(ฉบับร่าง) เสนอเข้าที่ประชุม
คณะทำงานตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล สถาบันฯ

**มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล**

**งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้**

สถาบันนวัตกรรมการเรียนรู้ มหาวิทยาลัยมหิดล ได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อให้การเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล เป็นไปด้วยความปลอดภัยเหมาะสม และสอดคล้องตามบทบัญญัติแห่งกฎหมายที่เกี่ยวข้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ดังนั้น งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้ จึงได้กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพ ดังนี้

**1. การเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล ประกอบด้วยมาตรฐานการดำเนินงาน ดังนี้**

1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
2) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
4) การกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ การลักลอบทำสำเนาข้อมูลส่วนบุคคล หรือการลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
5) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล

**2. การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล**

งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่ครอบคลุมการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามมาตรฐานของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 และมาตรการป้องกันที่ได้กำหนดขึ้น เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัย อันรวมถึงแต่ไม่จำกัดเพียงมาตรฐานที่เกี่ยวข้องตามรายละเอียดดังต่อไปนี้

| ลำดับของมาตรการรักษาความมั่นคงปลอดภัย | มาตรการรักษาความมั่นคงปลอดภัย |
|---|---|
| 1. ข้อมูลใน NAS (Network Attached Storage) | • มีการกำหนดสิทธิ์ในการเข้าถึงแฟ้มข้อมูล โดยแยกสิทธิ์ตามกลุ่มงานและส่วนบุคคล<br>• มีการสำรองข้อมูลที่จำเป็นเก็บไว้ที่ DR-Site |
| 2. ข้อมูลในเครื่องคอมพิวเตอร์ | • มีการตั้งค่ารหัสผ่านสำหรับเข้าใช้งานคอมพิวเตอร์ส่วนบุคคล<br>• มีการกำหนดการใช้งาน Internet ให้ใช้งานภายใต้ proxy ของมหาวิทยาลัย<br>• สามารถสำรองข้อมูลไปยัง NAS ของสถาบันฯได้ |
| 3. การส่งต่อข้อมูลในกลุ่มงาน | • มีการตั้งค่ารหัสผ่านการเปิดไฟล์ โดยจัดทำคู่มือการตั้งค่ารหัสให้กับไฟล์ข้อมูลเอกสารให้บุคลากรได้นำไปปฏิบัติตาม |

**3. แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำหรับระบบสารสนเทศและเว็บไซต์ สถาบันนวัตกรรมการเรียนรู้ มหาวิทยาลัยมหิดล**

งานเทคโนโลยีสารสนเทศ สถาบันนวัตกรรมการเรียนรู้ ได้กำหนดแนวทางในการคุ้มครองข้อมูล ส่วนบุคคลที่เกี่ยวข้องกับระบบสารสนเทศและเว็บไซต์ของสถาบันฯ เพื่อให้เป็นไปตามแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำหรับระบบสารสนเทศและเว็บไซต์ มหาวิทยาลัยมหิดล ลงวันที่ 2 ธันวาคม พ.ศ.2564 ดังนี้

**3.1 นิยามคำจำกัดความ**

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

“**ผู้ดูแลระบบ**” หมายความว่า ผู้ทำหน้าที่บริหารและจัดการระบบคอมพิวเตอร์ในสถาบันฯ โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้งและการปรับปรุงซอฟต์แวร์ สร้างออกแบบและบำรุงรักษาบัญชีผู้ใช้

“**ระบบสารสนเทศ**” หมายความว่า ระบบงานหรือโปรแกรมประยุกต์ที่ประกอบด้วย ฮาร์ดแวร์หรือตัวอุปกรณ์ และซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่พัฒนาบนระบบเว็บแอปพลิเคชัน (Web Application) ที่ผู้ใช้งานเปิดใช้งานด้วยโปรแกรมเบราว์เซอร์ (Web Browser) ที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายข้อมูล เพื่อสนับสนุนการปฏิบัติงานของสถาบันนวัตกรรมการเรียนรู้ ตามวัตถุประสงค์ ภารกิจ และอำนาจหน้าที่ตามกฎหมายของมหาวิทยาลัย

“**เว็บไซต์**” หมายความว่า แหล่งที่เก็บรวบรวมข้อมูลเอกสารและสื่อประสมที่เข้าถึงได้ผ่านอินเทอร์เน็ต เพื่อนำเสนอข้อมูลส่วนงานของมหาวิทยาลัย

**3.2 แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล เกี่ยวกับเรื่องนี้ ดังต่อไปนี้**

**1. ข้อมูลเบื้องต้น**

1.1 แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำหรับระบบสารสนเทศและเว็บไซต์สถาบันนวัตกรรมการเรียนรู้ จัดทำขึ้นเพื่อใช้บังคับตามประกาศมหาวิทยาลัยมหิดลเรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563

1.2 กำหนดขอบเขตให้การคุ้มครองข้อมูลส่วนบุคคลนี้ ใช้กับการดำเนินการใด ๆ ของสถาบันฯ ต่อข้อมูลส่วนบุคคลที่สถาบันฯ รวบรวม จัดเก็บ หรือตามวัตถุประสงค์เท่านั้น

**2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล**

2.1 การเก็บรวบรวมข้อมูลส่วนบุคคลของสถาบันนวัตกรรมการเรียนรู้

1. ระบบสารสนเทศจะเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น ทั้งข้อมูลของผู้ใช้บริการ และของผู้ซึ่งได้รับมอบหมายหรือรับมอบอำนาจที่ถูกต้องตามกฎหมาย ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้ดำเนินการตามประกาศด้านความเป็นส่วนตัวของข้อมูลส่วนบุคคล (Privacy Notice) ของสถาบันนฯ ซึ่งสถาบันนฯจะนำข้อมูลดังกล่าวไปดำเนินการตามขั้นตอนต่อไป

2. การเก็บรวบรวมข้อมูลส่วนบุคคลโดยการกรอกข้อมูลทางกระดาษ แล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์ โดยสถาบันนวัตกรรมการเรียนรู้ จะเก็บข้อมูลเท่าที่จำเป็น โดยมีวิธีการดังนี้ สถาบันนวัตกรรมการเรียนรู้ จะให้เจ้าหน้าที่ที่เกี่ยวข้องเป็นผู้แปลงข้อมูลส่วนบุคคลของผู้ใช้บริการที่ได้กรอกลงในระบบสารสนเทศของสถาบันฯ ทั้งนี้ สถาบันฯ จะรักษาข้อมูลของการให้บริการดังกล่าวข้างต้นไว้เป็นความลับ เว้นแต่กรณีอื่น ๆ ตามที่กาหนดไว้ในประกาศมหาวิทยาลัยมหิดล เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2563

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

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

5. จัดให้ระบบมีระยะเวลาสำหรับผู้ใช้บริการตรวจสอบข้อมูลส่วนบุคคลก่อนที่จะทำการยืนยัน เพื่อให้ระบบบันทึกข้อมูลได้ถูกต้อง

2.2 การพัฒนาเว็บไซต์

1. ผู้ดูแลเว็บไซต์ต้องแจ้งวัตถุประสงค์ของการใช้ข้อมูลที่ได้รับมาบนหน้า นโยบายความเป็นส่วนตัวให้ชัดเจนตัวอย่าง เช่น

- เพื่อเสนอข่าวสาร
- เพื่อให้บริการที่ท่านร้องขอมาเสร็จสมบูรณ์
- เพื่อให้แน่ใจว่าเว็บไซต์นั้นเกี่ยวข้องกับความต้องการของท่าน
- เพื่อช่วยเราในการสร้างหรือเผยแพร่เนื้อหาที่เกี่ยวข้องเหมาะสมกับท่านที่สุด
- เพื่อแจ้งให้ท่านทราบในกรณีที่มีการเปลี่ยนแปลง นโยบายความเป็นส่วนตัว หรือเงื่อนไขการใช้หากจำเป็น
- เพื่อติดต่อท่านผ่านช่องทางการลงทะเบียน เช่น “ติดต่อเรา” หรือสอบถามข้อมูลอื่น ๆ
- เพื่อช่วยให้ท่านใช้งานเว็บไซต์ได้อย่างง่าย
- เพื่อปฏิบัติตามกฎระเบียบข้อบังคับ
- เพื่อใช้ในการบันทึกจัดเก็บภายใน
- เพื่อจัดทำแบบสอบถาม เกี่ยวกับสิ่งที่ท่านสนใจ

2. ควรจัดให้มีช่องทางสื่อสารแบบมั่นคงปลอดภัยกับข้อมูลส่วนบุคคล โดยการเข้ารหัสลับข้อมูล เมื่อส่งผ่านข้อมูลบนระบบเครือข่ายสื่อสาร อาทิ การใช้ SSL อนึ่ง ในกรณีที่หน่วยงานยังไม่สามารถดำเนินการเรื่อง SSL ได้ ขอให้มีแผนการดำเนินงานที่ชัดเจนและเร่งรัดกำกับติดตามได้

3. มีการตรวจสอบเว็บไซต์ เนื่องจากสถาบันฯมีการดำเนินการในประเด็นดังต่อไปนี้

- การเก็บข้อมูลผู้ใช้บริการ
- มีระบบสมัครสมาชิก
- มีการระบุแจ้งเตือนให้ผู้ใช้บริการรับทราบด้วยว่า ข้อมูลเก็บอะไรบ้าง ถ้าไม่ได้เก็บข้อมูลที่ระบุถึงตัวตนได้สามารถเขียนแจ้งรวมกับการใช้งานคุกกี้

4. กรณีการนำเสนอหน้าเว็บของการประชาสัมพันธ์ ซึ่งมีรูปภาพที่ถ่ายติดใบหน้าสถาบันฯ มีการแจ้งผู้ที่ถูกถ่ายรูปไว้ก่อน เช่น แจ้งติดป้ายประกาศในงาน หรือแจ้งตอนลงทะเบียน

2.3 การใช้งานคุกกี้ (Cookies)

1. งานเทคโนโลยีสารสนเทศ สถาบันฯ มีการใช้งาน “คุกกี้” (Cookies) เพื่อช่วยอำนวยความสะดวกให้แก่ผู้ใช้บริการในการเข้าถึงเว็บไซต์และบริการธุรกรรมทางอิเล็กทรอนิกส์ของมหาวิทยาลัย โดย “คุกกี้” เป็นไฟล์ข้อมูลขนาดเล็กซึ่งจะถูกส่งไปยังโปรแกรมเบราว์เซอร์ (Web Browser) ของผู้ใช้บริการ และอาจมีการบันทึกลงในเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ผู้ใช้บริการใช้เข้าถึงเว็บไซต์และบริการธุรกรรมทางอิเล็กทรอนิกส์ของมหาวิทยาลัย โดยคุกกี้มีประโยชน์สำคัญในการทำให้เว็บไซต์สามารถจดจำการตั้งค่าต่าง ๆ บนอุปกรณ์ของผู้ใช้บริการได้ ทำให้การเข้าใช้บริการมีความสะดวกและเป็นไปอย่างปกติ

2. กรณีผู้ดูแลระบบพัฒนาโปรแกรม“คุกกี้” ควรเก็บข้อมูลส่วนบุคคลที่จำเป็นต้องใช้เท่านั้น และไม่ควรเก็บรหัสผ่านและข้อมูลเลข CVV บัตรเครดิตไว้ในคุกกี้ โดยผู้ดูแลระบบต้องมีระบบการป้องกันความมั่นคงปลอดภัยของการเก็บข้อมูลส่วนบุคคลดังกล่าว ทั้งนี้กองเทคโนโลยีสารสนเทศอาจทำการ Audit ระบบพัฒนาโปรแกรม“คุกกี้”เป็นครั้งคราว หรือขอให้ส่วนงานส่งข้อมูลเพิ่มเติมในบางเงื่อนไข รวมถึงขอให้ปรับแก้ไขได้ กรณีตรวจพบว่ามีความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลหรือความมั่นคงปลอดภัยของการเก็บข้อมูลส่วนบุคคล

2.4 การเก็บข้อมูลสถิติเกี่ยวกับผู้ใช้บริการ (User Information)

งานเทคโนโลยีสารสนเทศ สถาบันฯ มีระบบสารสนเทศในการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยข้อมูลสามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ หากเป็นกรณีสถิติของรายบุคคล เพื่อประโยชน์ตามวัตถุประสงค์ ภารกิจ และอำนาจหน้าที่ตามกฎหมายของมหาวิทยาลัย

2.5 สิทธิในการให้ข้อมูลของผู้ใช้บริการ

งานเทคโนโลยีสารสนเทศ สถาบันฯ มีการระบุข้อมูลที่มีการจัดเก็บข้อมูลผ่านทางระบบสารสนเทศของสถาบันฯ โดยมีข้อมูลบางประเภทที่ผู้ใช้บริการมีสิทธิเลือกที่จะ “ให้” หรือ “ไม่ให้” ก็ได้ โดยข้อมูลที่จำเป็นต่อการประมวลผลและการดำเนินการของการใช้ระบบสารสนเทศของสถาบันฯ จะมีการทำสัญลักษณ์ไว้ เช่น ระบุด้วยตัวอักษรสีแดง หรือจะมีเครื่องหมาย (*) เช่น ชื่อ-นามสกุล หมายเลขโทรศัพท์ เป็นต้น ทั้งนี้ผู้ใช้บริการสามารถเลือกที่จะให้หรือไม่ให้ข้อมูลอื่นที่ไม่มีการทำสัญลักษณ์ดังกล่าว เช่น ชื่อกลาง เป็นต้น

2.6 การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

งานเทคโนโลยีสารสนเทศ สถาบันฯ จะไม่นำข้อมูลส่วนบุคคลที่เก็บรวบรวม จัดเก็บ ใช้ และเปิดเผยไปดำเนินการอื่น นอกเหนือไปจากวัตถุประสงค์ที่ได้ระบุไว้ ตามภารกิจและหน้าที่ตามกฎหมายของมหาวิทยาลัยมหิดล

2.7 บันทึกผู้เข้าชมเว็บ (Log Files)

งานเทคโนโลยีสารสนเทศ สถาบันฯ จัดให้มีการจัดเก็บข้อมูลบันทึกกิจกรรมการใช้งาน หรือการเก็บบันทึกการเข้าออกและระหว่างการเข้าใช้บริการระบบสารสนเทศของผู้ใช้บริการโดยอัตโนมัติ ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคล เช่น หมายเลขไอพี (IP Address) ประเภทของเว็บเบราว์เซอร์ (Web Browser) ที่เข้าใช้งานระบบสารสนเทศ (Browser Type) ซึ่งเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำ

ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 ที่กำหนดให้เก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบสารสนเทศ

2.8 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

เพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสม และป้องกันการเปลี่ยนแปลงข้อมูลดังกล่าวโดยมิชอบ งานเทคโนโลยีสารสนเทศ สถาบันฯ มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้บริการอย่างเหมาะสม โดยสอดคล้องตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย