ประกาศสำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา

ที่ ๐๖๕/๒๕๖๘

เรื่อง แนวปฏิบัติด้านความปลอดภัยในการพัฒนาระบบสารสนเทศ มหาวิทยาลัยบูรพา

เพื่อให้การดำเนินการด้านความปลอดภัยของระบบสารสนเทศของมหาวิทยาลัยบูรพา เป็นไปตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยบูรพาที่ ๑๓๔๓/๒๕๖๘ เรื่องมาตรการการจัดการ และการแจ้งข้อมูลและสารสนเทศของมหาวิทยาลัย เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และป้องกันความเสี่ยงจากช่องโหว่ระดับร้ายแรง ข้อมูลรั่วไหล และการโจมตีทางไซเบอร์

อาศัยอำนาจตามความในข้อ ๔ (๑๐) ของคำสั่งมหาวิทยาลัยบูรพา ที่ ๑๖๘๖/๒๕๖๗ เรื่อง การมอบอำนาจส่วนงานให้หัวหน้าส่วนงานปฏิบัติการแทน ฉบับลงวันที่ ๒๕ กันยายน พ.ศ.๒๕๖๗ ประกอบกับมติที่ประชุมคณะกรรมการบริหารสำนักคอมพิวเตอร์ ครั้งที่ ๑๐/๒๕๖๘ เมื่อวันที่ ๑๕ ธันวาคม พ.ศ.๒๕๖๘ สำนักคอมพิวเตอร์จึงออกประกาศ ไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักคอมพิวเตอร์ ที่ ๐๖๕/๒๕๖๘ เรื่อง แนวปฏิบัติด้านความปลอดภัยในการพัฒนาระบบสารสนเทศ มหาวิทยาลัยบูรพา”

ข้อ ๒ ประกาศนี้ให้บังคับใช้ตั้งแต่วันที่ ๑ มกราคม พ.ศ.๒๕๖๙

ข้อ ๓ ในประกาศนี้

“มหาวิทยาลัย” หมายถึง มหาวิทยาลัยบูรพา

“สำนักคอมพิวเตอร์” หมายถึง สำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา

“**ส่วนงาน**” หมายถึง ส่วนงานตามมาตรา ๙ แห่งพระราชบัญญัติมหาวิทยาลัยบูรพา พ.ศ. ๒๕๕๐

“ระบบสารสนเทศ” หมายถึง โปรแกรม เว็บไซต์ แอปพลิเคชัน หรือบริการใด ๆ ที่มีการประมวลผลหรือจัดเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยมหาวิทยาลัยพัฒนาขึ้นหรือได้ว่าจ้างให้ผู้อื่นพัฒนาขึ้น ที่เข้าถึงได้จากภายนอกมหาวิทยาลัยบูรพา หรือเข้าใช้งานผ่านบัญชีผู้ใช้งานของมหาวิทยาลัย เพื่อใช้ในการรวบรวม จัดเก็บ ประมวลผล และเผยแพร่ข้อมูลและสารสนเทศ เพื่อประกอบการตัดสินใจและการบริหารงานของมหาวิทยาลัย

/รวมทั้งเพื่อ...

เอกสารนี้ลงนามด้วยลายเซ็นอิเล็กทรอนิกส์ ตรวจสอบได้ที่ (https://e-sign.buu.ac.th/verify)

รวมทั้งเพื่อให้บริการแก่บุคคลหรือหน่วยงานภายนอก

“Certificate” หมายความว่า เอกสารหรือหนังสือรับรองที่ยืนยันว่าระบบสารสนเทศได้ผ่านการตรวจสอบด้านความมั่นคงปลอดภัย และได้รับอนุญาตให้นำขึ้นใช้งานจริง

ข้อ ๔ การจำแนกระบบสารสนเทศ แบ่งเป็น ๓ กลุ่มดังนี้

๔.๑ ระบบสารสนเทศที่พัฒนาขึ้นโดยสำนักคอมพิวเตอร์

๔.๒ ระบบสารสนเทศที่ส่วนงานพัฒนาขึ้นและมีการจัดเก็บโดยเครื่องแม่ข่ายของสำนักคอมพิวเตอร์

๔.๓ ระบบสารสนเทศที่ส่วนงานพัฒนาขึ้นแต่มีการจัดเก็บที่เครื่องแม่ข่ายที่ส่วนงานจัดหาเอง

ข้อ ๕ ขั้นตอนการดำเนินการในการตรวจสอบช่องโหว่ด้านความปลอดภัย

๕.๑ การลงทะเบียนระบบสารสนเทศ ระบบสารสนเทศทุกระบบในข้อ ๔ จะต้องทำการลงทะเบียนระบบสารสนเทศ โดยจะต้องแจ้งข้อมูลพื้นฐานของระบบสารสนเทศให้สำนักคอมพิวเตอร์ทราบ เพื่อให้นำเข้าสู่กระบวนการตรวจสอบด้านความปลอดภัยต่อไป โดยมีข้อมูลดังต่อไปนี้

๑. ชื่อระบบสารสนเทศ

๒. “URL” หรือ (Uniform Resource Locator) ซึ่งหมายถึง ที่อยู่หรือแหล่งอ้างอิงของทรัพยากรบนเครือข่ายอินเทอร์เน็ต ที่ระบุเส้นทางหรือที่ตั้งของเว็บไซต์ ระบบสารสนเทศหรือไฟล์ที่สามารถเข้าถึงได้ผ่านเครือข่าย

๓. วัตถุประสงค์การพัฒนาระบบสารสนเทศ

๔. ส่วนงานผู้รับผิดชอบ

สำหรับระบบสารสนเทศในข้อ ๔.๑ และ ๔.๒ สำนักคอมพิวเตอร์จะดำเนินการลงทะเบียนระบบสารสนเทศให้ แต่ระบบสารสนเทศในข้อ ๔.๓ ส่วนงานจะต้องทำบันทึกข้อความหรือแจ้งข้อมูลข้างต้นผ่านช่องทางอื่นที่สำนักคอมพิวเตอร์กำหนด

๕.๒ เครื่องมือประเมินช่องโหว่ด้านความปลอดภัยและคุณภาพซอร์สโค้ด สำนักคอมพิวเตอร์จะใช้เครื่องมือสำหรับประเมินช่องโหว่ด้านความปลอดภัย ดังนี้

๕.๒.๑ “Nessus (Nessus® Vulnerability Scanner)” เป็นซอฟต์แวร์ที่ใช้สำหรับตรวจสอบและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย เพื่อระบุความเสี่ยงและข้อบกพร่องที่อาจถูกโจมตีได้

๕.๒.๒ “SonarQube (SonarQube® Static Code Analysis Tool)” เป็นซอฟต์แวร์ที่ใช้สำหรับตรวจสอบและวิเคราะห์ซอร์สโค้ด (รหัสต้นฉบับ) ของระบบสารสนเทศ เพื่อประเมินคุณภาพและตรวจหาช่องโหว่ด้านความมั่นคงปลอดภัยของซอร์สโค้ด

/ระบบสารสนเทศ...

เอกสารนี้ลงนามด้วยลายเซ็นอิเล็กทรอนิกส์ ตรวจสอบได้ที่ (https://e-sign.buu.ac.th/verify)

ระบบสารสนเทศตามข้อ ๔.๑ จะถูกตรวจสอบด้วยเครื่องมือตามข้อ ๕.๒.๑ และ ๕.๒.๒ ส่วนระบบสารสนเทศตามข้อ ๔.๒ และ ๔.๓ จะถูกตรวจสอบด้วยเครื่องมือตามข้อ ๕.๒.๑ เท่านั้น อย่างไรก็ตามสำนักคอมพิวเตอร์แนะนำให้ส่วนงานหรือหน่วยงานที่พัฒนาระบบสารสนเทศตามข้อ ๔.๒ และ ๔.๓ ควรมีการตรวจสอบและวิเคราะห์ซอร์สโค้ดตามเครื่องมือ ๕.๒.๒ ด้วย

๕.๓ การออกใบรับรอง (Certificate) ระบบสารสนเทศที่ผ่านการตรวจสอบด้านความปลอดภัยและคุณภาพซอร์สโค้ด ระบบสารสนเทศที่ผ่านการตรวจสอบด้านความปลอดภัยและคุณภาพซอร์สโค้ดด้วยเครื่องมือตามข้อ ๕.๒ แล้ว สำนักคอมพิวเตอร์จะออกหนังสือรับรองการตรวจสอบ โดยหนังสือรับรองจะมีอายุ ๖ เดือนนับตั้งแต่วันที่ออกหนังสือ สำหรับระบบสารสนเทศที่**ไม่ผ่าน**การรับรอง สำนักคอมพิวเตอร์จะ**ไม่อนุญาต**ให้ระบบเปิดการใช้งานจริง หรือเปิดให้ใช้งานได้เฉพาะการเข้าถึงจากเครือข่ายภายในมหาวิทยาลัยบูรพาเท่านั้น หรือปิดการเข้าถึงระบบสารสนเทศทั้งภายในและภายนอก แล้วแต่กรณีของระดับความรุนแรงด้านความปลอดภัย จนกว่าจะมีผ่านการรับรองด้านความปลอดภัย

สำนักคอมพิวเตอร์จะทำการแจ้งเตือนหน่วยงานหรือส่วนงานที่ดูแลระบบสารสนเทศ ให้ทำการแก้ไขช่องโหว่ด้านความปลอดภัย รวมถึงการแจ้งเตือนเมื่อใกล้ถึงวันหมดอายุการรับรองอย่างน้อย ๑ เดือน รายละเอียดการตรวจสอบตามเอกสารแนบท้ายประกาศ หมายเลข ๑

ข้อ ๖ การจัดการกับข้อมูลส่วนบุคคล ระบบสารสนเทศทุกระบบ จะต้องดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และประกาศอื่นที่เกี่ยวข้องที่ประกาศเพิ่มเติม

ข้อ ๗ ให้มีการเก็บบันทึกข้อมูล (Log) ของการใช้งานระบบสารสนเทศเพื่อใช้ตรวจสอบย้อนกลับ เมื่อเกิดเหตุผิดปกติ เช่น การโจมตี การรั่วไหล หรือการเข้าถึงโดยไม่ได้รับอนุญาต ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม

ข้อ ๘ การสำรองข้อมูล ระบบสารสนเทศควรมีการสำรองข้อมูลสำคัญตามมาตรฐานสากลในการสำรองข้อมูล (Data Backup Standard) อย่างน้อยให้ได้ตามกฎ ๓-๒-๑ (๓-๒-๑ Backup Rule) โดยมีหลักการคือ **“ต้องมีข้อมูลอย่างน้อย ๓ ชุด เก็บไว้บน ๒ สื่อที่แตกต่างกัน และอย่างน้อย ๑ ชุดอยู่นอกสถานที่ (off-site)”** และมีการกำหนดมาตรฐานการกู้คืนข้อมูลของระยะเวลาสูงสุดของข้อมูลที่ยอมรับได้ว่าจะสูญหาย เมื่อเกิดเหตุ (RPO : Recovery Point Objective) อย่างน้อย ๒๔ ชั่วโมง และควรทำการทดสอบการ Restore อย่างน้อยปีละ ๑ ครั้ง

/สำหรับระบบ...

เอกสารนี้ลงนามด้วยลายเซ็นอิเล็กทรอนิกส์ ตรวจสอบได้ที่ (https://e-sign.buu.ac.th/verify)

สำหรับระบบสารสนเทศตามข้อ ๔.๓ ที่มีความประสงค์ในการสำรองข้อมูลในพื้นที่จัดเก็บข้อมูลของสำนักคอมพิวเตอร์ จะต้องดำเนินการตามที่สำนักคอมพิวเตอร์กำหนด และอาจมีค่าธรรมเนียมในการดำเนินงานและการบำรุงรักษาตามอัตราที่สำนักคอมพิวเตอร์กำหนดและได้รับความเห็นชอบจากมหาวิทยาลัยบูรพา

ข้อ ๙ สำหรับระบบสารสนเทศของมหาวิทยาลัยบูรพาหรือระบบสารสนเทศของส่วนงาน ที่ใช้อยู่ก่อนประกาศนี้จะมีผลบังคับใช้ ให้ดำเนินการตรวจสอบด้านความปลอดภัยตามข้อ ๕ ของประกาศนี้ให้แล้วเสร็จภายใน ๑ ปี แต่หากในระหว่างที่รอการดำเนินการ สำนักคอมพิวเตอร์มีการตรวจสอบพบหรือได้รับการแจ้งเหตุการโจมตีทางไซเบอร์หรือพบการรั่วไหลของข้อมูลจากระบบสารสนเทศใด สำนักคอมพิวเตอร์จะทำการระงับการใช้งานระบบสารสนเทศนั้นในทันที และแจ้งให้หน่วยงานหรือส่วนงานผู้รับผิดชอบระบบสารสนเทศนั้นดำเนินการแก้ไข โดยจะเปิดให้ใช้งานได้เฉพาะการเข้าถึงจากเครือข่ายภายในมหาวิทยาลัยบูรพาเท่านั้น หรือปิดการเข้าถึงระบบสารสนเทศทั้งภายในและภายนอกแล้วแต่กรณีของระดับความรุนแรงด้านความปลอดภัย จนกว่าการแก้ไขจะแล้วเสร็จและผ่านการรับรองด้านความปลอดภัย

ข้อ ๑๐ ให้ผู้อำนวยการสำนักคอมพิวเตอร์รักษาการตามประกาศนี้

ในกรณีที่มีปัญหาในการตีความหรือมีปัญหาในการปฏิบัติตามประกาศนี้ ให้ผู้อำนวยการสำนักคอมพิวเตอร์ มีอำนาจวินิจฉัยชี้ขาดตามคำแนะนำของคณะกรรมการบริหารสำนักคอมพิวเตอร์ คำวินิจฉัยของผู้อำนวยการสำนักคอมพิวเตอร์ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๔ ธันวาคม พ.ศ. ๒๕๖๘



(ผู้ช่วยศาสตราจารย์จักริน สุขสวัสดิ์ชน)
ผู้อำนวยการสำนักคอมพิวเตอร์ ปฏิบัติการแทน
อธิการบดีมหาวิทยาลัยบูรพา

เอกสารนี้ลงนามด้วยลายเซ็นอิเล็กทรอนิกส์ ตรวจสอบได้ที่ (https://e-sign.buu.ac.th/verify)

เอกสารแนบท้ายหมายเลข ๑

เกณฑ์การประเมินความปลอดภัยและคุณภาพซอร์สโค้ด

เพื่อให้การออกหนังสือรับรองระบบสารสนเทศ (Certificate) เป็นไปตามมาตรฐานและสอดคล้องกับแนวปฏิบัติด้านความปลอดภัยในการพัฒนาระบบสารสนเทศ สำนักคอมพิวเตอร์จึงได้กำหนดรายละเอียดเครื่องมือและเกณฑ์การ "ผ่าน" การตรวจสอบ ดังนี้

๑. เครื่องมือที่ใช้ในการประเมิน (Assessment Tools) สำนักคอมพิวเตอร์ใช้เครื่องมือมาตรฐานสากลในการตรวจสอบความมั่นคงปลอดภัย ดังนี้

๑.๑ Nessus ทำหน้าที่ตรวจสอบและประเมินช่องโหว่ของระบบปฏิบัติการ ระบบเครือข่ายและซอฟต์แวร์ที่เกี่ยวข้อง (Infrastructure & Web Vulnerability) เพื่อระบุความเสี่ยงที่อาจถูกโจมตี (สำหรับทุกระบบตามข้อ ๔ ตามประกาศ)

๑.๒ SonarQube ทำหน้าที่ตรวจสอบและวิเคราะห์คุณภาพของซอร์สโค้ด (Static Application Security Testing: SAST) เพื่อหาจุดบกพร่องทางตรรกะ และช่องโหว่ด้านความปลอดภัยในระดับการเขียนโปรแกรม (สำหรับระบบตามข้อ ๔.๑)

๒. เกณฑ์การประเมินช่องโหว่ ด้วยเครื่องมือ Nessus ระบบสารสนเทศจะต้องได้รับการตรวจสอบและมีผลการตรวจสอบตามเกณฑ์ ดังนี้

- **ระดับวิกฤต (Critical Severity)** ต้องเท่ากับศูนย์ **(ไม่อนุญาตให้มี)**
- **ระดับสูง (High Severity)** และ**ระดับปานกลาง (Medium Severity)** ควรแก้ไขให้หมด แต่หากมีความจำเป็นทางเทคนิค ต้องได้รับการอนุมัติผ่อนผันจากผู้อำนวยการสำนักคอมพิวเตอร์หรือผู้ที่ได้รับมอบอำนาจจากผู้อำนวยการสำนักคอมพิวเตอร์เป็นลายลักษณ์อักษร พร้อมแผนการลดความเสี่ยง (Mitigation Plan)

๓. เกณฑ์คุณภาพซอร์สโค้ดด้วยเครื่องมือ SonarQube ระบบจะต้องผ่านเกณฑ์ Security Rating ต้องมีผลการประเมินไม่ต่ำกว่าระดับ C (A, B หรือ C)

๔. ขั้นตอนการดำเนินการ

๑. ส่งตรวจสอบ ผู้รับผิดชอบส่งระบบให้สำนักคอมพิวเตอร์ตรวจสอบด้านความปลอดภัย (Scan)

๒. รายงานผลการตรวจสอบ สำนักคอมพิวเตอร์ส่งรายงานผล (Report) กลับไปยังผู้รับผิดชอบภายใน ๗ วันทำการ

๓. แก้ไข ผู้รับผิดชอบดำเนินการแก้ไข (Fix) ตามรายงานผลการตรวจสอบ

เอกสารนี้ลงนามด้วยลายเซ็นอิเล็กทรอนิกส์ ตรวจสอบได้ที่ (https://e-sign.buu.ac.th/verify)

๔. ตรวจซ้ำ (Re-scan) แจ้งสำนักคอมพิวเตอร์เพื่อตรวจอีกครั้ง ถ้าผ่านให้ออกใบรับรอง ถ้าผลการตรวจสอบยังปรากฏช่องโหว่ระดับวิกฤติอยู่ สำนักคอมพิวเตอร์จะทำการจัดส่งรายงานกลับไปยังผู้รับผิดชอบเพื่อแก้ไขอีกครั้ง

๕. ออกใบรับรอง สำนักคอมพิวเตอร์จะออกหนังสือรับรอง (Certificate) อายุ ๖ เดือน ให้กับระบบที่ผ่านเกณฑ์การตรวจสอบ

เอกสารนี้ลงนามด้วยลายเซ็นอิเล็กทรอนิกส์ ตรวจสอบได้ที่ (https://e-sign.buu.ac.th/verify)