2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
1	ขั้นตอนที่ 1 : ทำการประเมินในภาพรวม (Plan : Holistic Approach, Policy)														
	1.1 รวบรวมกฎหมาย กฎระเบียบด้านเทคโนโลยีสารสนเทศที่ต้องปฏิบัติ	1) กฎระเบียบด้านความมั่นคงปลอดภัยสารสนเทศที่มีต่อหน่วยงานที่เกี่ยวข้อง (Cybersecurity roles and responsibilities for the entire workforce and third party stakeholder)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	↔	↔										
	1.2 รวบรวมข้อมูลเอกสารความรู้ และศึกษามาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO27001:2013		งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	↔	↔										
	1.3 รวบรวมวัสดุ ครุภัณฑ์ รวมทั้งข้อมูลที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (Asset Management)		งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	↔	↔										
	1.3.1 การจัดการวัสดุ ครุภัณฑ์ (Assset Management)	1) ด้านอุปกรณ์และระบบที่ใช้ภายในองค์กร (Physical devices and systems within the organization are inventoried)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			↔	↔								

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		2) ด้านระบบปฏิบัติการและแอพลิเคชั่นต่างๆ (Software Platforms and applications)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→								
		3) ด้านการสื่อสารภายในองค์กร (Organizational communication and Data flows are mapped)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→								
		4) ด้านการสื่อสารภายนอกองค์กร (External information systems are catalougued)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→								
		5) ทรัพยากรที่เกี่ยวข้องกับงาน (Resources are prioritized based on their classification, criticalty and business value)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT			←	→								
2	ขั้นตอนที่ 2 การกำหนดขอบเขต ตัวชี้วัดและแนวทางการดำเนินงาน (Do ; Implement, Operate ,Measure)														
	2.1 ระบบบริหารจัดการองค์กร (Business Environment)	1) การกำหนดกรอบในการจัดทำวัตถุประสงค์ (Objectives) รวมถึงทิศทางและหลักการในการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										
		2) การคำนึงถึงข้อกำหนดทางธุรกิจและกฎหมาย รวมถึงข้อบังคับตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		3) การกำหนดนโยบายการบริหารความเสี่ยงให้สอดคล้องตามพันธกิจขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	→										
		4) การบริหารจัดการความเสี่ยงเชิงกลยุทธ์ขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←		→									
		5) การกำหนดมาตรการบริหารจัดการความสี่ยงและผลกระทบที่เกิดขึ้น	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←		→									
		6) แต่งตั้งคณะกรรมการอำนวยการและคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									
		9) แต่งตั้งคณะทำงานขับเคลื่อนนโยบายความมั่นคงปลอดภัยสารสนเทศ ในระดับสำนัก/กอง/ศูนย์/เขต	ทุกสำนัก/กอง/ศูนย์/เขต ภายในกรมสนับสนุนบริการสุขภาพ		←	→									
	2.2 นโยบายองค์กร (Governance Policy)	1) การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									
		2) การกำหนดนโยบายการบริหารจัดการความเสี่ยงตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		3) การกำหนดข้อกฎหมายและระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									
	2.3 นโยบายการจัดการความเสี่ยง (Risk Management Strategy)	1) การระบุความเสี่ยงและการจัดลำดับความสำคัญ ซึ่งสามารถใช้เป็นหลักฐาน ตามลักษณะโครงสร้างพื้นฐานขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT	←	—	→									
		2) การดำเนินการจัดการเกี่ยวกับการคุกคามจากสื่อแหล่งต่างๆ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT				←	→							
		3) การจัดทำเอกสารการบริหารจัดการกรณีเกิดการบุกรุกจากภายในและภายนอกองค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									
		4) การระบุผลกระทบจากภัยคุกคามและความเสี่ยงที่ส่งผลกระทบต่อองค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									
		5) การระบุผลกระทบทางธุรกิจที่อาจจะเกิดขึ้นและแนวทางแก้ไข	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/ทุกงานในกลุ่ม IT		←	→									
	2.4 อนุมัตินโยบายโดยผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศ กรมสนับสนุนบริการสุขภาพ		CSO กรมสนับสนุนบริการสุขภาพ		←	→									

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
3	ขั้นตอนที่ 3 การดำเนินงานตามแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Check : Monitor, Review and Analysis)														
	3.1 การสร้างการรับรู้ ทำความเข้าใจให้บุคลากรในทุกระดับ (Mind Set)	1) ประชุมคณะกรรมการอำนวยการรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Steering Committee)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)				↔						↔		
		2) ประชุมชี้แจงและประกาศนโยบายการดำเนินงานตามแนวทางมาตรฐาน ISO/IEC 27001	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)				↔								
		3) ประชุมคณะทำงานรักษาความมั่นคงปลอดภัยสารสนเทศ (IT Security Working Group)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)			↔						↔			
		4) ประชุมเชิงปฏิบัติการเพื่อกำหนดแนวทางการดำเนินงานตามมาตรฐาน ISO/IEC 27001	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)				↔			↔					
		5) ประชุมคณะทำงานขับเคลื่อนนโยบายความมั่นคงปลอดภัยสารสนเทศ (IT Security Working Group)	ทุกสำนัก/กอง/ศูนย์/เขต ภายในกรมสนับสนุนบริการสุขภาพ					↔					↔		
	3.2 ทำการประเมินระบบสารสนเทศในภาพรวม (Holistic Approach) โดยใช้ เทคนิค Gap Analysis ตามมาตรฐาน ISO/IEC 27001 (จัดจ้างบุคคลภายนอก)	1) ประเมินผลกระทบทางธุรกิจซึ่งอาจเกิดจากความล้มเหลวในความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)/				↔	↔							

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		2) ประเมินโอกาสในการเกิดขึ้นของความล้มเหลวที่มีต่อความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)					←	→						
		3) การคำนวณระดับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)						←	→					
		4) การพิจารณาความสามารถในการยอมรับความเสี่ยงในเกณฑ์ที่ยอมรับได้	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)							←	→				
		5) การประเมินความคุ้มค่าคุ้มทุน จากการดำเนินงานตามนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ ทั้งส่วนกลาง (1 แห่ง) และภูมิภาค (12+5 แห่ง)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)							←				→	
	3.3 ดำเนินการตามแผนจัดการความเสี่ยง (Risk Management) ใน 3 มุมมอง คือ ด้านบุคลากร ด้านกระบวนการและด้านเทคโนโลยี	1) ดำเนินการตรวจจับความผิดพลาดของผลลัพธ์ที่ได้จากการประมวลผล และทบทวนวิธีการปฏิบัติงาน เช่น การทำ Hardening, การจัดฝึกอบรม Security Awareness Training หรือ การจัดทำระบบ centralized Log Management	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)					←	→			←	→		

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		2) ทบทวนประสิทธิผลของการดำเนินงานตามนโยบายความมั่นคงปลอดภัยสารสนเทศตามที่กำหนด เช่น Vulnerability Assessment, Penetration Testing, Hardening, การติดตั้ง patch	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)							←	→			←	→
		3) วัดประสิทธิผลของการดำเนินงานตามแผนจัดการความเสี่ยง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท) / Info Security gr.									←	→		
		4) ทบทวนการประเมินความเสี่ยงตามแผนจัดการความเสี่ยง (Continuous Audit)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ (พท)											←	→
4	ขั้นตอนที่ 4 การปรับปรุงการดำเนินงานตามแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Act : Maintain and Improve)														
	4.1 การตรวจประเมินโดยกลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ (Pre Assessment by Internal Auditor)	1) การประเมินผลตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท) /กลุ่มตรวจสอบภายใน										←	→	
		2) การแก้ไขข้อบกพร่องจากการตรวจประเมินตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)											←	→

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
	4.2 การตรวจประเมินจากผู้เชี่ยวชาญภายนอก (Pre Assessment by External Auditor)	1) การประเมินผลตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)/กลุ่มตรวจสอบภายใน	ดำเนินการ ปี ๒๕๖๓											
		2) การแก้ไขข้อบกพร่องจากการตรวจประเมินตามแนวทางการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	ดำเนินการ ปี ๒๕๖๓											
	4.3 ผู้บริหารระดับสูงตัดสินใจสนับสนุนในการปฏิบัติตามมาตรฐาน ISO/IEC 27001	1) ดำเนินการแก้ไขข้อบกพร่องจากองค์กรที่ยังไม่ได้ปฏิบัติตามมาตรฐานอย่างเป็นรูปธรรม (Corrective Action)	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	ดำเนินการ ปี ๒๕๖๓											
	4.4 การจัดเตรียมเอกสารแสดงการประยุกต์ใช้งาน (SOA : Statement of Applicability)	1) เป็นเอกสารที่แสดงถึงรายการของหัวข้อในการควบคุม (Control) วัตถุประสงค์ในการควบคุม (Control Objectives) และเหตุผลในการเลือกหัวข้อในการควบคุม	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท) / ทุกหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ								จัดทำเอกสาร SOA เพื่อรองรับการประเมินปี ๒๕๖๓				

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
5	ขั้นตอนที่ 5 การควบคุม กำกับ ติดตาม (Control)														
	5.1 การควบคุมกำกับ	1) นโยบายความมั่นคงปลอดภัย : โดยจะต้องได้รับการอนุมัติจากผู้บริหารระดับสูง เผยแพร่อย่างทั่วถึง มีการมอบนโยบายการดูแลความมั่นคงปลอดภัย : ผู้บริหารระดับสูง จะต้องให้การสนับสนุนอย่างเต็มที่ / มีการกำหนดทิศทางชัดเจน / มีการมอบหมายงานและสร้างการรับรู้ รวมถึงการสร้างรูปแบบการประสานงานภายในองค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)			↔			↔			↔		↔	↔
		2) การจัดการทรัพย์สิน : สิ่งใดๆ ที่มีคุณค่ากับองค์กร ซึ่งจะรวมไปถึงเครื่องมือ อุปกรณ์ ฮาร์ดแวร์ ซอฟท์แวร์ ฐานข้อมูล บุคลากร สาธารณูปโภคต่างๆ จะต้องมีการจัดทำบัญชีทรัพย์สินทั้งหมดตามมาตรฐาน	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)			↔			↔			↔		↔	↔

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		3) ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร : มีการกำหนดบทบาทหน้าที่ความรับผิดชอบของบุคลากร พนักงาน รวมทั้งหน่วยงานภายนอกที่ชัดเจน โดยจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		←	→									
		4) ความมั่นคงปลอดภัยทางกายภาพ : มีการกำหนดพื้นที่ มีการกำหนดแนวปฏิบัติตามมาตรฐานความมั่นคงปลอดภัย รวมทั้งแนวทางการทำลายตามมาตรฐานด้วย	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		←	→									
		5) การบริหารการสื่อสารและการดำเนินการ : มีการจัดทำเอกสาร วิธีการปฏิบัติงาน มีการแบ่งหน้าที่ความรับผิดชอบ เพื่อลดโอกาสการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือมีการใช้ผิดวัตถุประสงค์ของทรัพย์สินขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)/ Info Security gr.		←	→									

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		6) การควบคุมการเข้าถึงระบบ (Access Control) มีการกำหนดนโยบายในการเข้าถึงระบบ (Access Control Policy) มีการจัดทำเอกสารชัดเจนและมีการทบทวนความต้องการขององค์กรและข้อกำหนดความมั่นคงปลอดภัย	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)/ Info Security gr.			←	→								
		7) การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ : องค์กรต้องจัดให้มีการวิเคราะห์และระบุถึงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศหรือเมื่อมีการปรับปรุงระบบที่มีอยู่ในปัจจุบัน ตลอดจนมาตรการที่เหมาะสมในการจัดการความเสี่ยง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)			↔			↔			↔			↔
		8) การจัดการเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ : มีการรายงานผ่านช่องทางการรายงานอย่างเหมาะสมด้วยความรวดเร็วเป็นไปได้ ตามบทบาทหน้าที่ความรับผิดชอบที่ชัดเจน	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		9) การบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity) : องค์กรมีการจัดกระบวนการในการสร้างความต่อเนื่องทางธุรกิจ มีแผนมีการนำไปปฏิบัติและมีการปรับปรุงแผนอย่างต่อเนื่อง สอดคล้องตามข้อกำหนด (Compliance) : การดำเนินการให้สอดคล้องตามข้อกฎหมาย ตามนโยบายความมั่นคงปลอดภัยสารสนเทศและการดำเนินการตรวจประเมินระบบสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
	5.2 ความตระหนักและการฝึกอบรมของบุคลากรกรมสนับสนุนบริการสุขภาพ	1) การลงทะเบียนเพื่อเข้าใช้งานในระบบ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		2) การสร้างความรู้ ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับบุคลากรและผู้เกี่ยวข้อง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		3) ผู้บริหารระดับสูงของกรมสนับสนุนบริการสุขภาพมีความรู้ ความเข้าใจ เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
	5.3 ความปลอดภัยของข้อมูล	1) ข้อมูลสารสนเทศได้รับการป้องกันตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		2) การส่งต่อข้อมูลได้รับการป้องกันตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		3) การบริหารจัดการครุภัณฑ์ที่เกี่ยวข้องตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		4) การบำรุงรักษาครุภัณฑ์ตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		5) การตรวจสอบความถูกต้องในการใช้เฟิร์มแวร์และความสมบูรณ์ของข้อมูล	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		6) การจัดสภาพแวดล้อมในการพัฒนาระบบสารสนเทศ ออกจากสภาพปกติ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
	5.4 กระบวนการและขั้นตอนในการป้องกันข้อมูล	1) การออกแบบระบบในการดูแลปกป้องข้อมูลตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	→									
		2) การประเมินและปรับปรุงข้อมูลตามแผนความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	→									
		3) การควบคุม กำกับ ดูแลระบบพื้นที่ห้อง Sever และครุภัณฑ์	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		4) การดำเนินการสำรองข้อมูลและการทดสอบเป็นระยะตามเกณฑ์ที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		5) การปฏิบัติตามนโยบาย ระเบียบ ข้อบังคับที่เกี่ยวข้องกับสภาพแวดล้อมในการบริหารทรัพย์สินขององค์กร	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		6) การทำลายข้อมูลตามแนวทางนโยบายรักษาความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		7) การปรับปรุงแนวทางการป้องกันข้อมูลที่มีประสิทธิภาพอย่างต่อเนื่อง	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		8) การกำหนดแผนบริหารจัดการต่อการตอบสนองเหตุการณ์ผิดปกติและแผนฟื้นฟูกู้คืนจากภัยพิบัติ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		←	→									
	5.5 การซ่อมบำรุง (Maintainance)	1) การจัดหา ซ่อมแซมสินทรัพย์ขององค์กรตามข้อกำหนดรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		2) การควบคุม กำกับ สินทรัพย์ครุภัณฑ์คอมพิวเตอร์ ที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
	5.6 ระบบการป้องกัน (Protective Technology)	1) การเก็บบันทึกข้อมูล เอกสารการดำเนินงาน ทบทวนตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←											→
		2) แนวทางในการปกป้องข้อมูลจาก Removable media ตามนโยบายความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		←	→									
		3) การมีระบบควบคุม กำกับทรัพย์สิน ครุภัณฑ์คอมพิวเตอร์ตามเกณฑ์มาตรฐานที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		←	→									

2019 ISMS MASTER PLAN [ISO 27001:2013]

ลำดับ	กิจกรรม	กิจกรรมย่อย	ผู้รับผิดชอบหลัก/งานที่เกี่ยวข้อง	ช่วงเวลาดำเนินการ											
				ตค.61	พย.	ธค.	มค.62	กพ.	มีค.	เมย.	พค.	มิย.	กค.	สค.	กย.62
		4) การควบคุมเครือข่ายการสื่อสารและระบบเชื่อมต่อตามเกณฑ์ที่กำหนด	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
	5.7 การรวบรวม Incident ของระบบสารสนเทศ เช่น ระบบล่ม, รายงานปัญหาไวรัส มัลแวร์ต่างๆ เป็นต้น	1) การรวบรวม Incident ของระบบสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→
		2) การกำหนดแนวทางและมาตรการในการป้องกันแก้ไขตามแนวทางการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)		↔	↔									
		3) การวิเคราะห์ความเสี่ยงและสาเหตุของผลกระทบที่มีโอกาสเกิดขึ้นในระบบ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)			↔			↔			↔		↔	↔
		4) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	งานพัฒนาระบบเทคโนโลยีสารสนเทศ(พท)	←	—	—	—	—	—	—	—	—	—	—	→