ชื่อหน่วยงาน .....

วันที่ดำเนินการ .....

			แบบประเมินตนเอง แนวปฏิบัติในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ เกี่ยวกับมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงานของรัฐ (ส่วนที่ ๑)	ดำเนินการแล้ว
มาตรการพื้นฐานสำหรับเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ กรณีมัลแวร์ เรียกค่าไถ่ สำหรับหน่วยงานของรัฐ				
	๑. จัดทำหรือทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ให้ครอบคลุมการสำรองข้อมูล การควบคุม			
	๒. สำรองข้อมูลที่สำคัญ			
		(๑) การสำรองข้อมูล ควรจัดทำอย่างน้อย ๒ เวอร์ชัน ไว้ในอุปกรณ์จัดเก็บข้อมูลที่ไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ ยกเว้นเวลาสำรองข้อมูล และในการสำรองข้อมูลแต่ละเวอร์ชันให้มีการจัดเก็บลงในอุปกรณ์ที่แตกต่างกัน		
		(๒) ทดสอบการกู้คืนข้อมูลที่สำรองเพื่อให้แน่ใจว่าสามารถนำมาใช้งานได้เมื่อต้องการ		
	๓. ควบคุมการเข้าถึงเครือข่าย และระบบสารสนเทศ			
		(๑) แยกส่วนเครือข่าย (Network segregation) ของระบบสารสนเทศตามรูปแบบการให้บริการ เพื่อลดผลกระทบจากการแพร่กระจายมัลแวร์ผ่านเครือข่าย		
		(๒) ทบทวนการกำหนดสิทธิการเข้าถึงเครือข่าย และระบบสารสนเทศตามความจำเป็นและการแบ่งแยกหน้าที่ (need to know, least privilege, separation of duties) รวมถึงควรตั้งค่าควบคุมในลักษณะการอนุญาตให้ใช้งานตามรายการสิทธิที่กำหนดไว้เท่านั้น (whitelisting)		
		(๓) กำหนดให้มีการยืนยันตัวตน (authentication) ตามสิทธิในการเข้าถึงระบบสารสนเทศ และเครือข่ายโดยไม่อนุญาตให้แชร์บัญชีผู้ใช้งาน		
	๔. ประเมินความเสี่ยงด้านระบบสารสนเทศ			
		(๑) จัดทำหรือทบทวนทะเบียนสินทรัพย์ (inventory of asset) รวมถึงข้อมูลที่สำคัญในการให้บริการ		
		(๒) จัดทำหรือทบทวนแผนผังการเชื่อมต่อเครือข่าย และระบบสารสนเทศที่ให้บริการ		
		(๓) จัดทำข้อมูลการติดต่อสำหรับผู้ดูแลหรือผู้ให้บริการสินทรัพย์ และเครือข่าย เพื่อเตรียมความพร้อมในกรณีที่ต้องการประสานการแก้ไขปัญหา หรือรับมือสถานการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น		
		(๔) ระบุความเสี่ยงที่อาจเกิดขึ้นสำหรับการให้บริการ เพื่อพิจารณาช่องทางสำรองสำหรับให้บริการ กรณีที่ช่องทางหลักได้รับผลกระทบ		
		(๕) จัดเตรียมเครื่องมือ อุปกรณ์ และทรัพยากรที่จำเป็นสำหรับการให้บริการผ่านช่องทางสำรอง		

	๕. จัดเก็บบันทึกกิจกรรม (log) ไปยังพื้นที่จัดเก็บในส่วนกลางที่มีการควบคุมการเข้าถึงอย่างรัดกุม เพื่อให้แน่ใจว่าข้อมูลดังกล่าวจะไม่ถูกทำลายหรือเปลี่ยนแปลง โดยบันทึกกิจกรรมควรครอบคลุม		
		(๑) ข้อมูลการใช้งานระบบสารสนเทศ เช่น application log	
		(๒) ข้อมูลการเชื่อมต่อทางเครือข่ายหรือระบบป้องกันการโจมตีทางเครือข่าย เช่น firewall log, intrusion prevention system (IPS) log	
		(๓) ข้อมูลบันทึกกิจกรรมของระบบปฏิบัติการ เช่น event log, system log, security log, audit log	
		(๔) การจัดเก็บข้อมูล log ควรมีระยะเวลาในการจัดเก็บที่เหมาะสมเพื่อประโยชน์ในการนำมาใช้งานภายหลัง ทั้งนี้ อาจพิจารณากำหนดระยะเวลาในการจัดเก็บ ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการโดยอนุโลม	
	๖. ทบทวน และยกเลิกบริการที่ไม่จำเป็นบนเครื่องให้บริการ		
	๗. กำหนดเจ้าหน้าที่ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับบริหารกับระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ		
	๘. ให้ความรู้กับผู้ใช้งานในหน่วยงานเกี่ยวกับการป้องกันตนเองจากการติดมัลแวรเรียกค่าไถ่ โดยอาจใช้สื่อประชาสัมพันธ์จากเว็บไซต์ไทยเซิร์ต (https://www.thaicert.or.th)		
มาตรการเพิ่มเติมสำหรับการดูแลบริการที่สำคัญ			
	๑. การสำรองข้อมูลในอุปกรณ์จัดเก็บข้อมูล ควรมีการเข้ารหัสลับเพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลในอุปกรณ์กรณีที่อุปกรณ์นั้นสูญหาย รวมถึงควรพิจารณานำอุปกรณ์จัดเก็บข้อมูลที่สำรองข้อมูลแล้วไปเก็บยังนอกพื้นที่		
	๒. ป้องกันการติดมัลแวร์		
		(๑) ติดตั้งโปรแกรมตรวจจับมัลแวร์บนเครื่องให้บริการ และเครื่องผู้ใช้งาน	
		(๒) อัปเดตซอฟต์แวร์ที่ใช้ให้บริการเป็นเวอร์ชันล่าสุด	
		(๓) ใช้ระบบป้องกันการโจมตีทางเครือข่าย เช่น intrusion prevention system (IPS)	
	๓. ตรวจจับพฤติกรรมของมัลแวร์ด้วยระบบหรือกลไกที่เหมาะสม เช่น การตรวจสอบการเชื่อมต่อทางเครือข่ายของเครื่องคอมพิวเตอร์ไปยังไอพีแอดเดรสหรือโดเมนของเครื่องควบคุมมัลแวร์ (command and control server) การตรวจสอบค่าแฮชของไฟล์มัลแวร์		
	๔. ตรวจสอบความผิดปกติของรายการบัญชีผู้ใช้งาน และข้อมูลบันทึกกิจกรรม (log) อย่างสม่ำเสมอ		
	๕. ตรวจสอบช่องโหว่ (vulnerability assessment) ของระบบสารสนเทศ หรือซอฟต์แวร์ที่ให้บริการ อย่างสม่ำเสมอ และให้รีบแก้ไขช่องโหว่ทันทีหากพบว่าเป็นความเสี่ยงที่รุนแรง ลงทะเบียนเพื่อขอรับการสนับสนุนเกี่ยวกับข้อมูลแจ้งเตือนภัยคุกคามทางไซเบอร์ และการดำเนินการตามมาตรการป้องกันและตรวจจับภัยคุกคามดังกล่าว ทางอีเมล thaicert-gms@thaicert.or.th		

	๖. ลงทะเบียนเพื่อขอรับการสนับสนุนเกี่ยวกับข้อมูลแจ้งเตือนภัยคุกคามทางไซเบอร์ และการดำเนินการตามมาตรการป้องกันและตรวจจับภัยคุกคามดังกล่าว ทางอีเมล thaicert-gms@thaicert.or.th	

ชื่อหน่วยงาน .....

วันที่ดำเนินการ .....

แบบประเมินตนเอง แนวปฏิบัติในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ เกี่ยวกับมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงานของรัฐ (ส่วนที่ ๒)			ดำเนินการแล้ว
แนวทางการดำเนินการรับมือสถานการณ์ กรณีหน่วยงานของรัฐพบความเสียหายที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่			
	๑. ตัดการเชื่อมต่อทางเครือข่าย สำหรับ		
		(๑) เครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เพื่อป้องกันการกระจายของมัลแวร์ไปยังระบบสารสนเทศอื่น	
		(๒) ระบบสำรองข้อมูล รวมถึงการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอก เพื่อป้องกันข้อมูลสำรองถูกเข้ารหัสลับ	
		(๓) ระบบสารสนเทศที่อยู่ในเครือข่ายเดียวกัน เพื่อป้องกันการกระจายของมัลแวร์ไประบบดังกล่าว	
	๒. สำรองข้อมูลที่ยังใช้งานได้อยู่จากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ ไปยังอุปกรณ์บันทึกข้อมูลภายนอก ซึ่งไม่ควรเป็นอุปกรณ์เดียวกับที่ใช้สำรองข้อมูล		
นอกจากนี้หน่วยงานของรัฐควรมีการดำเนินการเพิ่มเติมดังนี้			
	๑. แจ้งเหตุไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และไทยเซิร์ต (ทางอีเมล report@thaicert.or.th)		
	๒. เปลี่ยนรหัสผ่านที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงรหัสผ่านที่ใช้งานผ่านระบบควบคุมบัญชีผู้ใช้งานทั้งหมด		
	๓. ตรวจสอบสายพันธุ์ของมัลแวร์เรียกค่าไถ่ โดยอาศัยข้อมูลที่ปรากฏในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เช่น นามสกุลของไฟล์ที่เปลี่ยนไป ข้อความที่ปรากฏบนหน้าจอในการเรียกค่าไถ่ เพื่อประเมินวิธีการแก้ไขปัญหา เช่น การกู้คืนข้อมูล		
	๔. หากมีความประสงค์ในการใช้เครื่องมือถอดรหัสลับข้อมูล ควรทำในสภาพแวดล้อมที่ไม่มีการเชื่อมต่อทางเครือข่าย เพื่อลดความเสี่ยงที่อาจเกิดจากการใช้เครื่องมือดังกล่าว		