มาตรฐานรายการตรวจสอบเครื่องแม่ข่ายเพื่อรองรับการพัฒนาระบบสารสนเทศให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
1	การพิสูจน์ตัวตนและการควบคุมการเข้าถึง (Authentication & Access Control) มาตรฐานที่อ้างอิง : OWASP 2021 (A01, A07), Zero Trust			
1.1	การควบคุมการเข้าถึงโดยใช้งาน IP Address Allowlist (รายการไอพีที่ได้รับอนุญาต) เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต และลดความเสี่ยงจากการโจมตีจากแหล่งที่ไม่รู้จัก			
	1.1.1 กำหนดรายการ IP Address หรือ URL/เครือข่ายที่อนุญาตให้เข้าถึงเครื่องแม่ข่าย			
	1.1.2 ไม่อนุญาตการเข้าถึงเครื่องแม่ข่ายจาก IP Address สาธารณะ			
	1.1.3 ทบทวนและปรับปรุงรายการ IP Address Allowlist			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	อย่างน้อยปีละครั้ง			
	1.1.4 ทดสอบการบล็อก IP Address นอก Allowlist อย่างน้อยปีละครั้ง			
1.2	กำหนดสิทธิการเข้าถึงโฟลเดอร์ระบบจัดการภายใน โดยให้สิทธิการเข้าถึงเฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้นโดยตั้งค่าการอนุญาตแบบ Least Privilege			
1.3	ตรวจสอบและปรับแต่งสิทธิ์ไฟล์ (Read/Write/Execute) ให้เหมาะสม โดยระบุสิทธิ์น้อยที่สุดเท่าที่จำเป็น (Principle of Least Privilege) ตัวอย่างเช่น ไฟล์ config (740), ไฟล์ log (640), scripts (750), ข้อมูลที่ละเอียดอ่อน (600) และเนื้อหาเว็บสาธารณะ (644)			
1.4	ตรวจสอบและทบทวนสิทธิ์อย่างน้อยปีละครั้ง			
1.5	ติดตั้งและกำหนดค่า Firewall สำหรับระบบฐานข้อมูล เพื่อป้องกันการเข้าถึงฐานข้อมูลที่ไม่พึงประสงค์			
1.6	จำกัดการเข้าถึงฐานข้อมูลเฉพาะเครื่องแม่ข่าย หรือโปรแกรมที่			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	เกี่ยวข้องเพื่อความปลอดภัยของข้อมูล (บางฐานข้อมูลอาจสามารถทำได้เพียงอย่างใดอย่างหนึ่ง)			
1.7	กำหนดสิทธิการใช้งานฐานข้อมูลตามบทบาทและหน้าที่เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่จำเป็น			
2	การเข้ารหัสข้อมูล (Data Encryption) มาตรฐานที่อ้างอิง : Cybersecurity Framework (NIST), Zero Trust			
2.1	จัดการระบบกุญแจเข้ารหัส (Key Management) ให้มั่นใจว่าข้อมูลที่ถูกเข้ารหัสจะสามารถถอดรหัสได้เฉพาะผู้ที่มีสิทธิ์เท่านั้นเพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต			
	2.1.1 การเลือกและใช้อัลกอริทึมเข้ารหัสที่เหมาะสม (Appropriate Encryption Algorithm Selection and Usage) ใช้อัลกอริทึมตามมาตรฐาน NIST SP 800-57 เช่น AES-256 (Advanced Encryption Standard) สำหรับข้อมูลสำคัญ และ TLS 1.2 ขึ้นไป (Transport Layer Security) สำหรับการสื่อสาร เลือกใช้ตามประเภทและความสำคัญของข้อมูล			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	2.1.2 การจัดการกุญแจตลอดวงจรชีวิต (Key Management Lifecycle) มีกระบวนการสร้าง จัดเก็บ หมุนเวียน และทำลายกุญแจอย่างปลอดภัย ใช้ HSM (Hardware Security Module) / TPM (Trusted Platform Module) / KMS (Key Management System) สำหรับจัดเก็บ ไม่ใช้ Config File หรือ Database เก็บกุญแจโดยตรง ไม่เก็บเป็น Plaintext แม้บนเครือข่ายภายใน			
	2.1.3 การควบคุมการเข้าถึงและการตรวจสอบ (Access Control and Audit) ใช้ RBAC (Role-Based Access Control) และ ACL (Access Control List) เพื่อจำกัดสิทธิ์การเข้าถึง นำหลักการ Least Privilege มาใช้ และบันทึกทุกกิจกรรมที่เกี่ยวข้องกับกุญแจเข้ารหัส (Key Access Logging) เพื่อตรวจสอบย้อนกลับ			
	2.1.4 การตรวจสอบและเฝ้าระวังระบบเข้ารหัส (Encryption System Monitoring and Surveillance) มีการตรวจสอบ			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	ระบบอย่างสม่ำเสมอ มีระบบแจ้งเตือนเมื่อมีความพยายามเข้าถึงที่ผิดปกติ และทดสอบประสิทธิภาพของการเข้ารหัสเป็นระยะ ใช้หลักการ Continuous Monitoring ตามแนวคิด Zero Trust			
	2.1.5 มีแผนรับมือเหตุการณ์และการกู้คืนกุญแจเมื่อเกิดการละเมิดความปลอดภัย มีกระบวนการกู้คืนกุญแจเข้ารหัสที่ชัดเจน (Key Recovery Procedures) และทดสอบอย่างน้อยปีละครั้ง รวมถึงมีขั้นตอนการจัดการเมื่อมีการเปลี่ยนแปลงบุคลากรที่เกี่ยวข้อง (Personnel Change Management)			
2.2	กำหนดค่าและดูแล TLS Certificates ซึ่งเป็นเทคโนโลยีที่ช่วยให้การสื่อสารระหว่างเครื่องแม่ข่ายและผู้ใช้งานมีความปลอดภัยเพื่อป้องกันการดักจับข้อมูล			
	2.2.1 ใช้ TLS เวอร์ชันตั้งแต่ 1.2 ขึ้นไป ปิดการใช้งาน SSL ทุกเวอร์ชัน และปิดการใช้งาน TLS ที่ต่ำกว่า 1.2 ลงไปทั้งหมด			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	2.2.2 เลือก Certificate จาก CA ที่น่าเชื่อถือ			
3	การป้องกันภัยคุกคาม (Threat Protection) มาตรฐานที่อ้างอิง : OWASP 2021 (A03, A05), Cybersecurity Framework			
3.1	กำหนดค่าเครื่องแม่ข่ายให้อยู่หลัง Web Application Firewall (WAF) ของมหาวิทยาลัยเพื่อป้องกันการโจมตีที่อาจเกิดขึ้นผ่านแอปพลิเคชันเว็บ โดย WAF จะต้องสามารถบล็อกการโจมตี เช่น SQL Injection, Cross-Site Scripting (XSS) และ Cross-Site Request Forgery (CSRF) ได้ และต้องปรับปรุงกฎของ WAF ให้มีประสิทธิภาพเสมอ			
3.2	ติดตั้งระบบป้องกัน Distributed Denial of Service (DDoS) ซึ่งเป็นการโจมตีที่ทำให้ระบบไม่สามารถให้บริการได้ (หากเครื่องแม่ข่ายอยู่ภายใต้การดูแลของศูนย์เทคโนโลยีดิจิทัลจะมีการติดตั้ง Firewall และ WAF)			
3.3	ตั้งค่า HTTP Response Headers ให้สามารถช่วยป้องกันช่องโหว่ด้านความปลอดภัย			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	3.3.1 X-Frame-Options : ตั้งค่าเป็น DENY เพื่อป้องกัน Clickjacking			
	3.3.2 X-XSS-Protection : ตั้งค่าเป็น 0 หรือใช้ CSP แทน			
	3.3.3 X-Content-Type-Options : ตั้งค่าเป็น nosniff เพื่อป้องกัน MIME type sniffing			
	3.3.4 Referrer-Policy : ตั้งค่าเป็น strict-origin-when-cross-origin เพื่อควบคุมข้อมูล referrer			
	3.3.5 Content-Type : ตั้งค่าให้ถูกต้อง เช่น text/html; charset=UTF-8 สำหรับหน้า HTML			
	3.3.6 Strict-Transport-Security : ใช้ max-age=63072000; includeSubDomains; preload เพื่อบังคับให้ใช้ HTTPS			
	3.3.7 Content-Security-Policy : กำหนดแหล่งที่มาของ			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	เนื้อหาที่อนุญาตให้โหลดได้เพื่อป้องกัน XSS			
	3.3.8 Access-Control-Allow-Origin : ระบุ origin ที่เฉพาะเจาะจงแทนการใช้ *			
	3.3.9 Cross-Origin-Opener-Policy : ตั้งค่าเป็น same-origin เพื่อแยก browsing context			
	3.3.10 Cross-Origin-Embedder-Policy : ตั้งค่าเป็น require-corp เพื่อควบคุมการโหลดทรัพยากรข้าม origin			
	3.3.11 Cross-Origin-Resource-Policy : ตั้งค่าเป็น same-site เพื่อจำกัดการโหลดทรัพยากรเฉพาะไซต์เดียวกัน			
	3.3.12 Permissions-Policy : ปิดการใช้งานฟีเจอร์ของเบราว์เซอร์ที่ไม่จำเป็น เช่น geolocation=(), camera=(), microphone=()			
	3.3.13 ลบ Expect-CT Header ออกจากโค้ดที่มีอยู่ทั้งหมด : เพื่อลดความเสี่ยงด้านความปลอดภัยจากการตั้งค่าที่ล้าสมัย			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	หรือขัดแย้งกับระบบปัจจุบัน และลดการใช้ทรัพยากรที่ไม่จำเป็นทำให้ประหยัดแบนด์วิดท์			
	3.3.14 ลบ Server Header : เพื่อไม่เปิดเผยข้อมูลของเซิร์ฟเวอร์			
	3.3.15 ลบ X-Powered-By Header : เพื่อไม่เปิดเผยข้อมูลเทคโนโลยีที่ใช้			
	3.3.16 ลบ X-AspNet-Version Header : เพื่อไม่เปิดเผยข้อมูลเวอร์ชัน .NET			
	3.3.17 ลบ X-AspNetMvc-Version Header : เพื่อไม่เปิดเผยข้อมูลเวอร์ชัน .NET MVC			
	3.3.18 X-DNS-Prefetch-Control : ตั้งค่าเป็น Off ถ้าไม่ต้องการให้มีการโหลด DNS ล่วงหน้า			
	3.3.19 ปิดการใช้ Public-Key-Pins (HPKP) : เพื่อลดช่องโหว่			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	ของการโจมตีแบบ MITM			
3.4	ปิดการแสดงเวอร์ชัน Server-Side Script Engine เพื่อไม่ให้ผู้ไม่ประสงค์ดีทราบข้อมูลที่เป็นช่องโหว่ของระบบ เช่น ถ้าใช้งาน Apache เป็น Web Server ต้องกำหนดค่าที่ไฟล์ httpd.conf หรือ apache2.conf โดยการเพิ่มบรรทัด ServerSignature Off ServerTokens Prod			
3.5	ควบคุมการแสดงข้อผิดพลาดของ Server เพื่อป้องกันไม่ให้ข้อมูลสำคัญรั่วไหลออกไป โดยการตั้งค่าให้แสดงข้อความทั่วไปแทนข้อความแสดงผลจากระบบ เช่น ใช้ข้อความว่า "เกิดข้อผิดพลาด" แทน "Error 500 : Database Connection Failed"			
4	การตรวจสอบและบันทึก (Logging & Monitoring) มาตรฐานที่อ้างอิง : Zero Trust, Cybersecurity Framework			
4.1	ตั้งค่าการบันทึกเหตุการณ์ด้านความปลอดภัย โดยเปิดใช้งาน system logging ให้บันทึกการเข้าสู่ระบบทั้งสำเร็จและ			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	ล้มเหลว, การใช้สิทธิ์ root/admin และการเปลี่ยนแปลงไฟล์สำคัญ			
4.2	ติดตั้งเครื่องมือป้องกันพื้นฐาน เช่น fail2ban (Linux) หรือ Windows Firewall with Advanced Security ตั้งค่าให้บล็อกการพยายามเข้าถึงที่ผิดปกติโดยอัตโนมัติ			
4.3	ทบทวนและวิเคราะห์ Log อย่างสม่ำเสมอ โดยใช้เครื่องมือพื้นฐาน เช่น grep (Linux) หรือ Event Viewer (Windows) เพื่อค้นหารูปแบบที่ผิดปกติเป็นประจำ			
4.4	ตั้งค่า Log Rotation เพื่อป้องกันพื้นที่เก็บข้อมูล Log เต็ม และสำรองข้อมูล Log ไปยัง External Storage			
4.5	จำกัดการเข้าถึงไฟล์ Log ให้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น เพื่อป้องกันการแก้ไขหรือลบ Log โดยไม่ได้รับอนุญาต			
5	การควบคุมการพัฒนาและทดสอบ (Development & Testing Controls) มาตรฐานที่อ้างอิง : OWASP 2021 (A04, A06)			
5.1	ปิดเครื่องแม่ข่ายหรือเครื่องแม่ข่ายเสมือนที่ไม่ได้ใช้งานเพื่อลด			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
	ความเสี่ยงในการถูกโจมตี			
5.2	จัดการการทดสอบเจาะระบบ (Penetration Testing) เพื่อหาช่องโหว่ของระบบ และแก้ไขก่อนที่จะถูกโจมตี โดยการทดสอบเจาะระบบอย่างน้อยปีละครั้ง เมื่อมีการ Upgrade/Patch ต้องทดสอบทุกครั้ง รายงานผลและแก้ไขช่องโหว่ตามนโยบายที่กำหนดไว้			
5.3	ลบโปรแกรมและไฟล์ที่ไม่ได้ใช้เพื่อลดความเสี่ยงในการถูกโจมตี			
5.4	เปลี่ยนค่าเริ่มต้นของเครื่องแม่ข่ายที่อาจเป็นช่องโหว่ เช่น รหัสผ่านเริ่มต้น และบัญชีผู้ใช้เริ่มต้นที่มากับเครื่องแม่ข่ายหรือตัวระบบที่ติดตั้ง			
5.5	ลบบัญชีผู้ใช้ที่ไม่ได้ใช้งานเพื่อป้องกันการเข้าถึงที่ไม่พึงประสงค์			
6	การจัดการ Dependencies และ Components มาตรฐานที่อ้างอิง : OWASP 2021 (A06, A08)			
6.1	อัปเดต Web Server Software เป็นเวอร์ชันปัจจุบันเพื่อความปลอดภัยและประสิทธิภาพที่ดีขึ้น			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
6.2	ควบคุมการอนุมัติการใช้ Plugins หรือ Third-party Components ซึ่งเป็นส่วนประกอบจากภายนอกเพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่ของส่วนประกอบเหล่านั้น			
7	การสำรองและกู้คืนข้อมูล (Data Backup & Recovery) มาตรฐานที่อ้างอิง : Cybersecurity Framework (NIST), Zero Trust			
7.1	จัดทำนโยบายและขั้นตอนการสำรองข้อมูลที่ชัดเจน เพื่อให้สามารถกู้คืนข้อมูลเมื่อเกิดปัญหาได้อย่างรวดเร็ว เช่น ทำ Full Backup อย่างน้อยสัปดาห์ละครั้ง, ทำ Incremental Backup ทุกวัน			
7.2	ติดตั้งระบบหรือกำหนดให้โปรแกรมสำรองข้อมูลตรวจสอบการสำรองข้อมูลเพื่อให้มั่นใจว่าข้อมูลถูกสำรองอย่างถูกต้อง			
7.3	จัดเก็บข้อมูลสำรองในสถานที่ที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูลจากเหตุการณ์ไม่คาดคิดหรือจากภัยธรรมชาติ เช่น Off-site หรือ Air gap			
7.4	ทดสอบการกู้คืนข้อมูลเพื่อให้มั่นใจว่าข้อมูลสามารถกู้คืนได้จริงอย่างน้อยปีละครั้ง			

แบบฟอร์มตรวจสอบสำหรับผู้ดูแลเครื่องแม่ข่ายตามมาตรฐานเพื่อการพัฒนาระบบสารสนเทศอย่างปลอดภัย				
ลำดับ	**หัวข้อ**	**ยอมรับได้**	**ยังต้องปรับปรุง**	**หมายเหตุ**
7.5	กำหนด Recovery Time Objective (RTO) คือ ระยะเวลาสูงสุดที่องค์กรสามารถยอมรับได้ในการกู้คืนระบบ แอปพลิเคชัน หรือบริการให้กลับมาใช้งานได้หลังจากเกิดเหตุขัดข้อง ก่อนที่จะส่งผลกระทบหรือเกิดความสูญเสียที่ไม่สามารถยอมรับได้ และ Recovery Point Objective (RPO) คือ ช่วงเวลาสูงสุดของข้อมูลที่สามารถสูญหายได้เมื่อต้องกู้คืนระบบหลังจากเกิดเหตุขัดข้องโดยกำหนดจากความถี่ของการสำรองข้อมูล (Backup) เพื่อให้สามารถวางแผนการกู้คืนได้อย่างมีประสิทธิภาพ			
7.6	ลบ/ทำลายสื่อบันทึกข้อมูลที่ไม่ใช้งานแล้วตามหลักการมาตรฐาน			
7.7	กำหนดระยะเวลาการเก็บข้อมูลสำรองเพื่อให้สามารถจัดการข้อมูลได้อย่างมีประสิทธิภาพ			