เวอร์ชันกำกับ: แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
สำหรับระบบสารสนเทศและเว็บไซต์ มหาวิทยาลัยมหิดล
Version 1.0
วันที่ออกเอกสาร วันที่ 2 ธันวาคม 2564

แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำหรับระบบสารสนเทศและเว็บไซต์มหาวิทยาลัยมหิดล

โดยที่เป็นการสมควรกำหนดแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำหรับระบบสารสนเทศและเว็บไซต์มหาวิทยาลัยมหิดล ดังต่อไปนี้

ข้อ ๑. ในประกาศนี้

“ผู้ใช้บริการ” หมายความว่า ผู้ที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์กับมหาวิทยาลัย ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล (Data Subject) เช่น บุคลากร นักศึกษา ผู้รับบริการ และผู้เข้าร่วมการวิจัย

“ผู้ดูแลระบบ” หมายความว่า ผู้ทำหน้าที่บริหารและจัดการระบบคอมพิวเตอร์ในส่วนงาน โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้งและการปรับปรุงซอฟต์แวร์ สร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้

“เจ้าหน้าที่” หมายความว่า ข้าราชการ พนักงานมหาวิทยาลัย และลูกจ้างของมหาวิทยาลัย

“ระบบสารสนเทศ” หมายความว่า ระบบงานหรือโปรแกรมประยุกต์ที่ประกอบด้วย ฮาร์ดแวร์หรือตัวอุปกรณ์และซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่พัฒนาบนระบบเว็บแอปพลิเคชัน (Web Application) ที่ผู้ใช้งานเปิดใช้งานด้วยโปรแกรมเบราว์เซอร์ (Web Browser) หรือโมบาย (Mobile Application) ที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายข้อมูล เพื่อสนับสนุนการปฏิบัติงานของส่วนงานต่างๆ ของมหาวิทยาลัย ตามวัตถุประสงค์ ภารกิจ และอำนาจหน้าที่ตามกฎหมายของมหาวิทยาลัย

“เว็บไซต์”หมายความว่า แหล่งที่เก็บรวบรวมข้อมูลเอกสารและสื่อประสมที่เข้าถึงได้ผ่านอินเทอร์เน็ต เพื่อนำเสนอข้อมูลส่วนงานของมหาวิทยาลัย

ข้อ ๒. แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล เกี่ยวกับเรื่องนี้ ดังต่อไปนี้

๒.๑ ข้อมูลเบื้องต้น

(๑) แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำหรับระบบสารสนเทศและเว็บไซต์ มหาวิทยาลัยมหิดล จัดทำขึ้นเพื่อใช้บังคับตามประกาศมหาวิทยาลัยมหิดลเรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

(๒) กำหนดขอบเขตให้การคุ้มครองข้อมูลส่วนบุคคลนี้ ใช้กับการดำเนินการใดๆ ของมหาวิทยาลัย ต่อข้อมูลส่วนบุคคลที่มหาวิทยาลัย รวบรวม จัดเก็บ หรือตามวัตถุประสงค์เท่านั้น

๒.๒ การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

๒.๒.๑ การเก็บรวบรวมข้อมูลส่วนบุคคลของมหาวิทยาลัยมหิดล

(๑) การบริการทางระบบสารสนเทศ ในแนวปฏิบัติตามประกาศนี้ จะหมายถึง ระบบสารสนเทศสำหรับผู้ใช้ที่เป็นบทบาท (User Role) ผู้ใช้บริการเท่านั้น จะไม่รวมถึง ผู้ใช้ที่เป็นบทบาทเจ้าหน้าที่หรือผู้ดูแลระบบ โดยระบบสารสนเทศจะเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น ทั้งข้อมูลของผู้ใช้บริการ และของผู้ซึ่งได้รับมอบหมายหรือรับมอบอำนาจที่ถูกต้องตามกฎหมาย ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้ดำเนินการตามประกาศด้านความเป็นส่วนตัวของข้อมูลส่วนบุคคล (Privacy Notice) ของมหาวิทยาลัย ซึ่งมหาวิทยาลัยจะนำข้อมูลดังกล่าวไปดำเนินการตามขั้นตอนต่อไป

(๒) การเก็บรวบรวมข้อมูลส่วนบุคคลโดยการกรอกข้อมูลทางกระดาษ แล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์ โดยมหาวิทยาลัยจะเก็บข้อมูลเท่าที่จำเป็นตามข้อ ๒.๒.๑ (๑) โดยมีวิธีการดังนี้ มหาวิทยาลัยจะให้เจ้าหน้าที่ที่เกี่ยวข้องเป็นผู้แปลงข้อมูลส่วนบุคคลของผู้ใช้บริการที่ได้กรอกลงในระบบสารสนเทศของมหาวิทยาลัย ทั้งนี้ มหาวิทยาลัยจะรักษาข้อมูลของการให้บริการดังกล่าวข้างต้นไว้เป็นความลับ เว้นแต่กรณีอื่นๆ ตามที่กำหนดไว้ในประกาศมหาวิทยาลัยมหิดล เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

(๓) กำหนดให้ทำการวิเคราะห์เขตข้อมูล (Field) ของข้อมูลส่วนบุคคลที่จะจัดเก็บด้วยเหตุผลของฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) หรือฐานความยินยอม (Consent Basis) และมีข้อความเตือนในครั้งแรกของการเข้าใช้ระบบสารสนเทศและเว็บไซต์ พร้อมระบุเขตข้อมูลของข้อมูลส่วนบุคคลที่จะจัดเก็บ และวัตถุประสงค์การนำไปใช้ ให้ผู้ใช้บริการทราบ โดยกรณีที่เป็นการจัดเก็บด้วยเหตุผลของฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis) ให้แสดงการรับทราบ ด้วยคำว่า รับทราบ / Accept และกรณีที่เป็นการจัดเก็บด้วยเหตุผลของฐานความยินยอม (Consent Basis) ให้แสดงความยินยอม ด้วยคำว่า ยินยอม / Agree

(๔) ควรจัดให้มีหน้าจอแสดงชื่อเขตข้อมูล (Field) ที่ชัดเจน เพื่อบ่งชี้ถึงข้อมูลส่วนบุคคลที่จะเก็บรวบรวม โดยมีเครื่องหมายระบุเขตข้อมูลให้ชัดเจนสำหรับเขตข้อมูลที่จำเป็นต้องกรอก (Required Field) และเขตข้อมูลที่ไม่จำเป็นต้องกรอก (Optional Field) โดยหากผู้ใช้บริการไม่กรอกข้อมูลที่จำเป็นต้องกรอก ระบบจะไม่จัดเก็บข้อมูลของผู้ใช้บริการ และไม่สามารถดำเนินการต่อไปได้

(๕) จัดให้ระบบมีระยะเวลาสำหรับผู้ใช้บริการตรวจสอบข้อมูลส่วนบุคคลก่อนที่จะทำการยืนยัน เพื่อให้ระบบบันทึกข้อมูลได้ถูกต้อง

๒.๒.๒ การพัฒนาเว็บไซต์

(๑) ผู้ดูแลเว็บไซต์ต้องแจ้งวัตถุประสงค์ของการใช้ข้อมูลที่ได้รับมาบนหน้า นโยบายความเป็นส่วนตัวให้ชัดเจน ตัวอย่างเช่น

- เพื่อเสนอข่าวสาร
- เพื่อให้บริการที่ท่านร้องขอมาเสร็จสมบูรณ์
- เพื่อให้แน่ใจว่าเว็บไซต์นั้นเกี่ยวข้องกับความต้องการของท่าน
- เพื่อช่วยเราในการสร้างหรือเผยแพร่เนื้อหาที่เกี่ยวข้องเหมาะสมกับท่านที่สุด
- เพื่อแจ้งให้ท่านทราบในกรณีที่มีการเปลี่ยนแปลง นโยบายความเป็นส่วนตัว หรือเงื่อนไขการใช้ หากจำเป็น
- เพื่อติดต่อท่านผ่านช่องทางการลงทะเบียน เช่น “ติดต่อเรา” หรือสอบถามข้อมูลอื่นๆ
- เพื่อช่วยให้ท่านใช้งานเว็บไซต์ได้อย่างง่าย
- เพื่อปฏิบัติตามกฎระเบียบข้อบังคับ
- เพื่อใช้ในการบันทึกจัดเก็บภายใน
- เพื่อจัดทำแบบสอบถาม เกี่ยวกับสิ่งที่ท่านสนใจ

(๒) ควรจัดให้มีช่องทางสื่อสารแบบมั่นคงปลอดภัยกับข้อมูลส่วนบุคคล โดยการเข้ารหัสลับข้อมูลเมื่อส่งผ่านข้อมูลบนระบบเครือข่ายสื่อสาร อาทิ การใช้ SSL อนึ่ง ในกรณีที่หน่วยงานยังไม่สามารถดำเนินการเรื่อง SSL ได้ ขอให้มีแผนการดำเนินงานที่ชัดเจนและเร่งรัดกำกับติดตามได้

(๓) ต้องตรวจสอบเว็บไซต์ กรณีส่วนงานมีการดำเนินการในประเด็นดังต่อไปนี้

- การเก็บข้อมูลผู้ใช้บริการ
- มีระบบสมัครสมาชิก
- การรับข่าวสาร (Subscribe) การสมัครรับข้อมูลข่าวสาร (ต้องมีช่องทางให้สามารถ Unsubscribe ได้)
- การติดตั้งระบบวิเคราะห์อื่นๆบนเว็บไซต์ เช่น Google Analytics หรือ Facebook Pixels หรือ Power BI ถ้าจะใช้ต้องแจ้งและให้ผู้ใช้บริการอนุญาตทุกครั้งเมื่อมีการเปิดใช้งาน
- การใช้งานเกี่ยวกับการบอกตำแหน่ง Web Beacons หรือ GPS ถ้าจะใช้ต้องแจ้งและให้ผู้ใช้บริการอนุญาตทุกครั้งเมื่อมีการเปิดใช้งาน

ถ้ามีการดำเนินการดังกล่าว ต้องเขียนระบุแจ้งเตือนให้ผู้ใช้บริการรับทราบด้วยว่า ข้อมูลเก็บอะไรบ้าง ถ้าไม่ได้เก็บข้อมูลที่ระบุถึงตัวตนได้สามารถเขียนแจ้งรวมกับการใช้งานคุกกี้

(๔) กรณีการนำเสนอหน้าเว็บของการประชาสัมพันธ์ ซึ่งมีรูปภาพที่ถ่ายติดใบหน้า ให้มีการแจ้งผู้ที่ถูกถ่ายรูปไว้ก่อน เช่น แจ้งในงาน หรือแจ้งตอนลงทะเบียน

๒.๒.๓ การใช้งานคุกกี้ (Cookies)

(๑) กรณีส่วนงานมีการใช้งาน “คุกกี้” (Cookies) เพื่อช่วยอำนวยความสะดวกให้แก่ผู้ใช้บริการในการเข้าถึงเว็บไซต์และบริการธุรกรรมทางอิเล็กทรอนิกส์ของมหาวิทยาลัย โดย “คุกกี้” เป็นไฟล์ข้อมูลขนาดเล็กซึ่งจะถูกส่งไปยังโปรแกรมเบราว์เซอร์ (Web Browser) ของผู้ใช้บริการ และอาจมีการบันทึกลงในเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ผู้ใช้บริการใช้เข้าถึงเว็บไซต์และบริการธุรกรรมทางอิเล็กทรอนิกส์ของมหาวิทยาลัย โดยคุกกี้มีประโยชน์สำคัญในการทำให้เว็บไซต์สามารถจดจำการตั้งค่าต่างๆ บนอุปกรณ์ของผู้ใช้บริการได้ ทำให้การเข้าใช้บริการมีความสะดวกและเป็นไปอย่างปกติ

ทั้งนี้ ส่วนงานจะต้องมีลิงก์เกี่ยวกับการใช้งานคุกกี้ (Cookies) เพื่อให้ผู้ใช้บริการเข้าไปกดอ่านได้ ซึ่งผู้ใช้บริการสามารถเลือกปฏิเสธและปิดการใช้งานคุกกี้บนโปรแกรมเบราว์เซอร์ (Web Browser) หรืออุปกรณ์ของผู้ใช้บริการได้ โดยผู้ใช้บริการยังคงสามารถเข้าเยี่ยมชมเว็บไซต์และบริการธุรกรรมทางอิเล็กทรอนิกส์ของมหาวิทยาลัยได้ แต่อาจพบบางส่วนของเว็บไซต์ไม่สามารถทำงานหรือให้บริการธุรกรรมทางอิเล็กทรอนิกส์ได้อย่างปกติ

(๒) กรณีผู้ดูแลระบบพัฒนาโปรแกรม“คุกกี้” ควรเก็บข้อมูลส่วนบุคคลที่จำเป็นต้องใช้เท่านั้น และไม่ควรเก็บรหัสผ่านและข้อมูลเลข CVV บัตรเครดิตไว้ในคุกกี้ โดยผู้ดูแลระบบต้องมีระบบการป้องกันความมั่นคงปลอดภัยของการเก็บข้อมูลส่วนบุคคลดังกล่าว ทั้งนี้กองเทคโนโลยีสารสนเทศอาจทำการ Audit ระบบพัฒนาโปรแกรม“คุกกี้”เป็นครั้งคราว หรือขอให้ส่วนงานส่งข้อมูลเพิ่มเติมในบางเงื่อนไข รวมถึงขอให้ปรับแก้ไขได้กรณีตรวจพบว่ามีความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลหรือความมั่นคงปลอดภัยของการเก็บข้อมูลส่วนบุคคล

๒.๒.๔ การเก็บข้อมูลสถิติเกี่ยวกับผู้ใช้บริการ (User Information)

มหาวิทยาลัยมีระบบสารสนเทศในการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยข้อมูลสามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ หากเป็นกรณีสถิติของรายบุคคล เพื่อประโยชน์ตามวัตถุประสงค์ ภารกิจ และอำนาจหน้าที่ตามกฎหมายของมหาวิทยาลัย

๒.๒.๕ สิทธิในการให้ข้อมูลของผู้ใช้บริการ

มหาวิทยาลัยมีการระบุข้อมูลที่มีการจัดเก็บข้อมูลผ่านทางระบบสารสนเทศของมหาวิทยาลัย โดยมีข้อมูลบางประเภทที่ผู้ใช้บริการมีสิทธิเลือกที่จะ “ให้” หรือ “ไม่ให้” ก็ได้ โดยข้อมูลที่จำเป็นต่อการประมวลผลและการดำเนินการของการใช้ระบบสารสนเทศของมหาวิทยาลัย จะมีการทำสัญลักษณ์ไว้ เช่น ระบุด้วยตัวอักษรสีแดง หรือจะมีเครื่องหมาย (*) เช่น ชื่อ-นามสกุล หมายเลขโทรศัพท์ เป็นต้น ทั้งนี้ ผู้ใช้บริการสามารถเลือกที่จะให้หรือไม่ให้ข้อมูลอื่นที่ไม่มีการทำสัญลักษณ์ดังกล่าว เช่น ชื่อกลาง เป็นต้น

๒.๓ การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

มหาวิทยาลัยอาจมีระบบสารสนเทศที่มีการเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ของผู้ใช้บริการ โดยที่ข้อมูลส่วนบุคคลของผู้ใช้บริการจะได้รับการเก็บรักษาเป็นความลับทั้งในรูปเอกสารและข้อมูลอิเล็กทรอนิกส์ รวมทั้งในระหว่างการส่งผ่านข้อมูลทุกขั้นตอน ทั้งนี้ จะอนุญาตให้เฉพาะเจ้าหน้าที่ของหน่วยงานหรือองค์กรที่เกี่ยวข้องหรือผู้มีสิทธิ ซึ่งได้ทำข้อตกลงหรือสัญญาที่เกี่ยวข้องข้างต้นในรูปแบบที่เหมาะสมกับมหาวิทยาลัย เช่น สัญญาว่าจะไม่เปิดเผยข้อมูลส่วนบุคคล (Non-disclosure Agreement : NDA) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA) ข้อตกลงเปิดเผยข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) จึงจะสามารถเข้าถึงข้อมูลของผู้ใช้บริการได้ ทั้งนี้ มหาวิทยาลัยกำหนดให้เจ้าหน้าที่ดังกล่าวต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่ประกาศไว้

๒.๔ การรวมข้อมูลจากที่มาหลายแห่ง

มหาวิทยาลัยอาจนำข้อมูลส่วนบุคคลที่ผู้ใช้บริการให้ข้อมูลดังกล่าวผ่านทางระบบสารสนเทศหรือบริการธุรกรรมทางอิเล็กทรอนิกส์ของมหาวิทยาลัย รวมเข้ากับข้อมูลที่ได้มาจากแห่งอื่น เพื่อทำให้ข้อมูลของมหาวิทยาลัยมีความครบถ้วนและถูกต้องเป็นปัจจุบัน และเพื่อประโยชน์ตามอำนาจและภารกิจของมหาวิทยาลัย

๒.๕ การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

มหาวิทยาลัยจะไม่ให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บ รวบรวมไว้ เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นกรณีที่เป็นการเปิดเผยข้อมูลตามที่กฎหมายกำหนดให้กระทำได้ หรือตามคำสั่งศาล หรือเจ้าหน้าที่ของรัฐที่มีอำนาจตามกฎหมาย ในกรณีที่มีการจ้างหน่วยงานอื่น (Outsource) ที่ดำเนินการเกี่ยวกับข้อมูลของผู้ใช้บริการ มหาวิทยาลัยจะกำหนดให้ผู้รับจ้างเก็บรักษาความลับและความปลอดภัยของข้อมูล โดยห้ามผู้รับจ้างนำข้อมูลดังกล่าวไปใช้นอกเหนือจากภารกิจ หรือกิจกรรมที่มอบหมายให้ดำเนินการ

กรณีที่มหาวิทยาลัยมีความจำเป็นต้องดำเนินการส่ง หรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เว้นแต่จะได้รับความยินยอมจากผู้ใช้บริการ หรือมีกฎหมาย กำหนดให้กระทำการส่ง หรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

๒.๖ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

มหาวิทยาลัยจะไม่นำข้อมูลส่วนบุคคลที่เก็บรวบรวม จัดเก็บ ใช้ และเปิดเผยไปดำเนินการอื่นนอกเหนือไปจากวัตถุประสงค์ที่ได้ระบุไว้ ตามภารกิจและหน้าที่ตามกฎหมายของมหาวิทยาลัย

๒.๗ บันทึกผู้เข้าชมเว็บ (Log Files)

ระบบสารสนเทศของมหาวิทยาลัยจัดให้มีการจัดเก็บข้อมูลบันทึกกิจกรรมการใช้งาน หรือการเก็บบันทึกการเข้าออกและระหว่างการเข้าใช้บริการระบบสารสนเทศของผู้ใช้บริการโดยอัตโนมัติ ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคล เช่น หมายเลขไอพี (IP Address) ประเภทของเว็บเบราว์เซอร์ (Web Browser) ที่เข้าใช้งานระบบสารสนเทศ (Browser Type) ซึ่งเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ที่กำหนดให้เก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบสารสนเทศ

๒.๘ การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

ในกระบวนการการให้บริการระบบสารสนเทศที่ผู้ใช้บริการให้ข้อมูลส่วนบุคคล มหาวิทยาลัยอนุญาตให้ผู้ใช้บริการสามารถแก้ไขข้อมูลให้ถูกต้องและปรับปรุงให้เป็นปัจจุบันได้ ภายในกระบวนการที่กำหนดอาทิ หากการขอรับบริการดังกล่าว ยังไม่ได้รับการพิจารณาหรือการอนุมัติได้ ณ ที่ทำการของหน่วยงานภายในมหาวิทยาลัย หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ให้บริการในกิจการหรือกิจกรรมในระบบสารสนเทศ ทั้งนี้ หากเป็นกรณีที่คำขอรับบริการได้รับการพิจารณาหรือการอนุมัติแล้ว ผู้ใช้บริการไม่สามารถแก้ไข ปรับปรุงข้อมูลส่วนบุคคลได้

๒.๙ การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

เพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม และป้องกันการเปลี่ยนแปลงข้อมูลดังกล่าวโดยมิชอบ มหาวิทยาลัยมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้บริการอย่างเหมาะสม โดยสอดคล้องตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

นอกจากนี้ มหาวิทยาลัยหรือส่วนงานควรมีระบบตรวจจับและป้องกันการโจมตีของเว็บแอปพลิเคชัน (Web Application Firewall) รวมถึงการออกแบบและพัฒนาระบบความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้สามารถป้องกันการโจมตีจากผู้ไม่ประสงค์ดี ตามรายการช่องโหว่ ๑๐ อันดับสำหรับระบบสารสนเทศบนเว็บที่เรียกว่า OWASP (Open Web Application Security Project) Top ๑๐ Vulnerabilities เป็นอย่างน้อย และกรณีที่ส่วนงานมีระบบสารสนเทศเกี่ยวกับบริการการชำระเงินผ่านบัตรเครดิต ควรอ้างอิงมาตรฐาน Payment Card Industry Data Security Standard (PCI DSS) ซึ่งเป็นมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีการจัดการเกี่ยวกับข้อมูลบัตรเครดิต ในการเก็บรักษา ประมวลผล และรับส่งข้อมูลบัตรได้อย่างมั่นคงปลอดภัย ให้สามารถป้องกันการฉ้อโกงซึ่งเกิดจากการทำธุรกรรมผ่านบัตรชำระเงิน