ประกาศมหาวิทยาลัยนเรศวร
เรื่อง นโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร
ตามมาตรฐาน OWASP Top 10

.....

เพื่อให้การจัดทำ Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร เป็นไปตามมาตรฐาน OWASP Top 10 และมาตรา 43 และ มาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อให้นักพัฒนาซอฟต์แวร์มีความตระหนักรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ (Cyber Security) ในการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร และเพื่อช่วยให้ซอฟต์แวร์, Web Application และ Mobile Application มีความปลอดภัยมากขึ้น รวมถึงสามารถบริหารจัดการความมั่นคงปลอดภัยเป็นไปอย่างมีประสิทธิภาพ และสอดคล้องกับแนวปฏิบัติในระดับสากล

อาศัยอำนาจตามความในมาตรา 20 มาตรา 21 และมาตรา 37 แห่งพระราชบัญญัติมหาวิทยาลัยนเรศวร พ.ศ. 2533 ประกอบกับมติคณะกรรมการบริหารมหาวิทยาลัยนเรศวร ในการประชุมครั้งที่ 22/2568 เมื่อวันที่ 18 พฤศจิกายน 2568 ให้กำหนดนโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร ตามมาตรฐาน OWASP Top 10 ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยนเรศวร เรื่อง นโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร ตามมาตรฐาน OWASP Top 10”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากประกาศเป็นต้นไป

ข้อ 3 ประกาศนี้ให้ใช้บังคับแก่ นิสิต บุคลากรมหาวิทยาลัยนเรศวร และส่วนงานต่างๆ ภายใต้โครงสร้างการบริหารมหาวิทยาลัย รวมถึงผู้พัฒนาซอฟต์แวร์จากหน่วยงานภาครัฐ หรือภาคเอกชนที่พัฒนา Web Application และ Mobile Application ให้กับมหาวิทยาลัยนเรศวร

ข้อ 4 ในประกาศนี้

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยนเรศวร

“อธิการบดี” หมายความว่า อธิการบดีมหาวิทยาลัยนเรศวร

“ส่วนงาน” หมายความว่า สำนักงานอธิการบดี บัณฑิตวิทยาลัย คณะ วิทยาลัย สถาบัน สำนัก ศูนย์ และหน่วยงานที่เรียกชื่ออย่างอื่นมีฐานะเทียบเท่าคณะที่เป็นส่วนราชการและที่สภามหาวิทยาลัยนเรศวรมีประกาศจัดตั้ง

"OWASP (Open Web Application Security Project)" หมายความว่า องค์กรไม่แสวงหากำไรที่ทำหน้าที่สร้างและเผยแพร่ความรู้ เครื่องมือ เอกสาร และมาตรฐานต่าง ๆ เพื่อปรับปรุงความมั่นคงปลอดภัยของซอฟต์แวร์และแอปพลิเคชันเพื่อทำให้ระบบคอมพิวเตอร์มีความปลอดภัยมากยิ่งขึ้นและเน้นวิจัยทางด้าน Web Application Security

"OWASP Top 10 หมายความว่า รายการความเสี่ยงด้านความปลอดภัยที่สำคัญที่สุด 10 อันดับแรกสำหรับ Web Application ซึ่งจัดทำโดย OWASP มีวัตถุประสงค์เพื่อให้เป็นแนวทางสำหรับนักพัฒนาและองค์กรต่างๆ ในการทำความเข้าใจและลดความเสี่ยงด้านความปลอดภัย ซึ่ง OWASP Top 10 จะมีการเปลี่ยนแปลงทุกปี"

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ผู้พัฒนาซอฟต์แวร์" หมายความว่า นิสิต บุคลากรมหาวิทยาลัยนเรศวร และส่วนงานต่างๆ ภายใต้โครงสร้างการบริหารมหาวิทยาลัย รวมถึงผู้พัฒนาซอฟต์แวร์จากหน่วยงานภาครัฐ หรือภาคเอกชนที่พัฒนา Web Application และ Mobile Application ให้กับมหาวิทยาลัยนเรศวร

ข้อ 5 นโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยตามมาตรฐาน OWASP Top 10 มีวัตถุประสงค์ดังนี้

(1) เพื่อกำหนดแนวทางในการพัฒนาซอฟต์แวร์ที่ปลอดภัยตามมาตรฐาน OWASP ให้กับหน่วยงานทั้งภายในและภายนอกมหาวิทยาลัย

(2) เพื่อให้หน่วยงานมีระเบียบการประเมินความเสี่ยงและบริหารช่องโหว่ (Vulnerability Management)

(3) เพื่อสร้างกระบวนการทำแผนตรวจสอบและทดสอบ (Testing) อย่างสม่ำเสมอ ครอบคลุม OWASP Top 10 เวอร์ชันปัจจุบัน และการประเมินด้านอื่นๆ

(4) เพื่อรวมมาตรการควบคุมเข้ากับระบบจัดการความมั่นคงของข้อมูลตาม ISO/IEC 27001 และนโยบายความมั่นคงปลอดภัยไซเบอร์

ข้อ 6 ให้ผู้พัฒนาซอฟต์แวร์ หรือส่วนงานที่ดำเนินการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยดำเนินการตามนโยบายนี้ โดยคำนึงถึงขอบเขต บทบาทและหน้าที่ แนวทางปฏิบัติการดำเนินงานตามมาตรฐาน OWASP Top 10 ตามเอกสารแนบท้ายประกาศนี้

ข้อ 7 การดำเนินการตามข้อ 6 กรณีที่เป็นข้อมูลส่วนบุคคลให้จัดระดับผลกระทบด้านการรักษาความลับระดับกลางเป็นอย่างน้อย ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และดำเนินการไม่น้อยกว่าข้อกำหนดขั้นต่ำท้ายประกาศนี้

ข้อ 8 นโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยตามมาตรฐาน OWASP Top 10 ถือเป็นมาตรฐานด้านการพัฒนา Web Application รวมไปถึง Mobile Application ของมหาวิทยาลัย เพื่อเป็นแนวทางในการดำเนินงานได้อย่างปลอดภัย เป็นไปตามนโยบายของรัฐ ดังนั้นผู้พัฒนาจึงควรยึดถือและปฏิบัติตามอย่างเคร่งครัด

ข้อ 9 ให้อธิการบดีเป็นผู้รักษาการตามประกาศนี้ กรณีที่มีปัญหาจากการปฏิบัติตามประกาศนี้ หรือที่ประกาศนี้มิได้กำหนดไว้ให้อธิการบดีเป็นผู้วินิจฉัยและคำวินิจฉัยนั้นให้ถือเป็นที่สุด

ประกาศ ณ วันที่ 1 ธันวาคม พ.ศ. 2568

(รองศาสตราจารย์ ดร.ศรินทร์ทิพย์ แทนธานี)
รักษาราชการแทนอธิการบดีมหาวิทยาลัยนเรศวร

เอกสารแนบท้ายประกาศมหาวิทยาลัยนเรศวร

นโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร
ตามมาตรฐาน OWASP Top 10

ฉบับลงวันที่ ๑ ธันวาคม พ.ศ. 2568

.....

**หลักการ**

ปัจจุบันเทคโนโลยีสารสนเทศและระบบ Web Application และ Mobile Application มีบทบาทสำคัญต่อการดำเนินงานของมหาวิทยาลัย ทั้งในด้านการบริหารจัดการ การให้บริการแก่นักศึกษา บุคลากร และประชาชน รวมถึงการจัดเก็บและประมวลผลข้อมูลสำคัญ ซึ่งอาจเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่มีความสำคัญเชิงยุทธศาสตร์ การพัฒนาและดูแลระบบ Web Application และ Mobile Application โดยขาดมาตรการ ด้านความมั่นคงปลอดภัยที่เหมาะสม อาจก่อให้เกิดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ เช่น การเจาะระบบ การขโมยข้อมูล การแก้ไขข้อมูลโดยมิชอบ หรือการหยุดชะงักของการให้บริการ ซึ่งอาจสร้างความเสียหายทางเศรษฐกิจ ชื่อเสียง และอาจนำไปสู่การละเมิดกฎหมาย

เพื่อให้การพัฒนาและบำรุงรักษา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร เป็นไปอย่างปลอดภัย มีมาตรฐาน และสอดคล้องกับ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) รวมถึงมาตรฐานความมั่นคงปลอดภัยสารสนเทศที่เป็นที่ยอมรับในระดับสากล จึงมีความจำเป็นต้องกำหนด นโยบายการพัฒนา Web Application และ Mobile Application ตามมาตรฐาน OWASP Top 10

มาตรฐาน OWASP Top 10 จัดทำโดย Open Web Application Security Project เป็นองค์กรไม่แสวงหาผลกำไรระดับนานาชาติที่ทำการวิจัยและจัดทำรายงานสรุปช่องโหว่ด้านความมั่นคงปลอดภัยที่พบมากที่สุดใน Web Application โดยเวอร์ชันล่าสุด (OWASP Top 10:2021) ได้ระบุ ๑๐ หมวดหมู่ความเสี่ยงที่สำคัญ ซึ่งหากนำมาเป็นแนวทางในการพัฒนา จะช่วยป้องกันการโจมตี ลดความเสี่ยงด้านความปลอดภัย และเพิ่มความเชื่อมั่นให้แก่ผู้ใช้บริการ

ดังนั้น จึงเห็นสมควรกำหนดนโยบายนี้ขึ้น เพื่อเป็นกรอบการดำเนินงานของหน่วยงานภายในมหาวิทยาลัยนเรศวรที่เกี่ยวข้องกับการพัฒนา จัดหา หรือปรับปรุงระบบ Web Application ให้ดำเนินการตามแนวปฏิบัติด้านความมั่นคงปลอดภัยตามมาตรฐานสากล และสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

**วัตถุประสงค์**

1. เพื่อกำหนดแนวทางในการพัฒนาซอฟต์แวร์, Web Application และ Mobile Application ให้มีให้มีความมั่นคงปลอดภัยตามมาตรฐาน OWASP Top 10

2. เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับ Web Application และ Mobile Application ของมหาวิทยาลัย

3. เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการในด้านความปลอดภัยของข้อมูลและการให้บริกา

4. เพื่อให้การพัฒนาระบบเป็นไปตามข้อกำหนดของกฎหมายและนโยบายด้านความมั่นคงปลอดภัย สารสนเทศของมหาวิทยาลัย

กำหนดมาตรฐานการพัฒนา จัดการ และควบคุมความปลอดภัยของ Web Application และ Mobile Application รวมถึงบริการดิจิทัลทั้งหมดของมหาวิทยาลัยนเรศวรให้สอดคล้องกับมาตรฐาน OWASP Top 10 เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ปกป้องข้อมูลของมหาวิทยาลัย นิสิต บุคลากร และผู้มีส่วนได้ส่วนเสีย

**ขอบเขต**

นโยบายนี้ครอบคลุม ดังต่อไปนี้

1. Web Application และ Mobile Application ที่พัฒนาเอง (in-house) ทุกระบบ

2. Web Application และ Mobile Application หรือบริการภายนอก (COTS/SaaS) ที่มหาวิทยาลัยนำมาใช้งาน หากมีการประมวลผลหรือจัดเก็บข้อมูลของมหาวิทยาลัย

3. Web Application และ Mobile Application และสคริปต์ที่นิสิต/บุคลากรพัฒนาขึ้นเพื่อการเรียนการสอนและวิจัยสถาบัน ซึ่งให้บริการแก่ผู้ใช้ภายนอก ภายใต้การเชื่อมต่อระบบเครือข่ายของมหาวิทยาลัย

4. Code ส่วนขยาย (plugins, modules) ที่ทำงานบนระบบของมหาวิทยาลัย

5. ระบบสารสนเทศที่อยู่ในสภาพแวดล้อมภายใต้ระบบคลาวด์ (Public, Private, Hybrid)

6. ทุกหน่วยงานภายในมหาวิทยาลัยนเรศวรที่มีบทบาทในการออกแบบ พัฒนา ทดสอบ ปรับปรุง หรือบริหารจัดการ Application

**คำนิยาม**

มหาวิทยาลัย หมายถึง มหาวิทยาลัยนเรศวร

อธิการบดี หมายถึง อธิการบดีมหาวิทยาลัยนเรศวร

ส่วนงาน หมายถึง สำนักงานอธิการบดี บัณฑิตวิทยาลัย คณะ วิทยาลัย สถาบัน สำนัก ศูนย์ และหน่วยงานที่เรียกชื่ออย่างอื่นมีฐานะ เทียบเท่าคณะที่เป็นส่วนราชการและที่สภามหาวิทยาลัยนเรศวรมีประกาศจัดตั้ง

OWASP หมายถึง องค์กรไม่แสวงหากำไรที่ทำหน้าที่สร้าง และเผยแพร่ความรู้ เครื่องมือ เอกสาร และมาตรฐานต่างๆ เพื่อปรับปรุงความมั่นคงปลอดภัยของซอฟต์แวร์และแอปพลิเคชันเพื่อทำให้ระบบคอมพิวเตอร์มีความปลอดภัยมากยิ่งขึ้นและเน้นวิจัยทางด้าน Web Application Security

OWASP Top 10 หมายถึง รายการความเสี่ยงด้านความปลอดภัยที่สำคัญที่สุด 10 อันดับแรกสำหรับเว็บแอปพลิเคชัน จัดทำโดย OWASP (Open Web Application Security Project) ซึ่งเป็นองค์กรไม่แสวงหาผลกำไร โดยมีวัตถุประสงค์เพื่อให้เป็นแนวทางสำหรับนักพัฒนาและองค์กรต่าง ๆ ในการทำความเข้าใจและลดความเสี่ยงด้านความปลอดภัย ทั้งนี้ OWASP Top 10 จะมีการเปลี่ยนแปลงทุกปี

ผู้พัฒนาซอฟต์แวร์ หมายถึง นิสิต บุคลากรมหาวิทยาลัยนเรศวร และส่วนงานต่างๆ ภายใต้โครงสร้างการบริหารมหาวิทยาลัย รวมถึงผู้พัฒนาซอฟต์แวร์จากหน่วยงานภาครัฐ หรือภาคเอกชนที่พัฒนา Web Application และ Mobile Application ให้กับมหาวิทยาลัยนเรศวร

Web Application หมายถึง โปรแกรมประยุกต์ซอฟต์แวร์ ที่ถูกออกแบบและพัฒนาเพื่อใช้งานผ่านเครือข่ายอินเทอร์เน็ตหรือเครือข่ายภายใน (Intranet) โดยเข้าถึงผ่าน เว็บเบราว์เซอร์ โดยไม่จำเป็นต้องติดตั้งโปรแกรมบนอุปกรณ์ผู้ใช้ Applicationประเภทนี้มักทำงานบน เว็บเซิร์ฟเวอร์ (Web Server) และเชื่อมต่อกับ ฐานข้อมูล (Database Server) หรือบริการอื่นๆ เพื่อให้บริการแก่ผู้ใช้งาน

Mobile Application หมายถึง โปรแกรมประยุกต์ซอฟต์แวร์ ที่ถูกออกแบบ พัฒนาและติดตั้งเพื่อใช้งานบนอุปกรณ์เคลื่อนที่ เช่น สมาร์ตโฟน แท็บเล็ต หรืออุปกรณ์พกพาอื่นๆ โดยทำงานบนระบบปฏิบัติการสำหรับอุปกรณ์เคลื่อนที่ ได้แก่ Android, iOS, HarmonyOS หรือระบบอื่นที่เทียบเท่า โดย Application ดังกล่าวอาจเป็นได้ ทั้ง Native Application, Hybrid Application หรือ Web Application (PWA) ซึ่งทำหน้าที่ในการให้บริการสารสนเทศ การสื่อสาร การศึกษา การบริหารจัดการ รวมถึงการประมวลผลข้อมูลที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย

**บทบาทและหน้าที่**

คณะผู้บริหารมหาวิทยาลัย มีหน้าที่รับผิดชอบกำกับดูแลภาพรวม ดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยของ Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร

Head of Information Security มีหน้าที่ควบคุมการกำหนดนโยบาย, วางกระบวนการตรวจประเมิน, ดูแลการสื่อสาร และรายงานความเสี่ยงต่อคณะผู้บริหารมหาวิทยาลัย

ผู้พัฒนาซอฟต์แวร์ มีหน้าที่ ปฏิบัติตาม Secure Coding ตามมาตรฐาน OWASP Top 10, ดำเนินการแก้ไขช่องโหว่ และ พร้อมทั้งเข้าร่วมฝึกอบรมด้านมาตรฐาน OWASP Top 10

**แนวทางปฏิบัติการดำเนินงานตามมาตรฐาน OWASP Top 10:2021**

1. **A01: Broken Access Control** : ควรดำเนินการควบคุมสิทธิ์การเข้าถึง (Access Control) เพื่อป้องกันการทำงานผิดพลาดจากผู้ไม่หวังดีที่สามารถเข้าถึงข้อมูลหรือฟังก์ชันที่ไม่ได้รับอนุญาตได้

2. **A02: Cryptographic Failures** : ควรดำเนินการใช้หรือตั้งค่าระบบเข้ารหัส (Cryptography) อย่างถูกต้อง เพื่อปกป้องข้อมูลที่เป็นความลับไม่ให้เกิดการรั่วไหล

3. **A03: Injection** : ควรตรวจสอบและกรองข้อมูลนำเข้าก่อนประมวลผล และใช้เทคนิคที่ปลอดภัย เช่น Parameterized Query หรือ Prepared Statement เพื่อลดความเสี่ยงจากการสอดแทรกคำสั่งที่ไม่พึงประสงค์ พร้อมทั้งกำหนดสิทธิ์การเข้าถึงฐานข้อมูลและระบบให้อยู่ในระดับที่จำเป็นเท่านั้น เพื่อป้องกันการโจมตีที่อาจเกิดขึ้น

4. **A04: Insecure Design** : ควรออกแบบระบบโดยบูรณาการแนวคิดด้านความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการวิเคราะห์ความต้องการ (Secure by Design) และใช้การประเมินความเสี่ยงหรือ Threat Modeling ประกอบ พร้อมทั้งกำหนดมาตรการควบคุมความปลอดภัยเชิงป้องกันไว้ล่วงหน้า เช่น การพิสูจน์ตัวตน การกำหนดสิทธิ์ และการปกป้องข้อมูลที่สำคัญ

5. **A05: Security Misconfiguration** : ควรกำหนดค่าระบบและซอฟต์แวร์ให้สอดคล้องกับแนวทางด้านความมั่นคงปลอดภัย เช่น ปิด Debug/Default Configuration ที่ไม่จำเป็น และปรับแต่งให้เหมาะสมกับสภาพแวดล้อมจริง รวมทั้งควรมีการตรวจสอบ แก้ไข และทดสอบการตั้งค่าอย่างสม่ำเสมอ เพื่อลดความเสี่ยงจากการโจมตีที่อาศัยช่องโหว่ด้านการกำหนดค่า

6. **A06: Vulnerable and Outdated Components** : ควรติดตามและอัปเดตเวอร์ชันของซอฟต์แวร์ Framework และ Library อย่างสม่ำเสมอ โดยใช้เฉพาะเวอร์ชันที่ผู้พัฒนารับรองว่าปลอดภัย พร้อมทั้งจัดทำรายการทรัพยากรซอฟต์แวร์ (Software Inventory) และใช้เครื่องมือสแกนช่องโหว่เพื่อตรวจสอบและแก้ไขทันทีเมื่อพบความเสี่ยง

7. **A07: Identification and Authentication Failures** : ควรใช้กลไกการพิสูจน์ตัวตนที่รัดกุม เช่น Multi-Factor Authentication (MFA) การจัดการรหัสผ่านอย่างปลอดภัย และการเข้ารหัสข้อมูลสำคัญ พร้อมทั้งกำหนดอายุการใช้งานของ Session และป้องกันการโจมตีที่เกี่ยวข้อง เช่น Session Hijacking หรือ Brute Force Attack

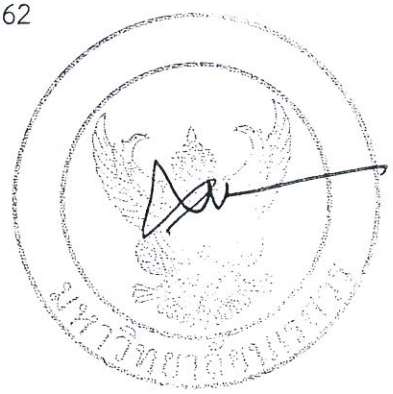
8. **A08: Software and Data Integrity Failures** : ควรใช้กลไกตรวจสอบความถูกต้องและความน่าเชื่อถือของซอฟต์แวร์หรือข้อมูล เช่น การใช้ Digital Signature, Checksum หรือ Code Signing ก่อนนำมาใช้งาน พร้อมทั้งจัดทำกระบวนการ CI/CD ที่ปลอดภัย มีการควบคุมสิทธิ์ในการปรับแก้โค้ด และตรวจสอบความถูกต้องของไฟล์หรืออัปเดตก่อนนำไปใช้งานจริง

9. A09: Security Logging and Monitoring Failures : ควรจัดทำระบบบันทึกเหตุการณ์ (Logging) และการตรวจสอบ (Monitoring) ที่ครอบคลุมและเก็บบันทึกอย่างเหมาะสม เพื่อใช้ในการวิเคราะห์และตรวจสอบย้อนหลัง พร้อมทั้งมีระบบ Monitoring และ Alert แบบเรียลไทม์ เพื่อให้สามารถตรวจจับและตอบสนองต่อเหตุการณ์ผิดปกติหรือการโจมตีได้อย่างทันท่วงที

10. A10: Server-Side Request Forgery (SSRF) : ควรตรวจสอบและจำกัดการป้อนค่า URL จากผู้ใช้ โดยใช้ Allowlist ของปลายทางที่อนุญาต และห้ามเข้าถึงระบบภายในหรือเมตะดาต้าที่สำคัญ พร้อมทั้งใช้กลไกป้องกันเพิ่มเติม เช่น การตรวจสอบ DNS, การกรองพารามิเตอร์ และการแยกเครือข่าย (Network Segmentation) เพื่อจำกัดความเสียหายจากการโจมตี

**เอกสารอ้างอิง**


1. OWASP Top 10:2021 – The Ten Most Critical Web Application Security Risks
2. OWASP Application Security Verification Standard (ASVS) 4.0
3. OWASP Secure Coding Practices Checklist
4. OWASP Software Assurance Maturity Model (SAMM)
5. NIST SP 800-218 (SSDF) – Secure Software Development Framework
6. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
7. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 256
8. ประกาศ/ระเบียบมหาวิทยาลัยนเรศวร ที่เกี่ยวข้อง

แบบฟอร์มการตรวจสอบรายการดำเนินงานพัฒนา Web Application และ Mobile Application
ของมหาวิทยาลัยนเรศวร ตามมาตรฐาน OWASP Top 10

**คำชี้แจง** ผู้พัฒนาซอฟต์แวร์ (ความหมายตามอ้างอิงประกาศมหาวิทยาลัยนเรศวร เรื่อง นโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร ตามมาตรฐาน OWASP Top 10) โปรดดำเนินการตรวจสอบ พร้อมทั้งระบุรายละเอียดการดำเนินการในแต่ละหัวข้อ เพื่อให้การพัฒนาและบำรุงรักษา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร เป็นไปอย่างปลอดภัย มีมาตรฐาน และสอดคล้องกับ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) รวมถึงมาตรฐานความมั่นคงปลอดภัยสารสนเทศที่เป็นที่ยอมรับในระดับสากล ผู้พัฒนาซอฟต์แวร์จึงมีความจำเป็นต้องดำเนินการตรวจสอบรายการการดำเนินการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร ตามมาตรฐาน OWASP Top 10 โดยมีรายละเอียดดังนี้

**แนวทางปฏิบัติการดำเนินงานตามมาตรฐาน OWASP Top 10:2021**

1. A01: Broken Access Control : ควรดำเนินการควบคุมสิทธิ์การเข้าถึง (Access Control) เพื่อป้องกันการทำงานผิดพลาดจากผู้ไม่หวังดีที่สามารถเข้าถึงข้อมูลหรือฟังก์ชันที่ไม่ได้รับอนุญาตได้

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

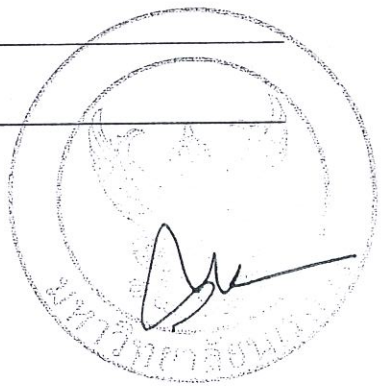
_____

_____

_____

_____

_____



2. A02: Cryptographic Failures : ควรดำเนินการใช้หรือตั้งค่าระบบเข้ารหัส (Cryptography) อย่างถูกต้อง เพื่อปกป้องข้อมูลที่เป็นความลับไม่ให้เกิดการรั่วไหล

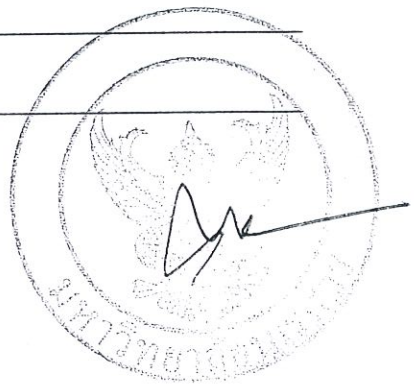
☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

3. A03: Injection : ควรตรวจสอบและกรองข้อมูลนำเข้าก่อนประมวลผล และใช้เทคนิคที่ปลอดภัย เช่น Parameterized Query หรือ Prepared Statement เพื่อลดความเสี่ยงจากการสอดแทรกคำสั่งที่ไม่พึงประสงค์ พร้อมทั้งกำหนดสิทธิ์การเข้าถึงฐานข้อมูลและระบบให้อยู่ในระดับที่จำเป็นเท่านั้น เพื่อป้องกันการโจมตีที่อาจเกิดขึ้น

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ



4. A04: Insecure Design : ควรออกแบบระบบโดยบูรณาการแนวคิดด้านความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการวิเคราะห์ความต้องการ (Secure by Design) และใช้การประเมินความเสี่ยงหรือ Threat Modeling ประกอบ พร้อมทั้งกำหนดมาตรการควบคุมความปลอดภัยเชิงป้องกันไว้ล่วงหน้า เช่น การพิสูจน์ตัวตน การกำหนดสิทธิ์ และการปกป้องข้อมูลที่สำคัญ

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

5. A05: Security Misconfiguration : ควรกำหนดค่าระบบและซอฟต์แวร์ให้สอดคล้องกับแนวทางด้านความมั่นคงปลอดภัย เช่น ปิด Debug/Default Configuration ที่ไม่จำเป็น และปรับแต่งให้เหมาะสมกับสภาพแวดล้อมจริง รวมทั้งควรมีการตรวจสอบ แก้ไข และทดสอบการตั้งค่าอย่างสม่ำเสมอ เพื่อลดความเสี่ยงจากการโจมตีที่อาศัยช่องโหว่ด้านการกำหนดค่า

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

6. A06: Vulnerable and Outdated Components : ควรติดตามและอัปเดตเวอร์ชันของซอฟต์แวร์ Framework และ Library อย่างสม่ำเสมอ โดยใช้เฉพาะเวอร์ชันที่ผู้พัฒนารับรองว่าปลอดภัย พร้อมทั้งจัดทำรายการทรัพยากรซอฟต์แวร์ (Software Inventory) และใช้เครื่องมือสแกนช่องโหว่เพื่อตรวจสอบและแก้ไขทันทีเมื่อพบความเสี่ยง

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

_____

_____

_____

_____

_____

7. A07: Identification and Authentication Failures : ควรใช้กลไกการพิสูจน์ตัวตนที่รัดกุม เช่น Multi-Factor Authentication (MFA) การจัดการรหัสผ่านอย่างปลอดภัย และการเข้ารหัสข้อมูลสำคัญ พร้อมทั้งกำหนดอายุการใช้งานของ Session และป้องกันการโจมตีที่เกี่ยวข้อง เช่น Session Hijacking หรือ Brute Force Attack

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

_____

_____

_____

_____

_____

8. A08: Software and Data Integrity Failures : ควรใช้กลไกตรวจสอบความถูกต้องและความน่าเชื่อถือของซอฟต์แวร์หรือข้อมูล เช่น การใช้ Digital Signature, Checksum หรือ Code Signing ก่อนนำมาใช้งาน พร้อมทั้งจัดทำกระบวนการ CI/CD ที่ปลอดภัย มีการควบคุมสิทธิ์ในการปรับแก้โค้ด และตรวจสอบความถูกต้องของไฟล์หรืออัปเดตก่อนนำไปใช้งานจริง

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

_____

_____

_____

_____

_____

9. A09: Security Logging and Monitoring Failures : ควรจัดทำระบบบันทึกเหตุการณ์ (Logging) และการตรวจสอบ (Monitoring) ที่ครอบคลุมและเก็บบันทึกอย่างเหมาะสม เพื่อใช้ในการวิเคราะห์และตรวจสอบย้อนหลัง พร้อมทั้งมีระบบ Monitoring และ Alert แบบเรียลไทม์ เพื่อให้สามารถตรวจจับและตอบสนองต่อเหตุการณ์ผิดปกติหรือการโจมตีได้อย่างทันท่วงที

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

_____

_____

_____

_____

_____

10. A10: Server-Side Request Forgery (SSRF) : ควรตรวจสอบและจำกัดการป้อนค่า URL จากผู้ใช้ โดยใช้ Allowlist ของปลายทางที่อนุญาต และห้ามเข้าถึงระบบภายในหรือเมตะดาต้าที่สำคัญ พร้อมทั้งใช้กลไกป้องกันเพิ่มเติม เช่น การตรวจสอบ DNS, การกรองพารามิเตอร์ และการแยกเครือข่าย (Network Segmentation) เพื่อจำกัดความเสียหายจากการโจมตี

☐ ดำเนินการเรียบร้อย ☐ ยังไม่ได้ดำเนินการ

รายละเอียดการดำเนินการ

_____

_____

_____

_____

_____

ทั้งนี้ ผู้พัฒนาซอฟต์แวร์ควรตระหนักถึงความมั่นคงปลอดภัยของระบบตั้งแต่ขั้นตอนการออกแบบ พัฒนา ทดสอบ และบำรุงรักษา โดยยึดหลักประกาศมหาวิทยาลัยนเรศวร เรื่อง นโยบายการพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร ตามมาตรฐาน OWASP Top 10 เพื่อป้องกันความเสี่ยงและช่องโหว่ที่อาจส่งผลกระทบต่อข้อมูล ผู้ใช้งาน และความเชื่อมั่นของมหาวิทยาลัยต่อไป

ขอรับรองว่า การพัฒนา (โปรดระบุชื่อระบบ Web Application / Mobile Application) ผ่านการตรวจสอบรายการดำเนินงานพัฒนา Web Application และ Mobile Application ของมหาวิทยาลัยนเรศวร ตามมาตรฐาน OWASP Top 10

ลงชื่อ_____ ลงชื่อ_____

(_____) (_____)

ผู้พัฒนาซอฟต์แวร์ ผู้รับรองแบบฟอร์ม

ลงชื่อ_____

(_____)

ผู้ดูแลระบบฯ ประจำหน่วยงาน

ลงชื่อ_____

(_____)

ตำแหน่ง _____

หน่วยงาน _____

ผู้บริหารหน่วยงานลงนามรับทราบ

**หมายเหตุ**

1. ผู้รับรองแบบฟอร์มจะต้องเป็นบุคลากรของมหาวิทยาลัยที่ควบคุมกำกับผู้พัฒนาซอฟต์แวร์ โดยผู้รับรองแบบฟอร์มสามารถเป็นบุคคลเดียวกันกับผู้ดูแลระบบฯ ประจำหน่วยงานได้
2. กรณีเป็นโครงการวิจัยจะต้องเป็นหัวหน้าโครงการวิจัยเป็นผู้รับรองแบบฟอร์ม พร้อมทั้งให้ผู้ดูแลระบบฯ ประจำหน่วยงานรับรองแบบฟอร์ม
3. ผู้บริหารของหน่วยงานจำเป็นต้องลงนามรับทราบแบบฟอร์มทุกครั้ง