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

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่**.....

แบบสอบทานระบบการควบคุมภายใน

ด้าน ระบบเทคโนโลยีสารสนเทศ

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ลำดับ	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
๑	แนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ			
	๑.๑ จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรและลงนามโดยผู้บริหารของหน่วยงาน ประกอบด้วยเนื้อหาอย่างน้อย ได้แก่			
	๑.๑.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ			
	๑.๑.๒ ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉิน			
	๑.๑.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ			
	๑.๑.๔ กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าว			
	๑.๒ ทบทวน ปรับปรุง นโยบายและข้อปฏิบัติให้เป็นปัจจุบัน			
	๑.๓ เผยแพร่แนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทางเว็บไซต์ของหน่วยงาน			
๒.	กำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศของหน่วยงาน (Access Control) ครอบคลุมทุกระดับ ได้แก่			
	๒.๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผล			
	๒.๒ กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้น เวลา และช่องทางการเข้าถึง			
	๒.๓ การควบคุมการเชื่อมต่อ VPN FTP หรือ Telnet กับระบบเครือข่ายหลัก			
๓.	การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)			
	๓.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์			
	๓.๒ ลงทะเบียนผู้ใช้งาน (User Registration)			
	๓.๓ ตัดรายชื่อผู้ใช้งานออกจากทะเบียน เมื่อเกษียณอายุราชการ โอน/ย้าย หรือลาออก			

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

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่**.....

แบบสอบทานระบบการควบคุมภายใน

ด้าน <u>ระบบเทคโนโลยีสารสนเทศ</u>

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

	๓.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยการจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศตามความเหมาะสม			
	๓.๕ ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ตามระยะเวลาอย่างน้อยปีละ ๑ ครั้ง			
๔.	การควบคุมการเข้าถึงเครือข่ายและระบบปฏิบัติการ (Network and Operating System Access Control)			
	๔.๑ ห้องปฏิบัติงานหรือห้องควบคุมระบบเครือข่ายเป็นพื้นที่เฉพาะบุคคลที่ได้รับอนุญาตและต้องมีการแบ่งพื้นที่เป็นสัดส่วนชัดเจน เช่น			
	๔.๑.๑ ส่วนปฏิบัติงาน (Operations Zone)			
	๔.๑.๒ ส่วนเครื่องแม่ข่าย (Server Zone)			
	๔.๑.๓ ส่วนเครื่องสำรองไฟ (UPS Zone)			
	๔.๒ การควบคุมการเข้า - ออก ห้องปฏิบัติการระบบเครือข่าย			
	๔.๓ สถานที่จัดเก็บอุปกรณ์เกี่ยวกับสารสนเทศมีการล็อคกุญแจเมื่อไม่มีการใช้งาน			
	๔.๔ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ			
	๔.๕ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ			
	๔.๖ การควบคุมการใช้งานคอมพิวเตอร์ส่วนบุคคล (PC)			
	๔.๗ การควบคุมการใช้งานคอมพิวเตอร์พกพา (Notebook)			
	๔.๘ การควบคุมการใช้งานอินเทอร์เน็ต (Internet)			
	๔.๙ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (WLAN)			
	๔.๑๐ การกำหนดระยะเวลาสิ้นสุดการเชื่อมต่อ กรณีไม่ใช้งานระบบสารสนเทศในระยะเวลาหนึ่ง (Session Timeout)			
	๔.๑๑ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)			
	๔.๑๒ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์			
๕.	แผนเตรียมความพร้อมกรณีฉุกเฉิน			

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

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่**.....

แบบสอบทานระบบการควบคุมภายใน

ด้าน <u>ระบบเทคโนโลยีสารสนเทศ</u>

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

	๕.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเป็นลายลักษณ์อักษรและลงนามโดยผู้บริหารของหน่วยงาน			
	๕.๒ ปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน			
	๕.๓ กำหนดหน้าที่และความรับผิดชอบของบุคลากรในการดูแลระบบสารสนเทศ และระบบสำรองข้อมูล			
	๕.๔ ทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมความพร้อมฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง			
๖.	การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ			
	๖.๑ คำสั่งแต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านสารสนเทศ			
	๖.๒ จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศ ได้แก่			
	๖.๒.๑ การวิเคราะห์ความเสี่ยง (Risk Analysis)			
	๖.๒.๒ การจัดลำดับความสำคัญความเสี่ยง (Risk Matrix)			
	๖.๒.๓ การจัดการความเสี่ยง (Risk Management)			
	๖.๒.๔ การยอมรับความเสี่ยง (Risk Treatment)			
	๖.๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง			

สรุปผลการสอบทาน

ลงชื่อ _____

ผู้สอบทาน