นโยบายการรักษาความมั่นคงปลอดภัย สารสนเทศทางไซเบอร์

Cybersecurity Policy

สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
Office of the Basic Education Commission

คำนำ

ในยุคแห่งการเปลี่ยนผ่านทางดิจิทัล (Digital Transformation) เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการขับเคลื่อนภารกิจและการให้บริการของหน่วยงานภาครัฐอย่างกว้างขวาง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในฐานะหน่วยงานหลักด้านการจัดการศึกษาของประเทศ ได้เล็งเห็นถึงความจำเป็นอย่างยิ่งในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) เพื่อให้การดำเนินงานการให้บริการ และการบริหารจัดการทรัพย์สินสารสนเทศของ สพฐ. เป็นไปอย่างมีประสิทธิภาพและต่อเนื่อง อันเป็นรากฐานสำคัญในการพัฒนาคุณภาพการศึกษาของชาติ

เพื่อให้เป็นไปตามกรอบแนวทางของหน่วยงานกำกับดูแล ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สพฐ. จึงจัดทำนโยบายความมั่นคงปลอดภัยทางไซเบอร์ฉบับนี้ขึ้น โดยกำหนดหลักเกณฑ์ แนวปฏิบัติ มาตรการควบคุม และกลไกในการกำกับดูแล ตลอดจนการเฝ้าระวังและตอบสนองต่อเหตุภัยคุกคาม รวมถึงกำหนดขอบเขตความรับผิดชอบให้แก่บุคลากรทุกระดับชั้น ที่ปรึกษา ผู้ให้บริการ ตลอดจนหน่วยงานภายนอกที่มีการเข้าถึงหรือใช้งานระบบสารสนเทศของ สพฐ. เพื่อให้ทุกฝ่ายได้ตระหนักถึงบทบาทหน้าที่และให้ความร่วมมือในการดำเนินงานภายใต้นโยบายนี้อย่างเป็นระบบ

นโยบายฉบับนี้ระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเพื่อลดความเสี่ยงและป้องกันความสูญเสียที่อาจเกิดขึ้น อันจะเป็นส่วนสำคัญในการขับเคลื่อนภารกิจและยุทธศาสตร์หลักของ สพฐ. ให้เป็นไปอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด ทั้งนี้ ขอให้บุคลากรและหน่วยงานผู้เกี่ยวข้องทุกภาคส่วนตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ปฏิบัติตามมาตรการและแนวทางที่กำหนดไว้อย่างเคร่งครัด และมีความรับผิดชอบต่อการใช้งานและปกป้องทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อร่วมกันสร้างความเชื่อมั่นและเสถียรภาพให้กับระบบการศึกษาของไทยต่อไป

สำนักเทคโนโลยีเพื่อการเรียนการสอน
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

สารบัญ

1. บทนำ

1.1 ความเป็นมา

สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้ตระหนักถึงบทบาทและความสำคัญของเทคโนโลยีสารสนเทศในการประกอบภารกิจ จึงได้พิจารณาให้มีการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยในเรื่องดังกล่าวอย่างมีประสิทธิภาพ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินงาน ทั้งนี้เพื่อให้สอดคล้องกับแนวทางของหน่วยงานกำกับดูแล ดังนั้นคณะผู้บริหารของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นเพื่อเป็นกฎระเบียบและข้อปฏิบัติในการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องในการดำเนินงานตามภารกิจของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อีกทั้ง เพื่อให้สอดคล้องกับหลักเกณฑ์และแนวทางการกำกับดูแลของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และพระราชบัญญัติการักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.2 วัตถุประสงค์

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ จัดทำขึ้นมาเพื่อเป็นให้คำแนะนำแก่ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ครอบคลุมการจัดการระบบสารสนเทศทั่วทั้ง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (ส่วนกลาง) ในลักษณะที่สอดคล้องและมีประสิทธิภาพซึ่งช่วยให้ภารกิจสามารถบรรลุเป้าหมายเชิงกลยุทธ์ได้ นอกจากนี้ นโยบายยังมีจุดมุ่งหมายเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน และทำให้มั่นใจว่า “สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน” ปฏิบัติตามข้อกำหนดทางกฎหมายและข้อบังคับทั้งหมด

โดยวัตถุประสงค์ดังกล่าว สามารถระบุดังต่อไปนี้

1.2.1 เพื่อให้บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศ ที่ปรึกษา และบุคคลหรือหน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน รับทราบเกี่ยวกับทิศทางและแนวทางของนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1.2.2 เพื่อให้บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศ ที่ปรึกษา และบุคคลหรือหน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1.2.3 เพื่อให้บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศ ที่ปรึกษา และบุคคล หรือ หน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน รับทราบถึง บทบาทหน้าที่และความรับผิดชอบต่อความมั่นคงปลอดภัยของระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน คงไว้ซึ่งการให้บริการได้อย่างมีประสิทธิภาพและมีเสถียรภาพ

1.3 คำจำกัดความ

ทรัพย์สินด้านเทคโนโลยีสารสนเทศจะรวมถึงทรัพย์สินที่ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (ส่วนกลาง) เป็นเจ้าของ เช่า ว่าจ้างพัฒนาขึ้นภายใน หรือซื้อซึ่งประกอบด้วยทรัพย์สินต่าง ๆ ดังนี้

คำศัพท์	ความหมาย
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน	สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (ส่วนกลาง)
นโยบาย	นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
ทรัพย์สินสารสนเทศ	1) ประเภทระบบ เช่น ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงาน ต่าง ๆ ทางคอมพิวเตอร์ 2) ประเภทอุปกรณ์ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงคอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ประเภทข้อมูล เช่น ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
ทรัพย์สินสารสนเทศที่มีความสำคัญ	ทรัพย์สินสารสนเทศที่เกี่ยวข้อง หรือจำเป็นต้องใช้ประกอบกับงานที่มีความสำคัญ เช่น เครื่องแม่ข่าย, อุปกรณ์เครือข่าย, คอมพิวเตอร์, โทรศัพท์ดิจิทัล, ระบบบันทึกเสียงทางโทรศัพท์
ระบบสารสนเทศที่มีความสำคัญ	ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ เช่น ระบบ E-office ระบบ Smart OBEC เป็นต้น
งานสำคัญ	งานที่เกี่ยวกับการให้บริการ หรืองานอื่น ๆ ของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ซึ่งหากมีการหยุดชะงักอาจส่งผลกระทบต่อผู้ใช้งานหลัก การดำเนินงาน ชื่อเสียง ฐานะ และผลการดำเนินงานของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานอย่างมีนัยสำคัญ
การใช้งานอุปกรณ์เคลื่อนที่	การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ เพื่อเข้าถึงระบบสารสนเทศที่มีความสำคัญโดยผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
ผู้รับดำเนินการ (outsource)	บุคคลจากภายนอก สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ซึ่งผู้ประกอบธุรกิจว่าจ้าง เพื่อให้ปฏิบัติงานอย่างต่อเนื่องและต้องใช้ดุลพินิจหรือการตัดสินใจในการปฏิบัติงานดังกล่าวแทน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
ผู้ให้บริการภายนอก	หน่วยงานภายนอกที่จัดหาสินค้าหรือบริการแก่ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน พร้อมกับทำการดูแลระบบในระยะเวลารับประกัน รวมทั้งผู้ให้บริการภายนอกที่มีบทบาทสำคัญในการสนับสนุนการจัดการฮาร์ดแวร์

คำศัพท์	ความหมาย
	ซอฟต์แวร์และการดำเนินงานสำหรับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ในการดูแล คัดลอกและแก้ไขข้อมูล พร้อมกับบันทึกการตรวจสอบจากการเข้ามายังสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานหรือผ่านการควบคุมจากระยะไกลได้ เพื่อแก้ไขปัญหาซอฟต์แวร์และระบบปฏิบัติการ ด้วยการตรวจสอบและปรับแต่งประสิทธิภาพของระบบ ตรวจสอบประสิทธิภาพและข้อผิดพลาดของฮาร์ดแวร์
ผู้ใช้งาน	บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศที่ปรึกษา และบุคคล หรือ หน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
ระบบคลาวด์	การให้บริการภายนอกด้านเทคโนโลยีสารสนเทศที่มีการนำเทคโนโลยี ด้านโครงข่าย Internet ผนวกกับมีระบบคอมพิวเตอร์ขนาดใหญ่ให้บริการจัดเก็บข้อมูล การประมวลผล หรือดำเนินการใด ๆ เกี่ยวกับข้อมูลหรือระบบสารสนเทศและสามารถปรับเปลี่ยนได้ตามความต้องการของผู้ใช้บริการ
ระบบสารสนเทศ	ระบบพื้นฐานของการทำงานต่าง ๆ ในรูปแบบของการจัดเก็บ การจัดการ เผยแพร่ โดยมีองค์ประกอบของระบบสารสนเทศ คือ ระบบคอมพิวเตอร์ ระบบเครือข่าย บุคคล กระบวนการ ข้อมูล เทคโนโลยี สถานที่
ผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีนัยสำคัญ	ผลกระทบที่ก่อให้เกิดความเสียหายต่อธุรกิจหรือที่ส่งผลให้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานไม่สามารถดำเนินงานได้อย่างต่อเนื่อง เช่น ระบบซื้อขายเสียหายไม่สามารถส่งคำสั่งซื้อขายได้ตามปกติ หรือผลกระทบที่ก่อให้เกิดความเสียหายต่อข้อมูลหรือทรัพย์สินของลูกค้า เนื่องจากการประมวลผลของระบบคอมพิวเตอร์หรือเนื่องจากการแก้ไข โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เป็นต้น

1.4 หน้าที่และความรับผิดชอบต่อนโยบาย

เพื่อให้บุคลากรภายในสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ทราบถึงบทบาทหน้าที่ความรับผิดชอบและการแบ่งแยกหน้าที่ดำเนินการตามนโยบาย ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ให้เป็นไปในทิศทางเดียวกัน จึงกำหนดหน้าที่และความรับผิดชอบ (Role and Responsibility) ต่อนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

1.4.1 ผู้บริหารระดับสูงหรือผู้บริหารความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่จัดทำทบทวนติดตาม ปรับปรุง อนุมัติและควบคุมติดตามการปฏิบัติงาน ให้เป็นไปตามนโยบายด้านความมั่นคงปลอดภัยไซเบอร์

1.4.2 คณะกรรมการความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่ ควบคุมดูแล ปฏิบัติตามและรายงานผลการปฏิบัติงานภายใต้นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

1.4.3 หน่วยงานและบุคลากรมีหน้าที่ปฏิบัติตามนโยบายด้านความมั่งคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อย่างเคร่งครัด

1.4.4 ผู้รับดำเนินการ ผู้ให้บริการจากภายนอกและผู้มาติดต่อ มีหน้าที่ปฏิบัติตามนโยบายด้านความมั่งคงปลอดภัยไซเบอร์ของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อย่างเคร่งครัด

1.5 การปฏิบัติตามนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ สามารถแบ่งระดับความสำคัญในการปฏิบัติของนโยบายได้ ดังนี้

1.5.1 ผู้บริหารสูงสุดของแต่ละสายงาน เป็นผู้รับผิดชอบ (Accountable Person) ในการบริหารจัดการความเสี่ยงและต้องดูแลผู้ใต้บังคับบัญชาของตนให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างถูกต้อง

1.5.2 หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เป็นผู้ทำหน้าที่ (Responsible Person) ในการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ตั้งแต่การเก็บรวบรวมข้อมูล การวิเคราะห์และประเมินด้านความเสี่ยง เพื่อใช้ในการวางแผนป้องกันภัยคุกคามทางไซเบอร์

1.5.3 หน่วยงานตรวจสอบและกำกับดูแล หรือผู้ตรวจสอบอิสระต้องตรวจสอบการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง พร้อมรายงานให้คณะกรรมการสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานรับทราบ

1.5.4 ต้องจัดให้มีการตรวจสอบด้านเทคนิคสำหรับอุปกรณ์คอมพิวเตอร์และโปรแกรมอย่างน้อยปีละ 1 ครั้ง และอาจใช้ผู้ตรวจสอบอิสระ เพื่อให้มั่นใจว่าได้มีการปฏิบัติตามการควบคุมที่กำหนดไว้ พร้อมรายงานให้คณะกรรมการของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานรับทราบ

1.5.5 ต้องมีการติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด

1.5.6 ต้องมีขั้นตอนหรือวิธีปฏิบัติเพื่อให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้

1.5.7 ต้องแจ้งหน่วยงานที่เกี่ยวข้องทันทีเมื่อมีกรณี หรือเหตุการณ์ที่ส่งผลกระทบต่อการรักษาความปลอดภัยนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

1.5.8 กรณีที่เกิดเหตุร้ายแรงซึ่งมีผลกระทบหรืออาจจะมีผลทางกฎหมายต้องแจ้งหน่วยงานภายนอก เช่น คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานตำรวจแห่งชาติ เป็นต้น

1.5.9 ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน เช่น หน้าที่ของผู้ใช้งานในกรณีที่พบว่าเครื่องคอมพิวเตอร์มีการติดไวรัส เป็นต้น

1.5.10 บุคลากรใหม่จะต้องลงนามรับทราบนโยบายยินยอมรับเงื่อนไขการใช้งานทรัพย์สินสารสนเทศ (Acceptable Use Policy) ในการยอมรับโยบายก่อนที่จะเข้าใช้งานระบบคอมพิวเตอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน หากมีการปรับปรุงนโยบายและข้อปฏิบัติต่าง ๆ บุคลากรจะต้องศึกษาและปฏิบัติตามนโยบายที่ได้ประกาศทางเว็บไซต์ ของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1.5.11 บุคลากรภายนอกจะต้องลงนามรับทราบในการยินยอมที่จะปกปิดความลับของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน พร้อมกับลงนามรับทราบในการยอมรับนโยบายที่ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน กำหนดและจะปฏิบัติตามอย่างเคร่งครัด ก่อนที่จะเข้าใช้งานระบบคอมพิวเตอร์ของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ที่ได้มีการจัดเตรียมไว้ให้เท่านั้น

การไม่ปฏิบัติตามนโยบาย หรือขัดต่อนโยบาย อาจทำให้ระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกโจรกรรม หรือนำไปใช้ในทางที่ผิด ซึ่งต้องมีการพิจารณาบทลงโทษในลักษณะตักเตือน การพักงาน การเลิกจ้าง ที่เป็นไปตามระเบียบวินัยและจรรยาบรรณของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1.6 ข้อยกเว้นและการไม่ปฏิบัติตามนโยบาย

ข้อยกเว้นที่เกี่ยวกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่อยู่ในระดับสำนักงานฯ สามารถทำได้โดยการเขียนคำร้องขอเป็นลายลักษณ์อักษร นำเสนอมายังผู้บริหารสูงสุดหรือผู้บริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อพิจารณาและนำเสนอขออนุมัติข้อยกเว้นจากคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

ข้อยกเว้นที่เกี่ยวข้องกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่โยงไปถึงหน่วยงาน หรือฝ่ายใดสามารถทำได้ โดยการเขียนคำร้องขอเป็นลายลักษณ์อักษร และนำเสนอขออนุมัติข้อยกเว้นจากผู้บริหารสูงสุดหรือผู้บริหารความมั่นคงปลอดภัยสารสนเทศ

การเขียนคำร้องขอข้อยกเว้นทั้ง 2 ระดับนั้นต้องระบุเหตุผลของการขอยกเว้น เปลี่ยนแปลงระยะเวลาที่มีผลบังคับใช้และแผนการวัดการควบคุมอื่น ๆ ที่วางไว้ คำร้องนี้จะกระทำเป็นรายกรณีไปแล้วแต่กรณีที่เกิดขึ้น คำร้องที่ได้รับอนุมัติจะจัดเก็บโดยสำนักเทคโนโลยีเพื่อการเรียนการสอน เพื่อใช้เป็นเอกสารอ้างอิงในอนาคตต่อไป

1.7 การสอบทานการปฏิบัติตามนโยบาย

หน่วยงานตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจะต้องทำการตรวจสอบการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตามแนวทางที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน กำหนดอย่างน้อยปีละ 1 ครั้ง และจัดทำรายงาน และรายงานต่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และหน่วยงานที่เกี่ยวข้อง ภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการ รวมทั้งประเมินความเหมาะสมของนโยบาย ให้สอดคล้องกับเทคโนโลยีสารสนเทศที่เป็นปัจจุบัน หากการสอบทานนั้นมีผลกระทบต่อการปฏิบัติงาน ให้ทำการนอกเวลางาน และรายงานต่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน รับทราบ หากมีเหตุการณ์ที่ส่งผลกระทบต่อการปฏิบัติตามนโยบายของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ให้รายงานต่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ทันที

1.8 การบำรุงรักษาและพัฒนานโยบาย

เพื่อให้นโยบาย รวมถึงข้อกำหนด กระบวนการ ขั้นตอนและแนวทางปฏิบัติและเอกสารใด ๆ ที่เกี่ยวข้อง มีความทันสมัยและนำมาประยุกต์ใช้งานได้จริง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จึงจัดให้มีการทบทวนนโยบาย ข้อกำหนด กระบวนการ ขั้นตอนการปฏิบัติ และรายละเอียดการปฏิบัติ แนวทางปฏิบัติ และเอกสารใด ๆ ที่เกี่ยวข้องกับนโยบาย นี้ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญหรือมีผลกระทบกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อให้นโยบาย กระบวนการ ขั้นตอนการปฏิบัติ

และรายละเอียดการปฏิบัติ แนวทางปฏิบัติ และเอกสารใด ๆ มีความเหมาะสม เพียงพอ และสอดคล้องกับข้อกฎหมาย รวมถึงมาตรฐานสากล ให้มีประสิทธิภาพอยู่เสมอ

2. รายละเอียดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์

2.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดทิศทางการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับความต้องการของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน กฎระเบียบที่เกี่ยวข้องและสื่อสารให้ผู้ใช้งานได้รับทราบถึงความสำคัญ หน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

2.1.1 ให้มีการจัดทำ เผยแพร่ และประกาศใช้นโยบายที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับ ภารกิจและพันธกิจของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

2.1.2 ให้มีการสื่อสารนโยบายฯ ให้กับผู้ใช้งาน ซึ่งรวมถึง บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศ ที่ปรึกษา และบุคคลหรือหน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานได้รับทราบและปฏิบัติตามอย่างเคร่งครัด

2.1.3 ให้มีการสอบทานและปรับปรุงเนื้อหาของนโยบายอย่างน้อยปีละหนึ่งครั้ง โดยให้สอดคล้องกับบริบท การเปลี่ยนแปลง และความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.2 การจัดโครงสร้างความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดโครงสร้าง หน้าที่และความรับผิดชอบ ทั้งในส่วนของบุคลากรภายในและผู้ให้บริการภายนอก ให้เป็นไปตามนโยบายและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

ให้มีการกำหนดโครงสร้าง หน้าที่และความรับผิดชอบโดยระบุเป็นส่วนหนึ่งในนโยบาย ระเบียบ/ขั้นตอนปฏิบัติ สัญญา เงื่อนไขข้อตกลง หรือเอกสารอื่นใดอย่างเป็นลายลักษณ์อักษร

2.2.1 ให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานและสอบทานการปฏิบัติงานระหว่างกันและจัดทำระเบียบปฏิบัติ

2.2.2 การตรวจสอบการปฏิบัติงานที่มีความเสี่ยงการเกิดทุจริตอย่างสม่ำเสมอ

2.3 การสร้างความมั่นคงปลอดภัยด้านบุคลากร

วัตถุประสงค์

เพื่อให้บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศ ที่ปรึกษา และบุคคลหรือหน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตระหนักถึงความสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติตามนโยบายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

นโยบาย

2.3.1 ให้มีระเบียบปฏิบัติการคัดเลือกบุคลากรตามหน้าที่และความรับผิดชอบโดยคำนึงถึงความมั่นคงปลอดภัยและระดับความสำคัญของข้อมูลที่เข้าถึงได้

2.3.2 ให้มีการระบุข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษรและกำหนดมาตรการลงโทษหากมีการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.3.3 ให้มีการสร้างความตระหนักรู้และให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้ใช้งานอย่างสม่ำเสมอ โดยมีการสื่อสารด้านความมั่นคงปลอดภัยผ่านสื่อประชาสัมพันธ์หรือทางจดหมายอิเล็กทรอนิกส์อย่างน้อยปีละ 1 ครั้ง

2.3.4 ให้ผู้ควบคุมงานสื่อสารนโยบายและความต้องการด้านความมั่นคงปลอดภัยให้กับผู้ให้บริการภายนอกตามขอบเขตความรับผิดชอบของผู้ให้บริการภายนอก

2.3.5 การละเมิด ฝ่าฝืน หรือไม่ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศมีผลให้ดำเนินการตามกระบวนการทางวินัย และการดำเนินคดีตามกฎหมายตามเจตนาและความร้ายแรงของการกระทำความผิด

2.3.6 ให้มีช่องทางเพื่อใช้แจ้งเหตุละเมิด ฝ่าฝืน หรือไม่ปฏิบัติตามนโยบาย รวมถึงใช้เป็นช่องทางรับฟังความคิดเห็นในการปรับปรุงนโยบายด้านความมั่นคงปลอดภัยให้เพียงพอและเหมาะสม

2.3.7 ให้มีระเบียบปฏิบัติการยุติการจ้างหรือเปลี่ยนแปลงหน้าที่การปฏิบัติงาน รวมถึงการเรียกคืนสินทรัพย์และสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูลเมื่อสิ้นสุดภาระหน้าที่

2.4 การบริหารจัดการสินทรัพย์สารสนเทศ

วัตถุประสงค์

เพื่อให้มีหน้าที่และความรับผิดชอบชัดเจนในการกำหนดมาตรการควบคุมและดูแลรักษาสินทรัพย์สารสนเทศ การจัดการตามระดับความสำคัญข้อมูลสารสนเทศ และการป้องกันความเสียหายจากการใช้งานสินทรัพย์สารสนเทศผิดวัตถุประสงค์

นโยบาย

2.4.1 ให้มีการจัดทำ ทบทวน และปรับปรุงรายการสินทรัพย์สารสนเทศที่สำคัญอย่างสม่ำเสมอ พร้อมทั้งระบุเจ้าของสินทรัพย์สารสนเทศและผู้ดูแล

2.4.2 ให้มีการระบุข้อตกลงการใช้สินทรัพย์สารสนเทศอย่างเป็นลายลักษณ์อักษรและห้ามไม่ให้ทำการเผยแพร่ข้อมูลสารสนเทศหรือทำการใด ๆ ที่ขัดกับนโยบายสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.4.3 ให้มีระเบียบปฏิบัติการเรียกคืนสินทรัพย์สารสนเทศเมื่อสิ้นสุดภาระหน้าที่หรือความจำเป็นที่ต้องใช้งาน

2.4.4 ให้มีการจัดชั้นความลับข้อมูลสารสนเทศ วิธีการที่ใช้บ่งชี้ชั้นความลับ และแนวทางการจัดการตามระดับชั้นความลับข้อมูล ได้แก่ การเข้าถึง การจัดเก็บ การทำซ้ำ การส่ง และการทำลาย

2.4.5 ให้มีมาตรการควบคุมที่เหมาะสมในการรักษาความมั่นคงปลอดภัยตามชั้นความลับข้อมูลสารสนเทศและตรวจสอบประสิทธิภาพของมาตรการอย่างสม่ำเสมอ

2.4.6 ให้มีมาตรการควบคุมการใช้งาน การขนย้าย และการทำลายสื่อบันทึกไม่ให้เกิดการรั่วไหล เสี่ยงต่อการสูญหายและกู้คืนข้อมูล

2.5 การควบคุมการเข้าถึงระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้การควบคุมการเข้าถึงและใช้งานระบบสารสนเทศของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อย่างเหมาะสมและมีสิทธิที่ตรงตามขอบเขตหน้าที่และความรับผิดชอบของผู้ใช้งาน

นโยบาย

2.5.1 ให้มีการควบคุมการเข้าถึงและควบคุมการใช้งานสารสนเทศและระบบสารสนเทศโดยยึดหลักการให้สิทธิที่น้อยที่สุด (Least Privilege) และการเข้าถึงตามความจำเป็นต้องรู้ (Need-to-know)

2.5.2 ให้มีการกำหนดสิทธิการเข้าถึง และใช้งานตามตามขอบเขตหน้าที่และความรับผิดชอบในการปฏิบัติงานหน้าที่ความรับผิดชอบของผู้ใช้งาน โดยกำหนดให้มีการควบคุมในส่วนต่าง ๆ ดังนี้

2.5.2.1 การเข้าถึงข้อมูลสารสนเทศ

2.5.2.2 การเข้าถึงระบบเครือข่าย

2.5.2.3 การเข้าถึงระบบปฏิบัติการ

2.5.2.4 การเข้าถึงระบบสารสนเทศหรือโปรแกรมประยุกต์

2.5.2.5 การเข้าถึงซอร์สโค้ดของระบบสารสนเทศ

2.5.3 ให้มีการทบทวนสิทธิการเข้าถึงเป็นประจำอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

2.5.4 ให้ยกเลิกสิทธิการเข้าถึงทันทีที่ผู้ใช้งานพ้นสภาพ หรือสิ้นสุดหน้าที่และความรับผิดชอบในการเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศที่เกี่ยวข้อง

2.6 การเข้ารหัสข้อมูล

วัตถุประสงค์

เพื่อให้ข้อมูลสารสนเทศมีความมั่นคงปลอดภัย ธำรงไว้ซึ่งความลับ ความถูกต้อง และป้องกันการรั่วไหลของข้อมูลสารสนเทศ

นโยบาย

2.6.1 ให้มีการใช้งานเทคโนโลยีการเข้ารหัสที่มีความปลอดภัยและเป็นไป ตามมาตรฐานสากลที่ได้รับการยอมรับ

2.6.2 ให้มีกระบวนการจัดการกุญแจเข้ารหัสตลอดวงจรชีวิตอายุกุญแจ

2.7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

วัตถุประสงค์

เพื่อให้การเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ใช้งานระบบสารสนเทศมีความมั่นคงปลอดภัย รวมถึงการควบคุมการดูแลอุปกรณ์และระบบสนับสนุนที่เพียงพอและเหมาะสม

นโยบาย

2.7.1 ให้มีการกำหนดประเภทพื้นที่ควบคุมที่ต้องมีการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

2.7.2 ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์แม่ข่าย และอุปกรณ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารภายในศูนย์คอมพิวเตอร์

2.7.3 มีการป้องกันการเข้าถึงศูนย์คอมพิวเตอร์สำหรับผู้ที่ไม่เกี่ยวข้องหรือผู้ที่ไม่ได้รับอนุญาต

2.7.4 อุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศที่สำคัญต้องจัดวางในตู้เซิร์ฟเวอร์ (Rack) ที่มีระบบกุญแจป้องกัน

2.7.5 ให้มีการควบคุมสภาพแวดล้อมภายในศูนย์คอมพิวเตอร์ และพื้นที่จัดวางอุปกรณ์ประมวลผลสารสนเทศ

2.7.6 ให้มีความเหมาะสม ได้แก่ มีการควบคุมอุณหภูมิและความชื้น ระบบตรวจจับสิ่งผิดปกติ และระบบป้องกันอัคคีภัย

2.7.7 ให้มีการดูแลบำรุงรักษาระบบสนับสนุนและระบบโครงสร้างพื้นฐาน (Facilities) และจัดให้มีการทดสอบระบบสำคัญ เช่น เครื่องกำเนิดไฟฟ้า ระบบตรวจจับควันไฟ อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 2 ครั้ง

2.7.8 ให้มีการควบคุมการนำระบบสารสนเทศ และอุปกรณ์ประเภทต่าง ๆ เข้าออกศูนย์คอมพิวเตอร์และพื้นที่ควบคุม

2.7.9 ให้มีกระบวนการบริหารจัดการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศที่ไม่มีการใช้งาน หรือการนำอุปกรณ์คอมพิวเตอร์กลับมาใช้งานใหม่

2.8 ความปลอดภัยด้านการดำเนินงาน

วัตถุประสงค์

เพื่อให้การปฏิบัติงานและดำเนินการระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเป็นไปอย่างถูกต้อง โดยลดความเสี่ยงที่เกิดจากการปฏิบัติงานไม่ถูกวิธี หรือขาดกระบวนการและแนวปฏิบัติที่ดี

นโยบาย

2.8.1 ให้มีการจัดทำขั้นตอนการปฏิบัติงาน โดยระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบอย่างชัดเจน

2.8.2 ให้มีการบริหารจัดการและควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

2.8.3 ให้มีการตรวจสถานะการทำงานของระบบสารสนเทศอย่างสม่ำเสมอ

2.8.4 ให้มีระบบป้องกันไวรัสคอมพิวเตอร์และโปรแกรมที่ไม่พึงประสงค์ (Malicious Software)

2.8.5 ให้มีการสำรองข้อมูลสารสนเทศและทดสอบสภาพพร้อมใช้งานอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

2.8.6 ให้มีการบันทึกข้อมูลการใช้งาน (Log) ระบบที่มีความสำคัญ โดยต้องเก็บข้อมูลให้เพียงพอต่อการใช้สืบค้นข้อมูลย้อนหลัง และจัดเก็บตามระยะเวลาที่กฎหมายระบุ

2.8.7 ให้มีการบริหารจัดการแพตช์ (Patch Management) และช่องโหว่ (Vulnerability Management) ที่ตรวจพบในระบบสารสนเทศที่สำคัญ

2.8.8 ให้มีการวางแผนและอนุมัติก่อนดำเนินการตรวจประเมินช่องโหว่ภายในระบบสารสนเทศ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการตรวจสอบ

2.8.9 ให้มีมาตรการควบคุมการใช้อุปกรณ์เคลื่อนที่ และมีการควบคุมการปฏิบัติงานจากเครือข่ายภายนอกสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.8.10 ให้มีมาตรการเข้ารหัส หรือมาตรการป้องกันข้อมูลที่เป็นความลับ หรือมีความสำคัญที่อยู่ในอุปกรณ์เคลื่อนที่และอุปกรณ์ที่ใช้ในการปฏิบัติงานจากเครือข่ายภายนอก สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.9 ความปลอดภัยทางเครือข่าย

วัตถุประสงค์

เพื่อให้ระบบเครือข่าย โปรโตคอล และวิธีการส่งผ่านข้อมูลสารสนเทศทั้งภายในและภายนอกสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีความมั่นคงปลอดภัย และมีการควบคุมป้องกันไม่ให้ข้อมูลสารสนเทศถูกเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

นโยบาย

2.9.1 ให้มีการบริหารจัดการและควบคุมระบบเครือข่าย และช่องทางที่ใช้สื่อสารทางข้อมูลทางอิเล็กทรอนิกส์ ให้มีความมั่นคงปลอดภัย

2.9.2 ให้มีอุปกรณ์ระบบเครือข่าย ระบบรักษาความปลอดภัยในระบบเครือข่าย ให้การสื่อสารและส่งผ่านข้อมูลมีความมั่นคงปลอดภัย

2.9.3 ให้มีการควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศภายใน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน การส่งออกไปยังภายนอกสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานและจัดให้มีการเข้ารหัสข้อมูลที่สำคัญ

2.9.4 ให้มีระบบจดหมายอิเล็กทรอนิกส์ที่มีความปลอดภัย และมีระบบป้องกันให้จดหมายอิเล็กทรอนิกส์ส่งถึงผู้รับอย่างปลอดภัย

2.10 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศมีความมั่นคงปลอดภัยของระบบสารสนเทศ

นโยบาย

2.10.1 ให้มีการคำนึงทั้งในส่วนของความต้องการของผู้ใช้งาน และความต้องการด้านความมั่นคงปลอดภัย ก่อนดำเนินการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ

2.10.2 ให้มีการทดสอบระบบทั้งในส่วนของความต้องการของผู้ใช้งาน และการควบคุมด้านความมั่นคงปลอดภัย ก่อนนำระบบมาใช้งาน

2.10.3 ให้มีการบริหารจัดการและควบคุมการเปลี่ยนแปลงในระบบสารสนเทศ

2.10.4 ให้มีการตรวจสอบซอร์สโค้ดในระบบที่พัฒนา ทั้งในส่วนที่ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน พัฒนาขึ้นเอง และจ้างผู้ให้บริการภายนอกพัฒนา (Outsource)

2.10.5 ให้มีการควบคุมการจ้างผู้ให้บริการภายนอกพัฒนาซอฟต์แวร์โดยระบุความต้องการด้านความมั่นคงปลอดภัยเป็นส่วนหนึ่งสัญญาและให้ระบุสิทธิในสินทรัพย์ทางปัญญา

2.10.6 ให้มีการควบคุมข้อมูลที่ใช้ในการทดสอบ โดยให้มีการอนุมัติจากผู้มีอำนาจในการอนุมัติก่อนการนำข้อมูลจริงมาใช้ทดสอบและมีการป้องกันทางเทคนิค เพื่อไม่ให้ข้อมูลที่สำคัญต่อการปฏิบัติงาน และข้อมูลส่วนบุคคลรั่วไหล

2.11 ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อให้กระบวนการที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการภายนอกมีคุณภาพและมีการคำนึงถึงข้อกำหนดด้านความมั่นคงปลอดภัย

นโยบาย

2.11.1 ให้มีการบริหารจัดการ การจัดหา การดำเนินการ การตรวจสอบ และการสิ้นสุดสัญญาผู้ให้บริการภายนอก โดยมีการพิจารณาความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

2.11.2 ให้มีการมอบหมายผู้รับผิดชอบที่ชัดเจนในการดูแลด้านความมั่นคงปลอดภัยของผู้ให้บริการภายนอก เช่น ผู้จัดการโครงการ หรือ ผู้ที่ได้รับมอบหมายให้เป็นผู้ดำเนินการควบคุมการดำเนินงาน เป็นต้น

2.11.3 ให้มีการสื่อสารความต้องการด้านความมั่นคงปลอดภัยไปยังผู้ให้บริการภายนอก และมีการตรวจสอบการดำเนินการให้เป็นไปตามนโยบายของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.11.4 ให้มีการระบุผลที่ตามมาหากมีการละเมิดนโยบายและข้อกำหนดด้านความมั่นคงปลอดภัยของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อย่างเป็นลายลักษณ์อักษรในสัญญา เช่น การยกเลิกสัญญา การดำเนินคดีทางกฎหมาย เป็นต้น

2.11.5 ให้มีการระบุหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอกในการรองรับสถานการณ์ไม่พึงประสงค์และการบริหารความต่อเนื่องของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานตามขอบเขตความรับผิดชอบของผู้ให้บริการ

2.12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด

วัตถุประสงค์

เพื่อให้มีการบริหารจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด โดยประกอบด้วยหน้าที่และความรับผิดชอบในการรับมือ การจัดการ และการเรียนรู้จากเหตุการณ์

นโยบาย

2.12.1 ให้มีการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ที่เกี่ยวข้องในการใช้งานระบบสารสนเทศของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.12.2 ให้มีช่องทางการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด

2.12.3 ให้มีการจัดทำและทดสอบกระบวนการตอบรับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่คาดคิด รวมถึงภัยทางไซเบอร์ที่อาจเกิดขึ้น

2.12.4 ให้มีกิจกรรมการเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิดเพื่อป้องกันการเกิดขึ้นของเหตุการณ์ในอนาคต

2.12.5 ให้มีกระบวนการจัดการหลักฐานทางอิเล็กทรอนิกส์เมื่อมีความจำเป็นต้องจัดส่งให้กับหน่วยงานทางกฎหมายและเป็นไปตามข้อกำหนดของกระบวนการยุติธรรม

2.13 การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน

วัตถุประสงค์

เพื่อให้บริการระบบสารสนเทศของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีความต่อเนื่อง และสามารถรองรับสถานการณ์ภัยพิบัติต่าง ๆ

นโยบาย

2.13.1 ให้มีแผนรองรับความต่อเนื่องในการดำเนินงาน และแผนเตรียมความพร้อมกรณีฉุกเฉิน สำหรับระบบสารสนเทศที่มีความสำคัญตามความต้องการของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.13.2 ให้มีการทดสอบสภาพความพร้อมใช้และทบทวนปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน

2.13.3 ให้มีระบบสำรองสำหรับระบบสารสนเทศที่มีความสำคัญ เพื่อให้สามารถให้บริการแก่บุคลากรในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศที่ปรึกษา และบุคคลหรือหน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานภายใต้การให้บริการระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานได้อย่างต่อเนื่อง

2.14 การปฏิบัติตามกฎหมาย ข้อบังคับ และข้อกำหนด

วัตถุประสงค์

เพื่อให้การดำเนินการในระบบสารสนเทศของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเป็นไปตามข้อกำหนด ข้อบังคับ กฎหมาย ระเบียบ/ขั้นตอนปฏิบัติ ทั้งจากข้อกำหนดที่มาจากหน่วยงานรัฐหน่วยงานกำกับดูแล และนโยบายที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

นโยบาย

2.14.1 ให้มีการทบทวนข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ และมาตรการรักษาความมั่นคงปลอดภัยของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ให้เป็นไปตามกฎหมาย ข้อกำหนดมีความเพียงพอและเป็นปัจจุบันอยู่เสมอ

2.14.2 ให้ใช้งานซอฟต์แวร์ที่ได้รับลิขสิทธิ์หรือได้รับสิทธิให้ใช้งานได้ถูกต้องตามกฎหมายเท่านั้น ห้ามไม่ให้ใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ ซอฟต์แวร์ผิดกฎหมาย และซอฟต์แวร์ที่แฝงชุดคำสั่งไม่พึงประสงค์ (Malicious Software)

2.14.3 ให้ปฏิบัติตามข้อกำหนดด้านการเข้ารหัสตามกฎหมาย และข้อกำหนดภายในประเทศและระหว่างประเทศที่เกี่ยวข้อง

2.14.4 ให้มีการป้องกันข้อมูลส่วนบุคคลไม่ให้ถูกเปิดเผย และมีการจัดการตามระดับชั้นความลับของข้อมูล

2.14.5 ให้ผู้บริหารทุกระดับกำกับและดูแลบุคลากรภายใต้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานที่มีการใช้งานระบบและทรัพย์สินสารสนเทศ ที่ปรึกษา และบุคคลหรือหน่วยงานภายนอก ที่เข้าใช้งาน/เข้าถึงระบบและทรัพย์สินสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ให้ปฏิบัติตามข้อกำหนดของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.14.6 ให้มีการตรวจสอบในการปฏิบัติตามนโยบายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อย่างน้อยปีละ 1 ครั้งโดยผู้ตรวจสอบที่เป็นอิสระ

2.14.7 ให้มีการตรวจสอบทางเทคนิคในระบบสารสนเทศที่สำคัญของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน อย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบที่มีความเชี่ยวชาญ และมีความเป็นอิสระจากระบบสารสนเทศที่ตรวจสอบ

คณะผู้จัดทำ

1)	นายทรงฤทธิ์ สร้อยอาภรณ์	นักวิชาการศึกษาชำนาญการพิเศษ สำนักเทคโนโลยีเพื่อการเรียนการสอน
2)	นางสาวเปรมฤทัย เลิศบำรุงชัย	นักวิชาการศึกษาชำนาญการพิเศษ สำนักเทคโนโลยีเพื่อการเรียนการสอน
3)	นายสมคิด จรียานุวัฒน์	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ สำนักเทคโนโลยีเพื่อการเรียนการสอน
4)	นางชุติมาศ น่วมอินทร์	นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักเทคโนโลยีเพื่อการเรียนการสอน
5)	นายธีรพงศ์ เรือนน้อย	นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักเทคโนโลยีเพื่อการเรียนการสอน
6)	นายพินิจ พุ่มนุ่ม	นักวิชาการคอมพิวเตอร์ปฏิบัติการ สำนักเทคโนโลยีเพื่อการเรียนการสอน
7)	นายชานนทร์ สุธนะวุฒิ	นักวิชาการศึกษาปฏิบัติการ สำนักเทคโนโลยีเพื่อการเรียนการสอน