บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มระบบเครือข่ายคอมพิวเตอร์ โทร.๔๓๒๕

ที่ กษ ๐๔๐๓/ว ๑๖๘ **วันที่** ๒๔ มีนาคม ๒๕๖๖

เรื่อง ขอส่งแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline)

เรียน หน่วยงานสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ตามหนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ด่วนที่สุด ที่ สกมช ๐๘๑๐/ว๑๕๐๑ ลงวันที่ ๑๖ ธันวาคม ๒๕๖๕ เรื่อง ขอส่งแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) เพื่อใช้เป็นแนวทางในการพัฒนาและดูแลเว็บไซต์ให้มีความมั่นคงปลอดภัย ให้กับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือผู้เกี่ยวข้อง นั้น

เพื่อให้การพัฒนาและดูแลระบบสารสนเทศของหน่วยงาน มีความมั่นคงปลอดภัยเป็นไปตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ขอให้ทุกหน่วยงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ปฏิบัติตามแผนปฏิบัติงานเพื่อใช้เป็นแนวทางในการพัฒนาและดูแลเว็บไซต์ให้มีความมั่นคงปลอดภัย ตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อทราบ และดำเนินการต่อไป

(นางสาวกนกพรรณ ชำนาญกิจ)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

แผนปฏิบัติงานเพื่อใช้เป็นแนวทางในการพัฒนาและดูแลเว็บไซต์ให้มีความมั่นคงปลอดภัย

ลำดับ	กิจกรรม	ระยะเวลา
๑	แจ้งหน่วยงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้รับทราบแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์	๑ วัน (๒๗ มี.ค. ๖๖)
๒	หน่วยงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ศึกษา ทำความเข้าใจ และดำเนินการเบื้องต้นตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ เพื่อรวบรวมข้อสงสัย ปัญหา การดำเนินการในส่วนที่เกี่ยวข้อง พร้อมนัดประชุม สรุปความเห็น	๑๐ วัน (๒๗ มี.ค. ๖๖ - ๗ เม.ย. ๖๖)
๓	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารประชุมร่วมกับหน่วยงานสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อสอบถาม แจ้งประเด็นข้อสงสัย หาวิธีการดำเนินการตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์	๑ วัน (๑๘-๒๑ เม.ย. ๖๖)
๔	ประชุมหน่วยงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อวางแผนและดำเนินการตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ โดยมีการประชุมติดตามสัปดาห์ละ ๑ ครั้ง (ในวันที่ ๑๐, ๑๗, ๒๔ เม.ย. ๖๖)	๑๕ วัน (๒๔ เม.ย. ๖๖ - ๑๒ พ.ค. ๖๖)
๕	ประชุมหน่วยงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อสรุปผลการดำเนินการตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์	๑ วัน (๑๕-๑๙ พ.ค. ๖๖)
๖	รายงานผลการดำเนินการตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ เพื่อนำเสนอผู้บริหารรับทราบต่อไป	๑ วัน (๒๒-๒๖ พ.ค. ๖๖)

แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์

หัวข้อ	รายละเอียด	ผลการดำเนินงาน	ผู้รับผิดชอบ
๑. ทำให้ระบบนิเวศของโดเมนมีความปลอดภัย (Secure domain ecosystems)			
	๑.๑ ตรวจสอบผู้รับจดทะเบียน (Registrar) และระเบียนระบบชื่อโดเมน (DNS records) สำหรับโดเมนทั้งหมด **แนวทาง** ผู้รับจ้างตรวจสอบ พร้อมรายงานผล		กคส.
	๑.๒ เปลี่ยนรหัสผ่านเริ่มต้นทั้งหมดที่ได้รับจากผู้รับจดทะเบียนโดเมนและ DNS ของชื่อผู้ใช้และรหัสผ่านเริ่มต้นไม่ปลอดภัย โดยปกติแล้วจะสามารถค้นหาได้บนอินเทอร์เน็ต การเปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นจะป้องกันการโจมตีที่ใช้ประโยชน์จากข้อมูลดังกล่าว **แนวทาง** ผู้รับจ้างตรวจสอบพร้อมรายงานผล		กคส.
	๑.๓ บังคับใช้การพิสูจน์และยืนยันตัวตนหลายปัจจัย (Multi-factor authentication : MFA) **แนวทาง** ผู้รับจ้างตรวจสอบ พร้อมรายงานผล		กคส.
	๑.๔ ติดตามตรวจสอบบันทึกความโปร่งใสของใบรับรอง (certificate transparency logs) เพื่อตรวจสอบเว็บไซต์ปลอมที่อาจใช้ชื่อโดเมนคล้ายกัน **แนวทาง** ตรวจสอบผ่าน https://developers.facebook.com/tools/ct/search/		กคส.
๒. ทำให้บัญชีผู้ใช้มีความปลอดภัย (Secure user accounts)			
	๒.๑ บังคับใช้การพิสูจน์และยืนยันตัวตนหลายปัจจัยกับบัญชีผู้ใช้ทั้งหมดที่เข้าถึงได้จากอินเทอร์เน็ต โดยให้ความสำคัญกับบัญชีผู้ใช้ที่มีสิทธิ์สูง (Privileged access) **แนวทาง** บังคับใช้การพิสูจน์และยืนยันตัวตน บัญชีผู้ใช้งานอินเทอร์เน็ตของบุคลากรกตส.		กฐส. กบส. กขส. กวส. กรส. กคส.
	๒.๒ จำกัดสิทธิ์ของผู้ใช้เท่าที่จำเป็น (Principle of least privilege) รวมทั้งปิดใช้งานบัญชีและสิทธิ์ที่ไม่จำเป็น **แนวทาง** ลบบัญชีผู้ใช้งานอินเทอร์เน็ต สตส. ตรวจสอบ/แจ้งลบบัญชีผู้ใช้งาน ผู้รับจ้าง(ดาร์ก้อนมูฟ) ดำเนินการลบบัญชีผู้ใช้งาน		กฐส. กบส. กขส. กวส. กรส. กคส.
	๒.๓ เปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นทั้งหมด **แนวทาง** ประชุมหน่วยงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อหาแนวทางร่วมกัน		กฐส. กบส. กขส. กวส. กรส. กคส.

หัวข้อ	รายละเอียด	ผลการดำเนินงาน	ผู้รับผิดชอบ
๓. ค้นหาและแก้ไขช่องโหว่อย่างต่อเนื่อง (Continuously scan for—and remediate -critical and high vulnerabilities)			
	๓.๑ แก้ไขช่องโหว่ระดับวิกฤต (Critical) และระดับสูง (High) ทั้งหมด ภายใน ๑๕ และ ๓๐ วัน ตามลำดับ ในระบบที่สามารถเข้าถึงได้ทางอินเทอร์เน็ต โดยสแกนหาช่องโหว่จากการตั้งค่า (Configuration vulnerabilities) และช่องโหว่ของซอฟต์แวร์ รวมถึงเปิดใช้งานการอัปเดตอัตโนมัติทุกครั้ง **แนวทาง** ศึกษาซอฟต์แวร์ที่ใช้ในการดำเนินการ		กคส.
	๓.๒ เปลี่ยนระบบปฏิบัติการ แอปพลิเคชันและฮาร์ดแวร์ ซึ่งหมดระยะเวลาการสนับสนุนโดยผู้ผลิต **แนวทาง** รายงานผลการตรวจสอบ รายละเอียด ดังนี้ ด้านซอฟต์แวร์ : ระบบปฏิบัติการ ฐานข้อมูล เว็บเซิร์ฟเวอร์ ด้านฮาร์ดแวร์ : ยี่ห้อ รุ่น ปีที่ได้มา ซีพียู ฮาร์ดดิส แรม		กฐส. กบส. กขส. กวส. กรส. กคส.
๔. ทำให้ข้อมูลระหว่างการขนส่งมีความปลอดภัย (Secure data in transit)			
	๔.๑ ปิดการใช้งาน Hypertext Transfer Protocol (HTTP); บังคับใช้ Hypertext Transfer Protocol Secure (HTTPS) และ HTTP Strict Transport Security (HSTS) ผู้ใช้งานเว็บไซต์คาดหวังว่าความเป็นส่วนตัวของพวกเขาจะได้รับการปกป้อง ดังนั้นเพื่อให้แน่ใจว่าการสื่อสารระหว่างเว็บไซต์และผู้ใช้ได้รับการเข้ารหัส จึงต้องบังคับใช้ HTTPS เสมอ และควรบังคับใช้ HSTS หากเป็นไปได้ **แนวทาง** กำหนดนโยบายการรักษาความปลอดภัยบนอุปกรณ์ป้องกันเครือข่าย (Firewall)		กคส.
	๔.๒ ปิดการใช้งานอัลกอริทึมที่ไม่มีความมั่นคงปลอดภัย เช่น SSLv๒, SSlv๓, ๓DES, RC๔ **แนวทาง** กำหนดนโยบายการรักษาความปลอดภัยบนอุปกรณ์ป้องกันเครือข่าย (Firewall)		กคส.
๕. สำรองข้อมูล (Backup data)			
	๕.๑ หมั่นสำรองข้อมูลอย่างสม่ำเสมอ โดยเฉพาะข้อมูลและระบบที่สำคัญเว็บไซต์ **แนวทาง** สำรองข้อมูลทุกวัน		กฐส. กบส. กขส. กวส. กรส. กคส.
	๕.๒ เก็บข้อมูลสำรองไว้ในที่ปลอดภัยและแยกทางกายภาพออกจากระบบ (Physically remote environment) **แนวทาง** แยกการจัดเก็บ external storage		กฐส. กบส. กขส. กวส. กรส. กคส.
	๕.๓ ทดสอบการกู้คืนข้อมูล **แนวทาง** อยู่ระหว่างดำเนินการ		กฐส. กบส. กขส. กวส. กรส. กคส.

หัวข้อ	รายละเอียด	ผลการดำเนินงาน	ผู้รับผิดชอบ
๖. ทำให้เว็บแอปพลิเคชันมีความปลอดภัย (Secure web applications)			
	๖.๑ ระบุและลดความเสี่ยงของการถูกโจมตีบนเว็บแอปพลิเคชันที่สำคัญ ๑๐ อันดับแรก (ข้อมูลเพิ่มเติมเกี่ยวกับความเสี่ยง ๑๐ อันดับแรกจาก OWASP[1] ศึกษาเพิ่มเติมได้ที่ https://owasp.org/www-project-top-ten/) จากนั้นจึงพิจารณาระบุและลดความเสี่ยงอื่น ๆ เป็นลำดับถัดไป อาทิ การปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยของระบบและเครือข่ายที่มีการใช้งานเทคโนโลยีอินเทอร์เน็ตจาก Center for Internet Security (CIS)[2] ศึกษาเพิ่มเติมได้ที่ https://www.cisecurity.org/controls **แนวทาง** แต่ละหน่วยงานศึกษาแนวทางการตรวจสอบ		กฐส. กบส. กขส. กวส. กรส. กคส.
	๖.๒ เปิดการบันทึกการใช้งาน (Logging) และตรวจสอบบันทึกการใช้งานกิจกรรมบนเว็บไซต์อย่างสม่ำเสมอ เพื่อตรวจหากิจกรรมที่ผิดปกติ ทั้งนี้ ควรส่งบันทึกการใช้งานดังกล่าวไปยังเซิร์ฟเวอร์ส่วนกลาง (Centralized log server) **แนวทาง** มอบหมายผู้รับผิดชอบ		กคส.
	๖.๓ ใช้การพิสูจน์และยืนยันตัวตนหลายปัจจัย สำหรับผู้ใช้งาน ซึ่งล็อกอินเข้าสู่เว็บแอปพลิเคชัน รวมถึงผู้ดูแลระบบที่มีการใช้งานโครงสร้างพื้นฐานของเว็บไซต์ด้วย **แนวทาง** จัดทำ checklist ระบบที่มีการล็อกอินเข้าสู่เว็บแอปพลิเคชัน		กฐส. กบส. กขส. กวส. กรส. กคส.
๗. ทำให้เว็บเซิร์ฟเวอร์มีความปลอดภัย (Secure web servers)			
	๗.๑ ตรวจสอบความปลอดภัยโดยอ้างอิงตาม security checklist ของแอปพลิเคชันนั้น ๆ เช่น Apache, MySQL และดำเนินการตั้งค่าให้มีความมั่นคงปลอดภัย (Harden configurations) **แนวทาง** แต่ละหน่วยงานศึกษาแนวทางการตรวจสอบ		กฐส. กบส. กขส. กวส. กรส. กคส.
	๗.๒ ใช้แอปพลิเคชันที่เชื่อถือได้และมีความจำเป็นสอดคล้องกับความต้องการขององค์กร รวมทั้งปิดการใช้งานฟีเจอร์ที่ไม่จำเป็น **แนวทาง** แต่ละหน่วยงานศึกษาแนวทางการตรวจสอบ		กฐส. กบส. กขส. กวส. กรส. กคส.
	๗.๓ ใช้การแบ่งส่วนและแยกเครือข่าย (network segmentation and segregation) - การแบ่งส่วนและแยกเครือข่ายจะทำให้ผู้โจมตีเคลื่อนไหว (move laterally) ในเครือข่ายได้ยากขึ้น ตัวอย่างเช่น		กคส.

[1] https://owasp.org/

[2] https://www.cisecurity.org/

หัวข้อ	รายละเอียด	ผลการดำเนินงาน	ผู้รับผิดชอบ
	การวางเว็บเซิร์ฟเวอร์ไว้บนเครือข่ายแบบ demilitarized zone (DMZ) ที่ถูกกำหนดค่าอย่างเหมาะสมจะจำกัดการรับส่งข้อมูลที่ได้รับอนุญาตระหว่างระบบภายในเครือข่ายแบบ DMZ และระบบในเครือข่ายภายในขององค์กร **แนวทาง** ขอคำปรึกษาผู้รับจ้างโครงการบำรุงรักษาระบบเครือข่ายและความปลอดภัย		
	๗.๔ ให้คำนึงไว้เสมอว่าทรัพย์สินอยู่ที่ไหน - ถ้าเรารู้ว่าข้อมูลสำคัญของเราอยู่ตรงไหน เราก็จะสามารถบริหารจัดการและจำกัดการเข้าถึงได้อย่างเหมาะสม		กคส.
๘. จัดลำดับความสำคัญโดยใช้ Web Security Cheat Sheet การดำเนินการเพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยนั้นสามารถดำเนินการได้หลายประการ ทั้งนี้ ควรพิจารณาจากประโยชน์ที่จะได้รับ (Security Benefit) และความยากง่ายในการดำเนินการ (Implementation Difficulty) ซึ่งจะทำให้องค์กรสามารถจัดลำดับความสำคัญในการดำเนินการได้ โดยมีคำแนะนำดังปรากฏในตารางนี้ (HTTPS, Public Key Pinning, Redirections from HTTP, Resource Loading, Strict Transport Security, TLS Configuration, Content Security Policy, Cookies, contribute.json, Cross-origin Resource Sharing, Cross-site Request Forgery Tokenization, Referrer Policy, robots.txt, Subresource Integrity, X-Content-Type-Options, X-Frame-Options, X-XSS-Protection) **แนวทาง** เรียงลำดับจากผลการทบทวนข้อมูลระบบสารสนเทศของกรมตรวจบัญชีสหกรณ์ ประจำปีงบประมาณ ๒๕๖๖ กับ Cheat sheet			กฐส. กบส. กขส. กวส. กรส. กคส.

กลุ่มระบบเครือข่ายคอมพิวเตอร์
เลขที่รับ ๑๕๐๒
วันที่ ๒๐ ธ.ค. ๒๕๖๕
เวลา ๑๕:๐๗ น.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
เลขที่รับ ๐๑๖๑
วันที่ ๒๐ ธ.ค. ๒๕๖๕
เวลา ๑๓.๔๐ น.

กรมตรวจบัญชีสหกรณ์
เลขรับ ๑๖๓๘๒
วันที่ ๒๐ ธ.ค. ๒๕๖๕
เวลา ๑๑.๔๐ น.

NCSA สกมช

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210 อีเมล contact@ncsa.or.th

ด่วนที่สุด

ที่ สกมช ๐๘๑๐/ว๑๕๐๑

๑๖ ธันวาคม ๒๕๖๕

เรื่อง ขอส่งแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline)

เรียน อธิบดีกรมตรวจบัญชีสหกรณ์

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline)

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จัดทำแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) เพื่อใช้เป็นแนวทางในการพัฒนาและดูแลเว็บไซต์ให้มีความมั่นคงปลอดภัย ให้กับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือผู้เกี่ยวข้อง

ในการนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงประชาสัมพันธ์ให้นำไปเป็นแนวทางในการพัฒนาและดูแลเว็บไซต์ของหน่วยงานให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น

จึงเรียนมาเพื่อโปรดพิจารณา

กลุ่มระบบเครือข่ายคอมพิวเตอร์ / ดำเนินการในแนวทางปฏิบัติฯ.
☑ ดำเนินการ วิเคราะห์แล้ว.
☐ ทราบ

ขอแสดงความนับถือ

พลอากาศตรี อมร ชมเชย

๒๐ ธ.ค. ๒๕๖๕

(นางสาวกนกพรรณ ชำนาญกิจ)
ผู้เชี่ยวชาญด้านโปรแกรมระบบบัญชีสหกรณ์
ราชการแทนผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
สำนักประสานงาน
โทรศัพท์ ๐ – ๒๑๔๒- ๖๘๘๕
e-mail : ncert@ncsa.or.th

เอกสารแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์