ประกาศมหาวิทยาลัยเทคโนโลยีสุรนารี
เรื่อง แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล
มหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. ๒๕๖๕

.....

โดยที่เป็นการสมควรกำหนดแนวปฏิบัติสำหรับการดำเนินการของหน่วยงานภายในมหาวิทยาลัยเทคโนโลยีสุรนารีที่ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งได้กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในมาตรา ๒๑ และมาตรา ๒๔ แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. ๒๕๓๓ ประกอบกับประกาศสำนักนายกรัฐมนตรี เรื่อง แต่งตั้งอธิการบดีมหาวิทยาลัยเทคโนโลยีสุรนารี ลงวันที่ ๑๔ กันยายน ๒๕๖๔ และมติคณะกรรมการดำเนินงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยเทคโนโลยีสุรนารี ในการประชุมครั้งที่ ๒/๒๕๖๕ เมื่อวันที่ ๒ พฤษภาคม ๒๕๖๕ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศมหาวิทยาลัยเทคโนโลยีสุรนารี เรื่อง แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล มหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. ๒๕๖๕"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๕ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

"มหาวิทยาลัย" หมายความว่า มหาวิทยาลัยเทคโนโลยีสุรนารี

"อธิการบดี" หมายความว่า อธิการบดีมหาวิทยาลัยเทคโนโลยีสุรนารี

"ศูนย์คอมพิวเตอร์" หมายความว่า ศูนย์คอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"การประมวลผลข้อมูลส่วนบุคคล" หมายความว่า การดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือแก้ไขข้อมูลส่วนบุคคล และให้หมายความรวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลด้วย

“เจ้าของข้อมูลส่วนบุคคล”	หมายความว่า ผู้ใช้บริการที่ให้ข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลในรูปแบบต่าง ๆ เช่น เอกสาร แบบฟอร์มการขอรับบริการ ไฟล์อิเล็กทรอนิกส์ การกรอกข้อมูลส่วนบุคคลผ่านระบบออนไลน์ ผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีสุรนารี หรือโรงพยาบาลมหาวิทยาลัยเทคโนโลยีสุรนารี เป็นต้น
“หน่วยงาน”	หมายความว่า บุคคลหรือหน่วยงานของมหาวิทยาลัยเทคโนโลยีสุรนารี ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งดำเนินการภายใต้ภารกิจของมหาวิทยาลัยเทคโนโลยีสุรนารี
“ตัวแทนของมหาวิทยาลัย”	หมายความว่า บุคคลหรือหน่วยงานของมหาวิทยาลัยเทคโนโลยีสุรนารี ซึ่งทำหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) มีหน้าที่ในการดูแลรักษาข้อมูลส่วนบุคคลของมหาวิทยาลัย รวมถึงการจัดการและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งดำเนินการภายใต้ภารกิจของมหาวิทยาลัยเทคโนโลยีสุรนารี ให้สอดคล้องตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
“สำนักงาน”	หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๔ แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ "จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด"

หน่วยงานต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล อย่างน้อยดังต่อไปนี้

๔.๑ มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

๔.๑.๑ ให้มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น กำหนดให้มีบันทึกการเข้าออกพื้นที่ กำหนดให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิผ่านเข้าออก มีการกำหนดรายชื่อผู้มีสิทธิเข้าถึง ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๔.๑.๒ ให้มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) แบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบ

๔.๒ มาตรการป้องกันด้านเทคนิค (technical safeguard)

๔.๒.๑ จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

๔.๒.๒ จัดให้มีอุปกรณ์ป้องกันการบุกรุกจากภายนอกและภายในมหาวิทยาลัย สามารถตรวจจับ ยับยั้ง และป้องกันผู้บุกรุกจากภายนอกและภายในมหาวิทยาลัย

๔.๒.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน เช่น การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

๔.๒.๔ จัดให้มีระบบสำรองและกู้คืนข้อมูลอย่างเหมาะสม เพื่อให้ระบบและหรือบริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

๔.๒.๕ มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

๔.๓ มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น

- มีบันทึกการเข้าออกพื้นที่

- มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่
- มีระบบกล้องวงจรปิดติดตั้ง
- มีการล้อมรั้วและล็อคประตูทุกครั้ง
- มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก

ทั้งนี้ ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

๔.๔ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

ข้อ ๕ แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา ๓๗ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ "ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ"

หน่วยงานต้องจัดให้มีมาตรการดำเนินการอย่างน้อยดังต่อไปนี้

๕.๑ การประเมินก่อนส่งมอบข้อมูล

๕.๑.๑ ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และหรือ นิติบุคคลรายอื่นนั้น ใช้เพื่อร้องขอข้อมูลส่วนบุคคล

๕.๑.๒ ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด (เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่ หรือเพียงปี พ.ศ. เกิด และรหัสไปรษณีย์ก็เพียงพอ) และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคล (เช่น ชื่อ-นามสกุล เลขประจำตัว ๑๓ หลัก) หรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงต่อการนำไปใช้ประโยชน์หรือไม่

๕.๒ เมื่อส่งมอบข้อมูล

๕.๒.๑ จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

๕.๒.๒ ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

๕.๒.๓ แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

๕.๓ หลังส่งมอบข้อมูล

๕.๓.๑ ติดตามการใช้งานเป็นครั้งคราว เช่น ทุก ๓ เดือน ๖ เดือน หรือ ๑ ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือ นิติบุคคลนั้น ลบทำลายข้อมูล

๕.๓.๒ กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา

ข้อ ๖ แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา ๓๗ (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ "จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม"

หน่วยงานต้องจัดให้มีมาตรการดำเนินการอย่างน้อยดังต่อไปนี้

๖.๑ ติดตามสม่ำเสมอ (เช่น ทุกสัปดาห์ หรือ ทุกเดือน) ว่าข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตนนั้น (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) มีรายการหรือมีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษาหรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) หรือ ตามที่ขอความยินยอมไว้) ทั้งนี้เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

๖.๑.๑ กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล (หรือขอถอนความยินยอม) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามแต่กรณี

๖.๑.๒ การลบทำลายข้อมูล หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพหรือระบบและการให้บริการด้านสังคมสงเคราะห์

(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์หรือเครื่องมือแพทย์

ทั้งนี้ ต้องจัดให้มีมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

ข้อ ๗ แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ "แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด"

หน่วยงานต้องจัดให้มีมาตรการดำเนินการอย่างน้อยดังต่อไปนี้

๗.๑ กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ตัวแทนของมหาวิทยาลัยให้ชัดเจน เช่น การส่งอีเมล และ แจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

๗.๒ กำหนดวิธีปฏิบัติให้ตัวแทนของมหาวิทยาลัยต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน ๗๒ ชั่วโมง (นับแต่ทราบเหตุ)

๗.๓ การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น

๗.๓.๑ ตัวอย่างกรณีความเสี่ยงต่ำ : ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

๗.๓.๒ ตัวอย่างกรณีความเสี่ยงสูง : เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์ (ตรวจพบ ๑ เดือนหลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน ๗๒ ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

๗.๓.๓ ตัวอย่างกรณีความเสี่ยงต่ำ: เจ้าหน้าที่ของหน่วยงานส่งอีเมลล์ไปยังผู้รับผิดพลาด ซึ่งแนบไฟล์รายชื่อผู้เข้าอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่อีเมลล์ และข้อจำกัดในการทานอาหาร ซึ่งมีเพียง ๒ คน ใน ๑๕ คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลล์ถูกส่งไปยังผู้เข้าอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตามแม้ข้อมูลสุขภาพจะถูกเผยแพร่ไปยังผู้ไม่เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำ ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

ข้อ ๘ แนวปฏิบัติเพื่อให้การดำเนินการสอดคล้องกับมาตรา ๓๗ (๕) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ “ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล” ยังไม่มีความจำเป็นที่มหาวิทยาลัยต้องดำเนินการใด ๆ ตามหน้าที่ในข้อนี้

ข้อ ๙ การไม่ปฏิบัติประกาศมหาวิทยาลัยเทคโนโลยีสุรนารี เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ อาจมีผลเป็นความผิดและถูกลงโทษทางวินัยตามกฎเกณฑ์ของมหาวิทยาลัย (สำหรับเจ้าหน้าที่หรือผู้ปฏิบัติงานของมหาวิทยาลัย) หรือตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล) ทั้งนี้ ตามแต่กรณีและความสัมพันธ์ที่ท่านมีต่อ มหาวิทยาลัยและอาจได้รับโทษตามที่กำหนดโดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งกฎหมายลำดับรอง กฎ ระเบียบ คำสั่งที่เกี่ยวข้อง

จึงประกาศมาเพื่อทราบและถือปฏิบัติอย่างเคร่งครัด

ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๕

(รองศาสตราจารย์ ดร.อนันต์ ทองระอา)
อธิการบดีมหาวิทยาลัยเทคโนโลยีสุรนารี