(ร่าง) แบบประเมินระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

สำหรับหน่วยงานที่ไม่มี SERVER

(WP/๒๕๖๕ - ป.I.๐๐๒)

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	มีคำสั่งหรือผู้รับผิดชอบด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของหน่วยงาน	คำสั่งหรือหลักฐานการมอบหมายผู้รับผิดชอบด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของหน่วยงาน					
๒	มีการสื่อสารนโยบายด้านความมั่นคงปลอดภัยของกรม ส.บ.ส. แก่เจ้าหน้าที่ทุกคนในหน่วยงาน	หลักฐานการสื่อสาร เช่น รายงานการประชุม/การแจ้งเวียน/แจ้งในสื่ออิเล็กทรอนิกส์					
๓	มีนโยบายหรือข้อปฏิบัติความมั่นคงปลอดภัย ด้านสารสนเทศ ที่สอดคล้องกับนโยบายของกรมฯ	นโยบายหรือข้อปฏิบัติ					
๔	รายงานผลการปฏิบัติตามนโยบายหรือข้อปฏิบัติที่กำหนด	รายงานการประชุม หรือรายงานผลการประเมินติดตาม					
๕	จัดให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยเพื่อให้เจ้าหน้าที่ขององค์กร มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ ๑ ครั้ง	-หลักฐานการจัดอบรม/ประชุม/แจ้งเวียน/แจ้งในสื่ออิเล็กทรอนิกส์					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๖	จัดทำ และ ปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย เช่น คู่มือระบบงานต่างๆ ทั้งในส่วนของผู้ใช้งาน และผู้รับผิดชอบด้านเทคโนโลยีสารสนเทศ	มีคู่มือและคู่มือได้รับการปรับปรุงเนื้อหา วันและเวลาให้ทันสมัยและเป็นปัจจุบัน					
๗	มีการแจ้งถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายหน่วยงานออกจากระบบต่างๆ	-หนังสือแจ้งขอถอดถอนสิทธิจากหน่วยงาน					
๘	มีการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งานสำหรับเจ้าหน้าที่ของหน่วยงาน อย่างน้อยปีละ ๑	หนังสือ/บันทึกการแจ้งทบทวนสิทธิ					
การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งาน รวมทั้งพัฒนาต่อยอดได้ในอนาคต							
ระบบสารสนเทศที่พัฒนาเสร็จสิ้นแล้ว (๙-๑๒)							
๙	มีเอกสารการสำรวจ/วิเคราะห์ความต้องการของผู้ใช้งานหรือไม่	-เอกสารการสำรวจความต้องการของผู้ใช้งานระบบ					
๑๐	ระบบที่พัฒนาสอดคล้องกับความต้องการของผู้ใช้งานหรือไม่	รายงานการประชุม/เอกสารที่นำเสนอระบบที่พัฒนา					
๑๑	มีคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ	คู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ					
๑๒	มีเอกสารการวิเคราะห์ออกแบบระบบ ซึ่งประกอบด้วย (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้าง	๑.แผนผังกระแสการไหลของข้อมูล(DFD/Use case) ๒.แผนผังโครงสร้างฐานข้อมูล(ER Diagram)/ความสัมพันธ์ของฐานข้อมูล					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	ฐานข้อมูล(ER Diagram) / ความสัมพันธ์ของฐานข้อมูล (๓)พจนานุกรมฐานข้อมูล	๓.พจนานุกรมฐานข้อมูล					
ระบบสารสนเทศที่อยู่ในช่วงการพัฒนายังไม่เสร็จสิ้น (๑๓-๒๐) ถ้ามี							
๑๓	มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งานหรือไม่	มีเอกสารการวิเคราะห์ความต้องการของผู้ใช้งานหรือไม่					
๑๔	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วนดังนี้หรือไม่ (๑)แผนผังกระแสการไหลของข้อมูล(DFD/Use case) (๒)แผนผังโครงสร้างฐานข้อมูล(ER Diagram)/ ความสัมพันธ์ของฐานข้อมูล (๓)พจนานุกรมฐานข้อมูล	มีเอกสารการวิเคราะห์ออกแบบระบบครบถ้วน					
๑๕	มีการพัฒนาแก้ไขระบบที่อยู่ในช่วงการพัฒนา	รายงานการประชุมหรือบันทึกข้อตกลงร่วมกัน					
๑๖	มีการทดสอบระบบโดยการทดสอบระบบ (ต้องแยกระบบจากระบบจริงที่ใช้งาน)	รายงานผลการทดสอบระบบโดยการทดสอบระบบต้องแยกระบบจากระบบจริงที่ใช้งาน					
๑๗	มีการฝึกอบรมการใช้งานระบบ	รายงานผลการฝึกอบรมการใช้งาน					
๑๘	มีคู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ	คู่มือการใช้งานทั้งของผู้ใช้งานและผู้ดูแลระบบ					
๑๙	มีการติดตั้งและการทดสอบระบบขึ้นใช้งานจริง	รายงานผลการติดตั้งและการทดสอบระบบขึ้นใช้งานจริง					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
๒๐	มีการประเมินความพึงพอใจของผู้ใช้งานระบบ	รายงานผลการประเมินความพึงพอใจของผู้ใช้งานระบบ					
๒๑	กรณีมีการพัฒนาระบบ ได้แจ้งให้กลุ่มเทคโนโลยีสารสนเทศทราบทุกครั้ง เพื่อเตรียมพื้นที่สำหรับระบบที่พัฒนาขึ้นใหม่	หนังสือแจ้งกลุ่มเทคโนโลยีฯ					
๒๒	กรณีที่เป็นเครื่องคอมพิวเตอร์แบบพกพา (Notebook) ที่ใช้ร่วมกัน . มีการกรอกแบบฟอร์มยืม-คืนเพื่อขออนุมัติการนำไปใช้งาน และป้องกันการสูญหาย	แบบฟอร์มยืม-คืนเครื่องคอมพิวเตอร์พกพาที่มีการบันทึกข้อมูลครบถ้วน					
๒๓	มีผู้รับผิดชอบกลั่นกรองข้อมูลก่อนเผยแพร่ผ่านเว็บไซต์	คำสั่งหรือข้อปฏิบัติที่กำหนดผู้รับผิดชอบในการกลั่นกรองข้อมูล					
๒๔	<u>มีแผนการสำรองข้อมูล</u> ซึ่งประกอบด้วย -รายชื่อของระบบงานสำคัญทั้งหมด -ชนิดของข้อมูล -ตำแหน่งหรือชื่อผู้รับผิดชอบในการสำรอง -ความถี่ในการสำรองข้อมูล -สถานที่เก็บ (รวมถึงการเก็บไว้นอกสถานที่ด้วย) <u>มีแบบฟอร์มบันทึกการสำรองข้อมูลตามแผน</u>การสำรองข้อมูล แบบฟอร์มควรประกอบด้วย	-แผนการสำรองข้อมูล -ผลการสำรองข้อมูล					

ลำดับที่	รายการที่ตรวจ	หลักฐาน	ผลการประเมิน			N/A	หมายเหตุ
			ถูกต้อง/ครบถ้วน	ไม่ถูกต้อง/ไม่ครบถ้วน	ไม่ได้ปฏิบัติ		
			N๑ = ๒	N๒ = ๑	N๓ = ๐		
	-ชื่อของระบบ -ชนิดของข้อมูล -ตำแหน่งหรือชื่อผู้ดำเนินการสำรอง -วัน เวลาที่สำรองข้อมูล เช่น วัน/เวลาที่เริ่มต้นและสิ้นสุด -สถานที่เก็บ (รวมถึงการเก็บไว้นอกสถานที่ด้วย) -ผลการสำรองข้อมูล (สำเร็จ/ไม่สำเร็จ) -การแก้ไขในกรณีที่ไม่สำเร็จ							
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.....