



แนวทางการประยุกต์ใช้มาตรฐาน การรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ ขององค์กรปกครองส่วนท้องถิ่น

สทศัน ไซตวงศ์¹, สุภากรณ ศรีดี² และกวิทร์ ศรีสัมฤทธิ์³

Received: January 14, 2026

Revised: February 27, 2026

Accepted: March 2, 2026

บทคัดย่อ

บทความวิชาการนี้มีวัตถุประสงค์เพื่อนำเสนอแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ขององค์กรปกครองส่วนท้องถิ่น (อปท.) ให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 ที่ประกาศโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยใช้วิธีการวิจัยเอกสาร (Documentary Research) ในการรวบรวมและสังเคราะห์ข้อมูลจากกฎหมาย มาตรฐานสากล และบริบทปัญหาของหน่วยงานท้องถิ่นที่มักเผชิญข้อจำกัดด้านงบประมาณและบุคลากร ผลการศึกษาพบว่า การนำมาตรฐานฯ มาประยุกต์ใช้ให้เกิดผลสัมฤทธิ์ต้องอาศัยแนวทางปฏิบัติใน 3 ระยะ ได้แก่ (1) ระยะการกำกับดูแล โดยเน้นการกำหนดเจ้าภาพผู้รับผิดชอบความเสี่ยง (Risk Owner) และการปรับปรุงข้อกำหนดในขอบเขตงาน (TOR) เพื่อควบคุมคุณภาพผู้ให้บริการภายนอกผ่านการประเมินช่องโหว่ (Vulnerability Assessment) (2) ระยะการสร้างภูมิคุ้มกันทางเทคนิค ผ่านการตั้งค่าความปลอดภัยขั้นพื้นฐานและการบริหารจัดการแพตช์ และ (3) ระยะการเฝ้าระวัง โดยส่งเสริมการใช้เครื่องมือประเมินตนเอง (Self-Assessment) การจัดทำแผนเผชิญเหตุ และการสร้างความร่วมมือระหว่างท้องถิ่นเพื่อแบ่งปันทรัพยากร ซึ่งแนวทางเหล่านี้จะช่วยยกระดับความมั่นคงปลอดภัยไซเบอร์และนำไปสู่การสร้างเชื่อมั่นทางดิจิทัล (Digital Trust) ให้แก่ประชาชนได้อย่างยั่งยืน

คำสำคัญ: มาตรฐานความปลอดภัยเว็บไซต์ / องค์กรปกครองส่วนท้องถิ่น / ความมั่นคงปลอดภัยไซเบอร์ / ความเชื่อมั่นทางดิจิทัล / สกมช.

¹ผู้รับผิดชอบบทความ: สทศัน ไซตวงศ์ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช E-mail: sahathuc@gmail.com

¹นักศึกษาคณะศึกษาศาสตร์ สาขาวิชานิติศาสตร์ สาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

²รองศาสตราจารย์ ดร. หลักสูตรปรัชญาดุษฎีบัณฑิต สาขานิติศาสตร์ สาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

³ดร. หลักสูตรปรัชญาดุษฎีบัณฑิต สาขานิติศาสตร์ สาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

Guidelines for Applying Website Security Standards to Enhance Cybersecurity in Local Government

Sahathust Chotivong¹, Supaporn Sridee² and Kawit Srisamrit³

Abstract

This academic article aims to propose guidelines for maintaining website security in Local Government in compliance with the Website Security Standards B.E. 2568 (2025) issued by the National Cyber Security Committee (NCSC). Employing documentary research, this study synthesizes data from relevant laws, international standards, and the specific context of LAOs, which often face constraints regarding budget and personnel. The findings suggest that effective implementation of the standards requires a three-phase approach: 1) Governance Phase, focusing on designating a Risk Owner and optimizing Terms of Reference (TOR) to control outsourcing quality through mandatory Vulnerability Assessments; 2) Technical Protection Phase, emphasizing fundamental secure configurations and patch management; and 3) Monitoring Phase, encouraging the use of self-assessment tools, actionable incident response plans, and inter-municipal collaboration for resource sharing. Implementing these guidelines will essentially enhance cybersecurity resilience and foster sustainable Digital Trust among citizens.

Keywords: Website security standards / Local government / Cybersecurity / Digital trust / NCSA

¹ **Corresponding Author:** Sahathust Chotivong, Faculty of Communication arts, Sukhothai Thammathirat Open University,
E-mail: sahathuc@gmail.com

¹ Student of Education program in Communication Innovation for Political and Local Administration, School of Communication Art, Sukhothai Thammathirat Open University

² Associate Professor Dr. of Education program in Communication Innovation for Political and Local Administration, School of Communication Art, Sukhothai Thammathirat Open University

³ Dr. of Education program in Communication Innovation for Political and Local Administration, School of Communication Art, Sukhothai Thammathirat Open University

1. บทนำ

ในปัจจุบันการพัฒนางองค์การปกครองส่วนท้องถิ่นสู่การเป็นรัฐบาลดิจิทัล (Digital Local Government) ถือเป็นยุทธศาสตร์สำคัญในการยกระดับประสิทธิภาพการให้บริการสาธารณะและการอำนวยความสะดวกแก่ประชาชน โดยมี เว็บไซต์ เป็นเครื่องมือสื่อสารหลักและเปรียบเสมือนประตูหน้าบ้านทางดิจิทัล (Digital Front Door) ที่เชื่อมโยงความสัมพันธ์ระหว่างรัฐกับประชาชน อย่างไรก็ตามท่ามกลางกระแสการเปลี่ยนแปลงทางเทคโนโลยี ภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรงและซับซ้อนยิ่งขึ้น โดยเฉพาะการโจมตีเว็บไซต์ของหน่วยงานภาครัฐในระดับท้องถิ่นที่มักตกเป็นเป้าหมายสำคัญไม่ว่าจะเป็นการเปลี่ยนแปลงหน้าเว็บไซต์ (Web Defacement) หรือการฝังโฆษณาเว็บพแนอนไลน์ซึ่งส่งผลกระทบต่อภาพลักษณ์และความน่าเชื่อถือขององค์กร สาเหตุสำคัญของปัญหาดังกล่าวส่วนหนึ่งเกิดจากข้อจำกัดด้านทรัพยากรบุคคลและงบประมาณขององค์กรปกครองส่วนท้องถิ่น รวมไปถึงการขาดแนวปฏิบัติที่เป็นมาตรฐานในการกำกับดูแลและบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ ด้วยเหตุนี้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) จึงได้ประกาศใช้ มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 เพื่อเป็นกลไกในการกำหนดกรอบการดำเนินงานขั้นพื้นฐานให้หน่วยงานของรัฐต้องถือปฏิบัติ เพื่อป้องกันและรับมือกับความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพ

สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทยยังคงน่าเป็นห่วง โดยสถิติพบว่าหน่วยงานด้านการศึกษาและหน่วยงานของรัฐตกเป็นเป้าหมายการโจมตีสูงสุด มีการโจมตีหน่วยงานการศึกษากว่า 632 ครั้ง และหน่วยงานรัฐอื่น ๆ กว่า 461 ครั้ง รูปแบบภัยคุกคามที่พบบ่อยที่สุดคือการแฮ็กเว็บไซต์เพื่อฝังโฆษณาพแนอนไลน์ (Web Defacement) และการโจมตีเพื่อเปลี่ยนแปลงหน้าเว็บไซต์ ซึ่งสอดคล้องกับแนวโน้มในปีที่พบการพยายามบุกรุกระบบ (Intrusion Attempts) สูงถึง 1,133 ครั้งในช่วงเดือนมกราคมถึงตุลาคม (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2566) ตัวเลขเหล่านี้สะท้อนให้เห็นว่าเว็บไซต์ของหน่วยงานท้องถิ่นมีความเสี่ยงสูงที่จะถูกใช้เป็นฐานในการก่ออาชญากรรมทางไซเบอร์หากขาดมาตรการป้องกันที่ได้มาตรฐาน

บทความวิชาการนี้จึงใช้วิธีการวิจัยเอกสาร (Documentary Research) โดยมุ่งเน้นการรวบรวมและสังเคราะห์ข้อมูลจากเอกสารทุติยภูมิ (Secondary Source) ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมาตรฐานสากลที่เกี่ยวข้อง เพื่อถอดบทเรียนจากมาตรฐานดังกล่าวสู่การปฏิบัติจริง ทั้งในมิติด้านการบริหารจัดการและการควบคุมทางเทคนิค สรุปเป็นแนวทางที่เหมาะสมกับบริบทขององค์กรปกครองส่วนท้องถิ่น เพื่อให้ผู้บริหารและเจ้าหน้าที่สามารถนำไปใช้เป็นกรอบในการยกระดับความมั่นคงปลอดภัยและสร้างความเชื่อมั่นทางดิจิทัล (Digital Trust) ให้แก่ประชาชนในพื้นที่ได้อย่างยั่งยืน

2. วัตถุประสงค์ของบทความ

2.1 เพื่อศึกษาและวิเคราะห์สาระสำคัญของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

2.2 เพื่อนำเสนอแนวทางปฏิบัติ (Guidelines) ที่เหมาะสมสำหรับการนำไปประยุกต์ใช้เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ในบริบทขององค์กรปกครองส่วนท้องถิ่น

3. สาระสำคัญของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

จากการศึกษาและวิเคราะห์เอกสาร มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 ซึ่งเป็นกฎหมายลำดับรองที่ออกตามความในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พบว่ามาตรฐานดังกล่าวถูกกำหนดขึ้นเพื่อเป็นเกณฑ์ขั้นต่ำ (Baseline Security) ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ถือปฏิบัติ โดยมีเจตนารมณ์เพื่อสร้างภูมิคุ้มกันทางไซเบอร์ให้กับบริการสาธารณะดิจิทัล มาตรฐานฉบับนี้ถูกออกแบบบนพื้นฐานหลักการความมั่นคงปลอดภัยสารสนเทศ 3 ประการ (CIA Triad) ได้แก่ 1) การรักษาความลับ (Confidentiality) การป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยเฉพาะข้อมูลส่วนบุคคลของประชาชน 2) ความถูกต้องครบถ้วน (Integrity) การป้องกันไม่ให้น้ำเว็บไซต์หรือข้อมูลถูกแก้ไขเปลี่ยนแปลงโดยมิชอบ และ 3) ความพร้อมใช้งาน (Availability) การรับประกันว่าระบบเว็บไซต์จะสามารถให้บริการประชาชนได้ตลอดเวลาโดยไม่หยุดชะงักจากการโจมตี ซึ่งมาตรฐานนี้ครอบคลุมทั้งระบบที่ติดตั้งภายในหน่วยงาน (On-Premises) และระบบบนคลาวด์ (Cloud) (ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568, 2568) ทั้งนี้ ผู้วิจัยได้สังเคราะห์สาระสำคัญออกเป็น 2 มิติหลัก เพื่อให้สอดคล้องกับบริบทการบริหารงานขององค์กรปกครองส่วนท้องถิ่น ได้แก่ มิติด้านการกำกับดูแลและการบริหารจัดการ และมิติด้านการควบคุมทางเทคนิค ดังนี้

3.1 มิติด้านการกำกับดูแลและการบริหารจัดการ มาตรฐานฯ ให้ความสำคัญสูงสุดกับบทบาทของผู้บริหารองค์กรและการวางโครงสร้างการทำงานที่ชัดเจน โดยนำหลักการบริหารความเสี่ยงระดับองค์กรมาประยุกต์ใช้ ซึ่งประกอบด้วยองค์ประกอบสำคัญ ดังนี้

3.1.1 การกำหนดนโยบายและโครงสร้างความรับผิดชอบ (Policy and Roles) หน่วยงานต้องจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์เป็นลายลักษณ์อักษร และสื่อสารให้บุคลากรรับทราบ ที่สำคัญคือต้องมีการระบุ เจ้าของความเสี่ยง (Risk Owner) และผู้รับผิดชอบดูแลระบบให้ชัดเจน เพื่อป้องกันปัญหาความคลุมเครือในการตัดสินใจเมื่อเกิดเหตุภัยคุกคาม

3.1.2 การบริหารจัดการผู้ให้บริการภายนอก (Third-Party Management) เนื่องจากหน่วยงานรัฐส่วนใหญ่นิยมใช้วิธีการจ้างเหมาบริการ (Outsourcing) มาตรฐานฯ จึงกำหนดให้หน่วยงานต้องระบุข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirements) ไว้อย่างชัดเจนในขอบเขตของงาน

(Terms of Reference: TOR) และสัญญาจ้าง โดยเฉพาะการกำหนดเงื่อนไขให้ผู้ให้บริการต้องส่งมอบรายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report) ก่อนการส่งมอบงาน และต้องมีการรับประกันการอัปเดตแพตช์ความปลอดภัยตลอดอายุสัญญา

ในการสื่อสารและเผยแพร่ข้อมูลบนเว็บไซต์ หน่วยงานท้องถิ่นต้องระมัดระวังการตีความ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่คลาดเคลื่อนจนนำไปสู่การปิดบังข้อมูลสาธารณะที่ควรเปิดเผย (เช่น ข้อมูลการจัดซื้อจัดจ้าง) หน่วยงานควรใช้วิธีการทำข้อมูลให้เป็นนิรนาม (Anonymization) หรือปกปิดเฉพาะข้อมูลอ่อนไหว แทนการลบข้อมูลทิ้งทั้งหมด เพื่อรักษาคุณภาพระหว่างการคุ้มครองสิทธิส่วนบุคคล และความโปร่งใสในการบริหารงาน (สลิทธ ทองมีนสุข และโชติกา เชียงหลิว, 2568)

3.1.3 การตรวจสอบและประเมินผล (Audit and Assessment) หน่วยงานต้องจัดให้มีการตรวจสอบสถานะความมั่นคงปลอดภัยของเว็บไซต์อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการปรับปรุงเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่ามาตรการป้องกันยังคงมีประสิทธิภาพและสอดคล้องกับสถานการณ์ภัยคุกคามปัจจุบัน

3.2 มิติด้านการควบคุมทางเทคนิค ในส่วนของการปฏิบัติการ มาตรฐานฯ ได้กำหนดมาตรการทางเทคนิคโดยอ้างอิงแนวปฏิบัติสากล อาทิ OWASP Top 10 และ NIST SP 800-63B (National Institute of Standards and Technology, 2017; OWASP Foundation, 2025) เพื่อปิดช่องโหว่ที่พบบ่อย โดยมีประเด็นสำคัญ ดังนี้

3.2.1 การเข้ารหัสข้อมูลและการสื่อสาร (Encryption) เว็บไซต์ของหน่วยงานรัฐต้องรองรับการเชื่อมต่อผ่านโปรโตคอล HTTPS (Hypertext Transfer Protocol Secure) เพื่อป้องกันการดักจับข้อมูลระหว่างการรับส่ง และต้องมีการบริหารจัดการใบรับรองอิเล็กทรอนิกส์ (SSL/TLS Certificate) ให้มีความถูกต้องและเป็นปัจจุบัน

3.2.2 การพิสูจน์ตัวตนและการจัดการสิทธิ์ (Authentication and Access Control) ระบบบริหารจัดการเว็บไซต์ (Back-end System) ต้องมีกลไกการพิสูจน์ตัวตนที่รัดกุม โดยมาตรฐานฯ ส่งเสริมให้ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับบัญชีผู้ดูแลระบบ และกำหนดสิทธิ์การเข้าถึงข้อมูลตามหลักความจำเป็น (Least Privilege) เพื่อจำกัดความเสียหายหากบัญชีถูกประนีประนอม

3.2.3 การจัดการช่องโหว่และการเฝ้าระวัง (Vulnerability Management and Monitoring) หน่วยงานต้องมีกระบวนการอัปเดตซอฟต์แวร์ ระบบปฏิบัติการ และส่วนเสริม (Plugins) ให้เป็นเวอร์ชันปัจจุบันอย่างสม่ำเสมอ (Patch Management) รวมถึงต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) อย่างน้อย 90 วัน ตามกฎหมาย เพื่อใช้เป็นหลักฐานในการสืบสวนสอบสวนหากเกิดเหตุการณ์ความมั่นคงปลอดภัย

4. สถานการณ์และข้อจำกัดขององค์กรปกครองส่วนท้องถิ่นในการรักษาความมั่นคงปลอดภัยไซเบอร์

แม้ว่ามาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 จะเป็นกฎหมายที่บังคับใช้กับหน่วยงานของรัฐทุกระดับ แต่ในทางปฏิบัติ องค์กรปกครองส่วนท้องถิ่น (อปท.) ซึ่งประกอบด้วย องค์กรบริหารส่วนจังหวัด เทศบาล และองค์การบริหารส่วนตำบล กลับต้องเผชิญกับความท้าทายและข้อจำกัดเชิงโครงสร้างที่แตกต่างจากหน่วยงานส่วนกลางอย่างสิ้นเชิง จากการศึกษาบริบทการทำงานพบว่า อุปสรรคสำคัญที่ส่งผลกระทบต่อประสิทธิภาพในการปฏิบัติตามมาตรฐานฯ มี 3 ประการสำคัญ ดังนี้

4.1 ข้อจำกัดด้านบุคลากรและองค์ความรู้ โครงสร้างอัตรากำลังขององค์กรปกครองส่วนท้องถิ่นส่วนใหญ่ ไม่ได้กำหนดตำแหน่ง นักวิชาการคอมพิวเตอร์ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ไว้ โดยเฉพาะ ภารกิจในการดูแลเว็บไซต์จึงมักถูกมอบหมายให้เป็นหน้าที่รองของเจ้าหน้าที่ฝ่ายประชาสัมพันธ์ ฝ่ายแผนงาน หรือนักจัดการงานทั่วไป ซึ่งขาดความรู้ความเข้าใจเชิงลึกในด้านเทคนิค (Technical Know-how) ตัวอย่างเช่น เมื่อเว็บไซต์เกิดเหตุขัดข้องจากการถูกโจมตีทางไซเบอร์ เช่น การถูกฝังโฆษณาเว็บพแนอนไลน์ (Web Defacement) เจ้าหน้าที่ผู้ดูแลมักไม่สามารถวิเคราะห์สาเหตุจากข้อมูลจราจรคอมพิวเตอร์ (Log Analysis) เพื่อหาช่องโหว่ได้ ทำได้เพียงการแจ้งผู้ให้บริการเพื่อกู้คืนข้อมูล (Restore) กลับมาเท่านั้น ซึ่งเป็นการแก้ปัญหาที่ปลายเหตุและทำให้ช่องโหว่เดิมยังคงอยู่ ส่งผลให้ระบบมีความเสี่ยงที่จะถูกโจมตีซ้ำในลักษณะเดิม

4.2 การพึ่งพาผู้ให้บริการภายนอกในระดับสูง เนื่องจากข้อจำกัดด้านบุคลากร การพัฒนาและดูแลเว็บไซต์ของท้องถิ่นจึงนิยมใช้วิธีการจ้างเหมาบริการจากภาคเอกชน (Outsourcing) เป็นหลัก ปัญหาที่พบคือ สัญญาจ้างมักเป็นแบบปีต่อปีหรือตามโครงการ ทำให้ขาดความต่อเนื่องในการดูแลรักษา (Maintenance Continuity) กรณีศึกษาที่พบบ่อย เมื่อมีการเปลี่ยนผู้รับจ้างรายใหม่ มักเกิดปัญหาการส่งต่อข้อมูล (Handover) ที่ไม่ครบถ้วน เช่น หน่วยงานไม่มีรหัสผ่านระดับผู้ดูแลระบบสูงสุด (Super Admin) หรือ Source Code ที่ได้รับมอบมา มีการเข้ารหัส (Encrypt) โดยผู้รับจ้างรายเดิม ทำให้หน่วยงานตกอยู่ในสภาวะ การถูกผูกขาดโดยเทคนิค (Vendor Lock-in) ไม่สามารถเข้าไปบริหารจัดการ อัปเดตแพตช์ความปลอดภัย หรือแก้ไขการตั้งค่าเซิร์ฟเวอร์ให้สอดคล้องกับมาตรฐานใหม่ได้ด้วยตนเอง จำเป็นต้องว่าจ้างรายเดิมต่อไปเรื่อยๆ อย่างหลีกเลี่ยงไม่ได้

4.3 ข้อจำกัดด้านงบประมาณและทรัพยากร การปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ระดับสูง มักต้องอาศัยงบประมาณในการจัดซื้ออุปกรณ์หรือซอฟต์แวร์ป้องกัน เช่น Web Application Firewall (WAF) หรือระบบตรวจจับผู้บุกรุก ซึ่งสำหรับท้องถิ่นขนาดเล็ก งบประมาณส่วนใหญ่ถูกจัดสรรไปเพื่อการพัฒนาโครงสร้างพื้นฐานและการบริการสาธารณะด้านอื่น ทำให้การตั้งงบประมาณเพื่อป้องกัน สิ่งที่ยังไม่เกิด (Intangible Risk) มักถูกจัดลำดับความสำคัญไว้ท้ายสุด

ผลกระทบที่เป็นรูปธรรม ด้วยงบประมาณที่จำกัด หน่วยงานท้องถิ่นจำนวนมากจึงเลือกใช้บริการเช่าพื้นที่เว็บไซต์แบบรวม (Shared Hosting) ราคาประหยัดที่มีมาตรการความปลอดภัยต่ำและใช้ทรัพยากรร่วมกับเว็บไซต์อื่นๆ ส่งผลให้เมื่อเว็บไซต์ใดเว็บไซต์หนึ่งในเซิร์ฟเวอร์เดียวกันถูกโจมตี เว็บไซต์ของหน่วยงานก็มีความเสี่ยงที่จะได้รับผลกระทบไปด้วย (Cross-site Contamination) ทำให้กลายเป็นเป้าหมายที่อ่อนแอ (Soft Target) ที่กลุ่มแฮกเกอร์มักใช้เป็นฐานในการโจมตีต่อไป

จากข้อจำกัดข้างต้น แสดงให้เห็นว่าการจะนำมาตรฐานฯ มาบังคับใช้กับองค์กรปกครองส่วนท้องถิ่น จะต้องอาศัย แนวทางปฏิบัติ (Guidelines) ที่ไม่เน้นความซับซ้อนทางเทคนิคจนเกินไป แต่เน้นการปรับกระบวนการบริหารจัดการและการสร้างกลไกควบคุมผู้ให้บริการภายนอกให้รัดกุมยิ่งขึ้น ซึ่งจะเป็นหัวใจสำคัญในหัวข้อถัดไป

5. แนวทางการประยุกต์ใช้มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ในบริบทองค์กรปกครองส่วนท้องถิ่น

จากการวิเคราะห์สาระสำคัญของมาตรฐานฯ และข้อจำกัดเชิงโครงสร้างขององค์กรปกครองส่วนท้องถิ่นข้างต้น ผู้เขียนขอเสนอแนวทางการประยุกต์ใช้มาตรฐาน (Guidelines) โดยเน้นกระบวนการที่ทำให้ได้จริง คุ่มค่า และยั่งยืน ซึ่งแบ่งออกเป็น 3 ระยะการดำเนินงาน ดังนี้

5.1 ระยะการกำกับดูแลและจัดทำข้อกำหนด เป็นขั้นตอนที่สำคัญที่สุดในการแก้ปัญหาเชิงโครงสร้าง โดยผู้บริหารท้องถิ่นต้องเปลี่ยนบทบาทจากการเป็นเพียงผู้เซ็นอนุมัติมาเป็นผู้กำกับดูแลความเสี่ยง

5.1.1 การกำหนดเจ้าภาพที่ชัดเจน ควรมีการแต่งตั้งคณะทำงานดูแลเว็บไซต์หรือมอบหมายให้มีเจ้าภาพหลัก (เช่น หัวหน้าสำนักปลัด หรือผู้อำนวยการกองวิชาการ หรือกองสารสนเทศ) รับผิดชอบในฐานะ Risk Owner เพื่อให้มีผู้มีอำนาจตัดสินใจเมื่อเกิดวิกฤต แทนที่จะปล่อยให้เป็นการละเลยของเจ้าหน้าที่ระดับปฏิบัติการเพียงลำพัง

5.1.2 การปฏิรูปกระบวนการจัดจ้าง ในการจ้างพัฒนาหรือบำรุงรักษาเว็บไซต์ครั้งต่อไป หน่วยงานต้องระบุเงื่อนไขในขอบเขตของงาน (TOR) ให้สอดคล้องกับมาตรฐานฯ อย่างเคร่งครัดโดยใช้การคำนึงถึงความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในกระบวนการจัดซื้อจัดจ้าง ได้แก่

1) *ความเป็นเจ้าของสิทธิ์* กำหนดให้ผู้รับจ้างต้องส่งมอบ Source Code และรหัสผ่านระดับผู้ดูแลระบบสูงสุด (Super Admin) ให้แก่หน่วยงาน เพื่อป้องกันปัญหา Vendor Lock-in

2) *การประกันคุณภาพความปลอดภัย* ผู้รับจ้างต้องส่งมอบรายงานผลการตรวจสอบช่องโหว่ (Vulnerability Assessment Report) จากผู้เชี่ยวชาญที่เป็นบุคคลที่สาม (Third Party) ก่อนการตรวจรับงวดงานสุดท้าย เพื่อยืนยันว่าเว็บไซต์ปราศจากช่องโหว่ร้ายแรงตามมาตรฐาน OWASP Top 10

5.1.3 การสร้างวัฒนธรรมความปลอดภัยแบบไม่จับผิด นอกเหนือจากมาตรการเชิงบังคับ ผู้บริหารท้องถิ่นควรส่งเสริมวัฒนธรรมองค์กรที่เอื้อต่อการรายงานความผิดปกติ โดยเปลี่ยนมุมมองจากการลงโทษผู้กระทำผิดพลาด (Blame Culture) มาเป็นการเรียนรู้ร่วมกัน เพื่อสนับสนุนให้เจ้าหน้าที่กล้ารายงานเหตุการณ์เมื่อสงสัยว่าตนเองตกเป็นเหยื่อของการหลอกลวง (Phishing) หรือทำผิดพลาดโดยไม่เจตนา ซึ่งจะช่วยให้หน่วยงานสามารถตรวจจับและระงับยับยั้งภัยคุกคามได้รวดเร็วกว่าการปิดบังข้อมูล (สุมาลี สิสุพรรณ และอภิรดี เพียรขุนทด, 2565)

5.2 ระยะการสร้างภูมิคุ้มกันทางเทคนิค มุ่งเน้นการปิดช่องโหว่พื้นฐานเพื่อลดโอกาสการถูกโจมตี โดยเน้นมาตรการที่ใช้งบประมาณต่ำแต่ได้ผลสูง (Quick Wins)

5.2.1 มาตรฐานความปลอดภัยขั้นพื้นฐาน (Security Hygiene)

1) *เว็บไซต์ต้องเปิดใช้งานการเข้ารหัสข้อมูล (HTTPS) ในทุกหน้า* เพื่อสร้างความเชื่อมั่นแก่ประชาชนผู้ใช้งาน และต้องมีการปิดหรือเปลี่ยนชื่อเส้นทางเข้าสู่ระบบหลังบ้าน (Default Admin Path) ของระบบ CMS (เช่น เปลี่ยนจาก /wp-admin เป็นชื่อเฉพาะที่คาดเดายาก)

2) หน่วยงานควรตรวจสอบและปิดช่องทางการเข้าถึงจากภายนอก ผ่านโปรโตคอลที่มีความเสี่ยงสูงหากไม่มีความจำเป็นต้องใช้งาน เช่น SSH, RDP, TELNET และ SMB เพื่อป้องกันการเจาะระบบจากระยะไกลและการแพร่กระจายของมัลแวร์ (Malware)

5.2.2 การจัดการสิทธิ์และการยืนยันตัวตน (Access Control)

1) บังคับใช้นโยบายรหัสผ่านที่รัดกุม (Strong Password Policy) และควรพิจารณาใช้เทคโนโลยีการยืนยันตัวตนแบบ 2 ขั้นตอน (2FA) สำหรับผู้ดูแลระบบ ซึ่งปัจจุบันมีเครื่องมือฟรี (เช่น Google Authenticator) ที่สามารถนำมาประยุกต์ใช้ได้โดยไม่ต้องลงทุนเพิ่ม นอกเหนือจากการใช้ MFA ทั่วไป หน่วยงานท้องถิ่นควรพิจารณาบูรณาการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลผ่านแอปพลิเคชัน ThaiID หรือระบบยืนยันตัวตน (SSO) ของกรมส่งเสริมการปกครองท้องถิ่น มาใช้สำหรับการเข้าสู่ระบบบริการประชาชน เพื่อลดภาระในการพัฒนาระบบความปลอดภัยเองและเป็นไปตามมาตรฐานระดับประเทศ (กรมส่งเสริมการปกครองท้องถิ่น ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น, 2558)

2) ควรมีการบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management) หน่วยงานควรจัดทำทะเบียนบัญชีผู้ใช้ (User Inventory) และสิทธิ์การเข้าถึง โดยต้องทบทวนสิทธิ์ (Access Review) อย่างน้อยปีละ 1 ครั้ง และระงับบัญชีทันทีเมื่อบุคลากรย้ายหรือลาออก

5.2.3 การบริหารจัดการแพตช์ กำหนดให้มีการตรวจสอบและอัปเดตเวอร์ชันของระบบปฏิบัติการและส่วนเสริม (Plugins) อย่างน้อยเดือนละ 1 ครั้ง เนื่องจากเว็บไซต์ท้องถิ่นส่วนใหญ่ถูกโจมตีผ่านช่องโหว่ของ Plugin ที่ล้าสมัย

5.3 ระยะการเฝ้าระวังและประเมิน เตรียมความพร้อมเพื่อรับมือเมื่อเกิดเหตุไม่คาดฝัน เพื่อจำกัดความเสียหายให้น้อยที่สุด และตรวจสอบสถานะความพร้อมอย่างต่อเนื่อง

5.3.1 การประเมินสถานะตนเอง (Self-Assessment) เนื่องจากท้องถิ่นอาจไม่มีงบประมาณจ้างที่ปรึกษาตรวจสอบได้บ่อยครั้ง จึงควรนำแบบรายการตรวจสอบการประเมินตนเอง (Self-Assessment Checklist) มาใช้เป็นเครื่องมือในการตรวจทานสถานะความมั่นคงปลอดภัยเบื้องต้น โดยเจ้าหน้าที่ผู้รับผิดชอบควรทำการประเมินทุกไตรมาส ครอบคลุมหัวข้อสำคัญ เช่น การสำรองข้อมูล (Backup) การต่ออายุใบรับรอง SSL และความสมบูรณ์ของ Log Files

5.3.2 การจัดเก็บข้อมูลจราจร (Log Management) ต้องตรวจสอบให้แน่ใจว่าระบบมีการบันทึก Log การใช้งานเว็บไซต์ย้อนหลังอย่างน้อย 90 วัน ตามมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่แก้ไขเพิ่มเติม) และต้องมีการสำรองไฟล์ Log นี้ไว้ในที่ปลอดภัยแยกจากตัวเครื่อง Web Server

5.3.3 แผนเผชิญเหตุและการบริหารความต่อเนื่องทางธุรกิจ (Incident Response and Business Continuity Planning) หน่วยงานควรจัดทำคู่มือปฏิบัติงานฉุกเฉิน (SOP) ที่ครอบคลุมทั้งมิติด้านเทคนิคและการให้บริการ โดยระบุขั้นตอนที่ชัดเจนเมื่อเกิดเหตุวิกฤต เช่น ขั้นตอนการตัดการเชื่อมต่อเครือข่าย และแผนสำรองการให้บริการ (Contingency Plan) ในรูปแบบที่ไม่อาศัยเทคโนโลยี

(Manual Process) สำหรับงานบริการสำคัญเร่งด่วน เช่น การรับชำระภาษีหรือการจ่ายเบี้ยยังชีพ เพื่อให้มั่นใจว่าภารกิจหลักขององค์กรปกครองส่วนท้องถิ่นจะยังคงดำเนินต่อไปได้แม้ระบบสารสนเทศหลักจะหยุดชะงัก และควรแถลงการณ์ชี้แจงประชาชนผ่านช่องทางที่เหมาะสม เพื่อให้เจ้าหน้าที่สามารถตอบสนองได้ทันทีโดยไม่ต้องรอคำสั่งการตามลำดับชั้นปกติ

5.3.4 ความร่วมมือเครือข่ายความมั่นคงปลอดภัยท้องถิ่น เพื่อข้ามผ่านข้อจำกัดด้านงบประมาณและบุคลากร องค์กรปกครองส่วนท้องถิ่นควรพิจารณาแนวทางการรวมกลุ่มพันธมิตรในระดับจังหวัดหรือภูมิภาค (Cluster) เพื่อแบ่งปันทรัพยากรร่วมกัน เช่น การจัดตั้งศูนย์เฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ร่วม หรือการแลกเปลี่ยนข้อมูลข่าวสารภัยคุกคาม (Threat Intelligence) ระหว่างกัน ซึ่งเป็นแนวปฏิบัติสากลที่ช่วยลดต้นทุนการดำเนินงานและเพิ่มอำนาจการต่อรองกับผู้ให้บริการภายนอก

6. บทสรุป

การประกาศใช้มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568 ถือเป็นจุดเปลี่ยนสำคัญที่กระตุ้นให้หน่วยงานภาครัฐต้องตระหนักถึงความสำคัญของการสร้างภูมิคุ้มกันทางไซเบอร์ แต่สำหรับองค์กรปกครองส่วนท้องถิ่น การปฏิบัติตามมาตรฐานดังกล่าวให้สัมฤทธิ์ผลนั้น มิได้ขึ้นอยู่กับการจัดซื้อเทคโนโลยีราคาสูงเพียงอย่างเดียว หากแต่ขึ้นอยู่กับความสามารถในการบริหารจัดการภายใต้ข้อจำกัดที่มีอยู่

บทความนี้ได้นำเสนอแนวทางปฏิบัติ (Guidelines) ที่มุ่งเน้นการแก้ปัญหาเชิงโครงสร้าง โดยเริ่มจากการปรับเปลี่ยนกระบวนการจัดจ้าง (Governance) ให้มีกลไกตรวจสอบคุณภาพความปลอดภัยที่เข้มงวด เช่น การกำหนดให้มีการประเมินช่องโหว่ (VA Scan) และการทดสอบเจาะระบบ (Pentest) ในเงื่อนไขการตรวจรับงาน ควบคู่ไปกับการสร้างมาตรการป้องกันทางเทคนิคขั้นพื้นฐาน (Protection) และการใช้เครื่องมือประเมินตนเอง (Self-Assessment) เพื่อเฝ้าระวังความเสี่ยงอย่างต่อเนื่อง

นอกจากนี้สำหรับความเสี่ยงระดับสูงที่ไม่สามารถกำจัดได้ด้วยงบประมาณปกติ (Residual Risk) ผู้บริหารอาจพิจารณาเครื่องมือทางการเงินสมัยใหม่ เช่น การประกันภัยไซเบอร์ (Cyber Insurance) (Taskin et al., 2025) เพื่อเป็นกลไกในการถ่ายโอนความเสี่ยงและคุ้มครองภาระค่าใช้จ่ายในการกู้คืนระบบหรือการเยียวยาความเสียหายที่อาจเกิดขึ้นในอนาคต

ท้ายที่สุดแล้ว การยกระดับความมั่นคงปลอดภัยเว็บไซต์ขององค์กรปกครองส่วนท้องถิ่น ไม่ใช่เพียงเพื่อให้รอดพ้นจากบทลงโทษทางกฎหมาย แต่เป้าหมายสูงสุดคือการสร้างความไว้วางใจทางดิจิทัล (Digital Trust) (Castelfranchi & Falcone, 2010) ให้เกิดขึ้นแก่ประชาชน เมื่อประชาชนเชื่อมั่นว่า ประตูด่านบ้านดิจิทัล ของท้องถิ่นมีความมั่นคงปลอดภัย การยอมรับและใช้งานบริการภาครัฐผ่านช่องทางดิจิทัลก็จะเกิดขึ้นตามมา ซึ่งจะนำไปสู่ความสำเร็จของการเป็นรัฐบาลดิจิทัลที่โปร่งใส ตรวจสอบได้ และยั่งยืนอย่างแท้จริง

7. เอกสารอ้างอิง

- กรมส่งเสริมการปกครองท้องถิ่น, ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น. (2558, 24 กันยายน). *การพัฒนาและปรับปรุงระบบยืนยันตัวตน (SSO) กรมส่งเสริมการปกครองท้องถิ่น* (ที่ มท 0806.2/ว4365) [หนังสือภายนอก]. ศูนย์เทคโนโลยีสารสนเทศท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น.
https://fa2.naxapi.com/localthai.org/dnm_file/st/1758762900090_29788_side1.pdf
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568. (2568, 16 กันยายน). *ราชกิจจานุเบกษา*. เล่ม 142 ตอนพิเศษ 304 ง. หน้า 33–35.
- สลิลธร ทองมีนสุข และโชติกา เชียงหลิว. (2568, 22 พฤษภาคม). *PDPA กับความเข้าใจผิดของรัฐสู่การปิดบังข้อมูลสาธารณะ*. สถาบันวิจัยเพื่อการพัฒนาประเทศไทย (TDRI),
<https://tdri.or.th/2025/05/misunderstood-pdpa-concealing-public-information-article/>.
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2566). *คู่มือกฎหมายไซเบอร์สำหรับประชาชน*. <https://www.ncsa.or.th/>
- สุมาลี สีสุพรรณ และ อภิรติ เพียรขุนทด. (2565). วัฒนธรรมปรับตัวเพื่อไปสู่การเป็นองค์กรดิจิทัลกรณีศึกษา องค์กรปกครองส่วนท้องถิ่นในเขตพื้นที่อำเภอเมือง จังหวัดขอนแก่น. *วารสารวิชาการร้อยแก่นสาร*, 7(8), 246–264
- สุภาภรณ์ สีสุพรรณ และอจิรภาส เพียรขุนทด. (2565). การปรับตัวเพื่อเข้าสู่การเปลี่ยนแปลงเป็นองค์กรดิจิทัลขององค์กรปกครองส่วนท้องถิ่นในเขตอำเภอเมือง จังหวัดขอนแก่น. *Journal of Roi Kaensam Academi*, 7(8), 246–264. <https://so02.tci-thaijo.org/index.php/JRKSA/article/view/255394/173313>
- Castelfranchi, C., & Falcone, R. (2010). *Trust Theory: A Socio-Cognitive and Computational Model*. Markono. <https://content.e-bookshelf.de/media/reading/L-574379-2b6320d159.pdf>
- National Institute of Standards and Technology. (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management* (NIST Special Publication 800–63B). U.S. Department of Commerce. [https://doi.org/10.6028/NIST.SP.800–63b](https://doi.org/10.6028/NIST.SP.800-63b)
- OWASP Foundation. (2025). *OWASP Top 10: 2025*. <https://owasp.org/Top10/2025/>
- Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber insurance adoption and digitalisation in small and medium-sized enterprises. *Information*, 16(1), 66. <https://doi.org/10.3390/info16010066>