Contingency Plan) เพื่อให้การบริหารและจัดการกับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีเกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น	1. เมื่อเกิดภัยพิบัติ เช่น อัคคีภัย ให้ผู้ใช้งานรีบเก็บแผ่น CD ซึ่งบรรจุข้อมูลสำรองซึ่งมีความสำคัญไปด้วยแล้วดำเนินการตามหลักปฏิบัติ/ขั้นตอนในแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ 2. เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบและดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า 1 วัน ในการดำเนินการแก้ไข ให้ออกประกาศแจ้ง	1. มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ 2. มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนดังกล่าว	1. มีการประชาสัมพันธ์และดำเนินการให้เป็นไปตามแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของสำนักงานปลัดกระทรวงสาธารณสุข	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
		แก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น 3. เมื่อเกิดกรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบทำการแก้ไขแล้วเสร็จ 4. เมื่อเกิดกรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบ ทำการตรวจสอบเหตุแห่งความเสียหายนั้นในเบื้องต้น พร้อมรายงานให้ผู้บังคับบัญชาทราบ พบว่าหากมีแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมา ได้ให้ดำเนินการโดยด่วน ทั้งนี้อาจประสานงานขอความช่วยเหลือจากผู้ที่ชำนาญในเรื่องดังกล่าว เพื่อดำเนินการด้วยก็ได้ หากไม่สามารถกู้คืนข้อมูลกลับมาได้ให้นำข้อมูลที่สำรองไว้มาใช้แทน กรณีที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไป เมื่อเกิดเหตุอุปกรณ์จัดเก็บข้อมูลเสียหาย ให้รายงานผู้บังคับบัญชาของตนทราบ แล้วแจ้งกลุ่มคอมพิวเตอร์เพื่อตรวจสอบเหตุแห่งความเสียหายนั้น			

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
		ในเบื้องต้น หากพบว่ามีแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมาได้ให้ดำเนินการโดยด่วน หากไม่สามารถกู้คืนข้อมูลกลับมาได้ ให้นำข้อมูลที่สำรองไว้มาใช้แทน จากนั้นให้ทำการส่งซ่อมอุปกรณ์จัดเก็บข้อมูลที่เสียหายดังกล่าวตามระเบียบของทางราชการต่อไป 5. เมื่อมีการระบาดของไวรัสคอมพิวเตอร์ในเครือข่าย เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการวิเคราะห์ความรุนแรงของไวรัสคอมพิวเตอร์และตัดการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ เพื่อดำเนินการแก้ไขปัญหาโดยรีบด่วนที่สุด พร้อมทั้งรายงานให้ผู้บังคับบัญชาทราบ			

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการ	สิ่งที่จะต้องดำเนินการในอนาคต	หมายเหตุ
11	**การมอบหมายเจ้าหน้าที่ผู้รับผิดชอบ** เพื่อมาตรการบริหารความเสี่ยงของสำนักงานปลัดกระทรวงสาธารณสุข เป็นไปอย่างมีประสิทธิภาพ	1.เจ้าหน้าที่ที่ได้รับมอบหมาย จะต้องปฏิบัติหน้าที่และดำเนินการให้เป็นไปตามที่ได้รับมอบหมาย	1. ดำเนินการควบคุมแก้ไขระบบสารสนเทศและเครือข่ายคอมพิวเตอร์มีผู้รับผิดชอบ คือ 1.1 คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงสาธารณสุข	1. กำกับและดูแลให้มีการดำเนินการของเจ้าหน้าที่ผู้รับผิดชอบ ให้เป็นไปตามอำนาจ หน้าที่ที่ได้รับมอบหมาย 2. เจ้าหน้าที่ผู้รับผิดชอบในแต่ละระบบ 2.1 เจ้าหน้าที่ดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ 2.2 เจ้าหน้าที่จากบริษัทที่สำนักงานปลัดกระทรวงสาธารณสุขได้ทำการ Outsource	