แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
(Personal Data Security)

มาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ด้วยเหตุนี้ การกีฬาแห่งประเทศไทยและกองทุนพัฒนาการกีฬาแห่งชาติ (ซึ่งต่อไปในมาตรการนี้ เรียกว่า “**กกท.**”) จึงกำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

๑. วัตถุประสงค์

แนวปฏิบัติฉบับนี้ กำหนดขึ้นเพื่อเป็นมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของ กกท. ที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลของพนักงาน ผู้ช่วยปฏิบัติงาน หรือประชาชนที่มารับบริการ ซึ่งถือเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. ขอบเขต

ใช้เป็นแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล สำหรับการกีฬาแห่งประเทศไทยและกองทุนพัฒนาการกีฬาแห่งชาติ

๓. คำจำกัดความ

๓.๑ บุคคล หมายความว่า บุคคลธรรมดา

๓.๒ ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

๓.๓ ข้อมูลส่วนบุคคลอ่อนไหว หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน ตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

๓.๔ เจ้าของข้อมูลส่วนบุคคล หมายความว่า บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่ กกท. เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๓.๕ ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๓.๖ พนักงาน หมายความว่า พนักงานของ กกท. และให้หมายความถึงรองผู้ว่าการการกีฬาแห่งประเทศไทย

๓.๗ ผู้ช่วยปฏิบัติงาน หมายความว่า บุคคลที่ กกท. จ้างให้ปฏิบัติงานโดยมีสัญญาจ้างเป็นรายปีงบประมาณ

๓.๘ การเก็บรวบรวมข้อมูลส่วนบุคคล หมายความว่า การจัดเก็บข้อมูลส่วนบุคคลที่ได้รับจากเจ้าของข้อมูลเพื่อวัตถุประสงค์ในการใช้งานของ กกท.

๓.๙ การประมวลผลข้อมูลส่วนบุคคล หมายความว่า การนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่เก็บรวบรวมไว้ไปใช้และเปิดเผยตามวัตถุประสงค์ของ กกท.

๓.๑๐ การเปิดเผยข้อมูลส่วนบุคคล หมายความว่า การนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลไปเผยแพร่ ด้วยวิธีการอย่างหนึ่งอย่างใด ผ่านช่องทางต่าง ๆ รวมถึงสื่อสังคมออนไลน์ทุกประเภท

๓.๑๑ ข้อมูลชีวภาพ หมายความว่า ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพ หรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพสแกนใบหน้า ข้อมูลสแกนม่านตา และข้อมูลสแกนลายนิ้วมือ เป็นต้น

๓.๑๒ สำนักงาน หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๓.๑๓ ความมั่นคงปลอดภัย หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

๔. การจัดทำมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

๔.๑ ครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะอยู่ในรูปแบบเอกสาร หรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

๔.๒ ต้องประกอบด้วยมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (Physical Measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

๔.๓ ต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่

- การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญ
- การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น
- การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

๔.๔ ต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง

๔.๕ สำหรับข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยจะต้องครอบคลุม ส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้อง เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Servers) เครื่องคอมพิวเตอร์ลูกข่าย (Clients) ระบบเครือข่าย (Network) ซอฟต์แวร์ (Software) และแอปพลิเคชัน (Application) เป็นต้น และควรประกอบด้วยมาตรการป้องกันหลายชั้น (multiple Layers of Security Controls) เพื่อลดความเสี่ยงในกรณีที่บางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

๔.๖ มาตรการในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้อย่างเหมาะสมตามระดับความเสี่ยง เสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งานตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ ประกอบกัน ดังนี้

ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (Access Control) ที่มีการพิสูจน์และยืนยันตัวตน (Identity Proofing and Authentication) และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (Authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (Need-to-Know Basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (Principle of Least Privilege)

ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน (User Registration and De-registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (Management of Privileged Access Rights) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็นการกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล

ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคล (Audit Trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๔.๗ สร้างเสริมความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy And Security Awareness)

๔.๘ ทบทวนมาตรการรักษาความมั่นคงปลอดภัย เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป หรือเมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม