ภาคผนวก ก. แบบประเมินสำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
การวางแผนเพื่อบริหารจัดการเว็บไซต์ (หัวข้อ 4)				
1	การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ (หัวข้อ 4.1)			
1.1	มีการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ (หัวข้อ 4.1 ข้อ 1)			
1.2	จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์ (หัวข้อ 4.1 ข้อ 2)			
1.3	ได้กำหนดมาตรการที่เกี่ยวข้องเพื่อป้องกันภัยคุกคามที่มีความสำคัญ (หัวข้อ 4.1 ข้อ 3)			
การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย (หัวข้อที่ 5)				
2	การตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) (หัวข้อที่ 5.1)			
2.1	มีการตรวจสอบและปรับปรุงส่วนประกอบของโปรแกรมสำหรับให้บริการเว็บให้เป็นเวอร์ชั่นปัจจุบันอย่างสม่ำเสมอ (หัวข้อที่ 5.1 ข้อ 1)			
2.2	มีการควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย (หัวข้อที่ 5.1 ข้อ 2)			
2.3	ได้กำหนดสิทธิในการเข้าถึงสารบบ (Directory) ที่ใช้เก็บไฟล์หรือโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับเครื่องบริการเว็บให้เหมาะสม เช่น กำหนดสิทธิโฟลเดอร์ที่เก็บหน้าเว็บเพจของระบบหลังบ้าน อนุญาตให้เฉพาะผู้ดูแลเข้าถึงได้เท่านั้น (หัวข้อที่ 5.1 ข้อ 3)			
2.4	มีการตรวจสอบและจัดการลบ ตัวอย่างโปรแกรม ตัวอย่างไฟล์ข้อมูล บัญชีผู้ใช้ที่ไม่ได้ใช้งาน เช่น บัญชีซึ่งมีการใช้งานระหว่างกระบวนการติดตั้งเครื่องบริการเว็บทั้งหมด (หัวข้อที่ 5.1 ข้อ 4)			
2.5	ได้ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้นของ ชื่อสารบบ ชื่อไฟล์ข้อมูล ตำแหน่งไฟล์ข้อมูล รหัสผ่าน ที่มากับการติดตั้งเครื่องบริการเว็บ (หัวข้อที่ 5.1 ข้อ 5)			
2.6	มีการควบคุมการเข้าถึงเครื่องบริการเว็บ และจำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอลที่อนุญาตให้เครื่องบริการเว็บ			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
	สามารถเชื่อมต่อ เช่น การกำหนด IP Whitelist ที่สามารถเข้าถึงเครื่องบริการเว็บ (หัวข้อที่ 5.1 ข้อ 6)			
2.7	ปิดบริการต่าง ๆ ที่ไม่จำเป็นบนเครื่องบริการเว็บ โดยเฉพาะบริการประเภท Remote Access (หัวข้อที่ 5.1 ข้อ 7)			
3	การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS) (หัวข้อที่ 5.2)			
3.1	มีการกำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) (หัวข้อที่ 5.2 ข้อ 1)			
3.2	ตรวจสอบว่ามีไฟล์หรือโปรแกรมเสริม (Plug-in Program) ที่ไม่จำเป็นหรือไม่ได้ใช้งานปรากฏอยู่หรือไม่ ถ้าตรวจพบผู้ดูแลเครื่องบริการเว็บต้องลบหรือถอนการติดตั้งไฟล์หรือโปรแกรมเสริมนั้นทันที (หัวข้อที่ 5.2 ข้อ 2)			
3.3	ตรวจสอบการอัพเดตเวอร์ชั่นของระบบบริหารจัดการเว็บไซต์อยู่เสมอ และอัพเดตเวอร์ชั่นให้เป็นปัจจุบัน (หัวข้อที่ 5.2 ข้อ 3)			
3.4	ลบบัญชีผู้ใช้ที่มากับการติดตั้งระบบบริหารจัดการเว็บไซต์ เปลี่ยนชื่อผู้ใช้ของบัญชีผู้ใช้นั้นหรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้นั้น ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัยแทน (หัวข้อที่ 5.2 ข้อ 4)			
3.5	เปลี่ยน Table Prefix ของฐานข้อมูลที่มาในระหว่างการติดตั้งระบบบริหารจัดการเว็บไซต์ (หัวข้อที่ 5.2 ข้อ 5)			
4	การตั้งค่าฐานข้อมูล (Database System) (หัวข้อที่ 5.3)			
4.1	มีการตั้งค่าฐานข้อมูล อนุญาตให้เฉพาะโปรแกรมประยุกต์ (Application) และเครื่องบริการเว็บที่เกี่ยวข้องเข้าถึงได้เท่านั้น (โปรแกรมประยุกต์ที่ใช้เกี่ยวข้องกับฐานข้อมูล เช่น MySQL Workbench) (หัวข้อที่ 5.3 ข้อ 1)			
4.2	ควบคุมการเข้าถึงระบบฐานข้อมูลด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ด่านกันบุกรุกหรือไฟร์วอลล์ (Firewall) (หัวข้อที่ 5.3 ข้อ 2)			
4.3	ตรวจสอบและปิดบริการ (Services, Extension) ที่ไม่จำเป็นหรือไม่ได้ใช้งาน ในระบบฐานข้อมูล เช่น PHPMyAdmin (หัวข้อที่ 5.3 ข้อ 3)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
4.4	จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลตามระยะเวลาที่กำหนด และลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล (หัวข้อที่ 5.3 ข้อ 4)			
4.5	ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งฐานข้อมูล หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ดังกล่าว ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัย (หัวข้อที่ 5.3 ข้อ 5)			
4.6	กำหนดค่าติดตั้งระบบฐานข้อมูลเพื่อไม่อนุญาตให้ใช้งานรหัสผ่านที่มีค่าว่าง (Null Password) (หัวข้อที่ 5.3 ข้อ 6)			
4.7	ตรวจสอบและลบแฟ้มชั่วคราว (Temporary File) ที่ถูกสร้างขึ้นระหว่างการติดตั้งระบบฐานข้อมูล (หัวข้อที่ 5.3 ข้อ 7)			
4.8	ปรับปรุงเวอร์ชั่นของโปรแกรมระบบฐานข้อมูล หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ (หัวข้อที่ 5.3 ข้อ 8)			
4.9	กำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้ (หัวข้อที่ 5.3 ข้อ 9)			
4.10	รหัสผ่านที่เก็บในฐานข้อมูล ต้องมีการเข้ารหัสเสมอ (หัวข้อที่ 5.3 ข้อ 10)			
5	การตั้งค่า Server-Side Script Engine (หัวข้อที่ 5.4)			
5.1	มีการควบคุมการเข้าถึงไฟล์หรือสารบบต่าง ๆ ให้เหมาะสมกับบทบาทของผู้ใช้ (Permission and Access Control) (หัวข้อที่ 5.4 ข้อ 1)			
5.2	ปรับปรุงเวอร์ชั่นของ Server-Side Script Engine หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ (หัวข้อที่ 5.4 ข้อ 2)			
5.3	กำหนดค่าติดตั้งไม่ให้ Server-Side Script Engine แสดงข้อมูลเวอร์ชั่นของ Server-Side Script Engine ที่เครื่องบริการเว็บใช้งาน ใน HTTP Header (หัวข้อที่ 5.4 ข้อ 3)			
5.4	กำหนดค่าติดตั้ง Server-Side Script Engine ไม่ให้มีการแสดงรายละเอียดของข้อความแสดงข้อผิดพลาด (Error Message) หากต้องมีรายละเอียดควรจะแสดงข้อมูลเท่าที่จำเป็น (หัวข้อที่ 5.4 ข้อ 4)			
6	การกำหนดและรักษารหัสผ่าน (หัวข้อที่ 5.5)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
6.1	ได้มีการจัดทำนโยบายการตั้งค่ารหัสผ่านให้มีความมั่นคงปลอดภัย (Strong Password) (หัวข้อที่ 5.5 ข้อ 1)			
6.2	กำหนดนโยบายให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ (หัวข้อที่ 5.5 ข้อ 2)			
6.3	ไม่เก็บรหัสผ่านที่ไม่มีการเข้ารหัสลับบนเครื่องบริการเว็บ หากจำเป็นต้องมีการเก็บรหัสผ่านควรอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด (หัวข้อที่ 5.5 ข้อ 3)			
การพัฒนาโปรแกรมประยุกต์บนเครื่องบริการเว็บอย่างมั่นคงปลอดภัย (หัวข้อที่ 6)				
7	มีการป้องกันการโจมตีจากเทคนิค SQL Injection (หัวข้อที่ 6.1)			
7.1	มีการจัดทำ Prepared Statement และ/หรือ Stored Procedure ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.1 ข้อ 1)			
7.2	มีการจัดทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.1 ข้อ 2)			
7.3	มีการทำ Encoding หรือทำ Sanitization ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.1 ข้อ 3)			
8	การป้องกันการโจมตีจากเทคนิค Session Hijacking (หัวข้อที่ 6.2)			
8.1	Session ID ที่มีข้อมูลการรับรองตัวตนของผู้ใช้บริการ (User Authentication Credential) ต้องมีการเข้ารหัสลับ (หัวข้อที่ 6.2 ข้อ 1)			
8.2	ต้องกำหนด Session Timeout ในระยะเวลาที่เหมาะสมของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.2 ข้อ 2)			
8.3	กำหนดค่า Session ID เป็นค่าสุ่มที่คาดเดาไม่ได้และไม่มีการใช้ซ้ำในระยะเวลาที่เหมาะสม (หัวข้อที่ 6.2 ข้อ 3)			
8.4	ต้องส่งค่า Session ID ในช่องทางการสื่อสารที่มีการเข้ารหัสลับ (Encrypted Connection) (หัวข้อที่ 6.2 ข้อ 4)			
9	การป้องกันการโจมตีจากเทคนิค Cross-Site Scripting ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3)			
9.1	มีการทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 1)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
9.2	มีการตรวจสอบข้อมูลชุดคำสั่งในเว็บไซต์ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 2)			
9.3	มีการทำ Output Validation ในลักษณะ Sanitization ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 3)			
9.4	มีการใช้งาน HTTPOnly Cookie flag ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 4)			
10	การป้องกันการโจมตีจากเทคนิค CSRF (หัวข้อที่ 6.4)			
10.1	มีการใช้งาน Unique Token และ/หรือตรวจสอบ Referrer ร่วมกับการส่งข้อมูล หรือคำสั่งผ่านแบบฟอร์ม ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.4 ข้อ 1)			
10.2	มีการใช้ Captcha ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.4 ข้อ 2)			
11	การป้องกันการโจมตีจากปัญหาข้อมูลลับรั่วไหล (Sensitive Data Exposure) (หัวข้อที่ 6.5)			
11.1	มีการออกแบบและควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Notification or Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้ายของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.5 ข้อ 1)			
11.2	พัฒนาเว็บไซต์โดยไม่ให้มีการใช้งาน Autocomplete ในแบบฟอร์มสำคัญของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.5 ข้อ 2)			
11.3	ไม่ใช้ชื่อ URL ที่คาดเดาได้ง่ายซึ่งใช้ในการเข้าถึงหน้าเว็บสำหรับผู้ดูแลเครื่องบริการเว็บ (Administrator Control Panel Web Page) (หัวข้อที่ 6.5 ข้อ 3)			
การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ (Security Incident Handling) (หัวข้อที่ 7)				
12	การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ (หัวข้อที่ 7.1)			
12.1	กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions) (หัวข้อที่ 7.1.1)			
12.1.1	ปิดการเชื่อมต่อของเว็บไซต์ (หัวข้อที่ 7.1.1 ข้อ 1)			
12.1.2	สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ (หัวข้อที่ 7.1.1 ข้อ 2)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
12.1.3	ตรวจสอบช่องทางการโจมตีและช่องโหว่ของเว็บไซต์ด้วยข้อมูลที่สำเนามา (หัวข้อที่ 7.1.1 ข้อ 3)			
12.1.4	ระหว่างการตรวจสอบจัดสร้างเว็บเพจแบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อชี้แจงสถานการณ์การปิดปรับปรุง (หัวข้อที่ 7.1.1 ข้อ 4)			
12.1.5	กู้คืนโปรแกรมที่เกี่ยวข้อง ข้อมูลเว็บ และฐานข้อมูลที่เกี่ยวข้องกับเว็บไซต์เป็นเวอร์ชั่นก่อนหน้าที่จะถูกโจมตี (หัวข้อที่ 7.1.1 ข้อ 5)			
12.1.6	ตรวจสอบช่องโหว่ของเว็บไซต์ (เวอร์ชั่นก่อนหน้าที่จะถูกโจมตี) ด้วยการทำ Vulnerability Assessment (หัวข้อที่ 7.1.1 ข้อ 6)			
12.1.7	แก้ไขช่องโหว่ของเว็บไซต์ที่ทำให้ผู้ประสงค์ร้ายสามารถเจาะเพื่อเข้าควบคุมระบบได้ (หัวข้อที่ 7.1.1 ข้อ 7)			
12.1.8	บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด (หัวข้อที่ 7.1.1 ข้อ 8)			
12.2	กรณีเว็บไซต์ถูกโจมตีในลักษณะ DoS (Denial of Service) (หัวข้อที่ 7.1.2)			
12.2.1	ปิดการเชื่อมต่อของเว็บไซต์ (หัวข้อที่ 7.1.2 ข้อ 1)			
12.2.2	สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ (หัวข้อที่ 7.1.2 ข้อ 2)			
12.2.3	ตรวจสอบหมายเลขไอพีที่ต้องสงสัยว่าจะเป็นการโจมตีด้วยข้อมูลที่สำเนามา (หัวข้อที่ 7.1.2 ข้อ 3)			
12.2.4	ปิดกั้นการเข้าถึงจากไอพีแอดเดรสดังกล่าว และแจ้งไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ตเพื่อหามาตรการที่รองรับ (หัวข้อที่ 7.1.2 ข้อ 4)			
12.2.5	บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด (หัวข้อที่ 7.1.2 ข้อ 5)			
12.3	กรณีโดเมนถูกขโมย (Domain Hijack) (หัวข้อที่ 7.1.3)			
12.3.1	เก็บรวบรวมหลักฐานที่เกิดขึ้นทั้งหมด เช่น วัน เดือน ปีที่ข้อมูลโดเมนเปลี่ยน หน้าจอของโดเมนที่ใช้งาน (หัวข้อที่ 7.1.3 ข้อ 1)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
12.3.2	ตรวจสอบกับผู้ลงทะเบียนโดเมนถึงสาเหตุของการเปลี่ยนแปลงโดเมน (หัวข้อที่ 7.1.3 ข้อ 2)			
12.3.3	แจ้งการถูกขโมยข้อมูลโดเมนกับผู้ลงทะเบียนโดเมนที่ใช้บริการโดยนำหลักฐานที่เกี่ยวข้องแนบไปด้วย (หัวข้อที่ 7.1.3 ข้อ 3)			
12.3.4	เมื่อได้รับสิทธิในการบริหารจัดการโดเมนคืนมาแล้ว ให้ตรวจสอบข้อมูลต่าง ๆ ที่ใช้ในการยืนยันตัวตน รวมถึงเปลี่ยนรหัสผ่านระบบบริหารจัดการโดเมน (หัวข้อที่ 7.1.3 ข้อ 4)			
12.3.5	บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด (หัวข้อที่ 7.1.3 ข้อ 5)			
13	การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ (หัวข้อที่ 7.2)			
13.1	เลือกโปรแกรมที่น่าเชื่อถือ หรือ ได้รับการแนะนำจากหน่วยงานที่เกี่ยวข้อง (หัวข้อที่ 7.2 ข้อ 1)			
13.2	ปรับรุ่นของโปรแกรมที่ใช้ในการตรวจสอบข้อบกพร่องให้เป็นรุ่นล่าสุด (หัวข้อที่ 7.2 ข้อ 2)			
13.3	หากการใช้โปรแกรมส่งผลกระทบกับการให้บริการของเครื่องบริการเว็บ ควรจะมีการสำรองข้อมูลทุกครั้งก่อนมีการใช้โปรแกรมตรวจสอบ (หัวข้อที่ 7.2 ข้อ 3)			
13.4	ควรใช้โปรแกรมมากกว่าสองโปรแกรมขึ้นไปในการตรวจสอบเพื่อเปรียบเทียบผลลัพธ์ที่ได้จาก (หัวข้อที่ 7.2 ข้อ 4)			
14	การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (หัวข้อที่ 7.3)			
14.1	การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือ ข้อมูลการใช้งานของผู้ใช้ (Log) ตามมาตรฐานฉบับนี้ ปฏิบัติตามข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (หัวข้อที่ 7.3)			
15	การสำรองข้อมูลเว็บไซต์ (หัวข้อที่ 7.4)			
15.1	มีการจัดทำแนวปฏิบัติในการสำรองข้อมูลของเครื่องบริการเว็บ (1) แนวปฏิบัติต้องสอดคล้องกับข้อกำหนดทางกฎหมาย			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
	(2) แนวปฏิบัติต้องสอดคล้องกับข้อผูกพันทางสัญญา (3) แนวปฏิบัติต้องสอดคล้องกับแนวนโยบายที่เกี่ยวข้องขององค์กร (4) จุดประสงค์และขอบเขตของแนวปฏิบัติ (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)			

แบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง (จากการตรวจสอบสถานะความมั่นคงปลอดภัย)

ตัวอย่างของแบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุงซึ่งเกิดจากการตรวจสอบสถานะความมั่นคงปลอดภัยของเว็บไซต์ตามข้อกำหนดและแนวทางในมาตรฐานฉบับนี้ และเมื่อพบรายการที่ไม่เป็นไปตามข้อกำหนดก็ให้ระบุรายการแก้ไขลงในแบบฟอร์มพร้อมกับกำหนดระยะเวลาในการแก้ไขเพื่อนำเสนอต่อผู้ที่เกี่ยวข้องต่อไป

วันที่ตรวจสอบสถานะ			**เว็บไซต์**				
โดยหน่วยงาน							
ลำดับที่	**วันที่รายงาน**	**คำอธิบายรายการที่ยังต้องปรับปรุง**	**สาเหตุ**	**การแก้ไขชั่วคราว**	**สิ่งที่ต้องแก้ไข**		
					รายการแก้ไข	**รับผิดชอบโดย**	**วันที่แล้วเสร็จ**