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

สำนักงานปลัดกระทรวงสาธารณสุข **วันที่.....**

แบบสอบทานระบบการควบคุมภายใน

ด้าน <u>ระบบสารสนเทศ</u>

ลำดับที่	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
๑	**ด้านนโยบาย**			
	๑.๑ จัดทำนโยบายเป็นลายลักษณ์อักษรและลงนามโดยผู้บริหารของหน่วยงาน			
	๑.๒ จัดทำนโยบายเกี่ยวกับการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ครอบคลุมทุกระดับ ได้แก่			
	- การเข้าถึงระบบสารสนเทศ			
	- การเข้าถึงระบบเครือข่าย			
	- การเข้าถึงระบบปฏิบัติการ			
	- การเข้าถึงโปรแกรมประยุกต์หรือ Application			
	๑.๓ กำหนดนโยบายเกี่ยวข้องกับการจัดทำระบบสำรองข้อมูล			
	๑.๔ จัดทำแผนบริหารความเสี่ยงทางด้านสารสนเทศของหน่วยงาน			
	๑.๕ คำสั่งแต่งตั้งคณะกรรมการบริหารความเสี่ยงทางด้านสารสนเทศของหน่วยงาน			
	๑.๖ การประกาศเผยแพร่นโยบายและข้อปฏิบัติให้ผู้ใช้งานทราบ เช่น ทาง website หนังสือเวียน			
	๑.๗ หน่วยงานมีการกำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจนเป็นลายลักษณ์อักษร			
๒	**ด้านการควบคุมการเข้าถึงและควบคุมการใช้งาน**			
	๒.๑ กำหนดสิทธิในการเข้าถึงเป็นลายลักษณ์อักษรที่ชัดเจน			
	๒.๒ ห้องปฏิบัติงานของฝ่ายสารสนเทศเป็นพื้นที่เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น			

ลำดับที่	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
	๒.๓ สถานที่เก็บอุปกรณ์ที่เกี่ยวข้องกับสารสนเทศภายในมีการล็อคกุญแจ เมื่อไม่มีการใช้งาน			
	๒.๔ มีระบบการป้องกันกรณีฉุกเฉิน เช่น เกิดอัคคีภัย โจรกรรม และอุทกภัย			
	๒.๕ มีกฎข้อบังคับการปฏิบัติตนของเจ้าหน้าที่ขณะปฏิบัติงานที่ชัดเจน เช่น ห้ามสูบบุหรี่หรือห้ามรับประทานอาหาร เครื่องดื่มภายในห้องปฏิบัติการ			
	๒.๖ เครื่อง UPS (เครื่องสำรองไฟ) มีเพียงพอ อยู่ในสถานะพร้อมใช้งาน เพื่อป้องกันข้อมูลสารสนเทศเสียหายกรณีไฟฟ้าดับ/ไฟฟ้าตก			
	๒.๗ มีแผนและระบบการตรวจสอบ บำรุงรักษาสายไฟฟ้าภายในห้องปฏิบัติการ, สายเคเบิล และอุปกรณ์คอมพิวเตอร์ Hardware ของหน่วยงานอยู่สม่ำเสมอ			
๓	**การเข้าถึงผู้ใช้งาน**			
	๓.๑ หน่วยงานจัดทำคู่มือการปฏิบัติงานให้กับผู้ใช้ (User)			
	๓.๒ หน่วยงานจัดให้มีการให้ความรู้ ความเข้าใจกับผู้ปฏิบัติงานอย่างต่อเนื่อง เช่น การเผยแพร่ทาง website, จัดอบรม			
	๓.๓ มีข้อกำหนดในการลงทะเบียนการเข้าใช้งานที่ชัดเจน			
	๓.๔ มีการกำหนดหลักเกณฑ์ในการอนุมัติการใช้งาน			
	๓.๕ มีหลักเกณฑ์ในการยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบ			
	๓.๖ การใช้งาน ๑ คนต่อ ๑ User ไม่มีการใช้ร่วม			
	๓.๗ กำหนดสิทธิในการใช้งานของ User แต่ละระดับชัดเจน			
๔	**การเข้าถึงระบบเครือข่าย**			
	๔.๑ กำหนดสิทธิการใช้งานเฉพาะบริการที่ได้รับสิทธิเท่านั้น			
	๔.๒ หน่วยงานกำหนดข้อปฏิบัติการเข้าถึงให้ผู้ใช้งานทราบ			
	๔.๓ หน่วยงานมีการควบคุมการเชื่อมต่อ Terminal กับระบบคอมพิวเตอร์หลัก อย่างรัดกุม			

ลำดับที่	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/สมบูรณ์	ไม่มี/ไม่ใช่/ไม่สมบูรณ์	
	๔.๔ ผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับการเข้าถึงบริการผ่านช่องทาง			
	๑) Website			
	๒) บันทึกแจ้งเวียน			
	๓) อื่น ๆ ระบุ.....			
	๔.๕ มีข้อกำหนดการยืนยันตัวบุคคลก่อนอนุญาตให้ผู้ใช้งานเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน			
๕	**การเข้าถึงระบบปฏิบัติการ**			
	๕.๑ หน่วยงานกำหนดขั้นตอนการเข้าถึงการใช้งานของระบบปฏิบัติการ			
	๕.๒ หน่วยงานกำหนดให้ผู้ใช้งานแสดงข้อมูลในการยืนยันตัวตนของผู้ใช้งาน			
	๕.๓ หน่วยงานกำหนดขั้นตอนการยืนยันตัวตนของผู้ใช้งาน (ถ้ามี)			
	๕.๔ หน่วยงานมีกำหนดรหัสผ่านที่สามารถทำงานอัตโนมัติได้			
	๕.๖ หน่วยงานมีการจำกัดหรือควบคุมการใช้โปรแกรมอรรถประโยชน์			
	๕.๗ หน่วยงานจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมต่าง ๆ			
๖	**การเข้าถึง Application และสารสนเทศ**			
	๖.๑ หน่วยงานกำหนดแนวปฏิบัติ ในการเข้าถึงสารสนเทศ Application ต่าง ๆ ของผู้ใช้งาน			
	๖.๒ ข้อจำกัดที่กำหนดเป็นไปตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน			
	๖.๓ หน่วยงานมีข้อกำหนดในการควบคุมคอมพิวเตอร์เคลื่อนที่การเข้าถึงสารสนเทศของหน่วยงาน			
	๖.๔ หน่วยงานกำหนดมาตรการเพื่อป้องกันความเสี่ยงจากการใช้คอมพิวเตอร์เคลื่อนที่และโทรศัพท์เคลื่อนที่			

ลำดับที่	รายการ	ผลการประเมิน		หมายเหตุ
		มี/ใช่/ สมบูรณ์	ไม่มี/ไม่ใช่/ ไม่สมบูรณ์	
๗	**การจัดระบบสำรองกรณีฉุกเฉิน** ๗.๑ หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบสำรองที่ชัดเจน			
	๗.๒ ทุกระบบที่จัดทำสำรองมีการรายงานผลการสำรอง			
	๗.๓ หน่วยงานมีการเตรียมแผนการเตรียมความพร้อมกรณีฉุกเฉิน			
	๗.๔ หน่วยงานกำหนดหน้าที่ความรับผิดชอบของบุคลากรที่ชัดเจน			
	๗.๕ หน่วยงานจัดให้มีการทดสอบระบบให้อยู่ในสภาพพร้อมใช้งาน			

สรุปผลการสอบทาน

_____

_____

_____

_____

_____

ลงชื่อ _____

(ผู้สอบทาน)