คณะกรรมการตรวจสอบภายในภาคีเครือข่าย ระดับเขต ระดับจังหวัด

ชื่อหน่วยงาน..... **หน่วยรับตรวจ**.....

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่**.....

แบบสอบทานระบบการควบคุมภายใน

ด้าน <u>ระบบเทคโนโลยีสารสนเทศ</u>

ลำดับ	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
๑.	ด้านนโยบายและแผน			
	๑.๑ จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศเป็นลายลักษณ์อักษรและลงนามโดยผู้บริหารของหน่วยงาน			
	๑.๒ จัดทำนโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศของหน่วยงาน ครอบคลุมทุกระดับ ได้แก่			
	๑.๒.๑ การควบคุมการเข้า - ออก ห้องปฏิบัติการระบบเครือข่าย			
	๑.๒.๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ			
	๑.๒.๓ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ			
	๑.๒.๔ การควบคุมการใช้งานคอมพิวเตอร์ส่วนบุคคล (PC)			
	๑.๒.๕ การควบคุมการใช้งานคอมพิวเตอร์พกพา (Notebook)			
	๑.๒.๖ การควบคุมการใช้งานอินเทอร์เน็ต (Internet)			
	๑.๒.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (WLAN)			
	๑.๓ จัดทำนโยบายและแนวปฏิบัติการสำรองข้อมูลและกู้คืนระบบ			
	๑.๔ มีการกำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจนเป็นลายลักษณ์อักษร			
	๑.๕ เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศทางเว็บไซต์ของหน่วยงาน			
	๑.๖ คำสั่งแต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน			
	๑.๗ จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่			
	๑.๗.๑ การวิเคราะห์ความเสี่ยง (Risk Analysis)			

คณะกรรมการตรวจสอบภายในภาคีเครือข่าย ระดับเขต ระดับจังหวัด

ชื่อหน่วยงาน..... **หน่วยรับตรวจ**.....

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่**.....

แบบสอบทานระบบการควบคุมภายใน

ด้าน <u>ระบบเทคโนโลยีสารสนเทศ</u>

ลำดับ	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
	๑.๗.๒ การจัดการความเสี่ยง (Rick Management)			
	๑.๗.๓ การยอมรับความเสี่ยง (Rick Treadment)			
๒.	ด้านการควบคุมระบบเทคโนโลยีสารสนเทศ			
	๒.๑ กำหนดสิทธิการเข้าถึงข้อมูลตามลำดับชั้นความลับเป็นลายลักษณ์อักษรที่ชัดเจน			
	๒.๒ ห้องปฏิบัติงานหรือห้องควบคุมระบบเครือข่ายเป็นพื้นที่เฉพาะบุคคลที่ได้รับอนุญาตและต้องมีการแบ่งพื้นที่เป็น			
	๒.๒.๑ ส่วนปฏิบัติงาน (Operations Zone)			
	๒.๒.๒ ส่วนเครื่องแม่ข่าย (Server Zone)			
	๒.๒.๓ ส่วนเครื่องสำรองไฟ (UPS Zone)			
	๒.๓ สถานที่จัดเก็บอุปกรณ์เกี่ยวกับสารสนเทศมีการล็อคกุญแจเมื่อไม่มีการใช้งาน			
	๒.๔ มีกฎข้อบังคับการปฏิบัติตนของเจ้าหน้าที่ขณะปฏิบัติงานและมีสัญลักษณ์การแจ้งเตือน ที่เห็นชัดเจน เช่น ห้ามสูบบุหรี่ห้ามนำอาหารและเครื่องดื่ม เข้ามารับประทาน			
	๒.๕ UPS (เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ) มีเพียงพอและอยู่ในสถานะพร้อมใช้งาน เพื่อป้องกันอุปกรณ์และข้อมูลสารสนเทศเสียหาย กรณีไฟฟ้าดับหรือไฟฟ้าตก			
	๒.๖ มีแผนและการตรวจสอบ บำรุงรักษาสายไฟฟ้า สายสื่อสารสายเคเบิล อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สำรองไฟฟ้า อุปกรณ์สำรองข้อมูล ภายในห้องปฏิบัติการ			
๓.	การเข้าถึงผู้ใช้งาน ๓.๑ หน่วยงานจัดทำคู่มือ/แนวปฏิบัติ การใช้งานระบบสารสนเทศของผู้ใช้งาน			
	๓.๒ หน่วยงานจัดให้มีการให้ความรู้ ความเข้าใจกับผู้ปฏิบัติงานอย่างต่อเนื่อง เช่น การเผยแพร่ข้อมูลทาง website จัดอบรม			
	๓.๓ มีข้อกำหนดในการลงทะเบียนการเข้าใช้งานที่ชัดเจน			
	๓.๔ มีการกำหนดหลักเกณฑ์ในการอนุมัติการใช้งาน			

คณะกรรมการตรวจสอบภายในภาคีเครือข่าย ระดับเขต ระดับจังหวัด

ชื่อหน่วยงาน..... **หน่วยรับตรวจ**.....

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่**.....

แบบสอบทานระบบการควบคุมภายใน

ด้าน <u>ระบบเทคโนโลยีสารสนเทศ</u>

ลำดับ	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
	๓.๕ มีหลักเกณฑ์ในการยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบ			
	๓.๖ การใช้งาน ๑ คน ต่อ ๑ User ไม่มีการใช้ร่วมกัน			
	๓.๗ กำหนดสิทธิในการใช้งานของ User แต่ละระดับชัดเจน			
๔.	การเข้าถึงระบบเครือข่าย			
	๔.๑ กำหนดสิทธิผู้ใช้งานเฉพาะบริการที่ได้รับสิทธิเท่านั้น			
	๔.๒ หน่วยงานกำหนดข้อปฏิบัติการเข้าถึงให้ผู้ใช้งานทราบ			
	๔.๓ หน่วยงานมีการควบคุมการเชื่อมต่อ VPN FTP หรือ Telnet กับระบบเครือข่ายหลัก อย่างรัดกุม			
	๔.๔ ผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับการเข้าถึงบริการผ่านช่องทาง ดังนี้			
	๔.๔.๑ Website			
	๔.๔.๒ บันทึกแจ้งเวียน			
	๔.๔.๓ อื่น ๆ ระบุ.....			
	๔.๕ มีข้อกำหนดการยืนยันตัวบุคคลก่อนอนุญาตให้ผู้ใช้งานเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน			
๕.	การเข้าถึงระบบปฏิบัติการ			
	๕.๑ หน่วยงานกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการ			
	๕.๒ หน่วยงานกำหนดให้ผู้ใช้งานแสดงข้อมูลในการยืนยันตัวตนของผู้ใช้งาน			
	๕.๓ หน่วยงานกำหนดขั้นตอนการยืนยันตัวตนของผู้ใช้งาน (ถ้ามี)			
	๕.๔ หน่วยงานมีการจำกัดหรือควบคุมการใช้โปรแกรมอรรถประโยชน์			
	๕.๕ หน่วยงานจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมต่างๆ			
๖.	การเข้าถึง Application และสารสนเทศ			
	๖.๑ หน่วยงานกำหนดแนวปฏิบัติ ในการเข้าถึงสารสนเทศ Application ต่างๆ ของผู้ใช้งาน			

คณะกรรมการตรวจสอบภายในภาคีเครือข่าย ระดับเขต ระดับจังหวัด

ชื่อหน่วยงาน..... **หน่วยรับตรวจ**.....

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่**.....

แบบสอบทานระบบการควบคุมภายใน

ด้าน <u>ระบบเทคโนโลยีสารสนเทศ</u>

ลำดับ	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
	๖.๒ ข้อจำกัดที่กำหนดเป็นไปตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน			
	๖.๓ หน่วยงานมีข้อกำหนดในการควบคุมคอมพิวเตอร์พกพา (Notebook) เข้าถึงสารสนเทศของหน่วยงาน			
	๖.๔ หน่วยงานกำหนดมาตรการเพื่อป้องกันความเสี่ยงจากการใช้คอมพิวเตอร์พกพา (Notebook) และโทรศัพท์เคลื่อนที่			
๗.	การจัดระบบสำรองกรณีฉุกเฉิน ๗.๑ หน่วยงานมีแนวปฏิบัติหรือหลักเกณฑ์ในการสำรองข้อมูลและกู้คืนระบบอย่างชัดเจน			
	๗.๒ ทุกระบบที่จัดทำการสำรองข้อมูลและกู้คืนระบบมีการรายงานผลการสำรองข้อมูลและกู้คืนระบบ			
	๗.๓ หน่วยงานมีการจัดทำแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ด้านระบบสารสนเทศ (BCP)			
	๗.๔ หน่วยงานจัดให้มีการซักซ้อมแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ด้านระบบสารสนเทศ			
	๗.๕ หน่วยงานจัดให้มีการทดสอบระบบสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งาน			

สรุปผลการสอบทาน

ลงชื่อ _____

ผู้สอบทาน