แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
การวางแผนเพื่อบริหารจัดการเว็บไซต์							
1	**การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์**						
	1.1		มีการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บไซต์				
	1.2		จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์				
	1.3		ได้กำหนดมาตรการที่เกี่ยวข้องเพื่อป้องกันภัยคุกคามที่มีความสำคัญ				
การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย							
2	**การตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software)**						
	2.1		มีการตรวจสอบและปรับปรุงส่วนประกอบของโปรแกรมสำหรับให้บริการเว็บให้เป็นเวอร์ชั่นปัจจุบันอย่างสม่ำเสมอ				
	2.2		มีการควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย				
	2.3		ได้กำหนดสิทธิในการเข้าถึงสารบบ (Directory) ที่ใช้เก็บไฟล์หรือโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับเครื่องบริการเว็บให้เหมาะสม เช่น กาหนดสิทธิโฟลเดอร์ที่เก็บหน้าเว็บเพจของระบบหลังบ้าน อนุญาตให้เฉพาะผู้ดูแลเข้าถึงได้เท่านั้น				
	2.4		มีการตรวจสอบและจัดการลบ ตัวอย่างโปรแกรม ตัวอย่างไฟล์ข้อมูล บัญชีผู้ใช้ที่ไม่ได้ใช้งาน เช่น บัญชีซึ่งมีการใช้งานระหว่างกระบวนการติดตั้งเครื่องบริการเว็บทั้งหมด				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
	2.5		ได้ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้นของ ชื่อสารบบ ชื่อไฟล์ข้อมูล ตาแหน่งไฟล์ข้อมูล รหัสผ่าน ที่มากับการติดตั้งเครื่องบริการเว็บ				
	2.6		มีการควบคุมการเข้าถึงเครื่องบริการเว็บ และจำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอลที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ เช่น การกำหนด IP Whitelist ที่สามารถเข้าถึงเครื่องบริการเว็บ				
	2.7		ปิดบริการต่าง ๆ ที่ไม่จำเป็นบนเครื่องบริการเว็บ โดยเฉพาะบริการประเภท Remote Access				
3	**การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS)**						
	3.1		มีการกาหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control)				
	3.2		ตรวจสอบว่ามีไฟล์หรือโปรแกรมเสริม (Plug-in Program) ที่ไม่จำเป็นหรือไม่ได้ใช้งานปรากฏอยู่หรือไม่ ถ้าตรวจพบผู้ดูแล เครื่องบริการเว็บต้องลบหรือถอนการติดตั้งไฟล์หรือโปรแกรมเสริมนั้นทันที				
	3.3		ตรวจสอบการอัพเดตเวอร์ชั่นของระบบบริหารจัดการเว็บไซต์อยู่เสมอ และอัพเดตเวอร์ชั่นให้เป็นปัจจุบัน				
	3.4		ลบบัญชีผู้ใช้ที่มากับการติดตั้งระบบบริหารจัดการเว็บไซต์ เปลี่ยนชื่อผู้ใช้ของบัญชีผู้ใช้นั้นหรือเปลี่ยนรหัสผ่านของบัญชี ผู้ใช้นั้น ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัยแทน				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
	3.5		เปลี่ยน Table Prefix ของฐานข้อมูลที่มาในระหว่างการติดตั้งระบบบริหารจัดการเว็บไซต์				
4	**การตั้งค่าฐานข้อมูล (Database System)**						
	4.1		มีการตั้งค่าฐานข้อมูล อนุญาตให้เฉพาะโปรแกรมประยุกต์ (Application) และเครื่องบริการเว็บที่เกี่ยวข้องเข้าถึงได้เท่านั้น (โปรแกรมประยุกต์ที่ใช้เกี่ยวข้องกับฐานข้อมูล เช่น MySQL Workbench)				
	4.2		ควบคุมการเข้าถึงระบบฐานข้อมูลด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ด่านกันบุกรุกหรือไฟร์วอลล์ (Firewall)				
	4.3		ตรวจสอบและปิดบริการ (Services, Extension) ที่ไม่จำเป็นหรือไม่ได้ใช้งาน ในระบบฐานข้อมูล เช่น PHPMyAdmin				
	4.4		จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลตามระยะเวลาที่กำหนด และลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล				
	4.5		ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งฐานข้อมูล หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ดังกล่าว ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัย				
	4.6		กำหนดค่าติดตั้งระบบฐานข้อมูลเพื่อไม่อนุญาตให้ใช้งานรหัสผ่านที่มีค่าว่าง (Null Password)				
	4.7		ตรวจสอบและลบแฟ้มชั่วคราว (Temporary File) ที่ถูกสร้างขึ้นระหว่างการติดตั้งระบบฐานข้อมูล				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
	4.8		ปรับปรุงเวอร์ชั่นของโปรแกรมระบบฐานข้อมูล หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ				
	4.9		กำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้				
	4.10		รหัสผ่านที่เก็บในฐานข้อมูล ต้องมีการเข้ารหัสเสมอ				
5	**การตั้งค่า Server-Side Script Engine**						
	5.1		มีการควบคุมการเข้าถึงไฟล์หรือสารบบต่าง ๆ ให้เหมาะสมกับบทบาทของผู้ใช้ (Permission and Access Control)				
	5.2		ปรับปรุงเวอร์ชั่นของ Server-Side Script Engine หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ				
	5.3		กำหนดค่าติดตั้งไม่ให้ Server-Side Script Engine แสดงข้อมูลเวอร์ชั่นของ Server-Side Script Engine ที่เครื่องบริการเว็บใช้งาน ใน HTTP Header				
	5.4		กำหนดค่าติดตั้ง Server-Side Script Engine ไม่ให้มีการแสดงรายละเอียดของข้อความแสดงข้อผิดพลาด (Error Message) หากต้องมีรายละเอียดควรจะแสดงข้อมูลเท่าที่จำเป็น				
6	**การกำหนดและรักษารหัสผ่าน**						
	6.1		ได้มีการจัดทำนโยบายการตั้งค่ารหัสผ่านให้มีความมั่นคงปลอดภัย (Strong Password)				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
	6.2		กำหนดนโยบายให้มีการเปลี่ยนรหัสผ่านอย่างสม่าเสมอ				
	6.3		ไม่เก็บรหัสผ่านที่ไม่มีการเข้ารหัสลับบนเครื่องบริการเว็บ หากจำเป็นต้องมีการเก็บรหัสผ่านควรอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด				
การพัฒนาโปรแกรมประยุกต์บนเครื่องบริการเว็บอย่างมั่นคงปลอดภัย							
7	**มีการป้องกันการโจมตีจากเทคนิค SQL Injection**						
	7.1		มีการจัดทำ Prepared Statement และ/หรือ Stored Procedure ของโปรแกรมประยุกต์บนเว็บ				
	7.2		มีการจัดทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ				
	7.3		มีการทำ Encoding หรือทำ Sanitization ของโปรแกรมประยุกต์บนเว็บ				
8	**การป้องกันการโจมตีจากเทคนิค Session Hijacking**						
	8.1		Session ID ที่มีข้อมูลการรับรองตัวตนของผู้ใช้บริการ (User Authentication Credential) ต้องมีการเข้ารหัสลับ				
	8.2		ต้องกำหนด Session Timeout ในระยะเวลาที่เหมาะสมของโปรแกรมประยุกต์บนเว็บ				
	8.3		กำหนดค่า Session ID เป็นค่าสุ่มที่คาดเดาไม่ได้และไม่มีการใช้ซ้ำในระยะเวลาที่เหมาะสม				
	8.4		ต้องส่งค่า Session ID ในช่องทางการสื่อสารที่มีการเข้ารหัสลับ (Encrypted Connection)				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
9	**การป้องกันการโจมตีจากเทคนิค Cross-Site Scripting ของโปรแกรมประยุกต์บนเว็บ**						
	9.1		มีการทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ				
	9.2		มีการตรวจสอบข้อมูลชุดคำสั่งในเว็บไซต์ของโปรแกรมประยุกต์บนเว็บ				
	9.3		มีการทำ Output Validation ในลักษณะ Sanitization ของโปรแกรมประยุกต์บนเว็บ				
	9.4		มีการใช้งาน HTTP Only Cookie flag ของโปรแกรมประยุกต์บนเว็บ				
10	**การป้องกันการโจมตีจากเทคนิค CSRF**						
	10.1		มีการใช้งาน Unique Token และ/หรือตรวจสอบ Referrer ร่วมกับการส่งข้อมูล หรือคาสั่งผ่านแบบฟอร์ม ของโปรแกรมประยุกต์บนเว็บ				
	10.2		มีการใช้ Captcha ของโปรแกรมประยุกต์บนเว็บ				
11	**การป้องกันการโจมตีจากปัญหาข้อมูลลับรั่วไหล (Sensitive Data Exposure)**						
	11.1		มีการออกแบบและควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Notification or Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้ายของโปรแกรมประยุกต์บนเว็บ				
	11.2		พัฒนาเว็บไซต์โดยไม่ให้มีการใช้งาน Autocomplete ในแบบฟอร์มสำคัญของโปรแกรมประยุกต์บนเว็บ				
	11.3		ไม่ใช้ชื่อ URL ที่คาดเดาได้ง่ายซึ่งใช้ในการเข้าถึงหน้าเว็บสำหรับผู้ดูแลเครื่องบริการเว็บ (Administrator Control Panel Web Page)				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ (Security Incident Handling)							
12	**การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์**						
	12.1		กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions)				
		12.1.1	ปิดการเชื่อมต่อของเว็บไซต์				
		12.1.2	สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนามาใช้ในการวิเคราะห์				
		12.1.3	ตรวจสอบช่องทางการโจมตีและช่องโหว่ของเว็บไซต์ด้วยข้อมูลที่สำเนามา				
		12.1.4	ระหว่างการตรวจสอบจัดสร้างเว็บเพจแบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อชี้แจงสถานการณ์การปิดปรับปรุง				
		12.1.5	กู้คืนโปรแกรมที่เกี่ยวข้อง ข้อมูลเว็บ และฐานข้อมูลที่เกี่ยวข้องกับเว็บไซต์เป็นเวอร์ชั่นก่อนหน้าที่จะถูกโจมตี				
		12.1.6	ตรวจสอบช่องโหว่ของเว็บไซต์ (เวอร์ชั่นก่อนหน้าที่จะถูกโจมตี) ด้วยการทำ Vulnerability Assessment				
		12.1.7	แก้ไขช่องโหว่ของเว็บไซต์ที่ทาให้ผู้ประสงค์ร้ายสามารถเจาะเพื่อเข้าควบคุมระบบได้				
		12.1.8	บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด				
	12.2		กรณีเว็บไซต์ถูกโจมตีในลักษณะ DoS (Denial of Service)				
		12.2.1	ปิดการเชื่อมต่อของเว็บไซต์				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
		12.2.2	สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนามาใช้ในการวิเคราะห์				
		12.2.3	ตรวจสอบหมายเลขไอพีที่ต้องสงสัยว่าจะเป็นการโจมตีด้วยข้อมูลที่สำเนามา				
		12.2.4	ปิดกั้นการเข้าถึงจากไอพีแอดเดรสดังกล่าว และแจ้งไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ตเพื่อหามาตรการที่รองรับ				
		12.2.5	บันทึกเหตุการณ์และขั้นตอนการดาเนินการที่เกิดขึ้นทั้งหมด				
	12.3		กรณีโดเมนถูกขโมย (Domain Hijack)				
		12.3.1	เก็บรวบรวมหลักฐานที่เกิดขึ้นทั้งหมด เช่น วัน เดือน ปี ที่ข้อมูลโดเมนเปลี่ยน หน้าจอของโดเมนที่ใช้งาน				
		12.3.2	ตรวจสอบกับผู้ลงทะเบียนโดเมนถึงสาเหตุของการเปลี่ยนแปลงโดเมน				
		12.3.3	แจ้งการถูกขโมยข้อมูลโดเมนกับผู้ลงทะเบียนโดเมนที่ใช้บริการ โดยนำหลักฐานที่เกี่ยวข้องแนบไปด้วย				
		12.3.4	เมื่อได้รับสิทธิในการบริหารจัดการโดเมนคืนมาแล้ว ให้ตรวจสอบข้อมูลต่าง ๆ ที่ใช้ในการยืนยันตัวตน รวมถึงเปลี่ยนรหัสผ่านระบบบริหารจัดการโดเมน				
		12.3.5	บันทึกเหตุการณ์และขั้นตอนการดาเนินการที่เกิดขึ้นทั้งหมด				
13	**การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์**						
	13.1		เลือกโปรแกรมที่น่าเชื่อถือ หรือ ได้รับการแนะนาจากหน่วยงานที่เกี่ยวข้อง				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
	13.2		ปรับรุ่นของโปรแกรมที่ใช้ในการตรวจสอบข้อบกพร่องให้เป็นรุ่นล่าสุด				
	13.3		หากการใช้โปรแกรมส่งผลกระทบกับการให้บริการของเครื่องบริการเว็บ ควรจะมีการสารองข้อมูลทุกครั้งก่อนมีการใช้โปรแกรมตรวจสอบ				
	13.4		ควรใช้โปรแกรมมากกว่าสองโปรแกรมขึ้นไปในการตรวจสอบเพื่อเปรียบเทียบผลลัพธ์ที่ได้จากการทดสอบ				
14	**การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์**						
	14.1		การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือ ข้อมูลการใช้งานของผู้ใช้ (Log) ตามมาตรฐานฉบับนี้ ปฏิบัติตามข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทาความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550				
15	**การสำรองข้อมูลเว็บไซต์**						
	15.1		มีการจัดทำแนวปฏิบัติในการสำรองข้อมูลของเครื่องบริการเว็บ				
			(1) แนวปฏิบัติต้องสอดคล้องกับข้อกาหนดทางกฎหมาย				
			(2) แนวปฏิบัติต้องสอดคล้องกับข้อผูกพันทางสัญญา				
			(3) แนวปฏิบัติต้องสอดคล้องกับแนวนโยบายที่เกี่ยวข้องขององค์กร				
			(4) จุดประสงค์และขอบเขตของแนวปฏิบัติ				

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ			รายการ	สถานะ			หมายเหตุ
				ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
			(5) บทบาทและหน้าที่ของผู้เกี่ยวข้อง				
			(6) เครื่องบริการเว็บที่เกี่ยวข้องกับแนวปฏิบัติ				
			(7) คำนิยามของศัพท์เฉพาะ โดยเฉพาะในทางกฎหมายและทางเทคนิค				
			(8) รายละเอียดของกฎหมาย ข้อผูกพันสัญญา และแนวนโยบายขององค์กรที่เกี่ยวข้อง				
			(9) ความถี่ของการสำรองข้อมูล				
			(10) ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองได้รับการดูแลรักษาและการป้องกันอย่างเหมาะสม				
			(11) ขั้นตอนสำหรับยืนยันว่าข้อมูลได้รับการทำลายหรือมีการเก็บรักษาเมื่อไม่มีความจำเป็นในการใช้งาน				
			(12) ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองสามารถถูกเรียกออกมาใช้งานได้อย่างถูกต้องในกรณีที่มีการร้องขอ				
			(13) ความรับผิดชอบของผู้ที่มีส่วนร่วมในการเก็บรักษา การป้องกัน และการทำลายข้อมูล				
			(14) ระยะเวลาในการเก็บรักษาข้อมูลแต่ละประเภท				
			(15) หน้าที่รับผิดชอบของทีมสำรองข้อมูล (หากมี)				

(ลงชื่อ) ..... (ผู้ตรวจสอบ)
(.....)
ตำแหน่ง .....

(ลงชื่อ) ..... (หัวหน้าหน่วยงาน)
(.....)
ตำแหน่ง .....

แบบตรวจสอบสถานะความมั่นคงปลอดภัยเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

(หน่วยงาน) ..... กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

☐ Website ☐ Web App ☐ Application

หัวข้อ	รายการ	สถานะ			หมายเหตุ
		ยอมรับได้	อยู่ระหว่างปรับปรุง	ไม่มี	
ข้อมูลเพิ่มเติม :					
ชื่อ Website					
1					
2					
3					
4					

ชื่อ Web Application / Web Service	
1	
2	
3	
4	
5	

ชื่อ Application	
1	
2	
3	
4	
5