(ร่าง) แบบประเมินระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

สำหรับกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม และหน่วยงานที่มี SERVER

(WP/๒๕๖๕ - ป.I.๐๐๑**)**

วัตถุประสงค์ เพื่อให้มั่นใจว่าหน่วยงานมีการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยที่ตรวจ .....

งวดที่ตรวจ ปีงบประมาณ พ.ศ.๒๕๖๕

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๑	จัดให้มีผู้รับผิดชอบหรือคำสั่งแต่งตั้งคณะกรรมการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศทำหรือปรับปรุงนโยบายหรือข้อปฏิบัติด้านความมั่นคงปลอดภัยอย่างน้อยปีละ ๑ ครั้ง	-หนังสือมอบหมายหรือคำสั่งแต่งคณะกรรมการ					
๒	สื่อสารให้เจ้าหน้าที่ทุกคนเห็นถึงความสำคัญของการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยขององค์กรโดยเคร่งครัดอย่างน้อยปีละ ๑ ครั้ง	-หนังสือแจ้งเวียน หรือการชี้แจงนโยบายด้านความมั่นคงฯ					
๓	จัดให้มีการประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัย อย่างน้อยปีละ ๑ ครั้ง โดยกำหนดให้มีวาระการประชุมที่ต้องหารือกันอย่างน้อยดังนี้ - การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงฯ และผลการตรวจสอบ - แผนการดำเนินการเชิง	รายงานการประชุมของคณะกรรมการบริหารฯ เกี่ยวกับการจัดการด้านความมั่นคงปลอดภัย <u>ต้องมีวาระการประชุมครบตามที่กำหนดไว้</u> รวมทั้งมีการจัดสรรทรัพยากรที่เพียงพอต่อการดำเนินการ					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ป้องกัน/แก้ไข จากผลการตรวจสอบดังกล่าว - การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป - การประเมินความเสี่ยงและแผนลดความเสี่ยง รวมทั้งจัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ ที่เพียงพอต่อการจัดการดังกล่าว						
๔	จัดให้มีนโยบายหรือข้อปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ ที่สอดคล้องกับนโยบายของกรมฯ	นโยบายหรือข้อปฏิบัติ					
๕	จัดให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยเพื่อให้เจ้าหน้าที่ขององค์กร มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ ๑ ครั้ง	-หลักฐานการจัดอบรม/ประชุม/แจ้งเวียน/แจ้งในสื่ออิเล็กทรอนิกส์					
๖	จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ ๑ ครั้ง และมีการจัดทำแผนเพื่อลดความเสี่ยง หรือปัญหาที่พบ	เอกสารการประเมินความเสี่ยงพร้อมแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ					
๗	จัดทำ และ ปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัยอย่างน้อยให้ครอบคลุมระบบงาน เครื่องเซิร์ฟเวอร์	คู่มือได้รับการปรับปรุงเนื้อหา วันและเวลาให้เป็นปัจจุบัน					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	และอุปกรณ์ที่มีความสำคัญดังนี้ o คู่มือระบบงานต่างๆ ทั้งในส่วนของผู้ใช้งาน และผู้ดูแลระบบ o คู่มือการตรวจสอบสถานะของเซิร์ฟเวอร์และระบบเครือข่าย o คู่มือการตรวจสอบระบบและอุปกรณ์ต่างๆ ในห้องเครื่อง o คู่มือการสำรองข้อมูล						
๘	มีการถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายหน่วยงานออกจากระบบต่างๆ ทั้งหมดโดยทันทีที่ได้รับแจ้งจากกลุ่มบริหารทรัพยากรบุคคลหรือจากหน่วยงาน	- แบบบันทึกข้อมูลการลาออกหรือย้ายหน่วยงาน -หนังสือขอถอดถอนสิทธิจากหน่วยงาน					
ตรวจห้อง SERVER (ข้อ ๙-๑๒)							
๙	ห้ามบุคคลภายนอกเข้าไปในห้อง SERVER โดยไม่มีกิจที่จำเป็น	บันทึกการเข้าออกของบุคคลภายนอก วันเวลาการเข้า-ออก และกิจที่ต้องปฏิบัติ					
๑๐	มีการตรวจสอบสภาพการทำงานของอุปกรณ์	บันทึกการตรวจสอบอุปกรณ์สนับสนุนการ					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	สนับสนุนการทำงานของระบบคอมพิวเตอร์ ได้แก่ ■ ระบบกระแสไฟฟ้า ■ ระบบการควบคุมความชื้น ■ ระบบการระบายอากาศ ■ ระบบการปรับอุณหภูมิ ■ ระบบกระแสไฟฟ้าสำรอง ■ ระบบ UPS ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ	ทำงานของระบบคอมพิวเตอร์ประจำวันหรือตามรอบเวลาที่กำหนด					
๑๑	ดำเนินการตรวจสอบทรัพยากรของเซิร์ฟเวอร์สำหรับระบบงานสำคัญอย่างน้อยสัปดาห์ละ ๑ ครั้ง สิ่งที่ควรตรวจสอบประกอบด้วย ปริมาณการใช้ CPU ปริมาณการใช้ฮาร์ดดิสก์ ปริมาณการใช้หน่วยความจำ และปริมาณการใช้เครือข่าย รวมทั้งควรมีการตรวจสอบการใช้งานเครือข่ายโดยภาพรวม	- แบบฟอร์มบันทึกผลการตรวจสอบการใช้ทรัพยากรของเซิร์ฟเวอร์สำหรับระบบงาน โดยให้พิจารณาเทียบกับปริมาณการใช้ทรัพยากรมากที่สุดสำหรับเซิร์ฟเวอร์ตรวจดูว่าเกินค่าหรือไม่ CPU ๖๐ RAM ๘๐ ฮาร์ดดิสก์ ๘๐					
๑๒	มีการวิเคราะห์ประเมินสมรรถนะ server และแนวทางการแก้ไข	-แบบวิเคราะห์การประเมินสมรรถนะ server -บันทึกการเสนอแนวทางแก้ไขถึงผู้บริหาร					
๑๓	<u>มีแผนการสำรองข้อมูล</u> ซึ่งประกอบด้วย -รายชื่อของระบบงานสำคัญทั้งหมด -ชนิดของข้อมูล	-แผนการสำรองข้อมูลที่มีข้อมูลครบถ้วน -ผลการสำรองข้อมูล					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	-ตำแหน่งหรือชื่อผู้รับผิดชอบในการสำรอง -ความถี่ในการสำรองข้อมูล -สถานที่เก็บ (รวมถึงการเก็บไว้นอกสถานที่ด้วย) <u>มีแบบฟอร์มบันทึกการสำรองข้อมูลตามแผน</u>การสำรองข้อมูล แบบฟอร์มควรประกอบด้วย -ชื่อของระบบ -ชนิดของข้อมูล -ตำแหน่งหรือชื่อผู้ดำเนินการสำรอง -วัน เวลาที่สำรองข้อมูล เช่น วัน/เวลาที่เริ่มต้นและสิ้นสุด -สถานที่เก็บ (รวมถึงการเก็บไว้นอกสถานที่ด้วย) -ผลการสำรองข้อมูล (สำเร็จ/ไม่สำเร็จ) -การแก้ไขในกรณีที่ไม่สำเร็จ						
๑๔	มีการลงทะเบียนสำหรับผู้ใช้งานใหม่ และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์มฯ	แบบฟอร์มลงทะเบียน					
๑๕	มีการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน สำหรับ<u>เจ้าหน้าที่ของหน่วยงาน</u> อย่างน้อยปีละ ๑	-หนังสือแจ้งให้หน่วยงานทบทวนสิทธิ					
การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต							
ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว (๑๖-๑๙)							
๑๖	มีเอกสารการสำรวจ/วิเคราะห์ความต้องการของ	-เอกสารการสำรวจความต้องการของผู้ใช้งานระบบ					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ผู้ใช้งานหรือไม่						
๑๗	ระบบที่พัฒนาสอดคล้องกับความต้องการของผู้ใช้งานหรือไม่	รายงานการประชุม/เอกสารที่นำเสนอระบบที่พัฒนา					
๑๘	มีคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ	คู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ					
๑๙	มีเอกสารการวิเคราะห์ออกแบบระบบ ซึ่งประกอบด้วย (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) / ความสัมพันธ์ของฐานข้อมูล (๓)พจนานุกรมฐานข้อมูล	๑.แผนผังกระแสการไหลของข้อมูล(DFD/Use case) ๒.แผนผังโครงสร้างฐานข้อมูล(ER Diagram)/ ความสัมพันธ์ของฐานข้อมูล ๓.พจนานุกรมฐานข้อมูล					
ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น (๒๐-๒๗) (ถ้ามี)							
๒๐	มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งานหรือไม่	เอกสารการวิเคราะห์ความต้องการของผู้ใช้งานหรือไม่					
๒๑	มีเอกสารการวิเคราะห์ออกแบบระบบซึ่งประกอบด้วย (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram) / ความสัมพันธ์ของฐานข้อมูล (๓)พจนานุกรมฐานข้อมูล	(๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram)/ ความสัมพันธ์ของฐานข้อมูล (๓)พจนานุกรมฐานข้อมูล					
๒๒	มีการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา	รายงานการประชุมหรือบันทึกข้อตกลงร่วมกัน					
๒๓	มีการทดสอบระบบโดยการทดสอบระบบ(ต้องแยกระบบจากระบบจริงที่ใช้	รายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบ					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	งาน)	จริงที่ใช้งาน					
๒๔	มีการฝึกอบรมการใช้งานระบบ	รายงานผลการฝึกอบรมการใช้งาน					
๒๕	มีคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ	คู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ					
๒๖	มีการติดตั้งและการทดสอบระบบขึ้นใช้งานจริง	รายงานผลการติดตั้งและการทดสอบระบบขึ้นใช้งานจริง					
๒๗	มีการประเมินความพึงพอใจของผู้ใช้งานระบบ	รายงานผลการประเมินความพึงพอใจของผู้ใช้งานระบบ					
๒๘	หน่วยงานมีระบบการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือปฏิบัติตามขั้นตอนการเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์หน่วยงานตามประกาศกรมเรื่องแนวทางการเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์ของหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ	ข้อกำหนดหรือข้อปฏิบัติการตรวจสอบคุณภาพข้อมูลสารสนเทศหรือฐานข้อมูลอย่างเป็นระบบหรือปฏิบัติตามขั้นตอนการเผยแพร่อย่างน้อยปีละ ๑ ครั้ง					
๒๙	กรณีที่เป็นเครื่องคอมพิวเตอร์แบบพกพา (Notebook) ที่ใช้ร่วมกัน . มีการกรอกแบบฟอร์มยืม-คืนเพื่อขออนุมัติการนำไปใช้งาน และป้องกันการสูญหาย	แบบฟอร์มยืม-คืนเครื่องคอมพิวเตอร์พกพาที่มีการบันทึกข้อมูลครบถ้วน					
๓๐	มีผู้รับผิดชอบกลั่นกรองข้อมูลก่อนเผยแพร่ผ่านเว็บไซต์	คำสั่งหรือข้อปฏิบัติที่กำหนดผู้รับผิดชอบในการกลั่นกรองข้อมูล					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๓๑	มีนโยบายหรือข้อปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล	นโยบายหรือข้อปฏิบัติ					
ผลรวม N๑, N๒ , N๓							
ผลรวม N๑+N๒+N๓							
ผลรวมจำนวนข้อ (โดยไม่นับรวมข้อที่เป็น N/A) X ๒							
คิดเป็นร้อยละ (N / ผลรวมจำนวนข้อ x ๑๐๐)							

เกณฑ์การประเมินผลระบบการควบคุมภายใน

คะแนน	ระดับ
๙๐ – ๑๐๐	ดีมาก
๘๐ – ๘๙.๙๙	ดี
๗๐ – ๗๙.๙๙	พอใช้
ต่ำกว่า ๗๐	ต้องปรับปรุง

ผู้รับตรวจ .....

(.....)

.....

ผู้ตรวจ/สอบทาน .....

(.....)

.....

วันที่.....เดือน.....พ.ศ.....