หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข **FRM 002.1**

รายงานผลการติดตามการปฏิบัติตามแผนการบริหารความเสี่ยง ปีงบประมาณ พ.ศ. 2553 ด้านการปฏิบัติการ (ระบบฐานข้อมูลสารสนเทศ)

สำหรับงวดตั้งแต่วันที่ 1 ตุลาคม 2552 - 16 สิงหาคม 2553

วัตถุประสงค์การควบคุม (เป้าหมาย/ตัวชี้วัด)		ความเสี่ยง/ปัจจัยเสี่ยง		มาตรการ / กิจกรรมการควบคุมความเสี่ยง	ผู้รับผิดชอบ / เจ้าของความเสี่ยง	สถานะ * การดำเนินการ	ระดับความเสี่ยงที่เหลืออยู่ (6)		ผลจากการใช้มาตรการ/กิจกรรมจัดการความเสี่ยง	ปัญหา/อุปสรรคและข้อคิดเห็น
(1)		(2)		(3)	(4)	(5)	ผลกระทบ	โอกาสเกิด	(7)	(8)
1. ส่วนราชการต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ	1.1 มีการถ่ายทอดนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสู่การปฏิบัติ	1.1 นโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศไม่ถูกถ่ายทอดสู่หน่วยงานส่วนกลาง สป.สธ.	1.1.1 หน่วยงานส่วนกลาง สังกัด สป.สธ. ไม่ได้รับทราบ นโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	1.1.1 แจ้งเวียนส่งระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้ทุกหน่วยงานส่วนกลางสังกัด สป.สธ. เมื่อธันวาคม 2552	ศทส.	★	3	2	เจ้าหน้าที่บางหน่วยงานยังไม่รับทราบว่ามีการประกาศใช้ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศภายใน สป.สธ.	หลายหน่วยงานไม่แจ้งเวียนระเบียบฯ ให้ทั่วถึงบุคลากรทุกคนภายในหน่วยงาน
			1.1.2 เจ้าหน้าที่ สป.สธ. ส่วนกลาง ไม่มีความรู้และความเข้าใจในนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเพียงพอ	1.1.2 จัดประชุมเชิงปฏิบัติการโครงการจัดการความเสี่ยงไอทีภายในสำนักงานปลัดกระทรวงสาธารณสุข ประจำปีงบประมาณ 2553 เพื่อชี้แจงให้เจ้าหน้าที่มีความรู้และความเข้าใจวิธีปฏิบัติ พร้อมทั้งตระหนักถึงความสำคัญ		★			มีการจัดประชุม เมื่อวันพุธที่ 21 กรกฎาคม 2553 ณ ห้องประชุมชัยนาทนเรนทร โดยมีผู้แทนหน่วยงานเข้าร่วมจำนวน 50 คน	- มีผู้แทนเข้าร่วมประชุมไม่ครบทุกหน่วยงานในสังกัด สป.สธ. - ผู้บริหารของหน่วยงานไม่มีเวลาเข้าร่วมประชุมด้วย - ผู้เข้าร่วมไม่ใช่ผู้รับผิดชอบด้าน IT
			1.1.3 นโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ไม่เหมาะสมกับปัจจัยแวดล้อมของ สป.สธ. จึงปฏิบัติไม่ได้จริง	1.1.3 ทบทวนและปรับแก้ ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้เหมาะสมกับปัจจัยแวดล้อมของ สป.สธ.		★			จัดทำคู่มือและข้อปฏิบัติสำหรับ USER โดยคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ	การกระตุ้นให้บุคลากรปฏิบัติตามคู่มืออย่างจริงจังนั้นทำได้ยากมาก

วัตถุประสงค์การควบคุม (เป้าหมาย/ตัวชี้วัด)		ความเสี่ยง/ปัจจัยเสี่ยง		มาตรการ / กิจกรรมการควบคุมความเสี่ยง	ผู้รับผิดชอบ / เจ้าของความเสี่ยง	สถานะ * การดำเนินการ	ระดับความเสี่ยงที่เหลืออยู่ (6)		ผลจากการใช้มาตรการ/กิจกรรมจัดการความเสี่ยง	ปัญหา/อุปสรรคและข้อคิดเห็น
(1)		(2)		(3)	(4)	(5)	ผลกระทบ	โอกาสเกิด	(7)	(8)
	1.2 มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศที่เหมาะสมกับปัจจัยแวดล้อมของ สป.สธ. และปฏิบัติได้จริง	1.2 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ ไม่สามารถปฏิบัติได้จริง	1.2.1 ไม่มีการซักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ	1.2.1.1 จัดทำ Flow Chart กระบวนการจัดการกรณีโดนเจาะระบบ 1.2.1.2 ประสานสำนักบริหารกลาง สป.สธ. ในการร่วมซ้อมแผนกรณีเกิดเหตุไฟไหม้ (อัคคีภัย)		★	4	1	- ศทส. ได้ทำการทดสอบสมมติเหตุการณ์โดนเจาะและกู้คืนระบบ ตาม Flow Chart สามารถปฏิบัติได้จริง เมื่อ 19 กรกฎาคม 2553 - กรณีไฟไหม้ ซ้อมร่วมกันกับ สำนักบริหารกลาง ในวันที่ 8 กันยายน 2553	ไม่มีอุปกรณ์ สำหรับทดสอบจริงทั้งระบบ
			1.2.2 ไม่มีงบประมาณจัดหาระบบสำรองฐานข้อมูลและสารสนเทศ หากเกิดเหตุการณ์/ซักซ้อม	1.2.2 เสนอของบประมาณประจำปีในการจัดหาระบบสำรองฐานข้อมูลสารสนเทศ		★			คำเสนอไม่ได้รับการตอบสนองทำให้ยังไม่มีระบบสำรองฐานข้อมูลสารสนเทศ และไม่มีมาตรการอื่นรองรับ	ไม่ได้รับจัดสรรงบประมาณในการจัดหา
	1.3 การใช้งาน Internet ผ่านเครือข่าย สป.สธ. ต้องมีการตรวจสอบสิทธิผู้ใช้งาน(Access rights) ทุกครั้ง	1.3 มีการเข้าใช้งาน Internet ผ่านเครือข่าย สป.สธ. ได้โดยไม่ผ่านการตรวจสอบสิทธิ หรือไม่ต้อง Login	1.3.1 อุปกรณ์ควบคุม เช่น Firewall , Proxy Server ทำงานผิดพลาด/ชำรุด	1.3.1 เสนอของบประมาณประจำปีในการจัดหาอุปกรณ์เครือข่ายคอมพิวเตอร์ทดแทนของเดิมที่เสื่อมสภาพและหมดอายุการใช้งาน		★	3	2	ไม่มีอุปกรณ์เครือข่ายคอมพิวเตอร์เพื่อทดแทนของเดิม	ไม่ได้รับงบประมาณในการจัดหา

วัตถุประสงค์ การควบคุม (เป้าหมาย/ตัวชี้วัด)		ความเสี่ยง/ปัจจัยเสี่ยง		มาตรการ / กิจกรรมการควบคุมความเสี่ยง	ผู้รับผิดชอบ / เจ้าของความเสี่ยง	สถานะ * การดำเนินการ	ระดับความเสี่ยงที่เหลืออยู่ (6)		ผลจากการใช้มาตรการ/กิจกรรมจัดการความเสี่ยง	ปัญหา/อุปสรรคและข้อคิดเห็น
(1)		(2)		(3)	(4)	(5)	ผลกระทบ	โอกาสเกิด	(7)	(8)
			1.3.2 หน่วยงานเชื่อมโยงเครือข่ายภายนอกโดยไม่ผ่าน ศทส.	1.3.2 จัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร และแจ้งเวียนหน่วยงาน					มีการประกาศใช้นโยบาย ฯ และแจ้งเวียนทุกหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ทราบ	บางหน่วยงานไม่ให้ความร่วมมือในการปฏิบัติตามนโยบายอย่างจริงจัง
2. ส่วนราชการต้องมีระบบเทคโนโลยีสารสนเทศเพื่อให้ประชาชนเข้าถึงข้อมูลข่าวสารและรับบริการได้อย่างเหมาะสม	2.1 ระยะเวลา Downtime ของระบบเครือข่าย Internet ไม่เกินร้อยละ 5 ของเวลาทั้งปี(นาที)	2.1 ระยะเวลา Downtime ของระบบเครือข่าย Internet เกินร้อยละ 5 ของเวลาทั้งปี (นาที)	2.1 ถูกโจมตีจาก Hacker /ไวรัสคอมพิวเตอร์/Spyware	2.1.1 มอบหมายเจ้าหน้าที่ทำการ Update Policy และ Upgrade Firmware ของอุปกรณ์เครือข่ายให้มีประสิทธิภาพ เหมาะสมกับเทคโนโลยีปัจจุบัน		★	3	3	มีการตรวจสอบตลอดเวลา ทำให้พบปัญหาและแก้ไขได้ก่อนเกิดการ Downtime	ไม่มีงบประมาณในการบำรุงรักษาเนื่องจาก Firmware ในการ Upgrade อุปกรณ์ต้องมีค่าใช้จ่าย
				2.1.2 ให้ทำบันทึกการตรวจสอบช่องโหว่เครือข่ายและการแก้ไขปัญหาเครือข่ายไว้เป็นหลักฐาน		★			สามารถปิดช่องโหว่บางจุดที่เกิดขึ้นบ่อยๆได้	เจ้าหน้าที่ไม่เพียงพอ
				2.1.3 จัดทำคู่มือวิธีการปฏิบัติ เช่น การจัดการไวรัสคอมพิวเตอร์และคู่มือการ Backup ข้อมูลสำคัญ		★			เจ้าหน้าที่บางส่วนใช้คู่มือและปฏิบัติตาม	ยังมีเจ้าหน้าที่อีกจำนวนมาก(ส่วนใหญ่)ยังไม่รับทราบและไม่ให้ความสำคัญในการปฏิบัติตาม

วัตถุประสงค์การควบคุม (เป้าหมาย/ตัวชี้วัด)	ความเสี่ยง/ปัจจัยเสี่ยง		มาตรการ / กิจกรรมการควบคุมความเสี่ยง	ผู้รับผิดชอบ / เจ้าของความเสี่ยง	สถานะ * การดำเนินการ	ระดับความเสี่ยงที่เหลืออยู่ (6)		ผลจากการใช้มาตรการ/กิจกรรมจัดการความเสี่ยง	ปัญหา/อุปสรรคและข้อคิดเห็น
(1)	(2)		(3)	(4)	(5)	ผลกระทบ	โอกาสเกิด	(7)	(8)
2.2 จำนวนครั้งที่เว็บไซต์กระทรวงล่มเฉลี่ยเดือนละไม่เกิน 1 ครั้ง	2.2 เว็บไซต์กระทรวงสาธารณสุขล่มบ่อย จำนวนครั้งเฉลี่ยเกินเดือนละ 1 ครั้ง	2.2 Webserver ถูกโจมตีจาก Hacker /ไวรัสคอมพิวเตอร์/ Spyware	2.2 มอบหมายเจ้าหน้าที่ ให้ทำการตรวจสอบ (Monitor) การแสดงผลหน้าเว็บไซต์ รวมทั้งดำเนินการแก้ไขปัญหาทันทีตลอดช่วงเวลาทำการ		★	5	2	ไม่พบการล่มของเว็บไซต์	แต่พบข้อผิดพลาดของ Content จากการดึงข้อมูลจากกรม และแจ้งผู้เกี่ยวข้องแก้ไขได้ทันที
2.3 มีการเชื่อมโยงเครือข่ายคอมพิวเตอร์ไปยังหน่วยงานในสังกัด สป.สธ. ส่วนภูมิภาค	2.3 เครือข่ายคอมพิวเตอร์ที่เชื่อมไปยังหน่วยงานในสังกัด สป.สธ. ส่วนภูมิภาค ถูกก่อกวน/โจมตี จากไวรัส หนอนอินเตอร์เน็ต Spam Trojan เป็นต้น	2.3.1 อุปกรณ์รักษาความปลอดภัยระบบเครือข่ายชำรุดหรือถูกใช้งานไม่เต็มประสิทธิภาพ 2.3.2 บุคลากรด้าน ICT ขาดความเชี่ยวชาญ ความรู้และทักษะในการดูแลรักษาระบบเครือข่าย	2.3.1 จ้างเจ้าหน้าที่ที่มีความเชี่ยวชาญเฉพาะในการเฝ้าระวัง ตรวจสอบระบบเครือข่ายตลอดเวลา 2.3.2 ให้ความรู้แก่บุคลากรผู้ปฏิบัติงานด้าน ICT โดยการจัดอบรม หรือประชุมสัมมนา		★	5	1	- มีการตรวจสอบเฝ้าระวังอย่างต่อเนื่อง และสามารถแก้ปัญหาได้อย่างรวดเร็ว - จัดประชุมวิชาการด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ปี 2553 (วันที่ 1–3 มิถุนายน 2553)	มีการเปลี่ยนแปลงบุคลากรผู้ปฏิบัติงานด้าน ICT บ่อยครั้ง เพราะความไม่ก้าวหน้าในสายวิชาชีพ ทำให้ขาดความต่อเนื่องในการดูแลระบบเครือข่าย

* สถานะการดำเนินการ

★ = ดำเนินการแล้วเสร็จตามกำหนด

✓ = ดำเนินการแล้วเสร็จล่าช้ากว่าเดิม

✖ = ยังไม่ดำเนินการ

○ = อยู่ระหว่างดำเนินการ

ชื่อผู้รายงาน.....นางสาวสุวันต์นา เสมอเนตร.....

ตำแหน่ง.....นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ.....

วันที่....23...../..สิงหาคม.../.....2553.....