ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมหาวิทยาลัยอุบลราชธานี
เรื่อง แนวปฏิบัติการรายงานเหตุละเมิดข้อมูลส่วนบุคคลภายในมหาวิทยาลัยอุบลราชธานี
พ.ศ. ๒๕๖๗

โดยที่เป็นการสมควรกำหนดแนวปฏิบัติการรายงานเหตุละเมิดข้อมูลส่วนบุคคลภายในมหาวิทยาลัยอุบลราชธานี

อาศัยอำนาจตามความในข้อ ๖ ของประกาศมหาวิทยาลัยอุบลราชธานี เรื่อง การคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยอุบลราชธานี พ.ศ. ๒๕๖๕ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมหาวิทยาลัยอุบลราชธานี ในการประชุมครั้งที่ ๑/๒๕๖๗ เมื่อวันพฤหัสบดีที่ ๕ กันยายน พ.ศ. ๒๕๖๗ จึงกำหนดแนวปฏิบัติการรายงานเหตุละเมิดข้อมูลส่วนบุคคลภายในมหาวิทยาลัยอุบลราชธานี ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมหาวิทยาลัยอุบลราชธานี เรื่อง แนวปฏิบัติการรายงานเหตุละเมิดข้อมูลส่วนบุคคลภายในมหาวิทยาลัยอุบลราชธานี พ.ศ. ๒๕๖๗

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"การละเมิดข้อมูลส่วนบุคคล" หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ข้อผิดพลาดบกพร่องหรืออุบัติเหตุหรือเหตุอื่นใด

"หัวหน้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" หมายความว่า หัวหน้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำมหาวิทยาลัยอุบลราชธานี

ข้อ ๔ ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน มีหน้าที่ต้องแจ้งแก่มหาวิทยาลัยเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล โดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่ง หรือหลายประเภท ดังต่อไปนี้

(๑) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๒) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๓) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ข้อ ๕ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำหน่วยงานภายใน ได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด ไม่ว่าโดยทางวาจา เป็นหนังสือ หรือวิธีการอื่นทางอิเล็กทรอนิกส์ หรือผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำหน่วยงานภายในทราบเอง ว่ามีหรือน่าจะมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน ต้องดำเนินการ ดังต่อไปนี้

(๑) ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลหรือไม่ โดยผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน พึงดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายในสามารถยืนยันได้ว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน ต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๒) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลตาม (๑) พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน ดำเนินการด้วยตนเองหรือสั่งการให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำหน่วยงานภายในหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี ที่จำเป็นและเหมาะสม

(๓) เมื่อพิจารณาจากข้อเท็จจริงตาม (๑) แล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ให้ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน แจ้งเหตุการละเมิดแก่มหาวิทยาลัยโดยไม่ชักช้าภายใน ๔๘ ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ข้อ ๖ ในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่มหาวิทยาลัย ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน ต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษรมายัง กองการเจ้าหน้าที่ สำนักงานอธิการบดี หรือโดยวิธีการส่งจดหมายอิเล็กทรอนิกส์ไปยัง pdpa@ubu.ac.th หรือวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่สามารถกระทำได้ โดยในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ต้องระบุสาระสำคัญดังต่อไปนี้ เท่าที่จะสามารถกระทำได้

(๑) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคลหรือลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายใน หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำหน่วยงานภายใน หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ได้รับมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

(๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๔) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลประจำหน่วยงานภายในใช้ หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ข้อ ๗ เมื่อมหาวิทยาลัยได้รับแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ตามข้อ ๖ แล้ว ให้หัวหน้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ดำเนินการให้เป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และที่แก้ไขเพิ่มเติมต่อไป

ประกาศ ณ วันที่ ๒๘ ตุลาคม พ.ศ. ๒๕๖๗

(นายฐิติเดช ลือตระกูล)
รองอธิการบดีฝ่ายแผนและพัฒนาคุณภาพองค์กร
ประธานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมหาวิทยาลัยอุบลราชธานี