



ประกาศสำนักงานกองทุนเพื่อความเสมอภาคทางการศึกษา
เรื่อง มาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบ
สำหรับผู้พัฒนาระบบ

โดยที่เป็นการสมควรกำหนดแนวปฏิบัติและมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งระบบของกองทุนเพื่อความเสมอภาคทางการศึกษา ให้สอดคล้องตามพระราชบัญญัติ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ รวมทั้งแนวปฏิบัติและมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งระบบสารสนเทศและเว็บไซต์ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ กำหนด ดังนั้น เพื่อให้การดำเนินการดังกล่าวเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศฉบับนี้เรียกว่า “ประกาศสำนักงานกองทุนเพื่อความเสมอภาคทางการศึกษา เรื่อง มาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบ สำหรับผู้พัฒนาระบบ”

ข้อ ๒ ประกาศฉบับนี้ให้มีผลใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“กองทุน” หมายความว่า กองทุนเพื่อความเสมอภาคทางการศึกษา

“สำนักงาน” หมายความว่า สำนักงานกองทุน

“ผู้จัดการ” หมายความว่า ผู้จัดการกองทุน

“ระบบ” หมายความว่า ระบบเทคโนโลยีสารสนเทศที่ใช้ในการดำเนินงานของกองทุน

“ผู้พัฒนาระบบ” หมายความว่า บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้สร้างระบบ หรือผู้พัฒนาระบบ หรือผู้ดูแลระบบ หรือผู้ที่มีการเชื่อมต่อกับระบบ

ข้อ ๔ ในการดำเนินงานที่เกี่ยวข้องกับระบบของกองทุน ผู้พัฒนาระบบจะต้องจัดให้ระบบมีความมั่นคงปลอดภัย ให้สอดคล้องตามมาตรฐานและแนวปฏิบัติของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงมาตรการอื่นใดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอย่างน้อยผู้พัฒนาระบบจะต้องดำเนินการ ดังต่อไปนี้

(๑) จัดให้มีการควบคุมการเข้าถึงระบบ (Access Control) อย่างเข้มงวด โดยต้องกำหนดสิทธิในการควบคุมหรือเข้าถึงเท่าที่จำเป็น และต้องแยกบัญชีผู้ใช้ทั่วไปกับบัญชีผู้ดูแลระบบออกจากกัน รวมทั้งงดใช้บัญชีผู้ร่วม (shared users) ในการใช้งานระบบ

(๒) จะต้องจัดให้มีการยืนยันตัวตนในการใช้งานระบบ ที่รัดกุม โดยใช้ MFA/2FA หรือ OTP ในการยืนยันตัวตน

(๓) ต้องมีการบันทึกและตรวจสอบการเข้าถึงระบบ (Audit Log) เพื่อให้สามารถตรวจสอบการเข้าถึงระบบในภายหลังได้ และต้องเก็บข้อมูลการเข้าถึงระบบไว้อย่างน้อย ๑๘๐ วัน

(๔) ในการจัดการข้อมูลของระบบ ผู้พัฒนาระบบจะต้องจัดให้มีการกำหนดชั้นความลับของข้อมูลในรูปแบบ Data Classification

(๕) จัดให้มีการเข้ารหัสข้อมูลที่จัดเก็บในระบบอย่างเหมาะสม ตามแนวทางปฏิบัติของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๖) ต้องมีการสำรองข้อมูลของระบบอย่างสม่ำเสมอ โดยต้องดำเนินการให้มั่นใจได้ว่า จะสามารถกู้คืนข้อมูลให้ระบบกลับมาใช้งานได้ตามปกติ

(๗) ในการพัฒนาระบบ ผู้พัฒนาระบบจะต้องแยกสภาวะแวดล้อมของระบบ Production กับระบบ Development และในการทดสอบการใช้งานระบบจะต้องทำการทดสอบในสภาวะแวดล้อมของระบบ Development ก่อนนำมาใช้ในระบบ Production

(๘) ต้องจัดให้มีการทบทวนบัญชีผู้ติดตามกรอบระยะเวลาอย่างสม่ำเสมอ หรือเมื่อกองทุนร้องขอ รวมทั้งต้องส่งผลการทบทวนบัญชีผู้ใช้อย่างสม่ำเสมอให้กองทุนทราบ

(๙) ต้องให้ความร่วมมือกับกองทุนในการดำเนินการประเมินความเสี่ยง และเมื่อพบความเสี่ยงเกิดขึ้น ผู้พัฒนาระบบจะต้องแจ้งให้กองทุนทราบโดยไม่ชักช้า รวมทั้งจะต้องดำเนินการด้วยตนเองหรือร่วมกับกองทุน เพื่อแก้ไขความเสี่ยงนั้นโดยเร็ว

(๑๐) จะปฏิบัติตามประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๗ และที่จะมีผลบังคับใช้ในอนาคต

(๑๑) จะต้องเผยแพร่และสื่อสารนโยบาย แนวปฏิบัติ และมาตรการ ของกองทุน ที่เกี่ยวข้องกับ การรักษาความมั่นคงปลอดภัยของระบบ ให้ผู้ใช้งานระบบรับทราบ

(๑๒) จัดให้มีการตรวจสอบความมั่นคงปลอดภัยของระบบ และรายงานผลการตรวจสอบให้กองทุนทราบ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อกองทุนร้องขอ

ข้อ ๕ ผู้พัฒนาระบบจะต้องให้ความร่วมมือกับกองทุนในการตรวจสอบการดำเนินงานตามประกาศนี้ หรือการตรวจสอบการดำเนินการใด ๆ เกี่ยวกับการพัฒนาระบบ

ข้อ ๖ กรณีมีเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภาวะฉุกเฉินใดเกิดขึ้น ผู้พัฒนาระบบจะต้องแจ้งเหตุดังกล่าวให้กองทุนทราบ โดยเร็ว

ข้อ ๗ โครงการหรือการดำเนินการเกี่ยวกับการพัฒนาระบบใดที่ได้ดำเนินการก่อนประกาศฉบับนี้มีผลใช้บังคับ ให้โครงการหรือการดำเนินการนั้นปฏิบัติตามบรรดากฎ ระเบียบ ประกาศ แนวปฏิบัติ หรือมาตรฐานที่มีผลบังคับใช้อยู่ในขณะนั้นไปก่อนโดยอนุโลม และให้ดำเนินการตามประกาศนี้ ในโอกาสแรกที่ผู้พัฒนาระบบสามารถดำเนินการได้ ทั้งนี้ ต้องไม่เกิน ๑๘๐ วัน นับแต่วันประกาศ

ข้อ ๘ กรณีมีปัญหาเกี่ยวกับการดำเนินการตามประกาศนี้ ให้ผู้จัดการเป็นผู้วินิจฉัยชี้ขาดและคำวินิจฉัยดังกล่าวถือเป็นที่สุด

ประกาศ ณ วันที่ ๘ กรกฎาคม พ.ศ. ๒๕๖๔



(นายไกรยศ ภัทรวาท)

ผู้จัดการกองทุนเพื่อความเสมอภาคทางการศึกษา