ประกาศสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
เรื่อง นโยบายและแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและดำเนินงานด้านข้อมูลสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและลดความเสี่ยงภัยคุกคามทางไซเบอร์ต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จึงมีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (Cybersecurity Policy) และนโยบายการบริหารจัดการความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (Information Technology Business Continuity Management Policy) เพื่อให้บุคลากรในสังกัดรับรู้และเข้าใจแนวทางดำเนินการเพื่อเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนด

อาศัยอำนาจตามความในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๕ และพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ จึงออกประกาศนโยบายและแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักคณะกรรมการการศึกษาขั้นพื้นฐาน เรื่อง นโยบายและแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓ นโยบายและแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามเอกสารแนบท้ายประกาศนี้ มีนโยบาย ๒ นโยบาย มีรายละเอียดเนื้อหา ดังต่อไปนี้

๓.๑ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (Cybersecurity Policy) เพื่อให้ทุกสำนักในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน รับทราบเกี่ยวกับทิศทางและแนวทางของนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ รับทราบถึง บทบาทหน้าที่ ความรับผิดชอบ และตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของระบบสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ ดังนี้

๑) การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

เพื่อกำหนดทิศทางการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับความต้องการของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน กฎระเบียบที่เกี่ยวข้องและสื่อสารให้ผู้ใช้งานได้รับทราบถึงความสำคัญ หน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

๒) การจัดโครงสร้างความมั่นคงปลอดภัยทางระบบสารสนเทศ

เพื่อกำหนดโครงสร้าง หน้าที่และความรับผิดชอบ ทั้งในส่วนของบุคลากรภายในและผู้ให้บริการภายนอก ให้เป็นไปตามนโยบายและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

๓) การสร้าง...

๓) การสร้างความมั่นคงปลอดภัยด้านบุคลากร

เพื่อให้บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ที่มีการใช้งานระบบและทรัพย์สินสารสนเทศ ที่ปรึกษา และบุคคลหรือหน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตระหนักถึงความสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติตามนโยบายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

๔) การบริหารจัดการสินทรัพย์สารสนเทศ

เพื่อให้มีหน้าที่และความรับผิดชอบชัดเจนในการกำหนดมาตรการควบคุมและดูแลรักษาสินทรัพย์สารสนเทศ การจัดการตามระดับความสำคัญข้อมูลสารสนเทศ และการป้องกันความเสียหายจากการใช้งานสินทรัพย์สารสนเทศผิดวัตถุประสงค์

๕) การควบคุมการเข้าถึงระบบสารสนเทศ

เพื่อให้การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อย่างเหมาะสมและมีสิทธิที่ตรงตามขอบเขตหน้าที่และความรับผิดชอบของผู้ใช้งาน

๖) การเข้ารหัสข้อมูล

เพื่อให้ข้อมูลสารสนเทศมีความมั่นคงปลอดภัย ธำรงไว้ซึ่งความลับ ความถูกต้อง และป้องกันการรั่วไหลของข้อมูลสารสนเทศ

๗) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

เพื่อให้การเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ใช้งานระบบสารสนเทศมีความมั่นคงปลอดภัย รวมถึงการควบคุมการดูแลอุปกรณ์และระบบสนับสนุนที่เพียงพอและเหมาะสม

๘) ความปลอดภัยด้านการดำเนินงาน

เพื่อให้การปฏิบัติงานและดำเนินการระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเป็นไปอย่างถูกต้อง โดยลดความเสี่ยงที่เกิดจากการปฏิบัติงานไม่ถูกวิธีหรือขาดกระบวนการและแนวปฏิบัติที่ดี

๙) ความปลอดภัยทางเครือข่าย

เพื่อให้ระบบเครือข่าย โปรโตคอล และวิธีการส่งผ่านข้อมูลสารสนเทศทั้งภายในและภายนอกสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีความมั่นคงปลอดภัย และมีการควบคุมป้องกันไม่ให้ข้อมูลสารสนเทศถูกเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

๑๐) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

เพื่อให้การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศมีความมั่นคงปลอดภัยของระบบสารสนเทศ

๑๑) ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

เพื่อให้กระบวนการที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการภายนอกมีคุณภาพ และมีการคำนึงถึงข้อกำหนดด้านความมั่นคงปลอดภัย

๑๒) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด

เพื่อให้มีการบริหารจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด โดยประกอบด้วยหน้าที่และความรับผิดชอบในการรับมือ การจัดการ และการเรียนรู้จากเหตุการณ์

๑๓) การบริหาร...

๑๓) การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน

เพื่อให้บริการระบบสารสนเทศของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีความต่อเนื่อง และสามารถรองรับสถานการณ์ภัยพิบัติต่าง ๆ

๑๔) การปฏิบัติตามกฎหมาย ข้อบังคับ และข้อกำหนด

เพื่อให้การดำเนินการในระบบสารสนเทศของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เป็นไปตามข้อกำหนด ข้อบังคับ กฎหมาย ระเบียบ/ขั้นตอนปฏิบัติ ทั้งจากข้อกำหนดที่มาจากหน่วยงานรัฐ หน่วยงานกำกับดูแล และนโยบายที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

๓.๒ นโยบายการบริหารจัดการความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (Information Technology Business Continuity Management Policy) เพื่อลดความเสี่ยงด้านการปฏิบัติงานและความต่อเนื่องในการปฏิบัติงาน ในด้านการรักษาความลับ ความสมบูรณ์และความพร้อมใช้งาน เพื่อให้ทุกสำนักในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานปฏิบัติตามข้อกำหนดทางกฎหมายและข้อบังคับทั้งหมด และเพื่อให้การบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศสามารถบรรลุวัตถุประสงค์ จึงกำหนดให้มีนโยบายการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พร้อมกำหนดให้มีการทบทวนเป็นประจำทุกปี ดังนี้

๑) จัดให้มีกระบวนการกำกับดูแลการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องสม่ำเสมอ โดยต้องกำหนดเป็นลายลักษณ์อักษร

๒) จัดให้มีการเผยแพร่ข้อมูล องค์ความรู้ที่เกี่ยวข้องกับการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ ให้แก่บุคลากรของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อสร้างความรู้ ความเข้าใจ และความตระหนัก ให้รู้ถึงความจำเป็นและความสำคัญของการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศเป็นประจำทุกปี

๓) จัดให้มีคณะกรรมการซึ่งทำหน้าที่รับผิดชอบโดยตรงในการควบคุมและกำกับดูแลการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ

๔) จัดให้มีคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ซึ่งทำหน้าที่รับผิดชอบโดยตรงในการทบทวนการวิเคราะห์ผลกระทบด้านการดำเนินงาน (Business Impact Analysis: BIA) และการประเมินความเสี่ยง (Risk Assessment: RA) โดยพิจารณาถึงปัจจัยต่าง ๆ ที่ส่งผลทำให้มีความจำเป็นในการจัดทำรายงานการวิเคราะห์ผลกระทบด้านการดำเนินงาน (Business Impact Analysis report: BIA report) และ/หรือรายงานประเมินความเสี่ยง (Risk Assessment report: RA report) ใหม่เป็นประจำทุกปี

๕) ให้มีผู้ปฏิบัติงาน ซึ่งทำหน้าที่รับผิดชอบโดยตรงเป็นศูนย์กลาง เพื่อประสานงานในการจัดทำรายงานการวิเคราะห์ผลกระทบด้านการดำเนินงาน (Business Impact Analysis report: BIA report) รายงานการประเมินความเสี่ยง (Risk Assessment report: RA report) และแผนความต่อเนื่องของด้านการดำเนินงาน (Business Continuity Plan: BCP) สำหรับหน่วยงานต่าง ๆ

๖) จัดให้มีการทดสอบแผนความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP) เพื่อทดสอบความพร้อมและซักซ้อมทำความเข้าใจให้แก่ข้าราชการบุคลากร และเจ้าหน้าที่ที่เกี่ยวข้องเป็นประจำทุกปี

๗) จัดให้...

๗) จัดให้มีการทบทวนแผนความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP) เพื่อให้มีความทันสมัยอยู่เสมอ

ข้อ ๔ ให้ถือปฏิบัติตามนโยบายและแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๗ มีนาคม พ.ศ. ๒๕๖๘

ว่าที่ร้อยตรี

(ธนุ วงษ์จินดา)

เลขาธิการคณะกรรมการการศึกษาขั้นพื้นฐาน