ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

พ.ศ. ๒๕๖๘

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) มาตรา ๒๒ (๑๓) และ (๑๖) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ในคราวการประชุมครั้งที่ ๖/๒๕๖๕ เมื่อวันที่ ๔ พฤศจิกายน ๒๕๖๕ มติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๔/๒๕๖๖ เมื่อวันที่ ๒๖ พฤศจิกายน ๒๕๖๖ และมติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๓/๒๕๖๘ เมื่อวันที่ ๒๙ สิงหาคม ๒๕๖๘ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการให้เว็บไซต์ของตน เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ที่กำหนดท้ายประกาศนี้

ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดำเนินการส่งเสริมและสนับสนุนให้หน่วยงานเอกชนนำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามแนบท้ายประกาศนี้ ไปปรับใช้เป็นแนวทางในสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยเว็บไซต์ของตนด้วย

ข้อ ๔ เพื่อประโยชน์ในการดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามข้อ ๓ วรรคหนึ่ง ให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการ ดังต่อไปนี้

(๑) กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศของเว็บไซต์

(๒) ประเมินและจัดระดับผลกระทบในแต่ละด้าน

(๓) ระบุข้อกำหนดขั้นต่ำที่ต้องดำเนินการ และระบุการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

(๔) ประเมินตนเอง (Self-Assessment) เพื่อตรวจสอบการดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

การดำเนินการตามวรรคหนึ่ง ให้เป็นไปตามแบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ ท้ายประกาศนี้ โดยให้หน่วยงานดำเนินการอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ เมื่อหน่วยงานดำเนินการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์และประเมินและจัดระดับผลกระทบตามข้อ ๔ วรรคหนึ่ง (๑) และ (๒) แล้ว ให้ดำเนินการ ดังนี้

(๑) กรณีผลกระทบระดับต่ำหรือระดับกลาง ให้หน่วยงานรายงานผลการประเมินตนเองตามแบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ท้ายประกาศนี้ พร้อมแนบเอกสารหลักฐานที่เกี่ยวข้อง เสนอต่อผู้บริหารระดับสูงสุดของหน่วยงานและเก็บรักษาไว้ที่หน่วยงานเพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติตรวจสอบ

(๒) กรณีผลกระทบระดับสูง ให้หน่วยงานรายงานผลการประเมินตนเอง ตามแบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ ท้ายประกาศนี้ พร้อมแนบเอกสารหลักฐานที่เกี่ยวข้อง เสนอต่อผู้บริหารสูงสุดของหน่วยงาน และหน่วยงานควบคุมหรือกำกับดูแล พร้อมส่งสำเนาให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ข้อ ๖ กรณีที่หน่วยงานดำเนินการประเมินตนเองตามข้อ ๔ วรรคหนึ่ง (๔) แล้วปรากฏว่า หน่วยงานยังมิได้ดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ของหน่วยงานหรือดำเนินการแล้วแต่ยังไม่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามประกาศนี้ ทั้งหมดหรือบางส่วน หน่วยงานต้องดำเนินการปรับปรุงให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามประกาศนี้กำหนด แล้วแต่กรณี

ก่อนการดำเนินการตามวรรคหนึ่ง ให้หน่วยงานจัดทำแบบฟอร์ม ค๒ แบบรายงานรายการที่ยังต้องปรับปรุง ท้ายประกาศนี้ แล้วแจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหารสั่งการไปยังผู้ที่เกี่ยวข้องเพื่อดำเนินการให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามประกาศนี้กำหนด

ข้อ ๗ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรักษาการตามประกาศนี้ และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีอำนาจตีความและวินิจฉัยชี้ขาดแล้วรายงานให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้ การตีความและคำวินิจฉัยของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้เป็นที่สุด

ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ. ๒๕๖๘
ประเสริฐ จันทรรวงทอง
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

เว็บไซต์เป็นองค์ประกอบที่สำคัญเพราะเป็นช่องทางในการเข้าถึงข้อมูล ผลิตภัณฑ์ หรือบริการของหน่วยงาน ถือเป็นประตูที่ใช้เชื่อมหน่วยงานกับอินเทอร์เน็ต หากเกิดภัยคุกคามทางไซเบอร์เพื่อขโมย แก้ไข หรือลบข้อมูลที่สำคัญของหน่วยงาน เช่น ข้อมูลลูกค้า ข้อมูลทางการเงิน จะส่งผลกระทบต่อการดำเนินการของหน่วยงาน จากสถิติในการรับมือภัยคุกคามทางไซเบอร์ ปี ๒๕๖๖ - ๒๕๖๗ พบว่า ร้อยละ ๔๔ ของภัยคุกคามไซเบอร์ทั้งหมดเกิดขึ้นกับเว็บไซต์ ประกอบด้วย Hacked Website (Defacement และ Gambling) และ Fake Website (๔) อย่างไรก็ตาม นอกจากภัยคุกคามทางไซเบอร์จะส่งผลกระทบต่อข้อมูลหรือระบบสารสนเทศของหน่วยงานแล้ว ยังส่งผลกระทบต่อการดำเนินงาน การให้บริการของหน่วยงาน อาจทำให้หน่วยงานสูญเสียรายได้ เสียชื่อเสียง และขาดความน่าเชื่อถืออีกด้วย ตัวอย่างเช่น การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลหน้าเว็บ (Web Defacement) การโจมตีเว็บไซต์เพื่อใช้เป็นฐานในการเผยแพร่มัลแวร์ (Malware Distribution) หรือการใช้เว็บไซต์เพื่อการหลอกลวง (Phishing Website) ซึ่งอาจทำให้หน่วยงานมีความเสี่ยงทางกฎหมาย และสำคัญที่สุดอาจส่งผลกระทบต่อความมั่นคงปลอดภัยในระดับประเทศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เล็งเห็นถึงความสำคัญในการป้องกัน รับมือ และบรรเทาผลกระทบจากภัยคุกคามที่จะเกิดขึ้นกับเว็บไซต์ จึงอาศัยหน้าที่และอำนาจในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (๕) มาตรา ๙ (๔) ซึ่งกำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจในการกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน และมาตรา ๒๒ (๑๓) ได้กำหนดให้ สกมช. มีหน้าที่และอำนาจในการศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ ดังนั้น สกมช. จึงได้แต่งตั้งคณะทำงานเพื่อจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ โดยมีหน้าที่ในการจัดทำ “มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เวอร์ชัน ๑.๐ หรือ Website Security Standard Version 1.0” เพื่อใช้เป็นข้อกำหนดด้านความมั่นคงปลอดภัยทางเว็บไซต์ขั้นต่ำให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องปฏิบัติตาม รวมถึงส่งเสริมและสนับสนุนให้หน่วยงานเอกชนนำไปปรับใช้เป็นแนวทางการรักษาความมั่นคงปลอดภัยเว็บไซต์ต่อไป

๑. ขอบเขต (Scope)

มาตรฐานฉบับนี้มีวัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยให้กับเว็บไซต์ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานเอกชน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ (๕) ซึ่งใช้เป็นข้อกำหนดขั้นต่ำให้เว็บไซต์ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) เว็บไซต์ที่มีข้อมูลสำคัญ เว็บไซต์ที่ให้บริการข้อมูลประชาชน เว็บไซต์ให้บริการเกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ และเว็บไซต์ของหน่วยงานที่มีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งมาตรฐานฉบับนี้ครอบคลุมถึงเว็บไซต์บนระบบขององค์กร (On-Premises) เว็บไซต์บนระบบคลาวด์ (Cloud Service) และเว็บไซต์ที่ใช้บริการเว็บโฮสติ้ง (Web Hosting) โดยขอบเขตของมาตรฐานฉบับนี้ แบ่งเป็น ๒ องค์ประกอบ ดังนี้

๑.๑ องค์ประกอบตามขอบเขต ประกอบด้วย

๑.๑.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

เป็นการบริหารจัดการและการดูแลด้านอื่น ๆ ที่เกี่ยวข้อง รวมถึงการบริหารจัดการและมาตรการควบคุมเชิงบริหาร เช่น นโยบายการพัฒนาและจัดการเว็บไซต์ และมาตรการควบคุมเชิงเทคนิค เช่น การควบคุมการเข้าถึงเว็บไซต์และข้อมูล เป็นต้น

๑.๑.๒ การรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

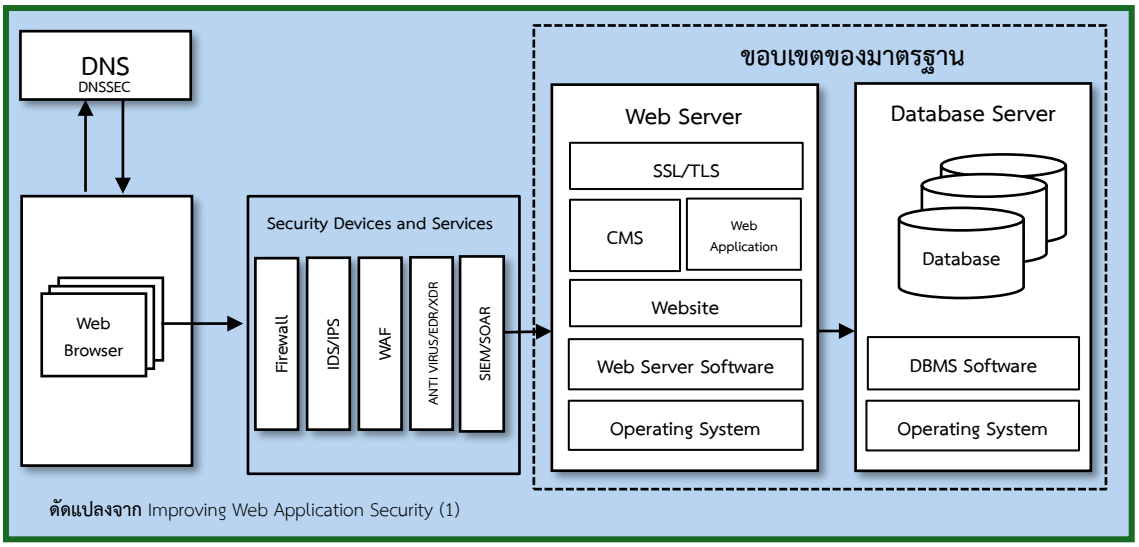
เป็นการดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ใน ๒ ส่วน ดังนี้

๑.๑.๒.๑ เครื่องบริการเว็บ (Web Server) ซึ่งประกอบด้วย เว็บไซต์ (Website) โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โปรแกรมประยุกต์บนเว็บ (Web Application) ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) ระบบปฏิบัติการ (Operating System) และโพรโทคอลสร้างความมั่นคงปลอดภัยในการสื่อสาร SSL/TLS

๑.๑.๒.๒ เครื่องบริการฐานข้อมูล (Database Server) ซึ่งประกอบด้วย ระบบฐานข้อมูล (Database System) ระบบปฏิบัติการ (Operating System) และระบบการจัดการฐานข้อมูล (DBMS Software)

๑.๒ องค์ประกอบอื่น ๆ นอกเหนือขอบเขต เป็นองค์ประกอบที่เกี่ยวข้องกับสภาพแวดล้อมความมั่นคงปลอดภัยของโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศของหน่วยงาน ประกอบด้วย ซอฟต์แวร์ด้านความมั่นคงปลอดภัย Endpoint Detection and Response (EDR) ระบบ Extended Detection and Response (XDR) ไฟร์วอลล์ (Firewall) การให้บริการป้องกัน Web Application (Web Application Firewall: WAF) เครื่องคอมพิวเตอร์แม่ข่าย Domain Name System (DNS Server) และ Domain Name System Security Extensions (DNSSEC) รวมถึงมาตรการควบคุมเชิงกายภาพ เช่น การควบคุมการเข้าถึงเครื่องบริการเว็บ (Web Server) ทางกายภาพ เป็นต้น ซึ่งเป็นองค์ประกอบที่หน่วยงานควรจะพิจารณาดำเนินการเพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์

ซึ่งขอบเขตของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ แสดงได้ดังภาพที่ ๑



ภาพที่ ๑ ขอบเขตของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

มาตรฐานฉบับนี้อ้างอิงข้อกำหนด ข้อเสนอแนะ และแนวปฏิบัติฯ จากมาตรฐานอื่น ๆ ที่เกี่ยวข้อง ตามหัวข้อ ๔ เอกสารอ้างอิง (Normative Reference) โดยมีรูปแบบของคำที่ใช้แสดงในมาตรฐานฉบับนี้ ดังนี้

“จะต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (Requirement) ซึ่งจะต้องปฏิบัติตาม

“ควรจะ” (should) ใช้ระบุสิ่งที่เป็นข้อเสนอแนะ (Recommendation) ซึ่งควรจะปฏิบัติตาม

“อาจจะ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (Permission) ซึ่งอาจจะปฏิบัติตาม

๒. โครงสร้างเอกสาร (Documents Structure)

มาตรฐานฉบับนี้มีโครงสร้างเอกสารดังแสดงในภาพที่ ๒ ประกอบด้วย

๒.๑. ข้อกำหนดในการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Governance) โดยอ้างอิงจากกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework: CSF 2.0) (๒) (หัวข้อที่ ๕)

๒.๒. ข้อกำหนดในการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Operation) โดยอ้างอิงจากประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) (หัวข้อที่ ๖) ประกอบด้วย

๒.๒.๑ การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification)

๒.๒.๒ การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection)

๒.๒.๓ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Website Security Detection)

๒.๒.๔ การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Website Incident Response)

๒.๒.๕ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Website Recovery)

๒.๓. การดำเนินการตามข้อกำหนดขั้นต่ำและแนวทางในการตรวจสอบให้เป็นไปตามมาตรฐานฉบับนี้ (หัวข้อที่ ๗) ประกอบด้วย

๒.๓.๑ การดำเนินการตามข้อกำหนดขั้นต่ำ

๒.๓.๒ แนวทางในการตรวจสอบและปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้

๒.๔. ข้อเสนอแนะนำและคำอธิบายเพิ่มเติม (ภาคผนวก ก และ ข) ซึ่งเป็นข้อเสนอแนะและเป็นการให้ข้อมูลเพิ่มเติมเพื่อการดำเนินการตามหัวข้อที่ ๕ และหัวข้อที่ ๖ ประกอบด้วย

๒.๔.๑ ข้อเสนอแนะนำและคำอธิบายเพิ่มเติมตามข้อกำหนด (หัวข้อ ๕) ในการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (ภาคผนวก ก)

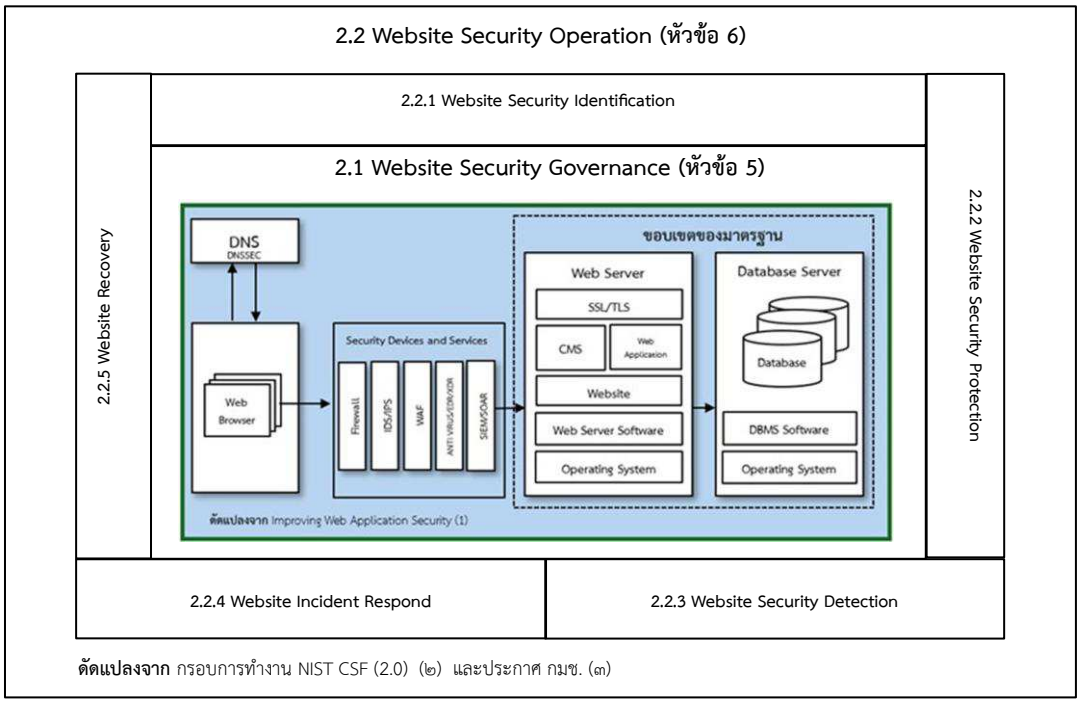
๒.๔.๒ ข้อเสนอแนะนำและคำอธิบายเพิ่มเติมตามข้อกำหนด (หัวข้อ ๖) ในการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (ภาคผนวก ข)

๒.๕. แบบฟอร์มเพื่อใช้ในการตรวจสอบให้เป็นไปตามมาตรฐานฉบับนี้ (ภาคผนวก ค)

๒.๕.๑ แบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะการรักษาความมั่นคงปลอดภัยของเว็บไซต์

๒.๕.๒ แบบฟอร์ม ค๒ แบบรายงานการแก้ไขรายการที่ยังต้องปรับปรุง

ซึ่งโครงสร้างของเอกสารมาตรฐานฉบับนี้ แสดงได้ดังภาพที่ ๒



ภาพที่ ๒ โครงสร้างของเอกสารมาตรฐานฉบับนี้

๓. นิยาม (Definitions)

ความหมายของศัพท์และศัพท์ทางเทคนิคที่ใช้กับมาตรฐานฉบับนี้ ฉบับนี้

๓.๑ การรักษาความมั่นคงปลอดภัย (Security) (๖) หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์ และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้น ๆ ประกอบด้วย ความมั่นคงปลอดภัยเชิงกายภาพ การดำเนินงาน การสื่อสาร เครือข่าย ข้อมูลข่าวสาร และส่วนบุคคล

๓.๒ เว็บไซต์ (Website) (๗, ๘) หมายถึง การรวบรวมหน้าเว็บเพจหลายหน้าที่แสดงข้อมูลบนอินเทอร์เน็ตเกี่ยวกับเรื่องใดเรื่องหนึ่ง เผยแพร่โดยบุคคลหรือองค์กรเดียว โดยมีการเชื่อมโยงกันผ่านทางไฮเปอร์ลิงก์ (Hyperlink) และเปิดด้วยโปรแกรมที่เรียกว่า เว็บเบราว์เซอร์ (Web Browser) โดยจัดเก็บไว้ในเวิลด์ไวด์เว็บ (WWW) เว็บเพจแรกที่พบ เรียกว่า โฮมเพจ (Homepage) ที่มีหัวข้อของข้อมูลในเว็บไซต์ จึงเปรียบเหมือนสารบัญที่ใช้ค้นหาข้อมูลต่อไป

๓.๓ เว็บเพจ (Webpage) (๘) หมายถึง เอกสารเว็บที่สร้างด้วยภาษา HTML หรือ Hypertext Markup Language ซึ่งเป็นภาษามาตรฐานที่ใช้ในการสร้างเว็บเพจ เพื่อแสดงข้อมูลบนอินเทอร์เน็ตเกี่ยวกับหัวข้อใดหัวข้อหนึ่ง ซึ่งประกอบเป็นส่วนหนึ่งของเว็บไซต์

๓.๔ เว็บเบราว์เซอร์ (Web Browser) (๘) หมายถึง โปรแกรมคอมพิวเตอร์ที่ใช้เรียกข้อมูลเว็บจากเครื่องบริการเว็บผ่านระบบเครือข่าย ทำให้สามารถแสดงข้อมูลบนอินเทอร์เน็ตได้

๓.๕ เว็บไซต์ที่ใช้ระบบขององค์กร (On-Premises) (๙, ๑๐) หมายถึง เว็บไซต์ที่เนื้อหาโปรแกรมสำหรับให้บริการเว็บ และโปรแกรมที่เกี่ยวข้องกับการให้บริการเว็บของเว็บไซต์ถูกเก็บอยู่ในเครือข่ายของผู้ให้บริการเว็บไซต์

๓.๖ เว็บไซต์ที่ใช้บริการกับเว็บโฮสติ้ง (Web Hosting) (๙) หมายถึง เว็บไซต์ที่เนื้อหาโปรแกรมสำหรับให้บริการเว็บ และโปรแกรมที่เกี่ยวข้องกับการให้บริการเว็บของเว็บไซต์ถูกเก็บอยู่ในเครือข่ายของผู้ให้บริการเครื่องบริการเว็บ

๓.๗ เว็บไซต์ที่ใช้ระบบคลาวด์ (Cloud Service) (๙, ๑๐) หมายถึง เว็บไซต์ที่มีเนื้อหาโปรแกรมสำหรับให้บริการเว็บ และโปรแกรมที่เกี่ยวข้องกับการให้บริการเว็บของเว็บไซต์ถูกเก็บอยู่ในเครื่องบริการเสมือนบนคลาวด์

๓.๘ เครื่องบริการเว็บ (Web Server) (๘, ๑๑) หมายถึง ระบบคอมพิวเตอร์ที่ให้บริการเวิลด์ไวด์เว็บ บนอินเทอร์เน็ต ซึ่งประกอบด้วย ฮาร์ดแวร์ ระบบปฏิบัติการ โปรแกรมคอมพิวเตอร์สำหรับให้บริการเว็บ และเนื้อหาเว็บไซต์ (เว็บเพจ) ที่ให้บริการเว็บไซต์และข้อมูลไปยังผู้ใช้อินเทอร์เน็ตผ่านระบบเครือข่าย

๓.๙ โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) (๑๒) หมายถึง โปรแกรมคอมพิวเตอร์ที่ติดตั้งบนเครื่องบริการเว็บเพื่อจัดการคำร้องขอข้อมูลเว็บจากผู้ใช้งาน เช่น โปรแกรม Apache โปรแกรม nginx และโปรแกรม Internet Information Service (IIS) เป็นต้น

๓.๑๐ โปรแกรมประยุกต์บนเว็บ (Web Application) หมายถึง โปรแกรมประยุกต์ที่มีความสามารถในการประมวลผลข้อมูลและการทำงานต่าง ๆ โดยเข้าถึงได้ผ่านเว็บเบราว์เซอร์

บนอินเทอร์เน็ต หรืออินทราเน็ต ซึ่งเขียนด้วยภาษาต่าง ๆ เช่น ภาษา HTML ภาษา JavaScript หรือภาษา Java และต้องอาศัยเว็บเบราว์เซอร์ในการเข้าถึง และเรียกใช้งานผ่านระบบเครือข่าย

๓.๑๑ ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) หมายถึง โปรแกรมที่ใช้ในการดูแลบริหารจัดการเว็บไซต์ผ่านส่วนต่อประสานแบบเว็บ ซึ่งง่ายต่อการบริหารจัดการเว็บเพจและการปรับปรุงค่าติดตั้งต่าง ๆ ที่เกี่ยวข้อง

๓.๑๒ ระบบปฏิบัติการ (Operating System) (๑๓) หมายถึง ชุดของซอฟต์แวร์ที่บริหารจัดการทรัพยากรฮาร์ดแวร์ของคอมพิวเตอร์ และให้บริการทั่วไปกับโปรแกรมคอมพิวเตอร์

๓.๑๓ โพรโทคอลสร้างความมั่นคงปลอดภัยในการสื่อสาร Secure Sockets Layer (SSL) และ Transport Layer Security (TLS) (๑๔) หมายถึง โพรโทคอลปกป้องความมั่นคงปลอดภัยการสื่อสารผ่านระบบเครือข่าย ในการตรวจสอบสิทธิ์และความมั่นคงปลอดภัยที่ใช้กันอย่างแพร่หลายในเบราว์เซอร์และเว็บเซิร์ฟเวอร์ โดยมีแนวทางการเลือกและใช้งานการใช้งาน Transport Layer Security (TLS) ตาม NIST SP 800-52 ซึ่งระบุถึงวิธีการใช้ TLS ในโปรแกรมประยุกต์ของหน่วยงานภาครัฐ ในปัจจุบันควรใช้โพรโทคอล TLS เวอร์ชันที่มีความมั่นคงปลอดภัยและไม่พบช่องโหว่หรือการโจมตี

๓.๑๔ เครื่องบริการฐานข้อมูล (Database Server) (๑๕) หมายถึง คอมพิวเตอร์หรืออุปกรณ์บนเครือข่ายที่ประมวลผลการร้องขอข้อมูลในฐานข้อมูล

๓.๑๕ ระบบฐานข้อมูล (Database System) หมายถึง โครงสร้างหรือชุดของข้อมูลที่ถูกจัดเก็บและจัดการเพื่อการเข้าถึง แก้ไข และประมวลผลข้อมูลอย่างมีประสิทธิภาพ ระบบนี้มักใช้เพื่อจัดเก็บข้อมูลที่ใช้ในการดำเนินธุรกรรมหรือการจัดการข้อมูลต่าง ๆ ในรูปแบบที่สามารถเข้าถึงได้อย่างรวดเร็วและปลอดภัย สามารถแบ่งได้เป็น ๒ ประเภท ได้แก่ ระบบฐานข้อมูลเชิงสัมพันธ์ (Relational Database) และระบบฐานข้อมูลแบบไม่มีโครงสร้าง (NoSQL Database)

๓.๑๖ ระบบการจัดการฐานข้อมูล (DBMS Software) (๑๖) หมายถึง ซอฟต์แวร์ที่ถูกออกแบบมาเพื่อช่วยในการบำรุงรักษาและใช้ประโยชน์ชุดข้อมูลที่มีขนาดใหญ่

๓.๑๗ เครื่องคอมพิวเตอร์แม่ข่าย Domain Name System (DNS Server) (๑๕, ๑๗) หมายถึง คอมพิวเตอร์หรืออุปกรณ์บนเครือข่ายที่เก็บรักษารายชื่อโดเมนเนม และให้บริการแปลงชื่อโดเมนเป็นเลขที่อยู่ไอพี

๓.๑๘ ส่วนขยายโพรโทคอล DNS (Domain Name System Security Extensions :DNSSEC (๑๘) หมายถึง ส่วนขยายที่ช่วยในการยืนยันความถูกต้องของที่มาและความสมบูรณ์ (Integrity) ของข้อมูลที่ส่งผ่านโพรโทคอล DNS

๓.๑๙ ไฟร์วอลล์ (Firewall) (๑๙) หมายถึง ฮาร์ดแวร์หรือซอฟต์แวร์ที่ป้องกันการเข้าถึงข้อมูลภายในเครือข่ายขององค์กรจากอินเทอร์เน็ตโดยไม่ได้รับอนุญาตเครื่องบริการเว็บ (Web Server)

๓.๒๐ การให้บริการป้องกัน Web Application (Web Application Firewall: WAF) (๒๐) หมายถึง ไฟร์วอลล์สำหรับโปรแกรมประยุกต์ที่ใช้โพรโทคอล HTTP โดยจะใช้กฎการกรองกับการติดต่อสื่อสารผ่านโพรโทคอล HTTP

๓.๒๑ ซอฟต์แวร์ด้านความมั่นคงปลอดภัย Endpoint Detection and Response (EDR) (๒๑) หมายถึง เครื่องมือบันทึกและจัดเก็บพฤติกรรมในระดับของระบบของอุปกรณ์ปลายทางและวิเคราะห์ข้อมูลเหล่านั้น เพื่อตรวจจับพฤติกรรมต้องสงสัย ให้ข้อมูลเกี่ยวกับบริบทของอุปกรณ์ปลายทาง ยับยั้งกิจกรรมที่มุ่งร้ายต่อระบบและให้คำแนะนำในการแก้ปัญหาระบบที่โดนโจมตี

๓.๒๒ ระบบ Extended Detection and Response (XDR) (๒๒) หมายถึง แพลตฟอร์มผสานการตรวจจับและตอบสนองเหตุการณ์ทางด้านความมั่นคงปลอดภัย โดยจะรวบรวมและหาความสัมพันธ์ของข้อมูลจากอุปกรณ์รักษาความมั่นคงปลอดภัยแต่ละประเภทโดยอัตโนมัติ

๔. เอกสารอ้างอิง (Normative References)

เอกสารที่ระบุต่อไปนี้ ให้ถือเป็นส่วนหนึ่งของมาตรฐานฉบับนี้ด้วย เอกสารที่มีการอ้างอิงโดยระบุปีให้ใช้เอกสารฉบับตามปีที่ระบุไว้ สำหรับเอกสารที่มีการอ้างอิงโดยไม่ระบุปี ให้ใช้เอกสารล่าสุด (รวมถึงการเพิ่มเติมต่าง ๆ)

๔.๑ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (๒๓)

๔.๒ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ.๒๕๖๖ (๒๔)

๔.๓ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓)

๔.๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ (๒๕)

๔.๕ คำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๒๖)

๔.๖ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (๒๗)

๔.๗ มาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน ๓.๐ (Government Website Standard Version 3.0) สำนักงานพัฒนารัฐบาลดิจิทัล (๒๘)

๔.๘ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ (๒๙)

๔.๙ คำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓๐)

๔.๑๐ กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST Cybersecurity Framework (CSF) 2.0 (๒)

๔.๑๑ ข้อเสนอแนะของ NIST Special Publication 800-88 Guidelines for Media Sanitization (๓๑)

๔.๑๒ ปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อยที่ ของมูลนิธิ Open Worldwide Application Security Project (OWASP) (๓๒)

๕. ข้อกำหนดการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Governance Requirement)

หน่วยงานจะต้องดำเนินการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ โดยดำเนินการในส่วนที่เกี่ยวข้อง[๑] [๒] อ้างอิงกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework: CSF 2.0) (๒) และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓) ดังนี้

๕.๑. การสำรวจบริบทของหน่วยงาน (Organization Context)

๕.๑.๑. หน่วยงานจะต้องมีการทำความเข้าใจสถานการณ์ต่าง ๆ ประกอบด้วย ภารกิจ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย การขึ้นต่อกัน และกฎหมาย กฎระเบียบ และข้อกำหนดของสัญญาที่เกี่ยวข้องกับการตัดสินใจในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ของหน่วยงาน ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๒. นโยบายด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Policies)

๕.๒.๑. หน่วยงานจะต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามบริบทขององค์กรและกลยุทธ์ด้านความมั่นคงปลอดภัยเว็บไซต์ โดยมีการจัดลำดับความสำคัญ มีการสื่อสาร รวมถึงมีการบังคับใช้ ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๕.๒.๒. หน่วยงานจะต้องมีการทบทวน ปรับปรุง สื่อสาร และบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อสะท้อนการเปลี่ยนแปลงความต้องการ ภัยคุกคาม เทคโนโลยี รวมถึงภารกิจของหน่วยงาน

---

[๑] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0

[๒] คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๕.๓. กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy)

๕.๓.๑. หน่วยงานจะต้องกำหนดวัตถุประสงค์การบริหารความเสี่ยงโดยได้รับความเห็นชอบจากผู้มีส่วนได้ส่วนเสียของหน่วยงาน และจะต้องมีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์เป็นลายลักษณ์อักษร โดยกรอบรวมถึงเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) วิธีการประเมินความเสี่ยง การเฝ้าระวังและติดตามความเสี่ยง ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๓.๒. หน่วยงานจะต้องพิจารณาดำเนินการตามคำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ในกรณีที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๓๐)

๕.๓.๓. หน่วยงานจะต้องมีการจัดทำ สื่อสาร และมีการเก็บรักษารายการความเสี่ยงที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ให้เป็นปัจจุบัน และติดตามระดับความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้

๕.๔. บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

๕.๔.๑. หน่วยงานจะต้องมีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนในการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๕.๔.๒. หน่วยงานจะต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำ และบริการจัดการเว็บไซต์ของหน่วยงาน รวมถึงการดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งต้องเป็นนิติบุคคลหรือเป็นส่วนหนึ่งของนิติบุคคลที่สามารถรับผิดตามกฎหมายได้ และมีการมอบหมายหน้าที่จะต้องทำโดยไม่ขาดช่วง

๕.๔.๓. หน่วยงานจะต้องมีการกำหนด สื่อสาร ทำความเข้าใจ และบังคับใช้บทบาท ความรับผิดชอบ และอำนาจที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ รวมถึงจัดสรรทรัพยากรให้เพียงพอตามกลยุทธ์ บทบาท ความรับผิดชอบ และนโยบายความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

๕.๕. การวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์

๕.๕.๑. หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์และความต้องการในการจัดทำเว็บไซต์ด้านฟังก์ชัน ด้านประสิทธิภาพ และที่สำคัญความต้องการด้านความมั่นคงปลอดภัย ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๕.๖. การกำหนดแนวทางด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

๕.๖.๑. หน่วยงานจะต้องมีแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐานตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการเตรียมความพร้อมใช้งาน (Availability) ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๖.๒. หน่วยงานจะต้องกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ ให้ประเมินและจัดระดับผลกระทบที่อาจจะเกิดขึ้น ๓ ระดับ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (๒๓) เพื่อระบุข้อกำหนดขั้นต่ำในการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

๕.๖.๓. หน่วยงานจะต้องดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ (๒๗) รวมถึงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ (๒๙) ในกรณีที่เว็บไซต์หน่วยงานมีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์

๕.๖.๔. หน่วยงานจะต้องดำเนินการตามมาตรฐานเว็บไซต์ภาครัฐ เวอร์ชัน ๓.๐ (Government Website Standard Version 3.0) หัวข้อที่ ๗ ความมั่นคงปลอดภัยสำหรับเว็บไซต์ในกรณีที่เป็นเว็บไซต์หน่วยงานภาครัฐ (๒๘)

๕.๖.๕. หน่วยงานจะต้องดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ที่ใช้บริการคลาวด์ (Cloud Service) ให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ (๒๕)

๕.๖.๖. หน่วยงานจะต้องพิจารณาเลือกผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ เช่น การดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) ของเว็บไซต์ ที่ได้รับการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม

๕.๖.๗. หน่วยงานจะต้องปฏิบัติตามคำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) ในกรณีที่เป็นเว็บไซต์หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (๒๖)

๕.๖.๘. หน่วยงานจะต้องมีการกำหนดแนวทางในการสำรองข้อมูลเพื่อลดผลกระทบที่เกิดขึ้น หากเว็บไซต์ของหน่วยงานโดนโจมตีจากภัยคุกคามทางไซเบอร์ รวมถึงความเสียหายจากภัยธรรมชาติหรือข้อผิดพลาดจากมนุษย์ ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ก

๕.๖.๙. หน่วยงานจะต้องมีการจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log Management) ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และที่แก้ไขเพิ่มเติม ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๕.๖.๑๐. หน่วยงานจะต้องกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ เพื่อป้องกันภัยคุกคามไซเบอร์ที่อาจจะเกิดกับผู้ใช้บริการเว็บไซต์ ผู้ใช้งานอินเทอร์เน็ตทั่วไป ผู้ให้บริการ โดยหน่วยงานอาจจะพิจารณาปฏิบัติตามข้อเสนอแนะของ NIST Special Publication 800-88 Guidelines for Media Sanitization (๓๑) ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ก

๖. ข้อกำหนดการดำเนินการและการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Security and Operation Requirements)

หน่วยงานจะต้องดำเนินการและรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security and Operation Requirements) โดยดำเนินการในส่วนที่เกี่ยวข้อง[๓] อ้างอิงประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ดังนี้

๖.๑. การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification)

๖.๑.๑. หน่วยงานจะต้องมีการจัดการทรัพย์สิน (Asset Management) การประเมินความเสี่ยง (Risk Assessment) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) และการจัดการผู้ให้บริการภายนอก (Third Party Management) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ข

๖.๒. การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection)

๖.๒.๑. หน่วยงานจะต้องกำหนดแนวทางในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) อย่างมั่นคงปลอดภัย เช่น พิจารณาใช้หลักการ DevSecOps ตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งานจริงโดยมีการคำนึงถึงสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยในการพัฒนาโปรแกรมประยุกต์บนเว็บ และอาจจะพิจารณาตัวอย่างการออกแบบเว็บไซต์ที่มีความมั่นคงปลอดภัย ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ข

๖.๒.๒. หน่วยงานจะต้องพิจารณาถึงปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อย ของมูลนิธิ OWASP (๓๒) ในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติมตามภาคผนวก ข

๖.๒.๓. หน่วยงานจะต้องพิจารณาการออกแบบสถาปัตยกรรมเว็บไซต์อย่างมั่นคงปลอดภัย ในส่วนของโครงสร้างของเว็บไซต์หรือโปรแกรมประยุกต์บนเว็บ โดยอาจจะมีส่วนประกอบ

---

[๓] คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ของการออกแบบที่คำนึงถึงการแบ่งส่วนเครือข่าย (Network segmentation) มีการจัดวางเครื่องบริการเว็บ (Web Server) และเครื่องบริการฐานข้อมูล (Database Server) ร่วมกับอุปกรณ์รักษาความมั่นคงปลอดภัย เช่น

(๑) ไฟร์วอลล์ (Firewall)

(๒) ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก (Intrusion Detection Systems: IDS/Intrusion Prevention Systems: IPS)

(๓) ซอฟต์แวร์ตรวจจับและตอบสนองภัยคุกคาม เช่น ซอฟต์แวร์ป้องกันไวรัส (Antivirus) ซอฟต์แวร์ EDR

(๔) การให้บริการป้องกัน Web Application (WAF)

หากหน่วยงานที่มีทรัพยากรเพียงพออาจจะพิจารณาผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยเพิ่มเติม ดังนี้

(๕) ระบบการจัดการเหตุการณ์และตอบสนองด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM)

(๖) ระบบ XDR

(๗) ระบบ SOAR (Security Orchestration, Automation, and Response)

ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๔. หน่วยงานจะต้องมีการควบคุมการเข้าถึง (Access Control) การทำให้ระบบมีความแข็งแกร่ง (System Hardening) มีการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) การบริหารจัดการสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) และมีบริหารจัดการแบ่งปันข้อมูล (Information Sharing) และมีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Awareness) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๕. หน่วยงานจะต้องพิจารณาการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือพิจารณาการพิสูจน์ตัวตนจากระบบเชื่อมโยงข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ตามข้อเสนอแนะของ สพร. นอกเหนือจากการควบคุมการเข้าถึง (Access Control) ข้อ ๖.๒.๔ เพื่อเพิ่มความมั่นคงปลอดภัยให้กับเว็บไซต์ โดยอาจจะพิจารณาเลือกจากสิ่งที่ผู้ใช้รู้ (Something they know) เช่น รหัสผ่าน สิ่งที่ผู้ใช้มี (Something they have) เช่น โทเค็นการตรวจสอบ หรือสิ่งที่ผู้ใช้เป็น (Something they are) เช่น ลายนิ้วมือ ลายฝ่ามือ หรือข้อมูลชีวมิติอื่น ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๖. หน่วยงานจะต้องตั้งค่าความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โปรแกรมประยุกต์บนเว็บ (Web Application) ระบบบริหารจัดการเว็บไซต์ (CMS) ระบบปฏิบัติการ (Operating System) และการตั้งค่าฐานข้อมูล ซึ่งมาตรฐานฉบับนี้มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๗. หน่วยงานจะต้องกำหนดแนวทางและการเลือกบริการที่เกี่ยวข้องกับเว็บไซต์ ประกอบด้วย เครื่องบริการเว็บ (Web Server) ระบบบริหารจัดการเว็บไซต์ (CMS) เลือกบริการโดเมนและชื่อโดเมน และขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๒.๘. หน่วยงานจะต้องตั้งค่าไฟร์วอลล์เพื่อควบคุมและป้องกันการบุกรุกต่าง ๆ ที่เกิดขึ้นกับเว็บไซต์ โดยควรจะพิจารณาหลักการตั้งค่าอย่างน้อย ดังนี้ การกำหนดนโยบายความมั่นคงปลอดภัย (Define Security Policies) การตั้งค่ากฎการกรอง (Configure Filtering Rules) การจำกัด การเข้าถึงโดยภูมิศาสตร์ (Geographic Restrictions) การป้องกันการโจมตี (Protect Against Attacks) การตรวจสอบและบันทึก (Monitoring and Logging) และการปรับปรุงและอัปเดตเป็นประจำ (Regular Updates) ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Detection)

๖.๓.๑. หน่วยงานจะต้องมีการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ซึ่งมาตรฐานฉบับนี้ มีข้อเสนอแนะและรายละเอียดเพิ่มเติม ตามภาคผนวก ข

๖.๔. การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Incident Response)

๖.๔.๑. หน่วยงานจะต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website security Incident Response Plan) และมีการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ของเว็บไซต์ รวมถึงแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) และการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Exercise) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓) ซึ่งมาตรฐานฉบับนี้ มีคำอธิบายเพิ่มเติม ตามภาคผนวก ข

๖.๕. การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Recovery)

๖.๕.๑. หน่วยงานจะต้องมีการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Resilience and Recovery) โดยจะต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) โดยอาจจะพิจารณารายละเอียดของแผนให้เป็นไปตามการบริหารความพร้อมต่อสภาวะวิกฤติ (การทำแผน BCP) ของสำนักงานคณะกรรมการพัฒนาระบบราชการ (๓๓) และจะต้องจัดให้มีการฝึกซ้อมให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓)

๗. แนวทางในการดำเนินการตามข้อกำหนดขั้นต่ำ และแนวทางในตรวจสอบและปฏิบัติให้เป็นไปตามมาตรฐานฉบับนี้

๗.๑ แนวทางในการดำเนินการตามข้อกำหนดขั้นต่ำ

๗.๑.๑ ให้หน่วยงานกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ของหน่วยงานครบทั้ง ๓ ด้าน ซึ่งประกอบด้วย ด้านการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้ (Availability) ตามส่วนที่ ๒ (ตาราง ค๑-ตาราง ค๕) ของแบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ (แบบฟอร์ม ค๑) ในภาคผนวก ค

๗.๑.๒ ให้หน่วยงานนำผลที่ได้ (ตาราง ค๑-ตาราง ค๕) มาระบุเกณฑ์การดำเนินการตามข้อกำหนดขั้นต่ำในการปฏิบัติตามมาตรฐานฉบับนี้ ในตาราง ค๖

๗.๑.๓ ให้หน่วยงานตรวจสอบหน่วยงานตนเพื่อ “ต้องปฏิบัติตาม” หรือ “ส่งเสริมให้ปฏิบัติตาม” ข้อกำหนดขั้นต่ำ ตามตาราง ค๗ จากนั้นดำเนินการตามแนวทางในการตรวจสอบและปฏิบัติให้เป็นไปตามมาตรฐาน ข้อ ๗.๒

๗.๒ แนวทางในการตรวจสอบและปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้

๗.๒.๑ กรณีที่หน่วยงานยังไม่ได้รับรอง ISO/IEC 27001 หรือที่ได้รับการรับรองแต่ขอบเขตของการรับรองไม่ครอบคลุมถึงเว็บไซต์ของหน่วยงาน จะต้องดำเนินการ ดังนี้

๗.๒.๑.๑ หน่วยงานกลุ่มที่ ๑ (หน่วยงานที่ต้องปฏิบัติตาม) หน่วยงานจะต้องประเมินตนเอง (Self-Assessment) ตามแบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ (แบบฟอร์ม ค๑) ในภาคผนวก ค อย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบการดำเนินการให้เป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐานฉบับนี้ ดังนี้

๑) เว็บไซต์ของหน่วยงานที่มีผลกระทบระดับต่ำ หรือระดับกลาง ให้หน่วยงานจัดทำรายงานผลการประเมินตนเอง (Self-Assessment) (แบบฟอร์ม ค๑) ในภาคผนวก ค และรายงานผลการแก้ไขรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค พร้อมแนบหลักฐาน เสนอต่อผู้บริหารสูงสุดของหน่วยงาน และเก็บรักษาไว้ที่หน่วยงาน

๒) หากเว็บไซต์ของหน่วยงานมีผลกระทบระดับสูง ให้หน่วยงานจัดทำรายงานผลการประเมินตนเอง (Self-Assessment) (แบบฟอร์ม ค๑) ในภาคผนวก ค และรายงานผลการแก้ไขรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค พร้อมแนบหลักฐาน เสนอต่อผู้บริหารสูงสุดของหน่วยงาน หน่วยงานควบคุมหรือกำกับดูแล และส่งสำเนาให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

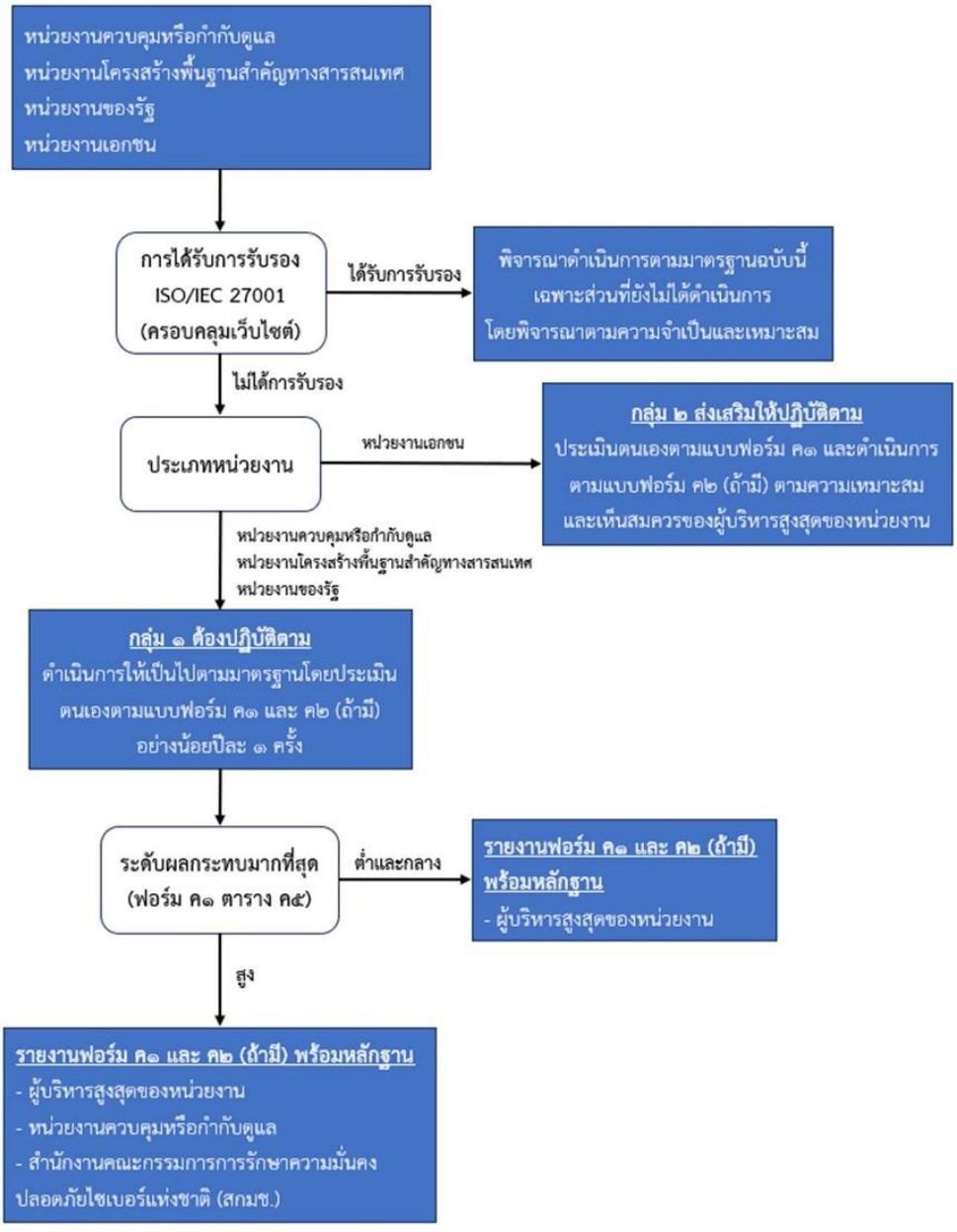
๓) หากหน่วยงานประเมินตนเองแล้ว พบว่า เว็บไซต์ของหน่วยงานมีข้อกำหนดที่มีผลการประเมิน “ยังต้องปรับปรุง” ให้หน่วยงานดำเนินการปรับปรุงตามแบบรายงานรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค

๗.๒.๑.๒ หน่วยงานกลุ่มที่ ๒ (หน่วยงานที่ส่งเสริมให้ปฏิบัติตาม) หน่วยงานจะต้องประเมินตนเอง (Self-Assessment) ตามแบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคง

ปลอดภัยสำหรับเว็บไซต์ (แบบฟอร์ม ค๑) ในภาคผนวก ค ซึ่งหากมีข้อกำหนดที่มีผลการประเมิน “ยังต้องปรับปรุง” หน่วยงานอาจจะพิจารณาดำเนินการปรับปรุงตามรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) ในภาคผนวก ค ตามความเหมาะสมและเห็นสมควรของผู้บริหารสูงสุดของหน่วยงาน

๗.๒.๒ กรณีหน่วยงานได้รับการรับรอง ISO/IEC 27001 ที่มีขอบเขตในการรับรองที่ครอบคลุมถึงเว็บไซต์ของหน่วยงานแล้ว หน่วยงานอาจจะพิจารณาดำเนินการตามมาตรฐานฉบับนี้เฉพาะส่วนที่ยังไม่ได้ดำเนินการตามมาตรฐาน ISO/IEC 27001 ตามที่หน่วยงานได้รับการรับรองนั้น โดยพิจารณาตามความจำเป็นและเหมาะสม

หน่วยงานสามารถศึกษาแนวทางในการปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้ ได้จากแผนผังในภาพที่ ๓



ภาพที่ ๓ แนวทางในการปฏิบัติเพื่อให้เป็นไปตามมาตรฐานฉบับนี้

ภาคผนวก ก

รายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติม
(ข้อ ๕)
(เป็นข้อมูลเพิ่มเติม)

ข้อ ๕.๑ ตัวอย่างในการดำเนินการในส่วนบริบทขององค์กร

การดำเนินการในส่วนบริบทองค์กรในหัวข้อการสำรวจบริบทของหน่วยงาน (Organization Context) ตามข้อกำหนดในการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Governance Requirement) หน่วยงานอาจจะพิจารณาดำเนินการ โดยมีรายละเอียดตามตารางที่ ก๑

ตาราง ก๑ ตัวอย่างในการดำเนินการในส่วนบริบทองค์กร

หัวข้อ	ตัวอย่างการดำเนินการ
ภารกิจของหน่วยงาน หน่วยงานจะต้องทำความเข้าใจภารกิจและรายงานการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์	ตัวอย่างที่ ๑ หน่วยงานมีการเผยแพร่พันธกิจของหน่วยงาน ตัวอย่างเช่น เผยแพร่ผ่านวิสัยทัศน์ พันธกิจ กลยุทธ์ทางการตลาดและบริการเพื่อใช้เป็นพื้นฐานในการระบุความเสี่ยงที่จะส่งผลกระทบต่อภารกิจของหน่วยงาน
ผู้มีส่วนได้ส่วนเสียภายในและภายนอก หน่วยงานมีความเข้าใจในความต้องการและความคาดหวังเกี่ยวกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้มีส่วนได้ส่วนเสียภายในและภายนอก	ตัวอย่างที่ ๑ หน่วยงานระบุผู้มีส่วนได้ส่วนเสียภายในที่มีส่วนเกี่ยวข้องและมีความคาดหวังทางด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น ความคาดหวังด้านประสิทธิภาพและด้านเสี่ยงของเจ้าหน้าที่ ผู้อำนวยการและที่ปรึกษา ความคาดหวังด้านวัฒนธรรมของพนักงาน ตัวอย่างที่ ๒ หน่วยงานระบุผู้มีส่วนได้ส่วนเสียภายนอกที่เกี่ยวข้องและความคาดหวังทางด้านความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างเช่น ความคาดหวังด้านความเป็นส่วนตัว ความคาดหวังทางธุรกิจของหุ้นส่วน ความคาดหวังในการปฏิบัติตามกฎระเบียบของหน่วยงานกำกับดูแล ความคาดหวังด้านจริยธรรมของสังคม
ข้อกำหนดทางกฎหมาย ข้อบังคับและสัญญา หน่วยงานมีความเข้าใจและมีการจัดการด้านข้อกำหนดทางกฎหมาย ข้อบังคับและข้อกำหนดของสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ รวมถึง ข้อผูกพันด้านความเป็นส่วนตัวและเสรีภาพของประชาชน	ตัวอย่างที่ ๑ หน่วยงานกำหนดกระบวนการเพื่อติดตามและจัดการข้อกำหนดทางกฎหมาย และข้อบังคับเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล ตัวอย่างที่ ๒ หน่วยงานกำหนดกระบวนการในการติดตามและจัดการข้อกำหนดตามสัญญาของการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของข้อมูลซัพพลายเออร์ ลูกค้า และคู่ค้า ตัวอย่างที่ ๓ หน่วยงานจัดกลยุทธ์ความมั่นคงปลอดภัยทางไซเบอร์สำหรับเว็บไซต์ของหน่วยงานให้สอดคล้องกับข้อกำหนดทางกฎหมาย ข้อบังคับ และข้อกำหนดตามสัญญา

หัวข้อ	ตัวอย่างการดำเนินการ
หน่วยงานได้ทำความเข้าใจและสื่อสารวัตถุประสงค์ ความสามารถและบริการที่สำคัญที่ขึ้นอยู่กับความคาดหวังของผู้มีส่วนได้ส่วนเสียของหน่วยงาน	ตัวอย่างที่ ๑ หน่วยงานกำหนดเกณฑ์ในการพิจารณาความสำคัญของสมรรถนะและบริการตามมุมมองของผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ตัวอย่างที่ ๒ หน่วยงานกำหนดการดำเนินงานของหน่วยงาน (จากการวิเคราะห์ผลกระทบทางธุรกิจ) สินทรัพย์และการดำเนินงานที่เป็นส่วนสำคัญต่อการบรรลุวัตถุประสงค์ของภารกิจ และมีผลกระทบของการสูญเสียทั้งหมด (หรือบางส่วน) ตัวอย่างที่ ๓ หน่วยงานจัดตั้งและสื่อสารวัตถุประสงค์ในการฟื้นตัวของการดำเนินการ เช่น ระยะเวลาสูงสุดที่จะกู้ข้อมูลได้ (RTO) เพื่อส่งมอบประสิทธิภาพและบริการที่สำคัญหลายสถานการณ์ เช่น หลังการโจมตี ระหว่างการกู้คืน และสภาวะปกติ
ผลลัพธ์ ความสามารถ และบริการหน่วยงานควรทำความเข้าใจและสื่อสาร วัตถุประสงค์ความสามารถ และบริการที่สำคัญของหน่วยงาน	ตัวอย่างที่ ๑ หน่วยงานสร้างรายการทรัพย์สินของที่เป็นทรัพยากรภายนอก (เช่น สิ่งอำนวยความสะดวก ผู้ให้บริการโฮสติ้งบนคลาวด์) และความสัมพันธ์กับสินทรัพย์ขององค์กรและฟังก์ชันทางธุรกิจ) ตัวอย่างที่ ๒ หน่วยงานระบุและจัดทำเอกสารการขึ้นต่อภายนอกซึ่งเป็นส่วนสำคัญที่จะกระทบต่อความสามารถหน่วยงาน รวมถึงการแบ่งปันข้อมูลกับหน่วยงานหรือบุคคลที่เหมาะสม

ข้อ ๕.๒ นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy)

ในการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy) ควรจะพิจารณาแนวทางได้จากประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ในภาคผนวก ค ตัวอย่างการประกาศนโยบาย ข้อ ๔ โดยครอบคลุมมาตรการและวิธีการรักษาความมั่นคงปลอดภัยเว็บไซต์ อุปกรณ์ หรือเทคโนโลยี ข้อแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยเบื้องต้นสำหรับผู้ใช้บริการเว็บไซต์ เป็นต้น หรืออาจจะพิจารณาจัดทำนโยบายตามตัวอย่างนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (๓๔)

หากหน่วยงานมีนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่แล้ว ควรจะพิจารณาถึงความครอบคลุมและสอดคล้องกับมาตรฐานฉบับนี้

ข้อ ๕.๓ กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy)

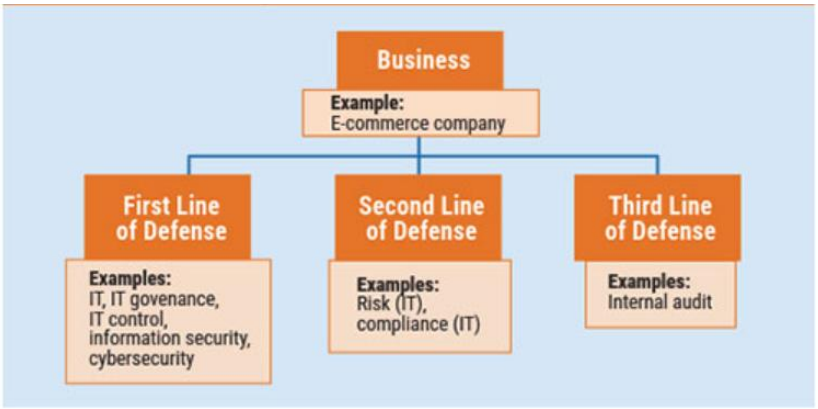
ความเสี่ยงที่ยอมรับได้ (Risk Appetite) หมายถึง ความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้ โดยธุรกิจยังคงดำเนินการได้บรรลุตามเป้าหมาย ส่วนความเสี่ยงและกำกับดูแลความเสี่ยงที่ยอมรับได้กำหนดขึ้นเพื่อใช้เป็นแนวทางกำหนดกลยุทธ์ขององค์กร ทั้งนี้ ความเสี่ยงที่ยอมรับได้ควรได้รับการกำหนดโดยผู้บริหารและอนุมัติโดยคณะกรรมการ การกำหนดความเสี่ยงที่ยอมรับได้ควรพิจารณาถึงความสมดุลระหว่างการเติบโต ความเสี่ยงและผลตอบแทนของหน่วยงาน ในขณะเดียวกันองค์กรควรบริหารความเสี่ยงที่เกิดขึ้นให้อยู่ในระดับที่ยอมรับได้ (๓๕)

ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) หมายถึง ระดับความเบี่ยงเบนจากความเสี่ยงที่ยอมรับได้ การดำเนินธุรกิจภายใต้ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ทำให้ผู้บริหารมั่นใจได้ว่า การดำเนินงานขององค์กรอยู่ภายในเกณฑ์หรือระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ซึ่งมีผลให้คณะกรรมการ และผู้บริหารขององค์กรมีความมั่นใจมากขึ้นว่าการดำเนินการของหน่วยงานจะสามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้ (๓๕)

ข้อ ๕.๔ บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

การถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) เป็นแนวคิดการบริหารความเสี่ยงและตรวจสอบที่เชื่อมโยงการทำงานของหน่วยงานต่าง ๆ เข้าด้วยกันในลักษณะของ “ชั้น” โดยหน่วยงานชั้นแรก (1st Line of Defense) คือ หน่วยงานที่เจ้าของความเสี่ยง (Risk Owner) ที่เผชิญกับความเสี่ยงโดยตรง เป็นผู้กำหนดการควบคุมต่อความเสี่ยง ที่อาจทำให้องค์กรไม่บรรลุวัตถุประสงค์ของหน่วยงานชั้นที่สอง (2nd Line of Defense) ประกอบด้วย หน่วยงานบริหารความเสี่ยงและกำกับการปฏิบัติงาน ภายใต้การควบคุมและกำกับดูแลของผู้บริหารระดับสูง และหน่วยงานชั้นที่สาม (3rd Line of Defense) คือ หน่วยงานตรวจสอบภายใน ทำหน้าที่ในการประเมินความเพียงพอของมาตรการต่าง ๆ โดยอยู่ภายใต้การดูแลของผู้ตรวจสอบภายนอกและหน่วยงานทางการ (๓๖)

หน่วยงานอาจจะพิจารณาประยุกต์หลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) กับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (๓๗) แสดงได้ดังภาพที่ ก๑



ภาพที่ ก๑ ตัวอย่างการประยุกต์หลักการควบคุม กำกับ
และตรวจสอบ (Three Lines of Defense)

จากภาพที่ ก๑ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจะต้องเป็นส่วนหนึ่งของกรอบการบริหารความเสี่ยงระดับองค์กร โดยมีโครงสร้างตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ดังนี้ หน่วยงานชั้นแรก (1st Line of Defense) คือ หน่วยงานด้านเทคโนโลยีสารสนเทศ (IT) ที่เป็นเจ้าของความเสี่ยง (Risk Owner) เช่น IT governance, IT control, Information Security หรือ Cyber Security ที่เผชิญกับความเสี่ยงโดยตรง เป็นผู้กำหนดการควบคุมต่อความเสี่ยงที่อาจทำให้องค์กรไม่บรรลุวัตถุประสงค์ของ หน่วยงานชั้นที่สอง (2nd Line of Defense) ประกอบด้วย หน่วยงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) และหน่วยงานกำกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Compliance) ภายใต้การควบคุมและกำกับดูแลของผู้บริหารระดับสูง และหน่วยงานชั้นที่สาม (3rd Line of Defense) คือ หน่วยงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ (IT Internal Audit) ทำหน้าที่ในการประเมินความเพียงพอของมาตรการต่าง ๆ โดยอยู่ภายใต้การดูแลของผู้ตรวจสอบภายนอกและหน่วยงานทางการ (๓๗)

ข้อ ๕.๕ การวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์

หน่วยงานควรจะมีการวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์ โดยมีขั้นตอนที่เสนอแนะไว้ ดังนี้

๑. การระบุขอบเขตและช่องทางการเข้าถึงเว็บไซต์ โดยมีการพิจารณาและระบุว่าเว็บไซต์ที่จะพัฒนาเปิดให้บริการเฉพาะบางกลุ่มงานภายในหน่วยงาน ทุกกลุ่มงานภายในหน่วยงาน หน่วยงานพันธมิตร ผู้ใช้งานบางกลุ่มที่อยู่นอกหน่วยงาน หรือเปิดให้บริการสาธารณะ รวมถึงกำหนดขอบเขตและช่องทางการเข้าถึงเว็บไซต์ซึ่งเป็นปัจจัยสำคัญในการพิจารณามาตรการและระดับในการรักษาความมั่นคงปลอดภัยของเว็บไซต์

๒. การระบุข้อมูล ระดับความสำคัญ และระดับความละเอียดอ่อนของข้อมูลที่มีการจัดเก็บ ประมวลผล และแสดงบนเว็บไซต์ เว็บไซต์มีการเก็บรวบรวม ประมวลผล และแสดงข้อมูลเฉพาะข้อมูลที่เป็นข้อมูลที่เปิดเผยต่อสาธารณะได้ หรือเป็นข้อมูลที่มีความสำคัญต่อหน่วยงาน เป็นความลับสามารถใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หากมีการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลควรมีมาตรฐานในการรักษาความเป็นส่วนตัวของเจ้าของข้อมูลอย่างเหมาะสม ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (๓๘) ตัวอย่างเช่น การเก็บรวบรวม และประมวลผลข้อมูลส่วนบุคคล มีการกำหนดให้มีกล่องข้อความยินยอมให้เก็บและประมวลผลข้อมูลส่วนบุคคล และควรระบุวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคล

๓. การระบุคุณสมบัติด้านความมั่นคงปลอดภัยที่ต้องการ เช่น หากต้องการรักษาความลับของข้อมูลควรมีการพิจารณาการเข้ารหัสข้อมูล (Encryption) ที่เหมาะสม หากต้องการรักษาความครบถ้วนแท้จริงของข้อมูลควรมีการพิจารณาใช้รหัสยืนยันข้อความ (Message Authentication Code: MAC) หรือลายมือชื่อดิจิทัล (Digital Signature) หากเป็นเว็บไซต์ที่ต้องมีความพร้อมใช้งานสูง ควรมีการเฝ้าระวังความพร้อมใช้งาน (Uptime Monitoring) และการเตรียมทรัพยากรสำรอง (Redundancy หรือ High Availability)

๔. การระบุกลุ่มผู้ใช้งาน พิจารณาถึงการกำหนดสิทธิการเข้าถึง และมาตรการควบคุมการเข้าถึงที่เหมาะสม ในแต่ละกลุ่มผู้ใช้งาน รวมถึงกำหนดสิทธิ์ในการเข้าถึง การกำหนดมาตรการควบคุมการเข้าถึงข้อมูล สารสนเทศ และระบบงานอย่างมั่นคงปลอดภัย

๕. การระบุระดับการรักษาความมั่นคงปลอดภัยตามที่กฎหมายและกฎระเบียบที่เกี่ยวข้อง สำหรับหน่วยงานที่มีให้การบริการบนเว็บไซต์จะมีกฎหมายหรือกฎระเบียบเฉพาะเกี่ยวกับความมั่นคงปลอดภัยและระดับการรักษาความมั่นคงปลอดภัย เช่น ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) ของบริการสำคัญ และการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ (๓๙)

ข้อ ๕.๖ การกำหนดแนวทางด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์

ข้อ ๕.๖.๑ แนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐาน

การกำหนดแนวทางด้านความมั่นคงปลอดภัยเพื่อปกป้องเว็บไซต์และข้อมูลอย่างเหมาะสมตามลำดับความสำคัญของทรัพย์สินและทรัพยากร แนวทางด้านความมั่นคงปลอดภัยที่หน่วยงานควรจะคำนึงถึงคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ด้าน ได้แก่

๑. การรักษาความลับ (Confidentiality) กรณีเว็บไซต์มีการจัดเก็บหรือใช้งานข้อมูลที่มีความละเอียดอ่อน และเข้าถึงได้เฉพาะกลุ่มผู้ใช้ที่ได้รับอนุญาตเท่านั้น เช่น ข้อมูลส่วนบุคคล ข้อมูลภายในหน่วยงาน หรือข้อมูลผลิตภัณฑ์ ควรจะมีมาตรการควบคุมการรักษาความลับที่เหมาะสม เช่น การเข้ารหัสและการควบคุมการเข้าถึง ทั้งระหว่างการจัดเก็บ (Data-at-rest) การส่งต่อ (Data-in-transit) และการใช้งาน (Data-in-use) โดยหน่วยงานควรจะพิจารณาถึงมาตรฐานการเข้ารหัสของแต่ละข้อมูลจะมีการเข้ารหัสมาตรฐานไม่เหมือนกัน เช่น ใช้มาตรฐานเข้ารหัสแบบ RSA ในข้อมูลละเอียดอ่อน การกรอกบัญชีผู้ใช้และรหัสผ่านเพื่อเข้าถึงข้อมูลที่ใช้ภายในหน่วยงาน

๒. การรักษาความครบถ้วนสมบูรณ์ (Integrity) กรณีที่เว็บไซต์มีข้อมูลสำคัญที่ต้องได้รับการปกป้องเพื่อให้มีความครบถ้วนสมบูรณ์ไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต และสามารถตรวจสอบได้หากข้อมูลถูกแก้ไข หน่วยงานควรจะพิจารณามาตรการการรักษาความครบถ้วนสมบูรณ์ของข้อมูล เช่น รหัสยืนยันข้อความ (Message Authentication Code: MAC) ลายมือชื่อดิจิทัล (Digital signature) หรือโพรโทคอลด้านความมั่นคงปลอดภัยอื่น ๆ นอกจากนี้ ควรจะมีมาตรการทบทวนข้อมูลให้มีความถูกต้องเป็นปัจจุบัน เพื่อปกป้องความถูกต้องของข้อมูลในระหว่างจัดเก็บ ส่งต่อ และใช้งาน

๓. การเตรียมความพร้อมใช้งาน (Availability) กรณีที่เว็บไซต์หน่วยงานไม่สามารถให้บริการกับผู้ใช้งานหรือประชาชนได้ ซึ่งมีสาเหตุมาจากหลายปัจจัย เช่น ภัยคุกคามทางไซเบอร์ ถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ อุปกรณ์เครือข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายชำรุดหรือไฟฟ้าดับ ดังนั้น หน่วยงานควรจะมีแผนการรับมือกับภัยคุกคาม หรือเหตุการณ์ไม่คาดคิดที่จะส่งผลต่อการให้บริการของเว็บไซต์ และควรจะมีมาตรการควบคุมปริมาณข้อมูลจราจรผ่านระบบเครือข่ายและมาตรการอื่นเพื่อป้องกันและลดผลกระทบจากการโจมตีแบบ Denial of Service (DoS) หรือ

Distributed Denial of Service (DDoS) รวมถึงควรจะพิจารณาสำรองข้อมูลและทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ ซึ่งหากหน่วยงานมีทรัพยากรเพียงพออาจจะพิจารณาจัดตั้งสถานที่เก็บข้อมูลสำรองในกรณีฉุกเฉิน

ข้อ ๕.๖.๘ รายละเอียดแนวทางในการสำรองข้อมูลเพื่อลดผลกระทบ

การสำรองข้อมูล (Backup) เป็นกระบวนการที่สำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลของหน่วยงาน และลดผลกระทบที่เกิดขึ้นหากถูกโจมตีจากภัยคุกคามทางไซเบอร์ รวมถึงเกิดเหตุการณ์ที่ไม่คาดคิด หรือความเสียหายจากภัยธรรมชาติ หรือข้อผิดพลาดจากมนุษย์ โดยหน่วยงานอาจจะพิจารณาองค์ประกอบในการสำรองข้อมูลอย่างน้อย ดังนี้

๑) กำหนดข้อมูลที่ต้องการสำรอง ในการบริหารจัดการเว็บไซต์เพื่อความมั่นคงปลอดภัยของหน่วยงาน จะต้องมีการกำหนดรายการข้อมูลที่จำเป็นสำหรับการสำรองข้อมูล ที่รองรับต่อการกู้คืนระบบจากปัญหาด้านต่าง ๆ เช่น ฐานข้อมูลระบบเว็บไซต์ ไฟล์การตั้งค่าระบบเว็บไซต์ ไฟล์เนื้อหาเว็บไซต์

๒) กำหนดเทคโนโลยี วิธีการสำรองข้อมูล และไซต์สำรอง ระบุเทคโนโลยีในการสำรองข้อมูล และรูปแบบการดำเนินการจัดเก็บฐานข้อมูลที่เหมาะสม เช่น การสำรองข้อมูลแบบเต็ม (Full backup) การสำรองข้อมูลแบบเพิ่มเติม (Incremental backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Differential backup) รวมถึงการจัดทำไซต์สำรองเพื่อการกู้คืนในภาวะฉุกเฉินให้เป็นไปตามแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ข้อ ๖.๕.๑ โดยอาจจะพิจารณารูปแบบการสำรองข้อมูลแบ่งตามประเภทของข้อมูล ตามตาราง ก๒

ตาราง ก๒ รูปแบบการสำรองข้อมูลแบ่งตามประเภทของข้อมูล

ประเภทข้อมูล	ความถี่ในการสำรองข้อมูล	ประเภทการสำรองข้อมูล	หมายเหตุ
ฐานข้อมูลที่มีการเปลี่ยนแปลงสูง	ทุก ๆ ๒๔ ชั่วโมง	Full Backup ประจำสัปดาห์ + Incremental ทุกวัน	สำรองข้อมูลที่เปลี่ยนแปลงตั้งแต่การสำรองล่าสุด
ไฟล์เอกสารสำคัญ	ทุก ๆ ๔๘ ชั่วโมง	Full Backup ประจำเดือน + Differential ทุกสัปดาห์	สำรองข้อมูลที่เปลี่ยนแปลงตั้งแต่การสำรองเต็มล่าสุด
ระบบไฟล์ทั่วไป	ทุกสัปดาห์	Full Backup	เหมาะสำหรับไฟล์ที่ไม่มีการเปลี่ยนแปลงบ่อย
ไฟล์สื่อ (วิดีโอ, ภาพ)	ทุกเดือน	Full Backup	ข้อมูลขนาดใหญ่ที่มีการเปลี่ยนแปลงน้อย
เอกสารที่ใช้งานไม่บ่อย	ทุก ๓-๖ เดือน	Full Backup	เอกสารที่ไม่จำเป็นต้องอัปเดตบ่อย

๓) กำหนดความถี่และพื้นที่ในการสำรองข้อมูล การกำหนดความถี่ในการสำรองข้อมูลควรจะพิจารณาจากความสำคัญของข้อมูล เช่น เป็นฐานข้อมูลหลักในการดำเนินการของหน่วยงาน เป็นฐานข้อมูลผู้ใช้งาน เป็นข้อมูลที่มีความสำคัญสูง จึงมีความจำเป็นต้องกำหนดให้มีการสำรองข้อมูลโดยมีความถี่ในการสำรองข้อมูลสูง พร้อมทั้งระบุตำแหน่งของการจัดเก็บข้อมูลสำรอง โดยจะต้อง

เป็นพื้นที่แยกจากพื้นที่ดำเนินการหลัก ซึ่งอาจจะใช้พื้นที่ในระบบคลาวด์ ไดรฟ์ภายนอก หรือเครื่องบริการอื่น ๆ

๔) ทดสอบแผนการสำรองข้อมูลและการกู้คืน การทดสอบแผนการสำรองข้อมูลและการสำรองข้อมูลอย่างครบถ้วนสมบูรณ์ภายในเวลาที่เหมาะสม รวมถึงทดสอบการกู้คืนและทดสอบการดำเนินการ เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์กับเว็บไซต์แล้ว ข้อมูลที่สำรองไว้จะนำกลับมาใช้งานได้จริง

ข้อ ๕.๖.๙ การจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log Management)

การจัดการข้อมูลจราจรทางคอมพิวเตอร์ เป็นกระบวนการที่มุ่งเน้นการเก็บรวบรวมและการจัดการกับบันทึกเหตุการณ์ที่เกิดขึ้นในระบบของหน่วยงาน เช่น บันทึกการเข้าถึงระบบ บันทึกการเปลี่ยนแปลงในการตั้งค่า หรือบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย โดยมีเป้าหมายหลักคือการเพิ่มการระบุและการตรวจสอบเหตุการณ์ที่เกิดขึ้น เพื่อช่วยให้สามารถตรวจสอบและติดตามกิจกรรมที่เกิดขึ้นได้อย่างมีประสิทธิภาพ นอกจากนี้ ยังช่วยให้สามารถทำการตรวจสอบและบันทึกข้อมูลการเปลี่ยนแปลง ทำให้สามารถติดตามและตรวจสอบผู้ใช้หรือบุคลากรที่มีความเกี่ยวข้องกับเหตุการณ์นั้นได้อย่างมีประสิทธิภาพ

ข้อ ๕.๖.๑๐ หลักปฏิบัติในการเลิกใช้งานเว็บไซต์

หน่วยงานที่ต้องการยุติการให้บริการเว็บไซต์ควรจะมีหลักปฏิบัติในการหยุดให้บริการเว็บไซต์เพื่อป้องกันภัยคุกคามที่อาจจะเกิดกับผู้ใช้บริการเว็บไซต์ ผู้ใช้งานอินเทอร์เน็ต และผู้ให้บริการเว็บไซต์ โดยหน่วยงานอาจจะพิจารณาหลักปฏิบัติในการหยุดให้บริการเว็บไซต์ ดังนี้

๑) แจ้งเตือนผู้ใช้งานถึงการหยุดให้บริการและวันที่จะหยุดให้บริการก่อนหยุดบริการจริง

๒) สำรองข้อมูลเว็บไซต์และฐานข้อมูลเพื่อป้องกันข้อผิดพลาดที่อาจจะเกิดขึ้น

๓) นำข้อมูลออกจากผู้ให้บริการเครื่องบริการเว็บ โดยอาจเหลือหน้าเว็บไซต์ที่แจ้งว่าเว็บไซต์ปิดบริการแล้วไว้ระยะเวลาหนึ่ง

๔) ยกเลิกบริการจากผู้ให้บริการเครื่องบริการเว็บ

๕) แจ้งเปลี่ยนสถานะชื่อโดเมนกับผู้ดูแล

๖) ตรวจสอบข้อมูลที่ยังหลงเหลืออยู่กับผู้ให้บริการค้นหาข้อมูล โดยอาจลองค้นหาข้อมูลเกี่ยวกับเว็บไซต์ที่เคยให้บริการ ถ้าพบว่ายังมีอยู่ให้ยื่นคำขอลบข้อมูลไปยังผู้ให้บริการค้นหาข้อมูล

๗) ถึงแม้ว่าจะมีการหยุดให้บริการเว็บไซต์แล้ว ควรพิจารณาว่ามีความจำเป็นจะต้องรักษาชื่อโดเมนให้อยู่ในการครอบครองหรือควบคุมของหน่วยงานต่อไปหรือไม่ เพื่อป้องกันไม่ให้ชื่อโดเมนที่มีความเกี่ยวข้องกับหน่วยงานแต่หมดอายุแล้ว ถูกผู้ไม่ประสงค์ดีเข้าครอบครองและนำไปแอบอ้างใช้งาน ทำให้ผู้เข้าเยี่ยมชมเว็บไซต์ของผู้ไม่ประสงค์ดีเกิดความเข้าใจผิดหรือถูกหลอกลวงได้

๘) หน่วยงานอาจจะพิจารณาแนวทางการทำลายข้อมูลของเว็บไซต์ที่เลิกใช้งานอย่างเหมาะสม ทั้งในรูปแบบเว็บไซต์ที่ใช้ระบบขององค์กร (On-Premises) และเว็บไซต์ที่ใช้ระบบคลาวด์ (Cloud Service) โดยอาจจะจัดระดับความสำคัญของข้อมูลและการทำลายข้อมูลตาม NIST Special Publication 800-88 Guidelines for Media Sanitization รวมถึงอาจจะตรวจสอบการยืนยันการทำลายข้อมูลของบริการเว็บโฮสติ้ง (Web Hosting) หรือแนวทางการทำลายข้อมูลของผู้ให้บริการหรือเจ้าของผลิตภัณฑ์

ข้อเสนอแนะของ NIST Special Publication 800-88 Guidelines for Media Sanitization

มาตรฐาน NIST SP 800-88 เป็นหนึ่งในมาตรฐานที่สำคัญสำหรับการทำลายสื่อเก็บข้อมูลชนิดต่าง ๆ อย่างเหมาะสมและถูกวิธี เป็นการกำหนดวิธีการและกระบวนการสำหรับการล้างข้อมูล (Media Sanitization) ในสื่ออิเล็กทรอนิกส์ เช่น Hard disk, RAM , ROM , Mount Storage, USB Drive , Smart Thing Storage, Mobile และข้อมูลบนระบบเครือข่ายต่าง ๆ โดยเน้นการสร้างความมั่นใจภายหลังการล้างข้อมูลว่าไม่มีข้อมูลที่จะหลงเหลืออยู่บนอุปกรณ์ก่อนนำกลับมาใช้ใหม่ ในการทำลายข้อมูลขึ้นอยู่กับปัจจัยหลายอย่าง เช่น ชนิดของอุปกรณ์ งบประมาณ ความเสี่ยงและความสำคัญของข้อมูล และผลกระทบต่อสิ่งแวดล้อม ดังนั้น เจ้าของข้อมูลทั้งตัวบุคคล บริษัท และหน่วยงานต่าง ๆ ควรประเมินปัจจัยหลาย ๆ อย่างก่อนการเปลี่ยนหรือเลิกใช้อุปกรณ์อิเล็กทรอนิกส์ โดยเพื่อเลือกวิธีการกำจัด และทำลายให้เหมาะสมกับความต้องการ และมีความมั่นคงปลอดภัย เพื่อลดความเสี่ยงของข้อมูลรั่วไหลหรือเปิดเผยของข้อมูลโดยไม่ได้รับอนุญาต โดยมีขั้นตอนหลักในการทำลายข้อมูล ๓ ขั้นตอน ดังนี้

๑. การลบข้อมูลทั้งหมดที่จัดเก็บไว้ในอุปกรณ์ (Clear) โดยใช้คำสั่งอ่านและเขียน รวมถึงการตั้งค่าเครื่องใหม่ (Reset) อุปกรณ์ให้เป็นการตั้งค่าจากโรงงานโดยเขียนใหม่ด้วยค่าใหม่ เหตุผลสำคัญของข้อมูลหน่วยงาน หรือข้อมูลบนระบบหลังจากเลิกใช้แล้ว หรือมีการลาออกของพนักงาน โดยใช้หลักการ Sanitize Data ในกรณี NIST SP 800-88 จะใช้ในรูปแบบของ Secure Erase

๒. กระบวนการการขัดขวางการกู้คืนในทุกกรณีโดยวิธีการลบล้าง (Purge) โดยใช้เทคนิคทางวิทยาศาสตร์เข้ามาเกี่ยวข้อง การทำลายข้อมูลเชิงการลบแบบ Degaussing ทำลายสนามแม่เหล็กก่อกวน รบกวนไม่ให้สามารถนำมาจัดเรียงได้ใหม่

๓. การทำลายข้อมูล (Destroy) ขั้นตอนกรณีเราไม่ใช้แล้วกับอุปกรณ์ในการเก็บข้อมูลทั้งหลาย ขั้นตอนการทำลายเป็นขั้นตอนที่ดีที่สุด ที่จะทำให้ปลอดภัยในทุกด้านทั้งทางกายภาพและเชิงการนำไปกู้ข้อมูลต่อ โดยอาจจะเป็นการหลอมละลาย ทุบทิ้งให้แหลกละเอียด หรือเผาไหม้ให้ไม่เหลือชิ้นส่วนที่สามารถนำมาใช้ได้

ภาคผนวก ข
รายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติม
(ข้อ ๖)
(เป็นข้อมูลเพิ่มเติม)

ข้อ ๖.๑ การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification)
การจัดการความเสี่ยง

ในบริบทของการรักษาความมั่นคงปลอดภัย ความเสี่ยง หมายถึง ระดับของผลกระทบต่อการดำเนินการของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือบุคคลที่เกิดจากการใช้งานระบบสารสนเทศ โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามและความน่าจะเป็นที่ภัยคุกคามอาจเกิดขึ้น การจัดการความเสี่ยง หมายถึง กระบวนการในการจัดการความเสี่ยงต่อการดำเนินการของหน่วยงาน ทรัพย์สินของหน่วยงาน หรือบุคคลที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ รวมถึงการประเมินความเสี่ยง การดำเนินการตามกลยุทธ์บรรเทาความเสี่ยง และการใช้เทคนิคและขั้นตอนในการเฝ้าระวังสถานะความมั่นคงปลอดภัยของระบบสารสนเทศอย่างต่อเนื่อง (๔๐)

ในทางปฏิบัติหน่วยงานไม่สามารถกำจัดความเสี่ยงทั้งหมดหรือทำให้ความเสี่ยงเป็นศูนย์ได้ แต่หน่วยงานสามารถลดความเสี่ยงให้อยู่ระดับที่หน่วยงานรับได้ เฝ้าระวังและรักษาระดับความเสี่ยงไม่ให้เกินระดับที่ตั้งไว้ได้ โดยอาจจะพิจารณาวิธีการและขั้นตอนการจัดการความเสี่ยงจากมาตรฐาน ISO/IEC 27005 ซึ่งเป็นมาตรฐานการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) และสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอาจจะพิจารณาปฏิบัติตามคำแนะนำของ สกมช. เรื่อง แนวปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (๓๐) ซึ่งกระบวนการพื้นฐานสำหรับการจัดการความเสี่ยงสำหรับเว็บไซต์ แบ่งเป็น ๔ กระบวนการ ดังนี้

การจัดการทรัพย์สิน (Asset Management)

การจัดทำรายการทรัพย์สินเป็นขั้นตอนแรกของการวางแผนการดำเนินการรักษาความมั่นคงปลอดภัยเพื่อให้ทราบว่าหน่วยงานมีทรัพย์สินใดที่จะต้องปกป้อง มีความเสี่ยงใดที่จะต้องจัดการตามลำดับความสำคัญด้วยทรัพยากรที่มีจำกัด และมีทรัพย์สินใดที่มีช่องโหว่ความมั่นคงปลอดภัยที่ต้องได้รับป้องกันก่อนเกิดการโจมตีทรัพย์สินหรือข้อมูลของหน่วยงาน

การจัดทำรายการทรัพย์สินควรรวมถึงทรัพย์สินที่จับต้องได้ เช่น เครื่องบริการเว็บ และทรัพย์สินที่จับต้องไม่ได้ เช่น โปรแกรมสำหรับให้บริการเว็บ สัญญา รวมถึงทรัพย์สินทางปัญญา รวมถึงบุคลากรและเอกสารที่เกี่ยวข้อง เช่น แผนภาพระบบ (System Diagram) โดยรายการทรัพย์สินควรระบุ และบันทึกข้อมูลที่เกี่ยวข้องกับทรัพย์สินอย่างน้อย ดังแสดงในตาราง ข๑

ตาราง ข๑ รายละเอียดที่ระบุในรายการทรัพย์สิน

รายการ	รายละเอียด
รหัสประจำทรัพย์สิน	ใช้สำหรับการระบุ ติดตาม และจัดการทรัพย์สิน ซึ่งประกอบด้วย รหัสซีเรียล ป้ายกำกับทรัพย์สิน และรหัสบาร์โค้ดหรือคิวอาร์โค้ด เป็นอย่างน้อย
ชื่อเรียกทรัพย์สิน	เพื่อใช้ในการระบุทรัพย์สิน

รายการ	รายละเอียด
คำอธิบายทรัพย์สิน	เพื่อให้ข้อมูลเพิ่มเติมเกี่ยวกับทรัพย์สินและวัตถุประสงค์ของการใช้งานทรัพย์สินโดยสังเขป
ฟังก์ชันที่สำคัญของทรัพย์สิน	เพื่อใช้ในการระบุหน้าที่และความสำคัญของทรัพย์สิน สนับสนุนการตรวจประเมินและการปฏิบัติตามข้อกำหนด
การจำแนกทรัพย์สิน	เพื่อจัดกลุ่มทรัพย์สินที่มีลักษณะที่เหมือนกัน โดยอาจแบ่งจำแนกกลุ่มตามประเภท ตำแหน่งที่อยู่ หรือความเป็นเจ้าของ เป็นต้น
เจ้าของและ/หรือผู้ดำเนินการ และ/หรือผู้ดูแลทรัพย์สิน	เป็นการระบุผู้ดูแลและรับผิดชอบทรัพย์สิน ซึ่งเป็นผู้ใช้งาน หรือจัดการทรัพย์สิน โดยอาจจะระบุช่องทางติดต่อด้วย
ตำแหน่งทางกายภาพของทรัพย์สิน	ระบุว่าทรัพย์สินมีการติดตั้ง การใช้งาน และจัดเก็บอยู่ที่ใด เพื่อใช้ในการติดตามทรัพย์สิน
วันเวลาการตรวจสอบทรัพย์สิน	เพื่อให้ทราบว่าทรัพย์สินยังสามารถติดตามได้และข้อมูลเกี่ยวกับทรัพย์สินยังมีความถูกต้อง
มูลค่าของทรัพย์สิน	เป็นปัจจัยในการพิจารณาระดับความสำคัญ และมาตรการที่จะต้องรักษาความมั่นคงปลอดภัยของทรัพย์สิน
วันที่บันทึกทรัพย์สินเข้าระบบ	บันทึกวันที่จดบันทึกรายการทรัพย์สินเข้าระบบของหน่วยงาน
สถานะใช้งานทรัพย์สิน	เพื่อระบุว่าทรัพย์สินอยู่ระหว่างการใช้งาน ใช้งานได้ปกติ ชำรุด หมดอายุ หรือจำหน่ายออก เป็นต้น
อายุการใช้งานของทรัพย์สิน	เพื่อให้ทราบอายุการใช้งานของทรัพย์สิน และเป็นข้อมูลแจ้งเตือนการดำเนินการใด ๆ กับทรัพย์สินที่หมดอายุการใช้งาน เช่น การต่ออายุการใช้งาน การต่ออายุการบำรุงรักษา การตัดบัญชีสินทรัพย์ และการจำหน่ายทรัพย์สิน
ระดับความสำคัญของทรัพย์สิน	โดยพิจารณาจากมูลค่าของทรัพย์สิน ผลกระทบที่จะเกิดขึ้นเมื่อทรัพย์สินเกิดชำรุด เสียหาย หรือถูกละเมิด เป็นต้น
ผู้ที่มีสิทธิ์ในการใช้งานทรัพย์สิน	โดยระบุว่าบุคคลที่สามารถเข้าถึงทรัพย์สิน รวมถึงสิทธิ์ในการใช้งานทรัพย์สิน
การขึ้นต่อกันของทรัพย์สิน	เพื่อระบุความสัมพันธ์ที่ทรัพย์สินหนึ่งต้องพึ่งพาหรือเชื่อมโยงกับอีกทรัพย์สินหนึ่งในการทำงานหรือให้บริการ
ลักษณะอื่นๆ ของทรัพย์สิน	เป็นการระบุข้อมูลอื่น ๆ ของทรัพย์สิน เช่น เวอร์ชันของโปรแกรม การตั้งค่า ระยะเวลาการรับประกัน ประวัติการซ่อมบำรุง รูปภาพของทรัพย์สิน

การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นหนึ่งในกระบวนการสำคัญในการบริหารจัดการความเสี่ยง เพื่อให้หน่วยงานสามารถจัดสรรทรัพยากรที่มีจำกัดเพื่อจัดการความเสี่ยงตามลำดับความสำคัญให้อยู่ในระดับที่หน่วยงานสามารถรับได้และคงระดับความเสี่ยงนั้นให้อยู่ในระดับที่กำหนด โดยหน่วยงานควรจะพิจารณาประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ

๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และควรจะมีการปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์

ในการประเมินความเสี่ยง หน่วยงานอาจจะพิจารณาประเมินความเสี่ยงได้ ๒ รูปแบบ ได้แก่ การประเมินความเสี่ยงเชิงปริมาณ ซึ่งเป็นการกำหนดค่าตัวแปรที่ใช้ในการประเมินความเสี่ยงแบบละเอียด และการประเมินความเสี่ยงเชิงคุณภาพ ซึ่งเป็นการแบ่งค่าตัวแปรเป็นกลุ่มหรือระดับ เช่น ต่ำ กลาง สูง หรือแบ่งเป็นระดับ ๑ ถึง ระดับ ๕ ถึงแม้ว่าการประเมินความเสี่ยงเชิงปริมาณจะช่วยให้สามารถเปรียบเทียบความเสี่ยงได้ชัดเจน แต่มีข้อเสียเนื่องจากใช้เวลามากและมีขั้นตอนยุ่งยาก ดังนั้น หลายสถานการณ์จึงเลือกใช้การประเมินความเสี่ยงเชิงคุณภาพ ซึ่งดำเนินการง่ายกว่าและสะท้อนความเสี่ยงได้ในภาพกว้าง ซึ่งในแต่ละหน่วยงานสามารถกำหนดระดับค่าตัวแปรให้เหมาะสมแต่ละหน่วยงาน ทั้งนี้ หน่วยงานควรใช้เกณฑ์เดียวกันเพื่อให้สามารถเปรียบเทียบระดับความเสี่ยงของแต่ละหน่วยย่อยภายในหน่วยงานได้

หน่วยงานอาจจะพิจารณาขั้นตอนหลักในการประเมินความเสี่ยง ดังนี้

๑) การระบุภัยคุกคาม เป็นขั้นตอนของการระบุภัยคุกคามที่อาจเกิดขึ้น และสร้างความเสียหายให้กับทรัพย์สิน รวมถึงภัยคุกคามที่เกิดจากบุคคล เช่น การละเมิดและโจรกรรมข้อมูล การติดมัลแวร์ และการขัดขวางการทำงานของระบบ และภัยคุกคามที่เกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ แผ่นดินไหว

๒) การระบุช่องโหว่ความมั่นคงปลอดภัย เป็นการระบุจุดอ่อนของระบบ ที่ผู้ไม่ประสงค์ดีสามารถใช้เพื่อเข้าถึงระบบและข้อมูลโดยไม่ได้รับอนุญาต นอกจากการระบุช่องโหว่ความมั่นคงปลอดภัยของซอฟต์แวร์แล้ว ยังต้องระบุช่องโหว่ความมั่นคงปลอดภัยของฮาร์ดแวร์ และของระบบอื่น ๆ ด้วย แหล่งข้อมูลที่สำคัญที่รวบรวมข้อมูลช่องโหว่ความมั่นคงปลอดภัย คือ โครงการ CVE Program โดย MITRE (๔๑) ซึ่งมีการรวบรวมช่องโหว่ความมั่นคงปลอดภัยที่มีการเปิดเผยสู่สาธารณะไว้

๓) การระบุความถี่ เป็นการประมาณการโอกาสเกิดภัยคุกคาม ในการประเมินความเสี่ยงเชิงปริมาณการระบุความถี่จะระบุเป็นค่าเฉลี่ยจำนวนครั้งที่ภัยคุกคามเกิดขึ้นต่อปี เช่น ๒ ครั้งต่อปี หรือ ๐.๑ ครั้งต่อปี (เกิด ๑ ครั้งทุก ๆ ๑๐ ปี) ส่วนการประเมินความเสี่ยงเชิงคุณภาพ การระบุความถี่มักจะระบุเป็นระดับ เช่น น้อย กลาง มาก หรือระดับ ๑ ถึงระดับ ๕

๔) การระบุผลกระทบ เป็นการประมาณการระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามต่อครั้ง ในการประเมินความเสี่ยงเชิงปริมาณ การระบุผลกระทบมักจะกำหนดเป็นมูลค่าของทรัพย์สินและค่าใช้จ่ายอื่น ๆ ที่เกี่ยวข้องหากทรัพย์สินเกิดความเสียหาย เช่น เครื่องบริการเว็บเสียหายจากไฟไหม้ มีมูลค่า ๒ แสนบาท ส่วนการประเมินความเสี่ยงเชิงคุณภาพการระบุผลกระทบมักจะระบุเป็นระดับ เช่น ต่ำ กลาง สูง หรือระดับ ๑ ถึง ระดับ ๕

๕) การวิเคราะห์ระดับความเสี่ยง เป็นการคำนวณได้จากโอกาสเกิดและผลกระทบ ในการวิเคราะห์ความเสี่ยงเชิงปริมาณ คำนวณได้จากความถี่ที่จะเกิดภัยคุกคามเฉลี่ยต่อปีคูณกับมูลค่าความเสียหายที่เกิดขึ้นต่อครั้ง เช่น โอกาสไฟไหม้เครื่องบริการเว็บเฉลี่ย ๐.๑ ครั้งต่อปี ไฟไหม้ต่อครั้ง

ทำให้เกิดความเสียหาย ๒๐๐,๐๐๐ บาท จะได้ความเสี่ยงเป็น ๒๐,๐๐๐ บาทต่อปี ส่วนการประเมินความเสี่ยงเชิงคุณภาพจะมีการทำตารางความเสี่ยงและกำหนดระดับความเสี่ยงดังแสดงในตาราง ข๒

ตาราง ข๒ ตัวอย่างตารางประเมินความเสี่ยงเชิงคุณภาพ

ระดับผลกระทบ / ระดับความถี่	๑	๒	๓
๓	กลาง	สูง	สูง
๒	ต่ำ	กลาง	สูง
๑	ต่ำ	กลาง	สูง

หลังจากการวิเคราะห์ความเสี่ยงหน่วยงานอาจจะเลือกวิธีการจัดการความเสี่ยงของแต่ละทรัพย์สินตามความเหมาะสม โดยควรจะพิจารณาตามลำดับความสำคัญ และทรัพยากรที่หน่วยงานมี โดยรายการที่มีความเสี่ยงสูงควรได้รับการจัดการและใช้มาตรการควบคุมที่เข้มงวด ในขณะที่รายการที่มีความเสี่ยงต่ำกว่า อาจจะพิจารณาปรับลดความเข้มข้นของมาตรการควบคุมได้ตามความเหมาะสม

การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

การประเมินความเสี่ยงจากช่องโหว่ (Vulnerability Assessment) เป็นกระบวนการที่ใช้เพื่อตรวจสอบและระบุช่องโหว่ของระบบคอมพิวเตอร์ โครงสร้างเครือข่ายสื่อสารข้อมูล เครื่องบริการเว็บ และเว็บแอปพลิเคชัน ที่อาจทำให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลและระบบ เช่น ช่องโหว่ในส่วนเสริมของระบบบริหารจัดการเว็บไซต์ ที่ยังไม่ได้รับการปรับปรุง การกำหนดค่าระบบที่ไม่ปลอดภัย หรือการปรับแต่งการตั้งค่าที่ไม่ถูกต้อง เป้าหมายหลักของการประเมินความเสี่ยงจากช่องโหว่ คือ การทำให้ระบบมีความแข็งแรงและปลอดภัยจากการโจมตีของผู้ไม่ประสงค์ดี โดยมีแนวทางในการดำเนินการ ดังนี้

๑) การสแกนช่องโหว่ ผู้ดูแลระบบใช้เครื่องมือในการสแกนช่องโหว่ เพื่อค้นหาช่องโหว่ของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือเว็บไซต์ ที่อาจเสี่ยงต่อการถูกโจมตี หน่วยงานควรมีการสแกนช่องโหว่เป็นประจำตามระยะเวลาที่เหมาะสม[๙] แต่ไม่ควรเกิน ๙๐ วัน

๒) การวิเคราะห์ผลการสแกน หลังจากการสแกนช่องโหว่เสร็จสิ้น ผู้ดูแลระบบจะวิเคราะห์ผลลัพธ์เพื่อระบุช่องโหว่ที่มีความเสี่ยงสูงและต้องการการแก้ไขโดยเร่งด่วน

๓) การสร้างรายงานและแนะนำ ผู้ดูแลระบบจะสร้างรายงานที่รวมข้อมูลเกี่ยวกับช่องโหว่ที่พบระดับความรุนแรง และข้อแนะนำเพื่อปรับปรุงความมั่นคงปลอดภัยของระบบ ซึ่งสามารถนำไปใช้เพื่อการปรับปรุงความมั่นคงปลอดภัยในหน่วยงานได้อย่างมีประสิทธิภาพ

---

[๙] ในการพิจารณาระยะเวลาที่เหมาะสมในการสแกนช่องโหว่ อาจจะพิจารณาอ้างอิงจากระยะเวลาของการใช้ประโยชน์จากช่องโหว่ ตัวอย่างเช่น รายงานของ Threat Research Unit, Qualys 42. Abbasi S. 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is 2023 [Available from: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one. ระบุว่าระยะเวลาในการใช้ประโยชน์จากช่องโหว่ของระบบในการโจมตีมีค่าเฉลี่ยอยู่ที่ 44 วัน หน่วยงานควรมีการสแกนช่องโหว่เป็นประจำทุก 30 วัน

การทดสอบการเจาะระบบ (Penetration Testing: Pentest)

การทดสอบการเจาะระบบ (Penetration Testing) เป็นกระบวนการที่ใช้เพื่อทดสอบความเข้าถึง และความแข็งแกร่งของระบบคอมพิวเตอร์ หรือโครงสร้างเครือข่าย โดยมีวัตถุประสงค์เพื่อค้นหาช่องโหว่ ที่มีโอกาสถูกโจมตีและเสี่ยงต่อความมั่นคงปลอดภัย โดยการทดสอบเจาะระบบจะดำเนินการโจมตีแบบเสมือนจริง ที่อาจมาจากผู้ไม่ประสงค์ดี เพื่อทราบถึงจุดอ่อนของระบบหรือแอปพลิเคชัน หน่วยงานอาจจะพิจารณาดำเนินการ ดังนี้

๑) การทดสอบการเจาะระบบเว็บแอปพลิเคชัน ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจะดำเนินการการทดสอบการเจาะระบบโดยลอกเลียนแบบการโจมตีจริง ๆ กับเป้าหมาย ซึ่งเป็นเว็บแอปพลิเคชัน เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ Cross-Site Scripting (XSS) หรือการเจาะระบบจากการแอบอ้างเป็นผู้ใช้ (User Impersonation)

๒) การทดสอบการเจาะระบบ โดยผู้เชี่ยวชาญจะทำการทดสอบการเจาะระบบ โดยพิจารณาจากการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access Control) และการหลบเลี่ยงการตรวจจับของอุปกรณ์ด้านความมั่นคงปลอดภัย เช่น หลบเลี่ยงการป้องกันไฟร์วอลล์ (Bypass Firewall) และหลบเลี่ยงการตรวจจับการบุกรุก (Bypass IDS/IPS) เป็นสำคัญ

ปัจจัยในการดำเนินการทดสอบการเจาะระบบเว็บไซต์อาจจะดำเนินการอย่างน้อย ดังนี้

๑) ขอบเขตของการทดสอบ โดยอาจจะทดสอบทั้งระบบหรือทดสอบเฉพาะส่วน เช่น ระบบเครือข่าย และระบบเว็บแอปพลิเคชัน

๒) ผู้ทดสอบระบบ โดยอาจจะใช้ผู้ปฏิบัติงานจากภายในหรือใช้บริการทดสอบเจาะระบบจากภายนอก

๓) รูปแบบการทดสอบ สามารถแบ่งตามข้อมูลที่ใช้ในการเจาะระบบ คือ การเจาะระบบแบบไม่มีข้อมูลหรือการจำลองการเจาะระบบจากภายนอก การเจาะระบบแบบมีข้อมูลทั้งหมดหรือการจำลองการเจาะระบบจากภายใน และการเจาะระบบแบบมีข้อมูลบางส่วน

๔) ค่าใช้จ่ายที่ใช้ในการทดสอบเจาะระบบ

๕) รายงานผลการทดสอบ โดยระบุรายละเอียดที่ต้องการ และรูปแบบในการรายงานที่สามารถนำไปใช้งานได้

หน่วยงานอาจจะพิจารณาเลือกผู้ให้บริการทดสอบเจาะระบบอย่างน้อย ดังนี้

๑) รูปแบบของการให้บริการ โดยเลือกผู้ให้บริการที่ทดสอบเจาะระบบทั้งด้วยระบบอัตโนมัติและผู้เชี่ยวชาญ

๒) ความสามารถของผู้เชี่ยวชาญที่ดำเนินการทดสอบเจาะระบบ โดยสามารถพิจารณาจากใบรับรองด้านการทดสอบเจาะระบบที่ได้รับ เช่น OSCP OSWE GPEN GWAPT หรือใบรับรองอื่นที่เกี่ยวข้อง

๓) ความน่าเชื่อถือของผู้ให้บริการ โดยสามารถพิจารณาได้จากผลการปฏิบัติงานที่ผ่านมา ชื่อเสียงของบริษัท และความพึงพอใจของผู้รับบริการในอดีต

๔) ความสามารถในการรักษาความมั่นคงปลอดภัยของข้อมูล โดยสามารถพิจารณาได้จากมาตรฐานทางด้านความมั่นคงปลอดภัยในการปฏิบัติงาน การตรวจสอบประวัติพนักงานในการจ้างงาน และการรับประกันความเสียหาย

๕) ค่าใช้จ่ายที่ใช้ในการทดสอบเจาะระบบ โดยอาจจะพิจารณาขอใบเสนอราคาจากผู้บริการหลายราย

ข้อ ๖.๒ การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection)

ข้อ ๖.๒.๑ การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย

การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย หมายถึง การปฏิบัติและมาตรการที่ใช้ระหว่างการสร้างโปรแกรมประยุกต์บนเว็บเพื่อลดความเสี่ยง และปิดช่องโหว่ด้านความมั่นคงปลอดภัยที่เป็นไปได้ ซึ่งรวมถึงขั้นตอนต่าง ๆ ของวงจรชีวิตการพัฒนา ตั้งแต่การวางแผนและออกแบบ ไปจนถึงการนำไปใช้ และการดูแลรักษา หน่วยงานอาจจะพิจารณาสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยของการพัฒนาโปรแกรมประยุกต์บนเว็บไซต์ ดังนี้

๑) การสร้างแบบจำลองภัยคุกคาม (Threat Modeling) เพื่อระบุความเสี่ยงด้านความมั่นคงปลอดภัย ช่องโหว่ และเวกเตอร์โจมตีที่อาจมีผลต่อโปรแกรมประยุกต์บนเว็บไซต์

๒) การเขียนโค้ดที่ปลอดภัย (Secure Coding Practices) หน่วยงานควรจะปฏิบัติตามข้อแนะนำและการสร้างโค้ดที่ปลอดภัย เพื่อลดความเสี่ยงที่พบบ่อย เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ XSS และ การโจมตีแบบ Cross-Site Request Forgery (CSRF)

๓) การตรวจสอบและทำความสะอาดข้อมูลที่รับเข้า (Input Validation and Sanitization) เพื่อป้องกันการป้อนข้อมูลที่เจาะจงจากผู้ไม่ประสงค์ดี การรับรองตนเองและการอนุญาต การนำเอากลไกการรับรองตนเองที่แข็งแกร่งเข้าไปเพื่อยืนยันตัวตนของผู้ใช้

๔) การควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงไปยังฟังก์ชันและทรัพยากรที่มีความสำคัญตามบทบาทและสิทธิ์ของผู้ใช้ การบริหารจัดการเซสชัน การใช้เทคนิคการบริหารจัดการเซสชันที่ปลอดภัยเพื่อปกป้องรหัสเซสชัน ป้องกันการโจมตีการปิดเซสชัน และรักษาความลับและความสมบูรณ์ของข้อมูลเซสชัน

๕) การเข้ารหัสข้อมูล มีความสำคัญที่พักอยู่และต่อเนื่อง โดยใช้ขั้นตอนวิธีการเข้ารหัสและโพรโทคอลการสื่อสารที่เป็นมาตรฐาน เพื่อป้องกันการเข้าถึงข้อมูลและการละเมิดข้อมูล

๖) การกำหนด Header ที่เหมาะสมในการตอบสนอง HTTP เพื่อเพิ่มความมั่นคงปลอดภัยต่อการโจมตีที่พบบ่อยในเว็บ เช่น การโจมตีแบบ XSS การโจมตีแบบ CSRF และการโจมตีด้วยการคลิก ไลบรารีและโปรแกรมช่วย การอัปเดตและแก้ไขไลบรารี และโปรแกรมช่วยที่ใช้ในแอปพลิเคชันเพื่อลดความเสี่ยงจากช่องโหว่ด้านความมั่นคงปลอดภัยที่ทราบ

๗) การทดสอบความมั่นคงปลอดภัยอย่างเป็นระบบ รวมถึงการทดสอบซึ่งเป็นการแทรกแซงการเข้าถึงการสแกนช่องโหว่

การออกแบบเว็บไซต์ที่มีความมั่นคงปลอดภัยเป็นขั้นตอนสำคัญในการพัฒนาเว็บไซต์ เพราะเป็นการป้องกันการโจมตีและการขโมยข้อมูลที่อาจเกิดขึ้น ควรพิจารณามาตรการป้องกันการโจมตีที่เข้มงวด เพื่อป้องกันภัยคุกคามทางไซเบอร์ต่าง ๆ เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ XSS และการโจมตี CSRF ซึ่งอาจทำให้ข้อมูลลูกค้าหรือข้อมูลที่สำคัญถูกขโมยหรือเปิดเผย หน่วยงานอาจจะพิจารณาแนวทางตัวอย่างในการออกแบบเว็บไซต์ที่มีความมั่นคงปลอดภัย ดังนี้

๑) การใช้ HTTPS เพื่อเข้ารหัสข้อมูลที่ถูกส่งระหว่างเครื่องบริการเว็บและผู้ใช้งาน

๒) การใช้กลไกการรับรองตัวตนสองขั้นตอน (Two-Factor Authentication) หรือการรับรองตัวตนหลายขั้นตอน (Multi-Factor Authentication) เพื่อเพิ่มความมั่นคงปลอดภัยในการเข้าถึงข้อมูล

๓) การตรวจสอบและวางแผนการป้องกันการโจมตีอย่างเป็นระบบ โดยใช้ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก IDS/ IPS หรือเครื่องมือตรวจสอบช่องโหว่ (Vulnerability Assessment Tool) เพื่อตรวจสอบและป้องกันการโจมตีต่าง ๆ ที่เป็นไปได้

๔) การเลือกใช้ Web Application Framework ที่มีความมั่นคงปลอดภัย

หลักการ DevSecOps

หลักการ DevSecOps เป็นแนวคิดในการผสานการพัฒนาซอฟต์แวร์ (Dev) ความมั่นคงปลอดภัย (Sec) และการดำเนินงาน (Ops) เข้าด้วยกันอย่างรวดเร็วและต่อเนื่อง โดยเน้นการสร้างซอฟต์แวร์ที่มีความมั่นคงปลอดภัยอย่างเร็วและมั่นคงตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งานจริง หลักการนี้ทำให้ทีมพัฒนาซอฟต์แวร์มีความรับผิดชอบต่อความมั่นคงปลอดภัยเป็นส่วนหนึ่งของกระบวนการ พัฒนาและการดำเนินงานทุกขั้นตอน หน่วยงานอาจจะพิจารณาแนวทางตัวอย่างในการปรับใช้หลักการ DevSecOps ดังนี้

๑) ทีมพัฒนาซอฟต์แวร์อาจใช้เครื่องมือการทดสอบความมั่นคงปลอดภัยในขั้นตอนการพัฒนาเพื่อตรวจสอบช่องโหว่และบั๊กของโค้ดอย่างเป็นระบบ

๒) ทีมพัฒนายังสามารถนำหลักการ Infrastructure as Code (IaC) มาใช้เพื่อสร้างและบริหารจัดการสถาปัตยกรรมของระบบที่มีความมั่นคงปลอดภัยอย่างมั่นคงและเป็นระบบ

๓) การใช้หลักการ Continuous Integration (CI) และ Continuous Deployment (CD) เป็นส่วนหนึ่งของการใช้ DevSecOps ที่ช่วยให้การพัฒนาซอฟต์แวร์และปรับปรุงระบบเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ

หน่วยงานอาจจะพิจารณาถึงการใช้หลักการ DevSecOps Maturity Model (DSOMM) ของมูลนิธิ OWASP (๔๓) มาใช้เพื่อวัดระดับวุฒิภาวะในการประยุกต์ใช้หลักการ DevSecOps ในการพัฒนาเว็บไซต์ให้มีความมั่นคงปลอดภัยในแต่ละมิติ ประกอบด้วย พัฒนาและการปรับใช้ (Build and Deployment) วัฒนธรรมและองค์กร (Culture and Organization) การนำไปปฏิบัติ (Implementation) การรวบรวมข้อมูล (Information Gathering) การทดสอบและการตรวจสอบ (Test and Verification)

ข้อ ๖.๒.๒ รายละเอียดปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อยของ OWASP

มูลนิธิ OWASP ซึ่งเป็นมูลนิธิที่ต้องการส่งเสริมความมั่นคงปลอดภัยที่เกี่ยวข้องกับการพัฒนาและใช้งานแอปพลิเคชัน ได้มีการรวบรวมและเผยแพร่ปัจจัยเสี่ยงทางความมั่นคงปลอดภัยของเว็บแอปพลิเคชันที่พบได้บ่อย ๑๐ อันดับแรก ซึ่งหน่วยงานสามารถพิจารณานำไปใช้ประโยชน์ในการพัฒนาแอปพลิเคชันบนเว็บไซต์เพื่อให้มีความมั่นคงปลอดภัย

ข้อ ๖.๒.๓ การออกแบบสถาปัตยกรรมเว็บไซต์อย่างมั่นคงปลอดภัย

ออกแบบโครงสร้างเว็บไซต์โดยการเชื่อมต่อ Front End, Back End, Database, Reverse Proxy

การเชื่อมต่อระหว่างส่วนหน้า (Front End) ส่วนหลัง (Back End) ฐานข้อมูล (Database) และ พร็อกซีย้อนกลับ (Reverse Proxy) เป็นส่วนสำคัญในโครงสร้างของเว็บไซต์หรือแอปพลิเคชันเพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพและเป็นระบบ โดยหน่วยงานอาจจะพิจารณาออกแบบโครงสร้างเว็บไซต์ ดังนี้

๑) ส่วนหน้า (Front End) เป็นส่วนที่ผู้ใช้งานสามารถเห็นและปฏิสัมพันธ์กับเว็บไซต์ได้ ซึ่งประกอบด้วย องค์ประกอบที่แสดงผลบนหน้าจอของผู้ใช้ เช่น หน้า HTML CSS และ JavaScript

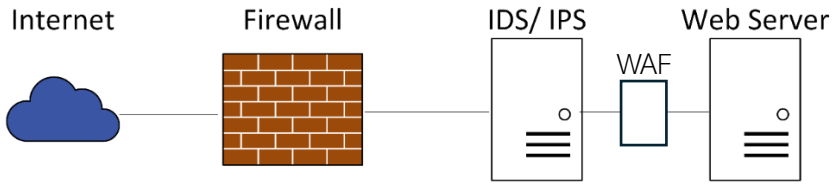
๒) ส่วนหลัง (Back End) เป็นส่วนที่ดูแลการประมวลผลและการจัดการข้อมูลของเว็บไซต์ โดยทำหน้าที่รับคำขอจากส่วนหน้า เพื่อการประมวลผล และส่งข้อมูลกลับไปยังส่วนหน้า รวมถึงการจัดการธุรกรรมกับฐานข้อมูล

๓) ฐานข้อมูล (Database) เป็นส่วนที่ใช้เก็บข้อมูลที่จำเป็นสำหรับการทำงานของเว็บไซต์หรือแอปพลิเคชัน เช่น ข้อมูลผู้ใช้ ข้อมูลสินค้า หรือข้อมูลการทำธุรกรรม

๔) พร็อกซีย้อนกลับ (Reverse Proxy) เป็นเทคโนโลยีที่ใช้เป็นตัวกลางในการจัดการและกระจายการร้องขอ (Requests) จากฝั่งผู้ใช้งาน (Client) ไปยังฝั่งเครื่องคอมพิวเตอร์แม่ข่าย (Server) (เครื่องบริการเว็บ) โดยช่วยเพิ่มประสิทธิภาพและความมั่นคงปลอดภัยในการให้บริการข้อมูลจากเว็บไซต์หรือแอปพลิเคชัน โดยสามารถใช้งานร่วมกับส่วนหลังและฐานข้อมูลได้เพื่อการจัดการและควบคุมการเข้าถึงข้อมูลอย่างมีประสิทธิภาพ

การวางเครื่องบริการเว็บ (Web Server) ร่วมกับอุปกรณ์ป้องกันความมั่นคงปลอดภัย

การวางเครื่องบริการเว็บและอุปกรณ์ป้องกันความมั่นคงปลอดภัยอื่น ๆ ในระบบเครือข่ายสื่อสารข้อมูลเป็นขั้นตอนสำคัญในการสร้างและรักษาพื้นที่ทำงานของเว็บไซต์หรือแอปพลิเคชันให้ปลอดภัย โดยการวางอุปกรณ์เหล่านี้ในตำแหน่งที่เหมาะสมภายในโครงสร้างของเครือข่ายเพื่อป้องกันการบุกรุกและความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นจากภัยคุกคามภายนอก ตัวอย่างเช่น อุปกรณ์ที่วางเข้าใช้ในการป้องกันความมั่นคงปลอดภัย เช่น ไฟร์วอลล์ (Firewall) ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก IDS/IPS และการให้บริการป้องกัน Web Application (WAF) สามารถจัดเป็นอุปกรณ์ที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายได้ โดยการตั้งค่าและวางอุปกรณ์เหล่านี้ให้เข้ากับโครงสร้างเครือข่ายอย่างเหมาะสม เพื่อให้สามารถตรวจจับและป้องกันการโจมตีได้อย่างมีประสิทธิภาพ ส่วนเครื่องบริการเว็บถือเป็นส่วนสำคัญที่รับผิดชอบในการให้บริการเนื้อหาและแอปพลิเคชันที่ถูกต้องต่อผู้ใช้งาน โดยมีความสำคัญที่จะติดตั้งและปรับแต่งเครื่องบริการเว็บเพื่อให้มีความเสถียรและปลอดภัยในการให้บริการ หน่วยงานอาจจะพิจารณาตัวอย่างการวางเครื่องบริการเว็บร่วมกับอุปกรณ์ความมั่นคงปลอดภัยเป็นอย่างน้อยดังแสดงในภาพที่ ข๑



ภาพที่ ข๑ การวางเครื่องบริการเว็บและอุปกรณ์ป้องกันความมั่นคงปลอดภัย

อุปกรณ์และบริการการรักษาความมั่งคงปลอดภัยพื้นฐาน

๑) ไฟร์วอลล์ (Firewall) เป็นเทคโนโลยีที่ใช้ในการป้องกันความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์ โดยการควบคุมและกรองการเข้าถึงข้อมูลที่เข้ามาหรือออกจากเครือข่าย เพื่อป้องกัน

การบุกรุกจากผู้ไม่ประสงค์ดี หรือการเข้าถึงที่ไม่ได้รับอนุญาตในเครือข่าย ไฟร์วอลล์จะทำหน้าที่เป็นกำแพงป้องกันระหว่างเครือข่ายภายในกับเครือข่ายภายนอก โดยตรวจสอบและบล็อกการเข้าถึงที่มีภาพลักษณ์ของการโจมตี หรือข้อมูลที่ไม่พึงประสงค์ โดยไฟร์วอลล์สามารถกำหนดกฎ (Rule) หรือนโยบายในการทำงานเพื่อป้องกันการบุกรุกจากภายนอก โดยตรวจจับและบล็อกการเข้าถึงที่มีความเสี่ยงได้ เช่น การโจมตีด้วยวิธีการหรือการเข้าถึงที่มิชอบด้วยการสแกนพอร์ต (Port Scanning) หรือการโจมตีด้วยการเข้าถึงที่ไม่เกี่ยวข้องด้วยการบล็อก IP ที่ไม่ได้รับอนุญาต การใช้ไฟร์วอลล์เป็นวิธีที่มีประสิทธิภาพในการป้องกันเครือข่ายจากการโจมตีต่าง ๆ และเป็นเครื่องมือสำคัญที่ช่วยให้เครือข่ายมีความมั่นคงปลอดภัยและป้องกันข้อมูลสำคัญของหน่วยงานไม่ให้ถูกเข้าถึงหรือโจมตีโดยผู้ไม่ประสงค์ดี

๒) ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก (Intrusion Detection Systems: IDS/Intrusion Prevention Systems: IPS) เป็นเทคโนโลยีที่ใช้ในการตรวจสอบและป้องกันความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์ โดยการตรวจจับและตอบสนองต่อพฤติกรรมที่เป็นอันตรายบนเครือข่าย ระบบตรวจจับการบุกรุก IDS มีหน้าที่ตรวจจับการกระทำที่มีความเสี่ยงหรือเป็นอันตรายบนเครือข่าย เช่น การสแกนพอร์ต (Port Scanning) การใช้งานช่องโหว่ (Exploits) หรือการโจมตีด้วยวิธีการอื่น ๆ โดย IDS จะทำหน้าที่แจ้งเตือนผู้ดูแลระบบเมื่อพบการกระทำที่เป็นอันตราย ส่วนระบบป้องกันการบุกรุก IPS มีหน้าที่ตรวจจับการบุกรุกและป้องกันการกระทำที่เป็นอันตรายโดยตรง ด้วยการบล็อกหรือตัดการเชื่อมต่อของผู้ไม่พึงประสงค์หรืออุปกรณ์ที่มีพฤติกรรมที่เป็นอันตราย เช่น การบล็อก IP address ที่มีลักษณะการโจมตี การบล็อกการเข้าถึงช่องโหว่ ช่วยลดความเสี่ยงในการสูญหายของข้อมูลหรือการเข้าถึงที่ไม่เหมาะสมในเครือข่าย

๓) การให้บริการป้องกัน Web Application (Web Application Firewall: WAF) เป็นเทคโนโลยีที่ใช้ในการป้องกันการโจมตีที่เป็นอันตรายต่อเว็บแอปพลิเคชัน โดยระบบนี้ทำหน้าที่ในการตรวจสอบและกรองข้อมูลที่มีการส่งผ่านมายังเว็บแอปพลิเคชัน เพื่อป้องกันการโจมตีที่อาจก่อให้เกิดความเสียหาย หรือการขโมยข้อมูล การให้บริการป้องกัน WAF จะมีความสามารถในการตรวจจับ และป้องกันการโจมตีต่าง ๆ ที่เป็นที่รู้จัก เช่น การโจมตีแบบ SQL Injection การโจมตีแบบ XSS การโจมตีแบบ CSRF และอื่น ๆ โดยการเปรียบเทียบข้อมูลที่ส่งผ่านมากับกฎหรือรูปแบบที่เป็นไปได้ของการโจมตี และบล็อกหรือจำกัดการเข้าถึงข้อมูลที่มีความเสี่ยง ดังนั้น การใช้บริการป้องกัน Web Application (WAF) เป็นส่วนสำคัญในการปกป้องเว็บแอปพลิเคชันจากการโจมตีและการหลอกลวง โดยช่วยลดความเสี่ยงในการสูญหายของข้อมูล การรั่วไหลของข้อมูล หรือการโจมตีที่เกิดขึ้นจากช่องโหว่ที่ไม่ได้รับการคาดหวัง นอกจากนี้ยังช่วยให้ผู้ดูแลระบบมีความสามารถในการตรวจจับและระบุการโจมตีอย่างรวดเร็วและมีประสิทธิภาพ

ผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยที่แนะนำเพิ่มเติม

๑) ระบบการจัดการเหตุการณ์และตอบสนองด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) เป็นเทคโนโลยีที่ใช้ในการรวบรวม การวิเคราะห์และการรายงานเหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่าย เพื่อตรวจจับและตอบสนองต่อความเสี่ยงหรือการบุกรุกต่าง ๆ ที่อาจเกิดขึ้น SIEM มุ่งเน้นไปที่การรวบรวมข้อมูลจากแหล่งต่าง ๆ

เช่น เหตุการณ์จากเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และแอปพลิเคชัน จากนั้น ระบบ SIEM จะทำการวิเคราะห์ข้อมูลเหล่านี้ เพื่อตรวจจับรูปแบบที่เป็นไปได้ของการโจมตี และให้การแจ้งเตือนแก่ผู้ดูแลระบบเมื่อพบความเสี่ยง หรือการเกิดเหตุการณ์ที่น่าสนใจ ระบบ SIEM มักมีความสามารถในการจัดการเหตุการณ์และตอบสนองต่อความเสี่ยง รวมถึงการสร้างรายงานเพื่อการวิเคราะห์และการสืบค้นข้อมูล ทำให้ผู้ดูแลระบบสามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ ช่วยให้หน่วยงานมีความมั่นคงปลอดภัยและสามารถตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพ

๒) ระบบ Extended Detection and Response หรือ XDR เป็นแนวคิดใหม่ในด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ซึ่งเน้นการรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์ในบริษัท และนำข้อมูลเหล่านี้มาวิเคราะห์เพื่อตรวจจับและตอบสนองต่อการโจมตีที่เกิดขึ้น ระบบ XDR มุ่งเน้นไปที่การรวบรวมข้อมูลจากแหล่งต่าง ๆ เพื่อสร้างมุมมองที่ครอบคลุมและลึกซึ้งของสถานการณ์ความมั่นคงปลอดภัย ทำให้ผู้ดูแลระบบสามารถตรวจจับการโจมตีที่มีรูปแบบซับซ้อนและความหลากหลายได้อย่างมีประสิทธิภาพ การใช้ระบบ XDR จะช่วยให้หน่วยงานมีความสามารถในการตรวจจับและตอบสนองต่อการโจมตีที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ ทำให้หน่วยงานค้นหาและแก้ไขปัญหาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพมากยิ่งขึ้น และช่วยลดความเสี่ยงในการเกิดความเสียหาย หรือสูญหายของข้อมูลสำคัญของหน่วยงาน

๓) Security Orchestration, Automation, and Response หรือ SOAR เป็นแนวคิดและเทคโนโลยีเพื่อการทำงานอัตโนมัติ และการรวมกลุ่มขั้นตอนการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัย เพื่อเพิ่มประสิทธิภาพและความรวดเร็วในการจัดการกับการละเมิดความมั่นคงปลอดภัยของเครือข่ายและระบบสารสนเทศ โดย SOAR มุ่งเน้นที่การรวมกลุ่ม และการประสานงานระหว่างกระบวนการต่าง ๆ ทำให้ผู้ดูแลระบบสามารถตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ โดยมีความสามารถในการประมวลผลข้อมูลการรายงานเหตุแบบอัตโนมัติ ทำให้การดำเนินการที่เกี่ยวข้องกับการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยเป็นไปอย่างมีระบบ การใช้ SOAR ทำให้หน่วยงานตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ลดภาระงานที่ต้องอาศัยมนุษย์ ทำให้หน่วยงานสามารถระบุ และการป้องกันการละเมิดความมั่นคงปลอดภัยของเครือข่ายและระบบสารสนเทศได้อย่างมีประสิทธิภาพ

<u>ข้อ ๖.๒.๔</u> การควบคุมการเข้าถึง (Access Control)

การกำหนดบทบาทและสิทธิ์การใช้งาน

บทบาทและสิทธิ์ในการควบคุมการเข้าถึงเป็นส่วนสำคัญในการจัดการความมั่นคงปลอดภัยของเว็บไซต์ โดยการกำหนดบทบาทและสิทธิ์ให้แก่ผู้ใช้แต่ละคนเพื่อให้ได้รับการเข้าถึงข้อมูลและทรัพยากรในระบบที่เหมาะสม เช่น เจ้าหน้าที่ด้านการเงินอาจมีสิทธิ์ในการเข้าถึงข้อมูลทางการเงิน ในขณะที่เจ้าหน้าที่ด้านการตลาดอาจมีสิทธิ์ในการเข้าถึงข้อมูลเกี่ยวกับการตลาดและ การส่งเสริมการตลาด ตัวอย่างเช่น ในระบบบริษัท XYZ มีการกำหนดบทบาทและสิทธิ์ให้แก่พนักงานแต่ละคน โดยเจ้าหน้าที่ด้านการเงินได้รับสิทธิ์การเข้าถึงและแก้ไขข้อมูลทางการเงินเท่านั้น ในขณะที่เจ้าหน้าที่

ด้านการตลาดมีสิทธิ์ในการอ่านข้อมูลเกี่ยวกับการตลาดและการส่งเสริมการตลาด แต่ไม่สามารถแก้ไขข้อมูลได้ ดังนั้นเมื่อมีการเข้าถึงระบบ ระบบจะต้องตรวจสอบบทบาทของผู้ใช้และให้สิทธิ์ที่เหมาะสมตามบทบาทที่กำหนดไว้ ทำให้มีการควบคุมการเข้าถึงข้อมูลและทรัพยากรในระบบอย่างมั่นคงและปลอดภัย

การกำหนดและรักษารหัสผ่าน

การกำหนดค่าและการรักษารหัสผ่านเป็นส่วนสำคัญในการควบคุมการเข้าถึงในระบบสารสนเทศ เนื่องจากรหัสผ่านเป็นองค์ประกอบสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบที่เปิดใช้งาน การกำหนดค่ารหัสผ่านที่มีความมั่นคงปลอดภัยและมีการป้องกันอย่างเหมาะสม จะช่วยลดความเสี่ยงจากการโจมตีและการขโมยข้อมูล โดยหน่วยงานอาจจะพิจารณาการดำเนินการกำหนดและรักษารหัสผ่าน ดังนี้

(๑) กำหนดข้อกำหนดในการสร้างรหัสผ่าน ระบบสามารถกำหนดข้อกำหนดเกี่ยวกับความยาวของรหัสผ่าน โดยหน่วยงานอาจจะพิจารณาอ้างอิงตามเอกสาร NIST SP 800-63B (๔๔)

(๒) การใช้เทคโนโลยีการเข้ารหัส ระบบสามารถใช้เทคโนโลยีการเก็บค่า Hash ของรหัสผ่านแทนการเก็บรหัสผ่านจริงในฐานข้อมูล และใช้โพรโทคอล HTTPS เพื่อรักษาความมั่นคงปลอดภัยขณะส่งข้อมูลรหัสผ่านผ่านเครือข่าย

(๓) การตั้งค่าการรักษาความมั่นคงปลอดภัย หน่วยงานจะต้องบังคับให้เปลี่ยนรหัสผ่านหากมีหลักฐานการถูกเจาะข้อมูล หรือขโมยข้อมูล

(๔) ขั้นตอนการเปลี่ยนรหัสผ่านควรเป็นขั้นตอนที่ปลอดภัย เช่น มีการส่งอีเมลเพื่อยืนยันตัวตนไปยังผู้ใช้งาน และยอมให้เปลี่ยนรหัสผ่านก็ต่อเมื่อมีการพิสูจน์ว่าผู้ใช้งานเข้าถึงอีเมลได้จริง

(๕) การเปลี่ยนรหัสผ่านควรเพิ่มขั้นตอนการยืนยันตัวตนเพื่อระบุได้ว่าไม่ใช่การใช้โปรแกรมอัตโนมัติ เช่น การใช้ CAPTCHA กรณีที่มีการเปลี่ยนแปลงข้อมูล โดยจะมีรูปภาพให้กรอกหรือเลือกในช่องยืนยันตัวตน

(๖) ตั้งค่า Session Lock เมื่อไม่มีการใช้งานเกิน ๑๕ นาทีหรือน้อยกว่า (๔๕)

(๗) ป้องกันการโจมตีแบบ Brute Force ด้วยการตั้งค่าให้จำกัดจำนวนครั้งที่ล็อกอินผิด เช่น เมื่อล็อกอินผิดต่อเนื่องเกิน ๕ ครั้ง ให้ระงับการใช้งานบัญชีนั้นชั่วคราว (อย่างน้อย ๑๕ นาที) รวมถึงตั้งค่าให้มีการแจ้งเตือนผู้ดูแลระบบเมื่อมีการล็อกอินผิดพลาดเกินจำนวนครั้งที่กำหนด

(๘) หากบัญชีใดที่ไม่มีการล็อกอินเกิน ๔๕ วัน หรือพิจารณาตามความเหมาะสมของหน่วยงาน ควรตั้งค่าให้ระงับการใช้งานบัญชีนั้นโดยอัตโนมัติ

การตั้งค่ารหัสผ่านใหม่

การตั้งรหัสผ่านใหม่หรือการต่ออายุรหัสผ่านในการควบคุมการเข้าถึงเป็นส่วนสำคัญในการรักษาความมั่นคงปลอดภัยของระบบ โดยรหัสผ่านที่มีอายุยืนยาวอาจเสี่ยงต่อการถูกโจมตีและการเข้าถึงอย่างไม่พึงประสงค์ ดังนั้น การต่ออายุรหัสผ่านเป็นกระบวนการที่สำคัญในการบริหารจัดการรหัสผ่านอย่างปลอดภัย ตัวอย่างเช่น

(๑) การตั้งค่านโยบายรหัสผ่าน โดยกำหนดให้ระบบอนุญาตให้รหัสผ่านมีความยาวสูงสุดอย่างน้อย ๖๔ ตัวอักษร และต้องเปลี่ยนรหัสผ่านทุกครั้งที่มีหลักฐานว่ารหัสผ่านรั่วไหล (๔๔)

(๒) การตั้งค่าให้ยอมรับอักขระ ASCII [RFC20] ที่สามารถพิมพ์ได้ทุกตัวและอักขระช่องว่างในรหัสผ่าน (๔๔)

(๓) การตั้งค่าควรตรวจสอบว่ารหัสผ่านที่ผู้ใช้ตั้งนั้นไม่ตรงกับรายการรหัสผ่านที่เคยรั่วไหลมาก่อนหน้านี้ และไม่ซ้ำกับรหัสผ่าน ๕ ชุดล่าสุดที่ผู้ใช้เคยตั้งมาแล้วก่อนหน้านี้ (๔๕)

(๔) การตั้งรหัสใหม่ควรเพิ่มขั้นตอนการยืนยันตัวตนเพื่อระบุได้ว่าไม่ใช่การใช้โปรแกรมอัตโนมัติ เช่น การใช้ CAPTCHA กรณีที่มีการเปลี่ยนแปลงข้อมูล โดยจะมีรูปภาพให้กรอกหรือเลือกในช่องยืนยันตัวตน

ข้อ ๖.๒.๕ การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือการพิสูจน์ตัวตนจากระบบเชื่อมโยงข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

หน่วยงานควรจะกำหนดให้ใช้การยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ระบบ ThaID (ไทยดี) หรือหน่วยงานอาจจะพิจารณาใช้งาน MFA ในลักษณะอื่นในการเพิ่มความมั่นคงปลอดภัยให้กับระบบงาน ซึ่งใช้การพิสูจน์ตัวตนก่อนที่จะมีการเข้าถึงทรัพยากรและระบบที่สำคัญ เป็นการตรวจสอบตัวตนของผู้ใช้งานโดยใช้ปัจจัยที่แตกต่างกันมากกว่าหนึ่งปัจจัย ประกอบด้วย สิ่งที่ผู้ใช้รู้ (Something they know) เช่น รหัสผ่าน สิ่งที่ผู้ใช้มี (Something they have) เช่น โทเค็นการตรวจสอบ หรือสิ่งที่ผู้ใช้เป็น (Something they are) เช่น ลายนิ้วมือ ลายฝ่ามือ หรือข้อมูลชีวมิติอื่น

หน่วยงานอาจจะพิจารณาตัวอย่างการใช้งาน MFA ดังนี้

(๑) การใช้รหัสผ่านและโทเค็น ผู้ใช้จะต้องป้อนรหัสผ่านที่ถูกต้องและยังต้องใช้โทเค็นการตรวจสอบที่ส่งไปยังโทรศัพท์มือถือหรืออุปกรณ์อื่น ๆ เพื่อรับรหัสยืนยันเพิ่มเติม

(๒) การใช้รหัสผ่านและลายนิ้วมือ ผู้ใช้จะต้องป้อนรหัสผ่านและใช้สแกนลายนิ้วมือเพื่อพิสูจน์และยืนยันตัวตน

(๓) การใช้รหัสผ่านและตรวจสอบใบหน้า ผู้ใช้จะต้องป้อนรหัสผ่านและต้องให้ระบบทำการตรวจสอบใบหน้าเพื่อพิสูจน์และยืนยันตัวตน

ข้อ ๖.๒.๖ การตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐาน

การตั้งค่าระบบปฏิบัติการ (Operating System)

หน่วยงานอาจจะพิจารณาคำแนะนำของ NIST SP 800-123 (๔๖) เพื่อการตั้งค่าความมั่นคงปลอดภัยของระบบปฏิบัติการเบื้องต้นที่สามารถนำไปประยุกต์ใช้กับระบบปฏิบัติการทุกประเภท โดยแบ่งออกเป็น ๓ ส่วน ดังนี้

๑) การถอนการติดตั้งส่วนของบริการ ซอฟต์แวร์ โพรโทคอลเครือข่าย และอื่นๆ ที่ยังไม่มีความจำเป็นต้องใช้งานออก โดยมีแนวปฏิบัติ คือ เมื่อเริ่มการติดตั้งระบบปฏิบัติการให้ติดตั้งในขั้นต่ำที่สุดให้เพียงพอต่อการตั้งค่าและปรับแต่งระบบเว็บไซต์แล้ว ค่อยติดตั้งส่วนของบริการอื่นที่ต้องการใช้งานเพิ่มเติมเท่าที่จำเป็น และหมั่นตรวจสอบและถอนการติดตั้งส่วนของบริการอื่นที่ไม่มีความจำเป็นต้องใช้งานออกหรือปิดการใช้งานหากไม่สามารถถอนการติดตั้งได้

๒) การตั้งค่าการยืนยันตัวตนของผู้ใช้งาน ดังนี้

(๑) ลบหรือปิดการใช้งานบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งในครั้งแรก

(๒) ปิดการใช้งานบัญชีผู้ใช้งานที่จำเป็นต้องมีในระบบแต่ยังไม่มีความจำเป็นต้องลงชื่อเข้าใช้งาน

(๓) สร้างกลุ่มของบัญชีผู้ใช้งานที่มีความสามารถในการเข้าถึงที่เหมาะสมและตรงกับหน้าที่ความรับผิดชอบ

(๔) สร้างบัญชีผู้ใช้งานเท่าที่จำเป็นและหลีกเลี่ยงการเปิดให้ใช้งานบัญชีผู้ใช้งานร่วมกัน

(๕) ตั้งค่าการตั้งเวลา (Time Synchronization) ให้ตรงกับ Time Server ที่เหมาะสมแบบอัตโนมัติ

(๖) ตั้งค่าข้อกำหนดของรหัสผ่านตามนโยบายการตั้งรหัสผ่านของหน่วยงาน

(๗) ตั้งค่าเพื่อป้องกันการเดารหัสผ่าน เช่น การตั้งค่าให้มีการหน่วงเวลาระหว่างการป้อนรหัสผ่านแต่ละครั้ง

(๘) ติดตั้งระบบการยืนยันตัวตนเพิ่มเติมที่จำเป็น เช่น ระบบตรวจสอบข้อมูลชีวมิติเพื่อการยืนยันตัวตน

๓) การตั้งค่าการควบคุมทรัพยากรอย่างเหมาะสม เช่น การตั้งค่าสิทธิ์ในการเข้าถึง สิทธิ์ในการเปลี่ยนแปลง และสิทธิ์ในการใช้งานทรัพยากรที่แตกต่างกันของผู้ใช้งานแต่ละประเภท และมีการสร้างสิ่งแวดล้อมเสมือน (Sandbox) สำหรับบางบริการ

หน่วยงานอาจจะพิจารณาการตั้งค่าเพื่อความมั่นคงปลอดภัยของแต่ละระบบปฏิบัติการ โดยสามารถศึกษาเพิ่มเติมได้จาก Security Technical Implementation Guides (STIGS) ของกระทรวงกลาโหมของสหรัฐอเมริกา (๔๗) และ CIS Benchmark ของบริษัท Center for Internet Security (CIS) (๔๘)

การตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software)

การตั้งค่าโปรแกรมสำหรับให้บริการเว็บเป็นกระบวนการที่สำคัญในการเริ่มต้นใช้งานเครื่องบริการเว็บ เมื่อทำการตั้งค่าโปรแกรมสำหรับให้บริการเว็บอย่างถูกต้องและเหมาะสมกับความต้องการของเว็บไซต์ จะช่วยให้การทำงานของเว็บไซต์เป็นไปอย่างมีประสิทธิภาพและปลอดภัยมากยิ่งขึ้น ตัวอย่างเช่น กำหนดค่าต่าง ๆ เช่น การกำหนดค่าพอร์ต (Port) การกำหนดค่าโฮสต์ (Host) และการกำหนดค่าการเชื่อมต่อฐานข้อมูล รวมถึงการใช้ Official Software ให้ปฏิบัติตามคำแนะนำเฉพาะของซอฟต์แวร์นั้นๆ เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ

หน่วยงานอาจจะพิจารณาการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บตาม CIS Benchmark (๔๘) ดังนี้

๑) การติดตั้งโปรแกรมสำหรับให้บริการเว็บให้ติดตั้งเวอร์ชันล่าสุด ตั้งค่าการอัปเดตให้มีการอัปเดตเป็นปัจจุบันอยู่เสมอ และเปิดการใช้งานเฉพาะโมดูลที่เกี่ยวข้องและจำเป็นกับการให้บริการเว็บไซต์เท่านั้น

๒) บัญชีการเข้าใช้งาน ควรเป็นบัญชีบริการที่ไม่สามารถถูกลงชื่อเข้าใช้โดยบุคคลอื่นได้ โดยให้มีการจำกัดสิทธิการใช้งานอยู่เฉพาะแค่โปรแกรมสำหรับให้บริการเว็บ

๓) ความเป็นเจ้าของและการอนุญาต ให้ Root หรือ Administrator เป็นเจ้าของแฟ้มและเอกสารของโปรแกรมสำหรับให้บริการเว็บ และมีการจำกัดสิทธิการเข้าถึง

๔) การตั้งค่าเครือข่าย ให้เชื่อมต่อกับพอร์ตที่จำเป็นต้องใช้งานในการให้บริการเว็บไซต์เท่านั้น และมีการตั้งค่า timeout เพื่อป้องกันการโจมตีประเภท DoS เช่น ค่าระยะเวลาการรักษาการติดต่อ (keep alive) ควรมีค่ามากกว่า ๐ และต่ำกว่า ๑๐ วินาที

๕) การปกปิดข้อมูล โดยพยายามลดการเปิดเผยข้อมูลจากการเชื่อมต่อ เช่น ข้อความแสดงโปรแกรมสำหรับให้บริการเว็บ และระบบปฏิบัติการที่ใช้งาน เช่น ปิดการแสดงค่ารายละเอียดของระบบกรณีที่มีปัญหาในการให้บริการเว็บไซต์

๖) การบันทึกการใช้งาน มีการตั้งค่าให้มีการบันทึกโดยละเอียดเกี่ยวกับการเข้าใช้งานและข้อผิดพลาดที่เกิดขึ้น

๗) การเข้ารหัสข้อมูล โดยให้มีการใช้งานโพรโทคอล HTTPS และ TLS เวอร์ชันล่าสุด โดยจะต้องมีการส่งต่อการติดต่อจากโพรโทคอล HTTP ไปยังโพรโทคอล HTTPS

๘) การกรองและจำกัดคำขอ โดยจำกัด IP ที่รับคำขอและจำกัดลักษณะของคำขอ เช่น ค่า timeout และความยาวของบัฟเฟอร์

การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS)

การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS) เป็นส่วนสำคัญในการดำเนินการเพื่อความมั่นคงปลอดภัย สำหรับการป้องกันการโจมตีจากภายนอกและป้องกันข้อมูลรั่วไหล หน่วยงานอาจจะพิจารณาหลักการที่สำคัญที่ต้องตั้งค่าระบบ CMS เพื่อเพิ่มความมั่นคงปลอดภัย

๑) แนวทางการใช้ส่วนเสริม (Plugin) อย่างมั่นคงปลอดภัย

การใช้ส่วนเสริมหรือปลั๊กอิน (Plugin) ใน CMS เป็นปัจจัยสำคัญที่ต้องพิจารณาอย่างรอบคอบ เพื่อป้องกันการโจมตีและไม่ให้เกิดข้อบกพร่องด้านความมั่นคงปลอดภัย ซึ่งส่วนเสริมที่มีให้บริการจำนวนมากอาจมีช่องโหว่ ภายหลังจากการสนับสนุนของผู้ให้บริการส่วนเสริมหยุดลง ดังนั้น การใช้งานส่วนเสริมหน่วยงานต้องให้ความสำคัญและมีความระมัดระวังในการใช้งาน โดยหน่วยงานอาจจะพิจารณาส่วนเสริมสำหรับความมั่นคงปลอดภัยของเว็บไซต์เป็นเครื่องมือที่ช่วยเสริมความมั่นคงปลอดภัยให้กับเว็บไซต์โดยเฉพาะ โดยการเพิ่มความสามารถพิเศษ หรือเพิ่มชั้นความมั่นคงปลอดภัยที่มีอยู่แล้วให้มีประสิทธิภาพในการตรวจสอบและป้องกันการภัยคุกคามอย่างมีประสิทธิภาพ ตัวอย่างส่วนเสริมที่น่าสนใจสำหรับความมั่นคงปลอดภัยของเว็บไซต์ ได้แก่ "Wordfence Security" สำหรับ WordPress ซึ่งมีความสามารถในการตรวจสอบและป้องกันการโจมตีต่าง ๆ ที่เป็นที่รู้จัก เช่น การโจมตีแบบ XSS การโจมตีแบบ SQL Injection และการบุกรุกแบบ brute force ร่วมกับการตรวจสอบไฟล์ที่เสี่ยงต่อภัยคุกคาม และการจัดการระดับความมั่นคงปลอดภัยของรหัสผ่านผู้ใช้งาน ทำให้ผู้ดูแลระบบสามารถป้องกัน และตรวจจับการละเมิดความมั่นคงปลอดภัยของเว็บไซต์ได้อย่างมีประสิทธิภาพ

๒) แนวทางการซ่อนหน้า Login

หน่วยงานอาจจะพิจารณาเปลี่ยนลิงก์ login ของเว็บไซต์จากค่า default เช่น aaa.go.th/wp-login.php ไปเป็นค่าอื่น เนื่องจากเป็นการป้องกันผู้ไม่หวังดีเข้ามาโจมตีหน้า Login ของเว็บไซต์ได้ โดยสามารถใช้ส่วนเสริม เช่น WPS hide login เป็นต้น

๓) การทำให้ CMS มีความแข็งแกร่ง (CMS Hardening)

การตั้งค่าความมั่นคงปลอดภัยให้กับระบบ CMS ของ Wordpress สามารถศึกษาได้จาก Developer Resource ของ Wordpress[๕] และระบบ CMS ของ Joomla สามารถศึกษาได้จากเว็บไซต์ Joomla! Documentation[๖] และระบบ CMS รายอื่น สามารถศึกษาได้จากเว็บไซต์ของระบบ CMS นั้นๆ โดยสามารถปรับให้เหมาะกับความต้องการ และสภาพแวดล้อมของแต่ละหน่วยงาน

การตั้งค่าโปรแกรมประยุกต์บนเว็บ

หน่วยงานควรจะตั้งค่าความมั่นคงปลอดภัยให้กับโปรแกรมประยุกต์บนเว็บ ตามหัวข้อที่ ๔ ของเอกสารข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (๒๗) โดยหน่วยงานอาจจะพิจารณาตัวอย่างการตั้งค่า เช่น การจัดทำ Prepared Statement และ/หรือ Store Procedure เพื่อป้องกันการโจมตีประเภท SQL Injection และการทำ Output Validation ในลักษณะ Sanitization เพื่อป้องกันการโจมตีประเภท XSS

ทั้งนี้ หากหน่วยงานต้องการตรวจสอบการตั้งค่าความมั่นคงปลอดภัยของโปรแกรมประยุกต์บนเว็บ หน่วยงานอาจจะพิจารณาใช้รายการตรวจสอบโปรแกรมประยุกต์บนเว็บของโครงการ Open Web Application Security Project (OWASP) ที่จัดตั้งโดย มูลนิธิ OWASP (๔๙) เพื่อเป็นการสร้างแนวปฏิบัติและกระบวนการที่ดีในระหว่างการตรวจสอบโค้ดและขั้นตอนการออกแบบเว็บไซต์ แบบรายการการตรวจสอบโปรแกรมประยุกต์บนเว็บ มีการจัดหมวดหมู่ตามการควบคุมเชิงรุก ๑๐ อันดับแรกของ OWASP ซึ่งหน่วยงานควรปรับให้เหมาะกับความต้องการและสภาพแวดล้อมของแต่ละหน่วยงาน

การตั้งค่าฐานข้อมูล

การตั้งค่าฐานข้อมูลเป็นกระบวนการสำคัญในการเริ่มต้นใช้งานเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลเพื่อเก็บข้อมูลและจัดการกับข้อมูลภายในระบบ เมื่อทำการตั้งค่าเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลอย่างถูกต้องและเหมาะสมกับความต้องการของระบบ จะช่วยให้การทำงานกับข้อมูลเป็นไปอย่างมีประสิทธิภาพและปลอดภัยมากยิ่งขึ้น การกำหนดค่าเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล ประกอบด้วย การตั้งค่าที่เกี่ยวข้องกับการเชื่อมต่อฐานข้อมูล การตั้งค่าระดับความมั่นคงปลอดภัย และการตั้งค่าความเร็วในการดำเนินการของฐานข้อมูล เพื่อให้เครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูลสามารถจัดการกับข้อมูลได้อย่างมีประสิทธิภาพและปลอดภัย สำหรับตัวอย่างการกำหนดค่าเครื่องคอมพิวเตอร์แม่ข่ายฐานข้อมูล เช่น ในการกำหนดค่าการเชื่อมต่อระหว่างฐานข้อมูลและแอปพลิเคชัน การกำหนดค่าสิทธิ์และการเข้าถึงข้อมูล และการกำหนดค่าการสำรองข้อมูล เพื่อให้การจัดการกับข้อมูลในฐานข้อมูลสามารถดำเนินการได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย โดยหน่วยงานอาจจะพิจารณารายละเอียดในการตั้งค่าฐานข้อมูล ดังนี้

---

[5] https://developer.wordpress.org/advanced-administration/security/hardening/

[6] https://docs.joomla.org/Security_Checklist/Joomla!_Setup

๑) การตั้งค่าการยืนยันตัวตน ใช้รหัสผ่านที่มีความมั่นคงปลอดภัยสูง

๒) การกำหนดสิทธิและบทบาท ใช้การจัดการการเข้าถึงตามบทบาท (Role-Based Access Control) ซึ่งจะแบ่งกลุ่มผู้ใช้งานตามบทบาทและให้สิทธิและการเข้าถึงตามบทบาท โดยจะใช้หลักการสิทธิ์ขั้นต่ำ (Least Privilege) ที่ให้สิทธิ์ที่จำเป็นในแต่ละบทบาทเพื่อเข้าใช้งานฐานข้อมูลเท่านั้น เพื่อจำกัดความเสียหายในกรณีที่ถูกโจมตี

๓) การตั้งค่าเครือข่าย เปิดรับการเข้าถึงข้อมูลจากพอร์ตที่จำเป็นและ IP ที่ได้รับอนุญาต และเปิดใช้งานการเข้ารหัส TLS ในการเชื่อมต่อฐานข้อมูล

๔) การสำรองข้อมูลและการกู้คืน ตั้งค่าให้มีการสำรองข้อมูลอย่างสม่ำเสมอและจัดเก็บในที่ที่ปลอดภัย และทดสอบการกู้คืนเป็นระยะเพื่อให้แน่ใจว่าสามารถกู้คืนข้อมูลได้เมื่อต้องการ

๕) การอัปเดต ตรวจสอบและอัปเดตซอฟต์แวร์ฐานข้อมูลให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

๖) การตรวจสอบและแจ้งเตือน เก็บบันทึกการเข้าถึงฐานข้อมูล (Access Logs) และตรวจสอบอย่างสม่ำเสมอ มีการแจ้งเตือนเมื่อตรวจพบการเข้าถึงฐานข้อมูลที่ผิดปกติ

ข้อ ๖.๒.๗ แนวทางและการเลือกบริการที่เกี่ยวข้องกับเว็บไซต์

การเลือกบริการจากผู้ให้บริการภายนอก ต้องใช้ความรอบคอบและการวางแผนเป็นอย่างดี โดยต้องคำนึงถึงปัจจัยด้านต่าง ๆ เช่น ความเชี่ยวชาญและประสบการณ์ คุณภาพและมาตรฐาน การสื่อสารและการรายงาน ความยืดหยุ่นและการปรับตัว และที่สำคัญความมั่นคงปลอดภัยและการปกป้องข้อมูล เป็นต้น มาตรฐานฉบับนี้ มีข้อเสนอแนะและแนวทางในการเลือกผู้ให้บริการภายนอกแบ่งตามบริการที่อยู่ในขอบเขตของเว็บไซต์ ดังนี้

การเลือกบริการเครื่องบริการเว็บ (Web Server)

กรณีที่หน่วยงานพิจารณาว่ามีความจำเป็นที่ต้องเลือกใช้บริการเครื่องบริการเว็บจากผู้ให้บริการภายนอก เช่น การใช้บริการเครื่องบริการเว็บบนคลาวด์ หน่วยงานอาจจะพิจารณาข้อควรคำนึงในการพิจารณาเลือกบริการเครื่องบริการเว็บ ดังนี้

๑) ขอบเขตความรับผิดชอบ หน่วยงานควรพิจารณาเลือกบริการเครื่องบริการเว็บตามขอบเขตความรับผิดชอบในการดูแลความมั่นคงปลอดภัยของเครื่องบริการเว็บ ซึ่งผู้ให้บริการมีบริการเครื่องบริการเว็บหลายรูปแบบ เช่น การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือน โดยผู้ใช้งานสามารถติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องด้วยตนเองทั้งหมด การให้บริการทรัพยากรการคำนวณและซอฟต์แวร์แพลตฟอร์มในการพัฒนาต่อยอดหรือการให้บริการเว็บแบบสำเร็จรูปโดยผู้ใช้งานสามารถตั้งค่าเครื่องบริการเว็บและติดตั้งส่วนเสริมด้วยตนเองได้ ซึ่งการให้บริการแต่ละรูปแบบจะมีการแบ่งความรับผิดชอบในการดูแลความมั่นคงปลอดภัยของเครื่องบริการเว็บที่ไม่เท่ากัน

๒) รูปแบบการจัดสรรทรัพยากร การเลือกรูปแบบการจัดสรรทรัพยากร มี ๒ รูปแบบ ประกอบด้วย แบบใช้ร่วมกัน (Shared) หรือแบบเป็นส่วนตัว (Dedicated หรือ Private) โดยการจัดสรรทรัพยากรแบบใช้ร่วมกันจะมีค่าบริการที่ต่ำกว่า แต่จะต้องใช้ทรัพยากรร่วมกันกับหน่วยงานอื่น ดังนั้น ควรมีการศึกษามาตรการในการควบคุมการเข้าถึงระบบและข้อมูลเพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาต เช่น ผู้ใช้ต่างหน่วยงานหรือบุคคลภายนอก เข้าถึงระบบและข้อมูล

ได้ การจัดสรรทรัพยากรแบบเป็นส่วนตัว ผู้ให้บริการจะแบ่งทรัพยากรและบริการให้ใช้เฉพาะผู้ใช้งานรายนั้น ๆ และส่วนใหญ่จะมีมาตรการควบคุมการเข้าถึงระบบและข้อมูลที่เข้มงวดกว่าแบบใช้ร่วมกัน

๓) การพิจารณาจากรูปแบบนโยบายการจัดการช่องโหว่ หน่วยงานอาจจะพิจารณาผู้ให้บริการที่มีนโยบายที่ชัดเจนในการค้นหาช่องโหว่ของซอฟต์แวร์ในเครื่องบริการเว็บ รวมถึงการป้องกันความเสียหายที่อาจจะเกิดจากช่องโหว่นั้น ๆ เช่น การแจ้งให้ผู้ใช้บริการทราบในทันที การ Patch หรือแก้ไขปัญหาเฉพาะหน้า (Workaround) ตามที่ผู้ผลิตซอฟต์แวร์หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่น่าเชื่อถือแนะนำ ตลอดจนมีแผนสำรองในกรณีที่เป็นช่องโหว่ที่ไม่สามารถหาวิธีแก้ไขหรือป้องกันความเสียหายได้ในระยะเวลาอันสั้น โดยต้องพิจารณาถึงความรับผิด (Liability) ที่ผู้ให้บริการที่ต้องชดเชยในกรณีที่เกิดความเสียหาย และในกรณีที่เกิดความบกพร่องจากการจัดการกับช่องโหว่จากผลกระทบที่คาดว่าจะได้รับ และระยะเวลาที่สามารถดำเนินการหาวิธีแก้ไขหรือป้องกันความเสียหายได้จนสำเร็จ

๔) นโยบายการรักษาความเป็นส่วนตัว การศึกษานโยบายความเป็นส่วนตัว (Privacy Policy) ของผู้ให้บริการเครื่องบริการเว็บ เพื่ออธิบายเกี่ยวกับการดำเนินการกับข้อมูลของผู้ใช้งานโดยผู้ให้บริการเครื่องบริการเว็บ เพื่อให้ผู้ใช้งานได้ทราบถึงการเก็บข้อมูล การใช้งานข้อมูล การแบ่งปันข้อมูลให้กับหน่วยงานอื่น การรักษาความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามกฎหมายเกี่ยวกับข้อมูลที่จะเกิดขึ้นกับข้อมูลของตน

๕) ความพร้อมใช้งาน (Uptime) การเลือกผู้ให้บริการเครื่องบริการเว็บที่มีความพร้อมใช้งาน (Uptime) ไม่ต่ำกว่าร้อยละ ๙๙.๙ โดยสามารถพิจารณาได้จากสถิติการให้บริการการรับรองความพร้อมใช้งานขั้นต่ำ และคำวิจารณ์ที่ผู้ให้บริการได้รับ

๖) การสำรองข้อมูลและกู้คืนข้อมูล (Backup and Restore) การเลือกผู้ให้บริการเครื่องบริการเว็บที่มีระบบสำรองข้อมูลอัตโนมัติ ตัวอย่างเช่น มีความถี่ในการสำรองข้อมูลอย่างน้อยวันละ ๑ ครั้ง และมีเครื่องมือในการสำรองข้อมูลที่อนุญาตให้ผู้ใช้งานสามารถสำรองข้อมูลด้วยตนเองตามความเหมาะสม และสอดคล้องกับความต้องการในการใช้งาน ทั้งนี้ จำเป็นต้องศึกษาวิธีการสำรองและกู้คืนข้อมูล หรือเลือกผู้ให้บริการที่มีเครื่องมือในการสำรองและกู้คืนข้อมูลที่ใช้งานได้ง่ายเพื่อตอบสนองต่อเหตุการณ์ที่เกิดได้อย่างรวดเร็ว เพื่อให้เว็บไซต์มีความพร้อมใช้งาน

๗) การได้รับการรับรองคุณภาพและมาตรฐาน ศึกษาข้อมูลเกี่ยวกับการได้รับการรับรองคุณภาพและมาตรฐานของผู้ให้บริการเครื่องบริการเว็บ เช่น การรับรองมาตรฐาน ISO/IEC 27001 หรือใบรับรองคุณภาพด้านเครือข่ายจากผู้จำหน่ายผลิตภัณฑ์ ซึ่งเป็นปัจจัยสำคัญที่บ่งบอกถึงคุณภาพการให้บริการ

๘) การให้บริการรักษาความมั่นคงปลอดภัย การเลือกผู้ให้บริการเครื่องบริการเว็บที่มีบริการเครื่องมือในการรักษาความมั่นคงปลอดภัย เช่น ไฟร์วอลล์ การให้บริการป้องกัน Web Application (WAF) เครื่องมือป้องกันการโจมตี DDoS ระบบตรวจจับการบุกรุกและระบบป้องกันการบุกรุก IDS/IPS และเครื่องมือป้องกันมัลแวร์ (Malware Protection)

๙) รูปแบบการให้บริการโอนย้ายไฟล์ข้อมูล (Remote File Transfer) การโอนย้ายไฟล์ข้อมูลระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ ควรต้องพิจารณาผู้ให้บริการ

เครื่องบริการเว็บที่มีช่องทางการโอนย้ายไฟล์ที่มั่นคงปลอดภัย รวมถึงมีการเข้ารหัสเพื่อรักษาความลับของข้อมูลระหว่างที่มีการโอนย้าย เช่น มีบริการ Secure File Transfer Protocol (SFTP) สำหรับกระบวนการโอนย้ายไฟล์

๑๐) การให้บริการสนับสนุน การเลือกผู้ให้บริการที่มีช่องทางการติดต่อฉุกเฉิน ในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อใช้ในการประสานงานทั้งจากผู้ใช้บริการและหน่วยงานอื่นในการรับมือต่อเหตุการณ์ภัยคุกคามอย่างทันท่วงที นอกจากนี้ การมีช่องทางการติดต่อฉุกเฉินโดยเฉพาะแสดงให้เห็นถึงการให้ความสำคัญกับความมั่นคงปลอดภัยของผู้ให้บริการ

๑๑) การรับรองอิเล็กทรอนิกส์ การเลือกผู้ให้บริการเครื่องบริการที่มีการขอใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือ TLS Certificate ซึ่งเป็นเครื่องมือที่สำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลสำคัญ เช่น ข้อมูลลูกค้า ข้อมูลบัตรเครดิต ที่มีการรับส่งกันระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ ซึ่งเป็นบริการที่จำเป็นสำหรับเว็บไซต์ด้านพาณิชย์อิเล็กทรอนิกส์ (e-Commerce Website) หรือหน่วยงานภาครัฐที่มีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยหน่วยงานอาจจะพิจารณาจากหัวข้อการเลือกประเภท TLS Certificate

การเลือกระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS)

หน่วยงานที่ใช้เว็บไซต์เป็นช่องทางในการเผยแพร่ข้อมูลของหน่วยงานที่มีการเปลี่ยนแปลงเนื้อหาน้อย เช่น ประวัติความเป็นมา และโครงสร้างองค์กร หรือการเปลี่ยนแปลงเป็นประจำ เช่น ข้อมูลข่าวสาร หลายหน่วยงานจึงพัฒนา และจัดทำเว็บไซต์ โดยระบบบริหารจัดการเว็บไซต์ CMS เพื่อความสะดวกในการบริหารจัดการ ซึ่งมีทั้งที่พัฒนาจากต่างประเทศ สามารถนำไปใช้งานต่อได้ฟรี และที่พัฒนาโดยบริษัทในประเทศไทย ซึ่งอาจมีการคิดค่าบริการหรือลิขสิทธิ์ในการใช้งาน ตัวอย่าง ระบบบริหารจัดการเว็บไซต์ CMS ที่นิยม เช่น WordPress, Joomla และ Drupal ถึงแม้ว่าการนำระบบบริหารจัดการเว็บไซต์ CMS มาใช้ในหน่วยงานจะมีประโยชน์ แต่ก็อาจมีช่องโหว่ด้านความมั่นคงปลอดภัยก่อให้เกิดความเสี่ยงได้ หน่วยงานจำเป็นต้องคำนึงถึงและมีมาตรการในการจัดการช่องโหว่ด้านความมั่นคงปลอดภัยอย่างเหมาะสม โดยหน่วยงานอาจจะพิจารณาแนวทางในการเลือกระบบบริหารจัดการเว็บไซต์ CMS ที่มีความมั่นคงปลอดภัย ดังนี้

๑) พิจารณาจากระบบบริหารจัดการเว็บไซต์ CMS มีการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัย รวมถึงควรมีเอกสารแนะนำแนวทางการติดตั้งและการตั้งค่าอย่างมั่นคงปลอดภัย (Security Best Practice) และ มีส่วนเสริม (Plugin) ที่ติดตั้งเพื่อรักษาความมั่นคงปลอดภัยที่ตรงตามความต้องการของหน่วยงาน

๒) พิจารณาจากคุณภาพของประชาคมนักพัฒนาระบบบริหารจัดการเว็บไซต์ CMS ในกรณีที่เป็น Open Source ซึ่งต้องอาศัยประชาคมของนักพัฒนาในการปรับปรุงระบบบริหารจัดการเว็บไซต์ CMS ให้ดีขึ้น ซึ่งการมีประชาคมนักพัฒนาที่มีขนาดใหญ่จะมีการสื่อสารภายใน และพัฒนาอย่างต่อเนื่อง (Active Developer Community) จะเป็นระบบบริหารจัดการเว็บไซต์ CMS ที่มีฟังก์ชันการทำงานตอบสนองต่อความต้องการของผู้ใช้งานได้มากกว่า รวมถึงมีการปรับเวอร์ชันหรือปรับปรุงระบบ เพื่อแก้ไขข้อบกพร่องและช่องโหว่ของระบบบริหารจัดการเว็บไซต์ CMS ซึ่งสังเกต

ได้จากความถี่ของการปรับเวอร์ชันหรือปรับปรุงระบบบริหารจัดการเว็บไซต์ CMS เพื่อแก้ไขช่องโหว่ หรือระยะเวลาใช้ในการพัฒนาตัวปรับรุ่น (Patch)

๓) พิจารณาจากแหล่งข้อมูลที่เกี่ยวกับการติดตั้ง การตั้งค่า และแนวทางการรักษาความมั่นคงปลอดภัยของระบบบริหารจัดการเว็บไซต์ CMS ที่ดี จะมีแหล่งข้อมูลและเอกสารสนับสนุนที่เกี่ยวข้องกับการติดตั้ง การตั้งค่า การปรับแต่งและแนวทางการรักษาความมั่นคงปลอดภัยให้กับระบบบริหารจัดการเว็บไซต์ CMS

การเลือกบริการโดเมนและชื่อโดเมน

การระบุเครื่องบริการเว็บที่เชื่อมต่อกับระบบเครือข่าย สามารถใช้ URL เพื่ออำนวยความสะดวกในการอ้างถึงเครื่องบริการเว็บบนเครือข่ายอินเทอร์เน็ต ซึ่ง URL จะมีความสัมพันธ์กับชื่อโดเมน ตัวอย่าง เช่น https://www.ncsa.or.th จะมีชื่อโดเมนที่มีการใช้เป็น ncsa.or.th ดังนั้น หน่วยงานต้องจดทะเบียนชื่อโดเมนของเว็บไซต์ก่อนการพัฒนาเว็บไซต์ ทำให้ชื่อโดเมนมีความสำคัญเป็นอันดับแรกในการจัดทำเว็บไซต์และการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ หลายครั้งเกิดเหตุการณ์ที่ชื่อโดเมนถูกแก้ไขและเปลี่ยนให้ชี้ไปยังเว็บไซต์หลอกลวง และเป็นช่องทางในการเข้าถึงบัญชีที่ใช้จดทะเบียนชื่อโดเมนโดยไม่ได้รับอนุญาต ทำให้ผู้ไม่หวังดีสามารถเข้าไปเปลี่ยนแปลงการตั้งค่าของชื่อโดเมนเพื่อนำไปใช้ในทางที่ผิด การเลือกผู้รับจดทะเบียนโดเมนจึงมีความสำคัญเป็นอย่างมาก หน่วยงานอาจจะพิจารณาแนวทางในการเลือกผู้รับจดทะเบียนชื่อโดเมน ดังนี้

๑) มีการยืนยันการลงทะเบียน โดยให้ผู้ขอจดทะเบียนยืนยันอีเมลของตนโดยการเข้าไปยังลิงก์บนเว็บเพจ ซึ่งระบุไว้ในอีเมลเปิดการใช้งาน (Activation Email) ที่ผู้รับจดทะเบียนส่งมา การบริการจดทะเบียนยังสามารถเพิ่มมาตรการความมั่นคงปลอดภัยโดยใช้การติดต่อไปยังหมายเลขโทรศัพท์ของผู้ขอจดทะเบียน เพื่อแจ้งหมายเลขสำหรับยืนยันการลงทะเบียน (Confirmation Number) ให้ผู้ขอจดทะเบียนนำหมายเลขมากรอกในแบบฟอร์มบนเว็บเพจเพื่อเปิดการใช้งานบัญชีหรืออนุญาตให้ทำธุรกรรมได้

๒) มีมาตรการในการเพิ่มความมั่นคงปลอดภัยให้กับรหัสผ่าน ให้เป็นไปตามแนวทางของ NIST SP 800-63B (๔๔)

๓) มีการแจ้งเตือนและการยืนยันการเปลี่ยนแปลงข้อมูลการลงทะเบียน ทั้งนี้ การเปลี่ยนแปลงข้อมูลต่าง ๆ ต้องมีการกำหนดขั้นตอนสำหรับการเปลี่ยนแปลงข้อมูลซึ่งต้องอาศัยการยืนยันจากหลายบุคคลที่เกี่ยวข้อง ซึ่งการยืนยันการเปลี่ยนแปลงลักษณะนี้จะช่วยป้องกันการเปลี่ยนแปลงจากผู้ประสงค์ร้ายที่อาจจะปลอมตัวเพื่อเข้ามาเอาข้อมูลจากบุคคลใดบุคคลหนึ่งได้

๔) มีรูปแบบการเลือกโดเมนระดับบนสุด (Top-Level Domain) และโดเมนระดับรอง (Second-Level Domain) เพื่อเพิ่มความน่าเชื่อถือของเว็บไซต์ จดจำได้ง่าย และช่วยในการกำหนดภาพลักษณ์ของเว็บไซต์ หน่วยงานอาจจะเลือกโดเมนระดับบนสุดให้เหมาะสมและสอดคล้องกับธุรกิจและเนื้อหาของเว็บไซต์ โดยหน่วยงานที่เป็นหน่วยงานในระดับสากลควรเลือกใช้โดเมนระดับสูงสุดหมวดทั่วไป .com .co หรือ .org ซึ่งเป็นโดเมนที่สามารถจดจำได้ง่ายและมีความน่าเชื่อถือ (๕๐) สำหรับเว็บไซต์ที่มีการเข้าถึงส่วนใหญ่จากประเทศไทยควรใช้โดเมนระดับบนสุดหมวดรหัสประเทศของไทย .th และใช้โดเมนระดับรองตามประเภทของหน่วยงานตามที่แสดงในตาราง ข๓

ในการขอใช้งาน .th ผู้ให้บริการจะดำเนินการตรวจสอบสิทธิ์การเป็นผู้ถือครอง ทำให้ชื่อโดเมนมีความน่าเชื่อถือมากยิ่งขึ้น

ตาราง ข๓ โดเมนระดับรองตามประเภทของหน่วยงาน

โดเมนระดับรอง	ประเภทของหน่วยงาน
.in	บุคคลทั่วไป
.ac	สถานศึกษา
.co	ธุรกิจเอกชน รัฐวิสาหกิจ และเครื่องหมายการค้า
.go	ส่วนราชการและหน่วยงานในกำกับของรัฐ
.mi	หน่วยงานทางทหาร
.or	องค์กรพัฒนาเอกชนหรือองค์กรเพื่อสังคม
.net	ผู้ได้รับอนุญาตประกอบกิจการโทรคมนาคม

๕) มีการเพิ่มความมั่นคงปลอดภัยด้วยการใช้ DNSSEC (Domain Name System Security Extensions) ซึ่งเป็นส่วนขยายการรักษาความมั่นคงปลอดภัยของระบบชื่อโดเมน ทำให้มั่นใจว่าข้อมูลที่ถูกส่งมานั้น ถูกส่งมาจากผู้ส่งที่ถูกต้องหรือเป็นเจ้าของที่แท้จริง และข้อมูลนั้นจะไม่ถูกรบกวนหรือปรับเปลี่ยนในระหว่างการจัดส่ง

การเลือกประเภท TLS Certificate

หน่วยงานอาจจะพิจารณาขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate ดังนี้

๑) ระดับความมั่นคงปลอดภัย (Security Level) โดยตรวจสอบให้แน่ใจว่ามีการใช้การเข้ารหัสที่มีความมั่นคงปลอดภัยสูง เช่น AES หรือ ChaCha20 มีการใช้กลไกการแลกเปลี่ยนกุญแจที่มีความมั่นคงปลอดภัยสูง และมีการใช้ฟังก์ชันแฮชที่มีความมั่นคงปลอดภัยสูง เช่น SHA-256 SHA-384

๒) ความเข้ากันได้ (Compatibility) โดยตรวจสอบความเข้ากันได้กับเว็บเบราว์เซอร์และ Client ที่เข้าถึงเว็บไซต์ โดยเว็บเบราว์เซอร์ที่ทันสมัยรองรับโพรโทคอล TLS 1.3 ดังนั้น จึงควรเลือกชุดรหัสที่เข้ากันได้กับเวอร์ชันนี้ และหลีกเลี่ยงโพรโทคอลที่เลิกใช้แล้ว (SSL 2.0, SSL 3.0) และการเข้ารหัสที่ไม่ปลอดภัย (RC4, DES)

๓) ประสิทธิภาพ (Performance) โดยพิจารณาเปรียบเทียบระหว่างระดับความมั่นคงปลอดภัยของการเข้ารหัสกับทรัพยากรที่ใช้ในการเข้ารหัส เช่น ChaCha20-Poly1305 ซึ่งเป็นการเข้ารหัสที่มีประสิทธิภาพสูงบนอุปกรณ์พกพา

๔) การรักษาความลับล่วงหน้า (Forward Secrecy) โดยเลือกใช้การเข้ารหัสที่รองรับการรักษาความลับล่วงหน้า (Forward Secrecy) เพื่อให้มีความมั่นใจว่ากุญแจที่ใช้ในการเชื่อมต่อจะไม่ถูกโจมตีแม้ว่ากุญแจส่วนตัวของเครื่องคอมพิวเตอร์แม่ข่ายจะถูกโจมตีในอนาคตก็ตาม

๕) การใช้ Cipher Suite ควรเลือกรหัสที่เป็นมาตรฐานรองรับการรักษาความลับล่วงหน้าและเข้ากันได้กับ Client เป้าหมายของผู้ให้บริการ

อีกหนึ่งปัจจัยสำคัญที่ต้องคำนึงถึงในการเลือก TLS Certificate คือ ระดับการรับรอง (Validation Level) การเลือกระดับการรับรองที่เหมาะสมจะเพิ่มความมั่นคงปลอดภัยและความน่าเชื่อถือของเว็บไซต์ ซึ่งบางหน่วยงานอาจมีกฎหมายหรือข้อบังคับในการเลือกระดับการรับรอง

ที่จะต้องปฏิบัติตาม จึงควรเลือกระดับการรับรองที่เหมาะสมกับเว็บไซต์ของหน่วยงาน โดยระดับการรับรอง แบ่งเป็น ๓ ระดับหลัก คือ Domain Validation (DV) Organization Validation (OV) และ Extended Validation (EV) หน่วยงานอาจจะพิจารณารายละเอียดในการเลือกระดับการรับรองโดยมีรายละเอียดดังแสดงในตาราง ข๔

ตาราง ข๔ แสดงรายละเอียดของระดับการรองรับของ TLS Certificate

รายการ	Domain Validation	Organization Validation	Extended Validation
การตรวจสอบ	- ความเป็นเจ้าของโดเมน	- ความเป็นเจ้าของโดเมน - การยืนยันตัวตนองค์กร	- ความเป็นเจ้าของโดเมน - การยืนยันการมีอยู่ของนิติบุคคลทางกฎหมาย ทางกายภาพ และการดำเนินงาน
ระยะเวลา	น้อย	ปานกลาง	มาก
ค่าใช้จ่าย	ต่ำ	ปานกลาง	สูง
ความน่าเชื่อถือ	ต่ำ	ปานกลาง	สูง
กรณีการใช้งาน	บล็อก เว็บไซต์ข้อมูล และเว็บไซต์ธุรกิจขนาดเล็กที่ความน่าเชื่อถือและความมั่นคงปลอดภัยมีความสำคัญแต่ไม่วิกฤติ	เว็บไซต์ธุรกิจ เว็บไซต์อีคอมเมิร์ซ และเว็บไซต์สาธารณะที่ต้องการความน่าเชื่อถือในระดับสูงขึ้น	เว็บไซต์ที่มีชื่อเสียง สถาบันการเงิน และเว็บไซต์อีคอมเมิร์ซที่ต้องการความน่าเชื่อถือในระดับสูงสุด

ข้อ ๖.๒.๘ รายละเอียดการตั้งค่าไฟร์วอลล์ขั้นต่ำ

ไฟร์วอลล์ (Firewall) เป็นเครื่องมือสำคัญในการควบคุมและป้องกันการบุกรุกต่าง ๆ ที่เกิดขึ้นกับเว็บไซต์ ซึ่งช่วยให้รักษาความมั่นคงปลอดภัยและความน่าเชื่อถือของข้อมูลในระบบเครือข่ายได้อย่างมีประสิทธิภาพ ไฟร์วอลล์ใช้ในการตรวจจับและควบคุมการเข้าถึงที่ไม่พึงประสงค์จากภายนอกเข้าสู่ระบบเครือข่าย โดยบล็อกการเข้าถึงที่มีความเสี่ยงและอนุญาตเฉพาะการเข้าถึงที่ถูกต้องตามกฎระเบียบที่กำหนดไว้ เช่น การบล็อก IP ที่มีความเสี่ยง การบล็อกการเข้าถึงตามพอร์ตที่ไม่ปลอดภัย หน่วยงานอาจจะพิจารณาหลักการตั้งค่าไฟร์วอลล์ ดังนี้

๑) กำหนดนโยบายความมั่นคงปลอดภัย (Define Security Policies) การกำหนดนโยบายความมั่นคงปลอดภัยที่ชัดเจน เป็นขั้นตอนที่สำคัญก่อนการตั้งค่าไฟร์วอลล์ เช่น การกำหนดถึงข้อมูลหรือบริการที่ต้องการการปกป้องและระบุถึงผู้ที่สามารถเข้าถึงได้

๒) ตั้งค่ากฎการกรอง (Configure Filtering Rules) การตั้งค่ากฎ (Rule) ในไฟร์วอลล์เพื่ออนุญาตหรือปฏิเสธการเข้าถึงข้อมูลบนเว็บไซต์ตามที่หน่วยงานกำหนดให้เหมาะสมกับกลุ่มเป้าหมาย ซึ่งจะต้องกำหนดกฎสำหรับการจราจร (Traffic) ทั้งขาเข้า (Inbound Rule) และขาออก (Outbound Rule)

การตั้งค่าไฟร์วอลล์ควรใช้หลักการ "Deny by Default" ซึ่งเป็นการตั้งค่าให้ระบบปฏิเสธการเข้าถึงทั้งหมดเป็นพื้นฐาน แล้วเพิ่มการอนุญาตการเข้าถึงที่จำเป็น ในส่วนที่เกี่ยวข้องกับการเข้าถึง

เว็บไซต์เท่านั้น โดยการเปิดเฉพาะพอร์ต 443 หรือ Hypertext Transfer Protocol Secure (HTTPS) ให้ปิดการใช้งานพอร์ต 80 ส่วนพอร์ตหรือบริการอื่น ๆ หากจำเป็นต้องเปิดใช้งาน ให้เลือกเปิดใช้งานโดยให้มีการเข้ารหัส ทั้งนี้ เพื่อเพิ่มความมั่นคงปลอดภัยให้ระบบ เป็นการลดโอกาสการถูกโจมตี และการเชื่อมต่อจากภายนอกจะทำได้ผ่านช่องทางที่จำเป็นและมีการอนุญาตไว้เท่านั้น ส่วนพอร์ตอื่น ๆ ให้หน่วยงานพิจารณาเปิดเฉพาะเท่าที่จำเป็น โดยให้กำหนดเฉพาะ IP ที่ใช้งาน

๓) จำกัดการเข้าถึงโดยภูมิศาสตร์ (Geographic Restrictions) กำหนดให้ไฟร์วอลล์ทำการปฏิเสธหรือจำกัดการเข้าถึงจากบางประเทศหรือภูมิภาคที่ไม่ต้องการหรือมีความเสี่ยงสูง

๔) ป้องกันการโจมตี (Protect Against Attacks) การใช้คุณสมบัติของไฟร์วอลล์เพื่อป้องกันการโจมตีต่าง ๆ เช่น DDoS, SQL injection และ XSS ด้วยการตั้งค่าความสามารถในการป้องกันการโจมตี

๕) การตรวจสอบและบันทึก (Monitoring and Logging) การตั้งค่าไฟร์วอลล์ ให้บันทึกกิจกรรมที่เกิดขึ้น เพื่อรองรับการตรวจสอบย้อนหลังและวิเคราะห์เหตุการณ์ที่เกิดขึ้น โดยการบันทึก Log ที่ดีจะช่วยให้สามารถตรวจสอบและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

๖) การปรับปรุงและอัปเดตเป็นประจำ (Regular Updates) การอัปเดตซอฟต์แวร์ไฟร์วอลล์ และกฎการกรองอย่างสม่ำเสมอ เป็นสิ่งที่สำคัญที่ต้องดำเนินการเพื่อให้มั่นใจว่าไฟร์วอลล์สามารถป้องกันภัยคุกคามจากสถานการณ์ด้านความมั่นคงปลอดภัยได้อย่างครอบคลุม

ข้อ ๖.๔ การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์
การรับมือเหตุการณ์ไม่คาดคิด

เหตุการณ์ไม่คาดคิดอาจเกิดได้จากหลายสาเหตุและอาจอยู่นอกเหนือการควบคุมของผู้ใช้งานและหน่วยงาน เมื่อเกิดเหตุการณ์ไม่คาดคิดแล้วอาจส่งผลกระทบกับระบบต่าง ๆ รวมถึงระบบเว็บไซต์ การเตรียมตัวรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์จึงเป็นสิ่งที่จำเป็นในการลดความเสียหายที่จะเกิดขึ้น ทั้งทางธุรกิจและชื่อเสียงภาพลักษณ์ โดยการมีแผนรับมือจะทำให้ระบบฟื้นฟูกลับมาใช้งานได้รวดเร็วยิ่งขึ้น ช่วยเพิ่มความเชื่อมั่นของลูกค้าและผู้มีส่วนได้ส่วนเสียกับธุรกิจและบริการ หน่วยงานอาจจะพิจารณาคำแนะนำและข้อควรพิจารณาในการตอบสนองต่อเหตุการณ์สำหรับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST เพื่อช่วยให้หน่วยงานต่าง ๆ มีความสามารถในการรับมือเหตุการณ์ทางไซเบอร์ ลดความสูญเสียที่เกิดขึ้นและใช้เวลาในการฟื้นฟูระบบที่สั้นลง ประกอบด้วย ๖ ส่วน (๕๑) ดังนี้

๑) การควบคุมและกำกับดูแล (Govern: GV) คือ มีการจัดทำ สื่อสาร และติดตามตรวจสอบกลยุทธ์การบริหารจัดการความเสี่ยงของหน่วยงาน ความคาดหวังของผู้มีส่วนได้ส่วนเสีย และนโยบาย

๒) การระบุความเสี่ยง (Identify: ID) คือ หน่วยงานเข้าใจถึงความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่เป็นปัจจุบัน

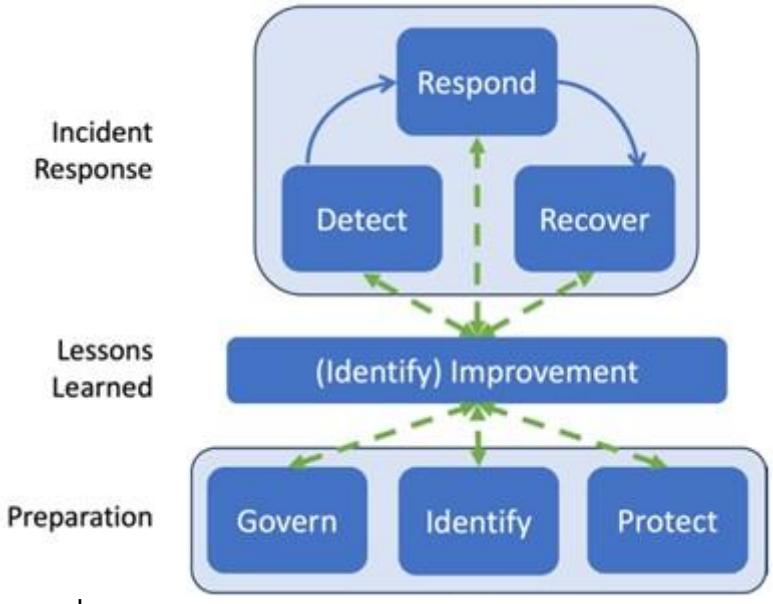
๓) การป้องกัน (Protect: PR) คือ การใช้เครื่องมือและกระบวนการต่าง ๆ ในการรับมือกับความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงาน

๔) การตรวจจับ (Detect: DT) คือ การตรวจจับและวิเคราะห์เหตุการณ์ที่มีลักษณะบ่งบอกถึงการถูกโจมตี

๕) การตอบสนอง (Respond: RS) คือ การดำเนินการเพื่อรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่ตรวจพบ

๖) การฟื้นฟู (Recover: RC) คือ การทำให้ทรัพย์สินและกระบวนการที่ถูกโจมตีกลับมามีสภาพเดิม

โดยการทำงานทั้ง ๖ ส่วนจะมีความสัมพันธ์กันตามภาพที่ ข๒ กล่าวคือ การควบคุมและกำกับดูแล การระบุความเสี่ยง และการป้องกัน จะเป็นกิจกรรมที่สนับสนุนการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ แต่จะไม่ได้เป็นส่วนหนึ่งของวงจรการรับมือเหตุการณ์ทางไซเบอร์โดยตรง ส่วนการตรวจจับ การตอบสนอง และการฟื้นฟูจะอยู่ในวงจรการรับมือเหตุการณ์ทางไซเบอร์ โดยมีการนำบทเรียนที่ได้จากทั้ง ๖ ส่วน มาทบทวนเพื่อพัฒนาแนวทางในการรับมือเหตุการณ์ที่ไม่คาดคิดอย่างต่อเนื่อง โดยจะมีกระบวนการวิเคราะห์ การจัดลำดับความสำคัญ และการนำผลที่ได้มาเป็นข้อมูลในการทำงานในทุกส่วน



ภาพที่ ข๒ รูปแบบวงจรการรับมือเหตุการณ์ทางไซเบอร์ตาม CSF 2.0

ภาคผนวก ค
แบบฟอร์มเพื่อใช้ในการตรวจสอบการดำเนินการให้เป็นไปตามมาตรฐานฉบับนี้

<u>โครงสร้างแบบฟอร์ม</u>

แบบฟอร์ม ค๑ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

แบบฟอร์ม ค๑ เป็นแบบตรวจรายการเพื่อการตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อให้หน่วยงานใช้ในการประเมินตนเอง (Self-Assessment) ให้เป็นไปตามมาตรฐานฉบับนี้ ทั้งกลุ่มที่ปฏิบัติตาม หรือกลุ่มที่ส่งเสริมให้ปฏิบัติตามข้อกำหนดขั้นต่ำ

แบบฟอร์ม ค๒ แบบรายงานการแก้ไขรายการที่ยังต้องปรับปรุง

แบบฟอร์ม ค๒ เป็นแบบรายงานการแก้ไขรายการที่ยังต้องปรับปรุงในกรณีที่หน่วยงานพบรายการที่ไม่เป็นไปตามข้อกำหนด ตามแบบฟอร์ม ค๑ ให้ระบุรายการที่ต้องการปรับปรุงลงในแบบฟอร์มนี้

<u>คำแนะนำ</u>

๑. ให้หน่วยงานดำเนินการกรอกข้อมูลที่เกี่ยวกับเว็บไซต์หน่วยงานของท่านในส่วนที่ ๑ และกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศในส่วนที่ ๒ โดยใส่เครื่องหมาย ✔ ลงในช่องที่มีข้อมูลตรงกับหน่วยงานของท่านมากที่สุด

๒. ให้หน่วยงานดำเนินการตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามแบบฟอร์ม ค๑ ในส่วนที่ ๓ โดยใส่เครื่องหมาย ✔ ลงในช่อง “การประเมิน” ในส่วนของ **<u>ข้อเสนอแนะ</u>** ๓ ระดับ ดังนี้

“ดำเนินการแล้ว” กรณีที่หน่วยงานดำเนินการตามรายการในข้อเสนอแนะที่ระบุว่า “จะต้อง” และ “ควรจะ” ครบถ้วน โดยให้ใส่รายละเอียดของหลักฐานในช่อง “หลักฐาน” และแนบพร้อมแบบฟอร์มนี้

“อยู่ในระหว่างดำเนินการ” กรณีที่หน่วยงานกำลังดำเนินการตามรายการในข้อเสนอแนะที่ระบุว่า “จะต้อง” และ “ควรจะ”

“ยังไม่ได้ดำเนินการ” กรณีที่หน่วยงานยังไม่ดำเนินการตามรายการในข้อเสนอแนะที่ระบุว่า “จะต้อง” และ “ควรจะ”

๓. จากนั้นให้ตรวจสอบ**<u>ข้อเสนอแนะในแต่ละข้อกำหนด</u>** โดยให้ใส่เครื่องหมาย ✔ ลงในช่อง “การประเมิน” ในส่วนของ**<u>ข้อกำหนด</u>** ๒ ระดับ ดังนี้

“ดำเนินการแล้ว” กรณีที่หน่วยงานดำเนินการตามข้อกำหนดครบถ้วน และข้อเสนอแนะในแต่ละข้อกำหนดมีสถานะเป็น “ดำเนินการแล้ว” ครบทุกข้อ

“ยังต้องปรับปรุง” กรณีที่หน่วยงานดำเนินการตามข้อกำหนดยังไม่ครบถ้วน และข้อเสนอแนะในแต่ละข้อกำหนดมีสถานะเป็น “อยู่ในระหว่างดำเนินการ” หรือ “ยังไม่ได้ดำเนินการ”

๔. หากรายการ**<u>ข้อกำหนด</u>**มีผลการประเมินเป็น “ยังต้องปรับปรุง” ให้หน่วยงานดำเนินการกรอกรายละเอียดในแบบรายงานรายการที่ยังต้องปรับปรุง (แบบฟอร์ม ค๒) เพื่อดำเนินการปรับปรุงแก้ไขข้อกำหนดที่ยังต้องปรับปรุงแก้ไขให้เป็นไปตามมาตรฐานฉบับนี้

๕. หลังจากหน่วยงานดำเนินการกรอกแบบฟอร์ม ค๑ และแบบฟอร์ม ค๒ แล้วให้หน่วยงานดำเนินการตามแนวทางในการตรวจสอบและปฏิบัติให้เป็นไปตามมาตรฐาน ข้อที่ ๗.๒

แบบฟอร์ม ค๑

แบบตรวจรายการเพื่อการตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

สำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
หน่วยงานของรัฐ และหน่วยงานเอกชน

<u>ส่วนที่ ๑</u> ข้อมูลเกี่ยวกับเว็บไซต์

ชื่อหน่วยงาน.....

ชื่อหน่วยงานควบคุมหรือกำกับดูแล ของท่าน.....

ประเภทหน่วยงาน ☐ หน่วยงานของรัฐ
☐ หน่วยงานควบคุมหรือกำกับดูแล (Regulator)
☐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)
☐ หน่วยงานเอกชน

เว็บไซต์ให้บริการด้าน.....

หน่วยงานภายในที่รับผิดชอบ (ระบุให้เป็นไปตามข้อ ๕.๔.๒).....

การเข้าถึงเว็บไซต์ หรือ URL.....

ประเภทของเว็บไซต์ ☐ เว็บไซต์หลักของหน่วยงาน ☐ เว็บไซต์ภายในหน่วยงาน (Intranet)
☐ อื่นๆ โปรดระบุ.....

วัตถุประสงค์ในการบริการเว็บไซต์ (เลือกได้มากกว่า ๑ ตัวเลือก)
☐ เว็บไซต์ที่ให้บริการข้อมูลของประชาชน
☐ เว็บไซต์ให้บริการเกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ
☐ เว็บไซต์ของหน่วยงานที่มีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์
☐ อื่น ๆ โปรดระบุ.....

รูปแบบการจัดทำเว็บไซต์ ☐ เว็บไซต์บนระบบขององค์กร (On-Premises)
☐ เว็บไซต์บนระบบคลาวด์ (Cloud Service)
☐ เว็บไซต์ที่ใช้บริการเว็บโฮสติ้ง (Web Hosting)
☐ อื่นๆ โปรดระบุ.....

วันที่ประเมินตนเอง (Self-Assessment).....

ผู้ตอบแบบสอบถาม.....ตำแหน่ง.....

สังกัดหน่วยงาน (ภายใน).....

เบอร์โทร.....อีเมล.....

<u>ส่วนที่ ๒</u> กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศ

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (๒๓)

ผลกระทบด้านที่ ๑ มูลค่าความเสียหายทางการเงินหรือทรัพย์สิน หรือต่อชื่อเสียงของหน่วยงาน

ตาราง ค๑ การประเมินผลกระทบต่อมูลค่าความเสียหายทางการเงินหรือทรัพย์สินหรือต่อชื่อเสียงของหน่วยงาน

วัตถุประสงค์/ระดับ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้อง (Integrity)	การรักษาสภาพพร้อมใช้งาน (Availability)
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลเพียง<u>เล็กน้อยหรืออย่างจำกัด</u> หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็น<u>ชั้นลับ</u>	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>เพียงเล็กน้อยหรืออย่างจำกัด</u>	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>เพียงเล็กน้อยหรืออย่างจำกัด</u>
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคลอย่างร้ายแรง หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็น<u>ชั้นลับมาก</u>	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรง</u>	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรง</u>
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อการดำเนินงาน ทรัพย์สิน หรือชื่อเสียงของหน่วยงานหรือบุคคล<u>อย่างร้ายแรงมาก</u> หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็น<u>ชั้นลับที่สุด</u>	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรงมาก</u>	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อการดำเนินงาน หรือทรัพย์สินของหน่วยงานหรือบุคคล<u>อย่างร้ายแรงมาก</u>

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ ความถูกต้อง☐ สภาพพร้อมใช้ **ระดับ** ☐ ต่ำ☐ กลาง☐ สูง

ผลกระทบด้านที่ ๒ จำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด

ตาราง ค๒ การประเมินผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด

วัตถุประสงค์/ระดับ	**การรักษาความลับ (Confidentiality)**	**การรักษาความถูกต้อง (Integrity)**	**การรักษาสภาพพร้อมใช้งาน (Availability)**
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดเพียงเล็กน้อยหรืออย่างจำกัด หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างเล็กน้อยหรืออย่างจำกัด	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างเล็กน้อยหรืออย่างจำกัด
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรง หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรง	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรง
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรงมาก หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรงมาก	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อจำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใดอย่างร้ายแรงมาก

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ ความถูกต้อง☐ สภาพพร้อมใช้ **ระดับ** ☐ ต่ำ☐ กลาง☐ สูง

ผลกระทบด้านที่ ๓ ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน

ตาราง ค๓ การประเมินผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน

วัตถุประสงค์/ระดับ	**การรักษาความลับ (Confidentiality)**	**การรักษาความถูกต้อง (Integrity)**	**การรักษาสภาพพร้อมใช้งาน (Availability)**
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วนอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลเพียงเล็กน้อยหรืออย่างจำกัด หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างเล็กน้อยหรืออย่างจำกัด	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างเล็กน้อยหรืออย่างจำกัด
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรง หรืออาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรง	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรง
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความสามารถในการดำเนินการตามหน้าที่ของหน่วยงานหรือบุคคลอย่างร้ายแรงมาก

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ความถูกต้อง ☐สภาพพร้อมใช้ **ระดับ** ☐ต่ำ ☐ กลาง☐ สูง

ผลกระทบด้านที่ ๔ ความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

ตาราง ค๔ การประเมินผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

วัตถุประสงค์/ระดับ	**การรักษาความลับ (Confidentiality)**	**การรักษาความถูกต้อง (Integrity)**	**การรักษาสภาพพร้อมใช้งาน (Availability)**
ต่ำ	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศเพียงเล็กน้อยหรืออย่างจำกัด หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับ	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อการความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างเล็กน้อยหรืออย่างจำกัด	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างเล็กน้อยหรืออย่างจำกัด
กลาง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรง หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับมาก	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรง	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรง
สูง	☐ ในกรณีที่การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าทั้งหมดหรือบางส่วน อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรงมาก หรือ อาจเปิดเผยข้อมูลลับที่ถูกกำหนดชั้นความลับเป็นชั้นลับที่สุด	☐ ในกรณีที่การแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรงมาก	☐ ในกรณีที่หน่วยงานไม่สามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ อาจส่งผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอย่างร้ายแรงมาก

ผลการประเมิน (นำไปกรอกในตาราง ค๕)

ผลกระทบมากที่สุด **เรื่อง** ☐ ความลับ ☐ความถูกต้อง ☐สภาพพร้อมใช้ **ระดับ** ☐ต่ำ ☐ กลาง☐ สูง

ตาราง ค๕ ตารางสรุปผลการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือสารสนเทศและการประเมินระดับผลกระทบ

ผลกระทบด้าน	วัตถุประสงค์ที่มีผลกระทบมากที่สุด	ระดับผลกระทบ
มูลค่าความเสียหายทางการเงินหรือทรัพย์สินหรือต่อชื่อเสียงของหน่วยงาน	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
จำนวนของผู้ใช้บริการของหน่วยงาน บุคลากรของหน่วยงานหรือประชาชนที่อาจได้รับอันตรายต่อชีวิต ร่างกาย อนามัย ทรัพย์สิน หรือความเสียหายอื่นใด	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
ความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ	☐ ความลับ ☐ ความถูกต้อง ☐ สภาพพร้อมใช้	☐ต่ำ ☐ กลาง ☐ สูง
ใส่ระดับผลกระทบมากที่สุด (นำผลไปใส่ในตาราง ค๖)		

ตาราง ค๖ ข้อกำหนดขั้นต่ำในการปฏิบัติตามมาตรฐานฉบับนี้ แบ่งตามผลกระทบจากการประเมิน

ผลกระทบ	เกณฑ์การดำเนินการตามข้อกำหนดขั้นต่ำ
☐ผลกระทบระดับ**สูง**	หน่วยงานจะต้องดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ทุกข้อ
☐ ผลกระทบระดับ**กลาง**	หน่วยงานจะต้องดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ดังนี้ **หัวข้อที่ ๕** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ทุกข้อ **หัวข้อที่ ๖** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ โดย ยกเว้น ข้อกำหนด ข้อ ๖.๑.๑ เฉพาะส่วนของการประเมินช่องโหว่และทดสอบเจาะระบบ และการจัดการผู้ให้บริการภายนอก (Third Party Management) ข้อ ๖.๒.๑ ข้อ ๖.๒.๓ (๕) - (๗) และข้อ ๖.๒.๔ เฉพาะส่วนของการแบ่งปันข้อมูล (Information Sharing)
☐ผลกระทบระดับ**ต่ำ**	หน่วยงานจะต้องดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ดังนี้ **หัวข้อที่ ๕** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ ทุกข้อ **หัวข้อที่ ๖** ดำเนินการตามข้อกำหนดในมาตรฐานฉบับนี้ โดย ยกเว้น ข้อกำหนด ข้อ ๖.๑.๑ ข้อ ๖.๒.๑ ข้อ ๖.๒.๓ (๔) - (๗) ข้อ ๖.๒.๔ เฉพาะส่วนการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) และการแบ่งปันข้อมูล (Information Sharing) ข้อ ๖.๓.๑ ข้อ ๖.๔.๑ และ ข้อ ๖.๕.๑

ตาราง ค๗ การระบุหน่วยงานที่ต้องปฏิบัติตามหรือส่งเสริมให้ปฏิบัติตามมาตรฐานฉบับนี้

กลุ่ม	ลักษณะหน่วยงาน	การปฏิบัติตามข้อกำหนด
☐ กลุ่มที่ ๑	๑) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๒) หน่วยงานควบคุมหรือกำกับดูแล ๓) หน่วยงานของรัฐ	**จะต้อง**ปฏิบัติตาม
☐ กลุ่มที่ ๒	๑) หน่วยงานเอกชน	**ส่งเสริม**ให้ปฏิบัติตาม

ส่วนที่ ๓ แบบตรวจรายการเพื่อตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
ข้อกำหนดการกำกับดูแลด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (หัวข้อ ๕)				
๑	**การสำรวจบริบทของหน่วยงาน (Organization Context) (หัวข้อ ๕.๑)**			
๑.๑	หน่วยงานจะต้องมีการทำความเข้าใจสถานการณ์ต่าง ๆ ที่เกี่ยวข้องกับการตัดสินใจในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ของหน่วยงาน โดยหน่วยงานอาจจะพิจารณารายละเอียดการดำเนินการสำรวจบริบทของหน่วยงาน (Organization Context) ตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๑.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๒	**นโยบายด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Policies) (หัวข้อ ๕.๒)**			
๒.๑	หน่วยงานจะต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามบริบทขององค์กรและกลยุทธ์ด้านความมั่นคงปลอดภัยเว็บไซต์ โดยมีการจัดลำดับความสำคัญ มีการสื่อสาร รวมถึงมีการบังคับใช้ (หัวข้อ ๕.๒.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์ตามบริบทขององค์กรและกลยุทธ์ด้านความมั่นคงปลอดภัยเว็บไซต์ โดยพิจารณาแนวทางได้จากประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ในภาคผนวก ค ตัวอย่างการประกาศนโยบาย ข้อ ๔ หรืออาจจะพิจารณาจัดทำนโยบายตามตัวอย่างนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Policy) ของ สกมช.	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		เฉพาะกรณีหน่วยงานมีนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่แล้ว หน่วยงานควรจะพิจารณาตรวจสอบและปรับปรุงให้ครอบคลุมและสอดคล้องกับมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๒.๒	หน่วยงานจะต้องมีการทบทวน ปรับปรุง สื่อสาร และบังคับใช้นโยบายความมั่นคงปลอดภัยสำหรับเว็บไซต์เพื่อสะท้อนการเปลี่ยนแปลงความต้องการ ภัยคุกคาม เทคโนโลยี รวมถึงภารกิจของหน่วยงาน (หัวข้อ ๕.๒.๒)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๓	**กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy) (หัวข้อ ๕.๓)**			
๓.๑	หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์การบริหารความเสี่ยงและมีการจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์เป็นลายลักษณ์อักษร (หัวข้อ ๕.๓.๑)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๓.๒	เฉพาะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานจะต้องพิจารณาดำเนินการประเมินความเสี่ยงตามคำแนะนำของ สกมช. เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๕.๓.๒)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๓.๓	หน่วยงานจะต้องมีการจัดทำ สื่อสาร และมีการเก็บรักษารายการความเสี่ยงที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ให้เป็นปัจจุบัน และติดตามระดับความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้ (หัวข้อ ๕.๓.๓)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๔	**บทบาทและความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (หัวข้อ ๕.๔)**			
๔.๑	หน่วยงานจะต้องมีการจัดโครงสร้างองค์กรให้มีการถ่วงดุล พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ โดยหน่วยงานอาจจะ ใช้แนวคิดการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) มาประยุกต์ใช้กับการจัดโครงสร้างองค์กรให้มีการถ่วงดุล ในการบริหารจัดการความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งมี	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		รายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๔.๑)		
๔.๒		หน่วยงานจะต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำและบริหารจัดการเว็บไซต์ของหน่วยงาน รวมถึงดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ซึ่งต้องเป็นนิติบุคคลหรือเป็นส่วนหนึ่งของนิติบุคคลที่สามารถรับผิดตามกฎหมายได้ และการมอบหมายหน้าที่จะต้องทำโดยไม่ขาดช่วง (หัวข้อ ๕.๔.๒)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๔.๓		หน่วยงานจะต้องกำหนด สื่อสาร ทำความเข้าใจและบังคับใช้บทบาท ความรับผิดชอบ และอำนาจที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ รวมถึงจัดสรรทรัพยากรให้เพียงพอ (หัวข้อ ๕.๔.๓)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๕	**การวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์ (หัวข้อ ๕.๕)**			
๕.๑		หน่วยงานจะต้องมีการกำหนดวัตถุประสงค์และความต้องการในการจัดทำเว็บไซต์ ด้านฟังก์ชัน ด้านประสิทธิภาพ และที่สำคัญความต้องการด้านความมั่นคงปลอดภัย โดยหน่วยงานควรจะมีการวางแผนกำหนดความต้องการด้านความมั่นคงปลอดภัยของเว็บไซต์ โดยพิจารณาให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๕.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖	**การกำหนดแนวทางด้านความมั่นคงปลอดภัยสำหรับเว็บไซต์ (หัวข้อ ๕.๖)**			
๖.๑		หน่วยงานจะต้องมีแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐานตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการเตรียมความพร้อมใช้งาน (Availability) โดยหน่วยงานควรจะดำเนินการตามแนวทางด้านความมั่นคงปลอดภัยในระดับพื้นฐาน ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๖.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๒		หน่วยงานจะต้องมีการกำหนดคุณลักษณะความมั่นคงปลอดภัยให้กับข้อมูลหรือสารสนเทศของเว็บไซต์ ตามคุณลักษณะด้านความมั่นคงปลอดภัยพื้นฐาน ๓ ระดับให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ (หัวข้อ ๕.๖.๒)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
๖.๓		<u>เฉพาะหน่วยงานมีการดำเนินการธุรกรรมทางอิเล็กทรอนิกส์</u> หน่วยงานจะต้องดำเนินการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ รวมถึงประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ (หัวข้อ ๕.๖.๓)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๔		<u>เฉพาะหน่วยงานภาครัฐ</u> หน่วยงาน<u>จะต้อง</u>ดำเนินการตามมาตรฐานเว็บไซต์ภาครัฐ (Government Website Standard) Version ๓.๐ หัวข้อที่ ๗ ความมั่นคงปลอดภัยสำหรับเว็บไซต์ (หัวข้อ ๕.๖.๔)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๕		<u>เฉพาะหน่วยงานที่มีเว็บไซต์ใช้บริการคลาวด์</u> หน่วยงาน<u>จะต้อง</u>มีการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ที่ใช้บริการคลาวด์ ให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ (หัวข้อ ๕.๖.๕)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๖		หน่วยงาน<u>จะต้อง</u>พิจารณาเลือกผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ เช่น การดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) ของเว็บไซต์ ที่ได้รับการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม (หัวข้อ ๕.๖.๖)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๗		<u>เฉพาะหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</u> หน่วยงาน<u>จะต้อง</u>ปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) ของ สกมช. (หัวข้อ ๕.๖.๗)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
๖.๘	หน่วยงานจะต้องมีการกำหนดแนวทางในการสำรองข้อมูลเพื่อลดผลกระทบที่เกิดขึ้นหากเว็บไซต์ของหน่วยงานโดนโจมตีจากภัยคุกคามทางไซเบอร์ โดยหน่วยงานอาจจะพิจารณาองค์ประกอบในการสำรองข้อมูล ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๕.๖.๘)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๙	หน่วยงานจะต้องมีการจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log Management) ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และที่แก้ไขเพิ่มเติม (หัวข้อ ๕.๖.๙)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๖.๑๐	หน่วยงานจะต้องกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ เพื่อป้องกันภัยคุกคามไซเบอร์ที่อาจจะเกิดกับผู้ใช้บริการเว็บไซต์ ผู้ใช้งานอินเทอร์เน็ตทั่วไป ผู้ให้บริการ โดยหน่วยงานควรจะกำหนดหลักปฏิบัติในการเลิกใช้งานเว็บไซต์ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ หรือหน่วยงานอาจจะพิจารณาการทำลายข้อมูลตามข้อเสนอแนะให้เป็นไปตาม NIST Special Publication 800-88 และขั้นตอนหลักของการทำลายข้อมูล (หัวข้อ ๕.๖.๑๐)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
ข้อกำหนดการดำเนินการและการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Security and Operation Requirement) (หัวข้อ ๖)				
๗	**การระบุความเสี่ยงที่จะเกิดขึ้นกับเว็บไซต์ (Website Security Identification) (หัวข้อ ๖.๑)**			
๗.๑	หน่วยงานจะต้องมีการจัดการทรัพย์สิน (Asset Management) การประเมินความเสี่ยง (Risk Assessment) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) และการจัดการผู้ให้บริการภายนอก (Third Party Management) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๑.๑)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องจัดทำทะเบียนทรัพย์สิน และตรวจสอบทะเบียนทรัพย์สิน อย่างน้อยปี ละ ๑ ครั้ง รวมถึงปรับปรุงทะเบียนทรัพย์สินทุกครั้ง หากมีการเปลี่ยนแปลงใดๆ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัย	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		ไซเบอร์ โดยอาจจะพิจารณาดำเนินการจัดการทรัพย์สิน ตามรายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้		
		หน่วยงานจะต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปี ละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญและปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอาจจะพิจารณาการประเมินความเสี่ยง (Risk Assessment) ใน ๒ รูปแบบ ได้แก่ การประเมินความเสี่ยงเชิงปริมาณและการประเมินความเสี่ยงเชิงคุณภาพ และอาจจะพิจารณาขั้นตอนหลักในการประเมินความเสี่ยง ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ที่ยอมรับได้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment) โดยอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน โดยครอบคลุมการให้บริการเว็บไซต์ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อาจจะพิจารณาขอบเขตของการประเมินช่องโหว่ของบริการที่สำคัญครอบคลุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ โครงสร้างเครือข่ายสื่อสารข้อมูล เครื่องบริการเว็บ และเว็บแอปพลิเคชัน และอาจจะพิจารณาดำเนินการ	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		ตามแนวทางในการประเมินช่องโหว่ ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้		
		หน่วยงานควรจะดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยพิจารณาดำเนินการอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และอาจจะพิจารณาปัจจัยในการดำเนินการทดสอบการเจาะระบบเว็บไซต์ รวมถึงเลือกผู้ให้บริการทดสอบเจาะระบบ โดยพิจารณาตามรายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะมีการตรวจสอบผู้ให้บริการภายนอก (Third Party Management) จะต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ในการดำเนินงานให้บริการเว็บไซต์ ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ในเงื่อนไขของสัญญา และควรจะพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ให้เป็นไปตาม	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์		
๘	**การป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับเว็บไซต์ (Website Security Protection) (หัวข้อ ๖.๒)**			
๘.๑		หน่วยงานจะต้องกำหนดแนวทางในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) อย่างมั่นคงปลอดภัย เช่น พิจารณาใช้หลักการ DevSecOps ตั้งแต่ขั้นตอนการพัฒนาจนถึงการใช้งานจริงโดยมีการคำนึงถึงสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยในการพัฒนาโปรแกรมประยุกต์บนเว็บ โดยหน่วยงานควรจะพิจารณาปรับใช้ตัวอย่างในการปรับใช้หลักการ DevSecOps และอาจจะพิจารณาสิ่งสำคัญในการรักษาความมั่นคงปลอดภัยของการพัฒนาโปรแกรมประยุกต์บนเว็บ รวมถึงอาจจะพิจารณาประยุกต์ใช้หลักการ DevSecOps โดยใช้หลักการ DSOMM ของมูลนิธิ OWASP ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๖.๒.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๘.๒		หน่วยงานจะต้องพิจารณาถึงปัจจัยเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ที่พบได้บ่อยของมูลนิธิ OWASP ในการพัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application) (หัวข้อ ๖.๒.๒)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
๘.๓		หน่วยงานจะต้องพิจารณาการออกแบบสถาปัตยกรรมเว็บไซต์อย่างมั่นคงปลอดภัย ในส่วนของโครงสร้างของเว็บไซต์หรือโปรแกรมประยุกต์บนเว็บ โดยอาจจะพิจารณาส่วนประกอบของการออกแบบที่คำนึงถึงการแบ่งส่วนเครือข่าย (Network segmentation) มีการจัดวางเครื่องบริการเว็บ (Web Server) และเครื่องบริการฐานข้อมูล (Database Server) ร่วมกับอุปกรณ์รักษาความมั่นคงปลอดภัย (หัวข้อ ๖.๒.๓)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หน่วยงานควรจะพิจารณาวางเครื่องบริการเว็บ (Web Server) ร่วมกับอุปกรณ์และบริการการรักษาความมั่งคงปลอดภัยพื้นฐาน เป็นอย่างน้อย หรืออาจจะพิจารณาวางเครื่องบริการเว็บ (Web Server) ร่วมกับการให้บริการป้องกัน Web Application (WAF) หรือหน่วยงานอาจจะพิจารณาวางเครื่องบริการเว็บ (Web Server) ร่วมกับผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยเพิ่มเติม ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาออกแบบโครงสร้างเว็บไซต์ออกเป็น ๔ ส่วน ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๔	หน่วยงานจะต้องมีการควบคุมการเข้าถึง (Access Control) และทำให้ระบบมีความแข็งแกร่ง (System Hardening) มีการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) และการแบ่งปันข้อมูล (Information Sharing) รวมถึงมีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Awareness) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๒.๔)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีการควบคุมการเข้าถึง (Access Control) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการทำให้ระบบมีความแข็งแกร่ง (System Hardening) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หน่วยงานจะต้องมีการบริหารจัดการเชื่อมต่อระยะไกล (Remote Connection) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการบริหารจัดการสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการแบ่งปันข้อมูล (Information Sharing) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Awareness) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๕	หน่วยงานจะต้องพิจารณาการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) หรือพิจารณาการพิสูจน์ตัวตนจากระบบเชื่อมโยงข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) ตามข้อเสนอแนะของ สพร. นอกเหนือจากการควบคุมการเข้าถึง (Access Control) ข้อ ๖.๒.๔ โดยหน่วยงานควรจะพิจารณาตรวจสอบตัวตนของผู้ใช้งานโดยใช้ปัจจัยที่แตกต่างกันมากกว่าหนึ่งปัจจัย และอาจจะพิจารณาตัวอย่างการใช้งาน MFA ให้เป็นไปตามรายละเอียดข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๖.๒.๕)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
๘.๖	หน่วยงานจะต้องตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โปรแกรมประยุกต์บนเว็บ (Web Application) ระบบบริหารจัดการเว็บไซต์ (CMS) ระบบปฏิบัติการ (Operating System) และการตั้งค่าฐานข้อมูล (หัวข้อ ๖.๒.๖)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานควรจะมีการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) โดยอาจจะพิจารณาการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานตาม CIS Benchmark ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาให้มีการตั้งค่าเพื่อความมั่นคงปลอดภัยพื้นฐานของโปรแกรมประยุกต์บนเว็บ (Web Application) ตามหัวข้อที่ ๔ ของเอกสารข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ โดยอาจจะพิจารณาใช้รายการตรวจสอบ Web Application ของโครงการ OWASP ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาหลักการที่สำคัญที่ต้องตั้งค่าระบบ CMS ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานควรจะพิจารณาการตั้งค่าเพื่อเพิ่มความมั่นคงปลอดภัยของระบบปฏิบัติการเบื้องต้นตาม NIST SP 800-123 ซึ่งนำไปประยุกต์ใช้กับระบบปฏิบัติการทุกประเภท	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หน่วยงานควรจะพิจารณารายละเอียดในการตั้งค่าฐานข้อมูลเพื่อให้มีความมั่นคงปลอดภัย ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๗	หน่วยงานจะต้องกำหนดแนวทางและการเลือกบริการที่เกี่ยวข้องกับเว็บไซต์ ประกอบด้วย เครื่องบริการเว็บ (Web Server) ระบบบริหารจัดการเว็บไซต์ (CMS) เลือกบริการโดเมนและชื่อโดเมน และขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate (หัวข้อ ๖.๒.๗)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือกบริการเครื่องบริการเว็บ โดยอาจจะพิจารณาแนวทางและการเลือกบริการ ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือก CMS ที่มีความมั่นคงปลอดภัย โดยอาจจะพิจารณาแนวทางและการเลือก CMS ซึ่งมีรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือกผู้รับจดทะเบียนชื่อโดเมน โดยอาจจะพิจารณาแนวทางและการเลือก ซึ่งรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องกำหนดแนวทางและการเลือกขั้นตอนวิธีการเข้ารหัส Cipher Suite ของ TLS Certificate โดยอาจจะพิจารณาแนวทางและการเลือก รวมถึงรายละเอียดในการเลือกระดับการรับรอง ซึ่งรายละเอียดตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๘.๘	หน่วยงานจะต้องตั้งค่าไฟร์วอลล์เพื่อควบคุมและป้องกันการบุกรุกต่าง ๆ ที่เกิดขึ้นกับเว็บไซต์ โดยควรจะพิจารณาหลักการตั้งค่าอย่างน้อย ดังนี้ การกำหนดนโยบายความมั่นคงปลอดภัย (Define Security Policies) การตั้งค่ากฎการกรอง (Configure Filtering Rules) การจำกัด		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
	การเข้าถึงโดยภูมิศาสตร์ (Geographic Restrictions) การป้องกันการโจมตี (Protect Against Attacks) การตรวจสอบและบันทึก (Monitoring and Logging) และการปรับปรุงและอัปเดตเป็นประจำ (Regular Updates) โดยอาจจะพิจารณาหลักการตั้งค่าไฟร์วอลล์ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้ (หัวข้อ ๖.๒.๘)			
๙	**มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Detection) (หัวข้อ ๖.๓)**			
๙.๑	หน่วยงานจะต้องมีการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๓.๑)		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีการสร้างกลไกและกระบวนการ เพื่อตรวจจับ จัดประเภท วิเคราะห์ และระบุว่ามีภัยคุกคามหรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องเว็บไซต์ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการทบทวนกลไกและกระบวนการอย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง ตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
๑๐	**การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Incident Response) (หัวข้อ ๖.๔)**			
๑๐.๑	หน่วยงานจะต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Incident Response Plan) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ของเว็บไซต์ รวมถึงแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) และการฝึกซ้อมความมั่นคงปลอดภัย ไซเบอร์สำหรับเว็บไซต์ (Website		☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
	Security Exercise) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๔.๑)			
		หน่วยงานจะต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website security Incident Response Plan) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอาจจะพิจารณาคำแนะนำและข้อควรพิจารณาในการตอบสนองต่อเหตุการณ์สำหรับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST ตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการสื่อสาร ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ของเว็บไซต์ และมีการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ (Website Security Exercise) โดยพิจารณาฝึกซ้อมอย่างน้อยปีละ ๑ ครั้ง ให้เป็นไปตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ ให้เป็นไปตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยหน่วยงานอาจจะพิจารณาระบุรายละเอียด ให้เป็นไปตามข้อเสนอแนะและคำอธิบายเพิ่มเติมของมาตรฐานฉบับนี้	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ทั้งในระดับชาติหรือระดับภาคส่วน เช่น ฝึกซ้อมกับ สกมช. หรือหน่วยงานควบคุม	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

ที่	ข้อกำหนด	ข้อเสนอแนะ	การประเมิน	หลักฐาน
		หรือกำกับดูแล รวมถึงตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามความเหมาะสม ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์		
๑๑	**การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Recovery) (หัวข้อ ๖.๕)**			
๑๑.๑	หน่วยงานจะต้องมีการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับเว็บไซต์ (Website Security Resilience and Recovery) โดยจะต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และจะต้องจัดให้มีการฝึกซ้อมให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (หัวข้อ ๖.๕.๑)	☐ ยังต้องปรับปรุง ☐ ดำเนินการแล้ว	
		หน่วยงานจะต้องมีจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอาจจะพิจารณาให้มีรายละเอียดของแผนตามการบริหารความพร้อมต่อสภาวะวิกฤติ (การทำแผน BCP) ของสำนักงานคณะกรรมการพัฒนาระบบราชการ	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	
		หน่วยงานจะต้องมีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรืออาจจะพิจารณาตามความเหมาะสมตามสภาพของหน่วยงาน ให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	☐ ดำเนินการแล้ว ☐ อยู่ในระหว่างดำเนินการ ☐ ยังไม่ได้ดำเนินการ	

แบบฟอร์ม ค๒ แบบรายงานรายการที่ยังต้องปรับปรุง

สำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และหน่วยงานเอกชน

<u>คำแนะนำ</u> เมื่อหน่วยงานพบรายการที่ไม่เป็นไปตามข้อกำหนด ที่มีสถานะ “ยังต้องปรับปรุง” ตามผลการประเมินตามแบบฟอร์ม ค๑ ให้ระบุรายการที่ยังต้องปรับปรุงลงในแบบฟอร์มนี้

วันที่ประเมินตนเอง (Self-Assessment).....หน่วยงานเจ้าของเว็บไซต์.....

ชื่อเว็บไซต์.....การเข้าถึงเว็บไซต์ หรือ URL.....

ลำดับ	ข้อกำหนดที่ยังต้องปรับปรุง	สาเหตุ	การปรับปรุงแก้ไขในเบื้องต้น	สิ่งที่ต้องการปรับปรุงแก้ไข		
				รายการแก้ไข	ผู้รับผิดชอบดำเนินการ	กำหนดวันที่แล้วเสร็จ

ผู้กรอกแบบรายงาน.....ตำแหน่ง.....

สังกัดหน่วยงาน (ภายใน).....เบอร์โทร.....อีเมล.....

บรรณานุกรม

๑. Mark Curphey JS, Erik Olson Improving Web Application Security: Threats and Countermeasures. Microsoft.

๒. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 2024 [updated 26/02/2024: [Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

๓. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ.

๔. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. สถิติภัยคุกคามทางไซเบอร์ ๒๕๖๖ [Available from: https://www.ncsa.or.th/service-statistics.html.

๕. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒ [Available from: https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF.

๖. วิไลลักษณ์ ก. คอมพิวเตอร์เบื้องต้น (ฉบับปรับปรุงครั้งที่ ๒). กรุงเทพฯ: มหาวิทยาลัยสุโขทัยธรรมาธิราช; ๒๕๖๖.

๗. สมาคมผู้ดูแลเว็บและสื่อออนไลน์ไทย. เว็บไซต์ (Website) คืออะไร? date unknown [Available from: https://www.webmaster.or.th/website.

๘. Cambridge University Press & Assessment. Cambridge English Dictionary date unknown [Available from: https://dictionary.cambridge.org/dictionary/english/.

๙. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. Website D.I.Y. ๒๕๖๗. Available from: https://www.etda.or.th/th/Useful-Resource/documents-for-download/Website-D-I-Y.aspx.

๑๐. Amazon Web Services I. What is Cloud Hosting? [Available from: https://aws.amazon.com/what-is/cloud-hosting/.

๑๑. National Institute of Standards and Technology. Web Server date unknown [Available from: https://csrc.nist.gov/glossary/term/web_server.

๑๒. Sciencedirect. Web Server Software 2016 [Available from: https://www.sciencedirect.com/topics/computer-science/web-server-software.

๑๓. National Institute of Standards and Technology. NIST Special Publication 800-152 A Profile for U.S. Federal Cryptographic Key Management Systems. 2015.

๑๔. National Institute of Standards and Technology. Secure Sockets Layer (SSL) date unknown [Available from: https://csrc.nist.gov/glossary/term/secure_sockets_layer.

๑๕. National Institute of Standards and Technology. NIST Special Publication 1800-15 Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD). 2021.

๑๖. Raghu Ramakrishnan JG. Database management systems. Boston: Mcgraw-Hill; 2003.

๑๗. National Institute of Standards and Technology. NIST Special Publication 1800-16 Securing Web Transactions: TLS Server Certificate Management. 2020.

๑๘. Kaufman DECW. Domain Name System Security Extensions 1997 [Available from: https://datatracker.ietf.org/doc/html/rfc2065.

๑๙. merriam-webster. fire wall 2024 [Available from: https://www.merriam-webster.com/dictionary/firewall.

๒๐. OWASP. Web Application Firewall 2024 [Available from: https://owasp.org/www-community/Web_Application_Firewall.

๒๑. Gartner. Endpoint Detection and Response (EDR) Solutions Reviews 2020 [Available from: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

๒๒. Gartner Research. Innovation Insight for Extended Detection and Response 2020 [updated 19 March 2020. Available from: https://www.gartner.com/en/documents/3982247.

๒๓. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ. ๒๕๖๖.

๒๔. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ ๒๕๖๖ [Available from: https://www.ncsa.or.th/.

๒๕. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์. ๒๕๖๗.

๒๖. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. คำแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ. ๒๕๖๖.

๒๗. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ. ๒๕๖๐.

๒๘. สำนักงานพัฒนารัฐบาลดิจิทัล. มาตรฐานเว็บไซต์ภาครัฐ (Government Website Standard Version 3.0) ๒๕๕๖.

๒๙. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย. ๒๕๕๕.

๓๐. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช). คำแนะนำ สกมช. เรื่อง แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๒๕๖๖.

๓๑. National Institute of Standards and Technology. NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization 2014 [Available from: https://csrc.nist.gov/pubs/sp/800/88/r1/final.

๓๒. OWASP. Welcome to the OWASP Top 10 2021 [Available from: https://owasp.org/Top10/.

๓๓. สำนักงานคณะกรรมการพัฒนาระบบราชการ. การบริหารความพร้อมต่อสภาวะวิกฤติ (การทำแผน BCP) ๒๕๖๓ [Available from: https://www.opdc.go.th/content/NjE3Mg.

๓๔. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ ๒๕๖๘ [Available from: https://www.ncsa.or.th/policy/WebsiteSecurityPolicy.

๓๕. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). นโยบายและคู่มือบริหารความเสี่ยง (Enterprise Risk Management Manual) ๒๕๖๔ Available from: https://www.dga.or.th

๓๖. บริษัท ปตท. จำกัด (มหาชน). มาตรการตรวจสอบการใช้ดุลยพินิจ ๒๕๖๕ [Available from: https://www.pttplc.com/.

๓๗. Ho A. Roles of Three Lines of Defense for Information Security and Governance 2018 [Available from: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance.

๓๘. สำนักงานเลขาธิการคณะรัฐมนตรี. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล. ๒๕๖๒ [Available from: https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF.

๓๙. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ๒๕๖๔ [Available from: https://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/188/T_0009.PDF.

๔๐. National Institute of Standards and Technology (NIST). FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems 2006 [Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

๔๑. U.S. Department of Homeland Security. CVE Program 1999 [Available from: https://cve.mitre.org/.

๔๒. Abbasi S. 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is 2023 [Available from: https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one.

๔๓. OWASP. Matrix DSOMM. 2024. [Available from: https://dsomm.owasp.org/

๔๔. National Institute of Standards and Technology. NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management 2024 [Available from: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf.

๔๕. Center for Internet Security. CIS Password Policy Guide 2021 [Available from: https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide.

๔๖. NIST. NIST SP 800-123 Guide to General Server Security 2008 [Available from: https://csrc.nist.gov/pubs/sp/800/123/final.

๔๗. Defense Information Systems Agency (DISA). STIGs Document Library 2025 [Available from: https://public.cyber.mil/stigs/downloads/.

๔๘. Center for Internet Security. CIS Benchmarks List 2025 [Available from: https://www.cisecurity.org/cis-benchmarks.

๔๙. OWASP. Web Application Checklist 2025 [Available from: https://owasp.org/www-project-developer-guide/draft/06-design/02-web-app-checklist/00-toc#checklist-define-security-requirements.

๕๐. Byers K. Domain Extensions: .com vs .org, .net, .io & 4 Other TLDs 2022 [updated 30/1/2022. Available from: https://growthbadger.com/top-level-domains/.

๕๑. National Institute of Standards and Technology (NIST). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile 2024 [Available from: https://csrc.nist.gov/pubs/sp/800/61/r3/final.