นโยบายการบริหารจัดการความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ

Information Technology Business Continuity Management Policy

สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
Office of the Basic Education Commission

คำนำ

ในปัจจุบัน ภัยคุกคามและเหตุการณ์ไม่ปกติรุนแรงที่ส่งผลต่อการดำเนินงานของหน่วยงานภาครัฐมีความหลากหลายและซับซ้อนมากขึ้น การหยุดชะงักของระบบเทคโนโลยีสารสนเทศเพียงเล็กน้อยอาจก่อให้เกิดผลกระทบในวงกว้างและรุนแรงได้อย่างคาดไม่ถึง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในฐานะหน่วยงานที่มีบทบาทสำคัญในการขับเคลื่อนระบบการศึกษาของประเทศ จึงได้จัดทำ **"แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)"** เพื่อเป็นกรอบแนวทางในการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (IT BCM) และรองรับสถานการณ์ฉุกเฉิน รวมถึงเพื่อลดผลกระทบที่อาจเกิดขึ้นกับการดำเนินงานหลักของสำนักงานฯ

แผนความต่อเนื่องทางธุรกิจฉบับนี้ ได้จัดทำขึ้นบนพื้นฐานของการประเมินความเสี่ยง (Risk Assessment: RA) และการวิเคราะห์ผลกระทบด้านการดำเนินงาน (Business Impact Analysis: BIA) ซึ่งผสานกับมาตรฐานการจัดการความเสี่ยงของหน่วยงาน และสอดคล้องกับพระราชบัญญัติ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง ด้วยเป้าหมายสำคัญคือการรักษาความปลอดภัย ความพร้อมใช้งาน และความสมบูรณ์ของข้อมูลสารสนเทศตลอดจนให้ความมั่นใจว่าหน่วยงานสามารถบริการและสานต่อภารกิจได้อย่างต่อเนื่องในทุกสถานการณ์

นอกจากนี้ แผนความต่อเนื่องทางธุรกิจได้ระบุแนวทางและมาตรการสำคัญ เช่น แผนการกู้คืนความเสียหายด้านเทคโนโลยีสารสนเทศ (IT DRP) แผนการรักษาความมั่นคงปลอดภัย (ซึ่งรวมถึงการจัดการวิกฤตเหตุการณ์ และเหตุฉุกเฉิน) รวมถึงการวางแผนความต่อเนื่องในการปฏิบัติงานตามภารกิจและพันธกิจของสำนักงานฯ เพื่อให้ผู้บริหารและบุคลากรของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตลอดจนหน่วยงานภายนอกและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ได้ตระหนักถึงบทบาท ความรับผิดชอบ และสามารถดำเนินการตามแนวทางปฏิบัติได้อย่างมีประสิทธิภาพ

การมีแผนความต่อเนื่องทางธุรกิจที่ชัดเจนและเป็นระบบ จะช่วยลดความเสี่ยงและจำกัดความเสียหายที่อาจเกิดขึ้น ตลอดจนเสริมสร้างความเชื่อมั่นและศักยภาพในการบริหารจัดการเหตุฉุกเฉินของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานได้อย่างยั่งยืน จึงขอให้ทุกหน่วยงานและบุคลากรที่เกี่ยวข้องให้ความร่วมมือปฏิบัติตามขั้นตอน มาตรการ และแนวทางที่กำหนดอย่างเคร่งครัด เพื่อรักษาความต่อเนื่องและเสถียรภาพของระบบการศึกษาของไทยให้ดำเนินไปได้อย่างราบรื่นและมีประสิทธิภาพสูงสุด

สำนักเทคโนโลยีเพื่อการเรียนการสอน
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

สารบัญ

1. บทนำ

1.1 ความเป็นมา

การบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (IT BCM) เป็นนโยบายของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ซึ่งกำหนดกรอบการดำเนินงานสำหรับหน่วยงานในการตอบสนองต่อภัยคุกคามภายในและภายนอกและรับประกันความพร้อมของหน่วยงาน ความยืดหยุ่น และความสามารถในการส่งมอบอำนาจต่อไปเมื่อเกิดภัยคุกคามดังกล่าว

การบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (IT BCM) ทำหน้าที่เป็นกรอบการจัดการเหตุฉุกเฉินสำหรับหน่วยงาน ซึ่งรวมถึงแผนการกู้คืนความเสียหายด้านเทคโนโลยีสารสนเทศ (IT DRP) แผนการรักษาความมั่นคงปลอดภัย (ซึ่งรวมถึงการจัดการวิกฤต เหตุการณ์ และเหตุฉุกเฉิน) และการวางแผนความต่อเนื่องทางด้านการดำเนินงานตามภารกิจและพันธกิจของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

การวางแผนความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (IT BCP) ขึ้นอยู่กับการประเมินความเสี่ยง (RA) และการวิเคราะห์ผลกระทบด้านการดำเนินงาน (BIA) โดยสร้างขึ้นจากมาตรฐานการจัดการความเสี่ยงของหน่วยงานที่มีอยู่ โดยพิจารณาถึงข้อบังคับของหน่วยงานโดยรวมและความต่อเนื่องของการดำเนินงานตามภารกิจของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1.2 วัตถุประสงค์

นโยบายการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ จัดทำขึ้นมาเพื่อเป็นการให้คำแนะนำแก่หน่วยงานสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในลักษณะที่สอดคล้องและมีประสิทธิภาพ ซึ่งช่วยให้ภารกิจและพันธกิจสามารถบรรลุเป้าหมายเชิงกลยุทธ์ได้ นอกจากนี้ นโยบายยังมีจุดมุ่งหมายเพื่อลดความเสี่ยงด้านการปฏิบัติงานและความต่อเนื่องในการปฏิบัติงาน ในด้านการรักษาความลับ ความสมบูรณ์และความพร้อมใช้งาน และทำให้มั่นใจว่าสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานปฏิบัติตามข้อกำหนดทางกฎหมายและข้อบังคับทั้งหมด

โดยวัตถุประสงค์ดังกล่าว สามารถระบุดังต่อไปนี้

1.2.1 เพื่อให้มั่นใจว่ากระบวนการหลักในการปฏิบัติงานของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานสามารถดำเนินการได้อย่างต่อเนื่องในระยะเวลาที่เหมาะสม เมื่อเกิดเหตุการณ์ไม่ปกติรุนแรงที่ทำให้การดำเนินงานหยุดชะงัก

1.2.2 เพื่อให้สามารถจำกัดผลกระทบหรือความเสียหายในด้านต่าง ๆ ให้เกิดน้อยที่สุดจากเหตุการณ์ไม่ปกติรุนแรงที่เกิดขึ้น

1.2.3 เพื่อใช้เป็นแนวทางในการกำกับดูแลและควบคุมการปฏิบัติด้านการบริหารความต่อเนื่องของการปฏิบัติงาน

1.3 คำจำกัดความ

ทรัพย์สินด้านเทคโนโลยีสารสนเทศจะรวมถึงทรัพย์สินที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เป็นเจ้าของ เช่า ว่าจ้างพัฒนาขึ้นภายใน หรือซื้อซึ่งประกอบด้วยทรัพย์สินต่าง ๆ ดังนี้ คือ

คำศัพท์	ความหมาย
การบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Information Technology Business Continuity Management: IT BCM)	องค์รวมของกระบวนการบริหาร ซึ่งชี้บ่งภัยคุกคามต่อองค์กรและผลกระทบของภัยคุกคามนั้นต่อการดำเนินงานของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และให้แนวทางในการสร้างขีดความสามารถให้แต่ละหน่วยงาน มีความยืดหยุ่นเพื่อการตอบสนองและปกป้องผลประโยชน์ ของผู้มีส่วนได้ส่วนเสียหลัก ชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าและส่งผลต่อภารกิจและพันธกิจ
แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Information Technology Business Continuity Plan: IT BCP)	เอกสารรวบรวม แผน ขั้นตอนและข้อมูล ซึ่งมีการจัดทำรวบรวมและบำรุงรักษาให้องค์กรพร้อมที่จะนำไปใช้เมื่อเกิดอุบัติการณ์เพื่อให้สามารถดำเนินการในกิจกรรมที่สร้างมูลค่าและส่งผลต่อภารกิจและพันธกิจ
การวิเคราะห์ผลกระทบด้านการดำเนินงาน และการประเมินความเสี่ยง (Business Impact Analysis and Risk Assessment)	กระบวนการการวิเคราะห์ผลกระทบ หรือความเสียหาย (เชิงปริมาณ และเชิงคุณภาพ) ที่มีสาเหตุทำให้เกิดจากการหยุดชะงักของกิจกรรมของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน การวิเคราะห์ผลกระทบต่อการดำเนินงานของหน่วยงานมีประโยชน์ในการระบุลำดับความสำคัญการกู้คืน ความต้องการทรัพยากรที่ใช้กู้คืน กลยุทธ์การกู้คืน และพนักงานที่มีความสำคัญ
กลยุทธ์ความต่อเนื่องในการดำเนินงาน	แนวทางที่องค์กรเลือกใช้เพื่อกู้คืนกระบวนการและสร้างความต่อเนื่องของการดำเนินงาน โดยผ่านการอนุมัติจากผู้บริหารด้านเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และผ่านการทดสอบในการตอบสนองต่อการหยุดชะงักในการดำเนินงาน
ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD)	ช่วงเวลาสูงสุดที่ธุรกิจหยุดชะงัก หากเกินกำหนดช่วงเวลานี้แล้วจะไม่สามารถทำให้การดำเนินงานฟื้นคืนสู่สภาพปกติได้
ระยะเวลาเป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อให้การส่งมอบภารกิจและพันธกิจตามที่ได้รับมอบหมาย บริการ และกิจกรรมหรือกระบวนการกลับสู่สภาวะปกติหลังจากการเกิดการหยุดชะงัก
เป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Point Objective: RPO)	เป้าหมายสถานะและความพร้อมใช้งานของข้อมูล (ทั้งอิเล็กทรอนิกส์และกระดาษ) ณ จุดเริ่มต้นของกระบวนการกู้คืน

คำศัพท์	ความหมาย
สถานที่ปฏิบัติงานสำรอง (Alternate Sites)	สถานที่ปฏิบัติงานทดแทน เพื่อดำเนินงานให้มีความต่อเนื่อง เมื่อเกิดการหยุดชะงักของการดำเนินงาน เนื่องจากสถานที่ปฏิบัติงานหลักไม่สามารถดำเนินงานได้ตามปกติ

1.4 หน้าที่และความรับผิดชอบต่อนโยบาย

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

1.4.1 ผู้บริหารระดับสูงหรือผู้บริหารความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่ อนุมัติและควบคุมติดตามการปฏิบัติงาน ให้เป็นไปตามนโยบายด้านความมั่นคงปลอดภัยไซเบอร์

1.4.2 คณะกรรมการความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่จัดทำ ทบทวนติดตาม ปรับปรุง ควบคุมดูแล ปฏิบัติตามและรายงานผลการปฏิบัติงานภายใต้นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

1.4.3 หน่วยงานและบุคลากร มีหน้าที่ ปฏิบัติตามนโยบายของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานอย่างเคร่งครัด

1.4.4 ผู้รับดำเนินการ ผู้ให้บริการจากภายนอกและผู้มาติดต่อ มีหน้าที่ปฏิบัติตามนโยบายของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานอย่างเคร่งครัด

1.5 การปฏิบัติตามนโยบาย

ต้องมีการติดตามการปฏิบัติงานของข้าราชการ บุคลากร และเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด และมีขั้นตอนหรือวิธีปฏิบัติเพื่อให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้ รวมถึงแจ้งหน่วยงานที่เกี่ยวข้องทันทีเมื่อมีกรณีหรือเหตุการณ์ที่ส่งผลกระทบต่อการดำเนินธุรกิจอย่างต่อเนื่อง และต้องแจ้งหน่วยงานภายนอกกรณีที่เกิดเหตุร้ายแรงซึ่งมีผลกระทบหรืออาจจะมีผลทางกฎหมาย เช่น คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานตำรวจแห่งชาติ เป็นต้น

การไม่ปฏิบัติตามนโยบาย หรือขัดต่อนโยบาย อาจทำให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเกิดความเสียหาย ถูกทำลาย ถูกโจรกรรม หรือนำไปใช้ในทางที่ผิด ซึ่งต้องมีการพิจารณาบทลงโทษที่เป็นไปตามระเบียบวินัยและจรรยาบรรณ

1.6 ข้อยกเว้นและการไม่ปฏิบัติตามนโยบาย

ข้อยกเว้นที่เกี่ยวกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่อยู่ในระดับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานสามารถทำได้ โดยการเขียนคำร้องขอเป็นลายลักษณ์อักษรขออนุมัติข้อยกเว้นจากผู้บริหารระดับสูงของหน่วยงาน

การเขียนคำร้องขอข้อยกเว้นต้องระบุเหตุผลของการขอยกเว้นการเปลี่ยนแปลงระยะเวลาที่มีผลบังคับใช้แลแผนการวัด การควบคุมอื่น ๆ ที่วางไว้ คำร้องนี้จะกระทำเป็นรายกรณีไปแล้วแต่กรณีที่เกิดขึ้น คำร้องที่ได้รับอนุมัติจะจัดเก็บโดยสำนักเทคโนโลยีเพื่อการเรียนการสอน เพื่อใช้เป็นเอกสารอ้างอิงในอนาคตต่อไป

1.7 การสอบทานการปฏิบัติตามนโยบาย

หน่วยงานตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจะต้องทำการตรวจสอบการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตามแนวทางที่กำหนดอย่างน้อยปีละ 1 ครั้ง และจัดทำรายงาน และรายงานต่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และหน่วยงานที่เกี่ยวข้อง ภายใน 30 วัน นับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการ รวมทั้งประเมินความเหมาะสมของนโยบายให้สอดคล้องกับเทคโนโลยีสารสนเทศที่เป็นปัจจุบัน หากการสอบทานนั้นมีผลกระทบต่อการปฏิบัติงานให้ทำการนอกเวลางาน และรายงานต่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน รับทราบ หากมีเหตุการณ์ที่ส่งผลกระทบต่อการปฏิบัติตามนโยบายของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ให้รายงานต่อคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ทันที

1.8 การบำรุงรักษาและพัฒนานโยบาย

เพื่อให้นโยบาย รวมถึงข้อกำหนด กระบวนการ ขั้นตอนและแนวทางปฏิบัติและเอกสารใด ๆ ที่เกี่ยวข้อง มีความทันสมัย และนำมาประยุกต์ใช้งานได้จริง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจึงจัดให้มีการทบทวนนโยบาย ข้อกำหนด กระบวนการ ขั้นตอนการปฏิบัติ และรายละเอียดการปฏิบัติ แนวทางปฏิบัติ และเอกสารใด ๆ ที่เกี่ยวข้องกับนโยบายนี้ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ หรือมีผลกระทบกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อให้นโยบาย กระบวนการขั้นตอนการปฏิบัติ และรายละเอียดการปฏิบัติ แนวทางปฏิบัติ และเอกสารใด ๆ มีความเหมาะสม เพียงพอและสอดคล้องกับข้อกฎหมายรวมถึงมาตรฐานสากลให้มีประสิทธิภาพอยู่เสมอ

2. นโยบายการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

เพื่อให้การบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศสามารถบรรลุวัตถุประสงค์ จึงกำหนดให้มีนโยบายการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พร้อมกำหนดให้มีการทบทวนเป็นประจำทุกปี ดังนี้

2.1 จัดให้มีกระบวนการกำกับดูแลการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องสม่ำเสมอ โดยต้องกำหนดเป็นลายลักษณ์อักษร

2.2 จัดให้มีการเผยแพร่ข้อมูล องค์ความรู้ที่เกี่ยวข้องกับการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ ให้แก่บุคลากรของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อสร้างความรู้ความเข้าใจ และความตระหนัก ให้รู้ถึงความจำเป็นและความสำคัญของการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศเป็นประจำทุกปี

2.3 จัดให้มีคณะกรรมการซึ่งทำหน้าที่รับผิดชอบโดยตรงในการควบคุมและกำกับดูแลการบริหารความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ

2.4 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

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

2.6 จัดให้มีการทดสอบแผนความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP) เพื่อทดสอบความพร้อมและซักซ้อมทำความเข้าใจให้แก่ข้าราชการ บุคลากร และเจ้าหน้าที่ที่เกี่ยวข้องเป็นประจำทุกปี

2.7 จัดให้มีการทบทวนแผนความต่อเนื่องของการดำเนินการด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP) เพื่อให้มีความทันสมัยอยู่เสมอ

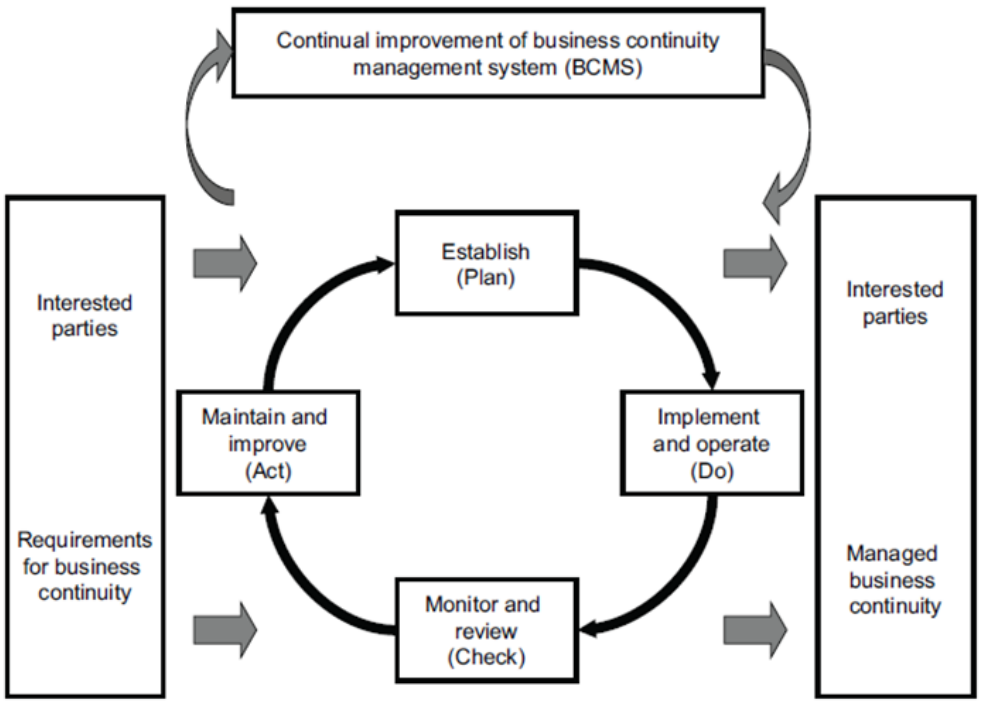
3. ภาคผนวก

3.1 กรอบการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCM Framework)

เพื่อให้การบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ มีแนวทางปฏิบัติที่ชัดเจนและเป็นไปในทิศทางเดียวกันทั้งองค์กร จึงได้กำหนดให้กรอบการบริหารจัดการความต่อเนื่องทางธุรกิจ (BCM Framework) ใช้มาตรฐานแนวปฏิบัติที่ดี ดังนี้

3.1.1 ISO 22301:2019 Business Continuity Management Systems

เป็นมาตรฐานเกี่ยวกับระบบบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ที่พัฒนาขึ้นโดยสถาบันมาตรฐานอังกฤษ (British Standard) ซึ่งข้อกำหนดต่าง ๆ ในมาตรฐานนี้จะใช้สำหรับการวางแผน การดำเนินการ การติดตามผล การตรวจประเมิน และการปรับปรุงระบบบริ หารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) โดยสามารถนำไปประยุกต์ใช้ได้ทั้งองค์กรซึ่งขอบเขตการบังคับใช้จะแตกต่างกันไปขึ้นอยู่กับสภาพแวดล้อมและความซับซ้อนของแต่ละองค์กร



3.1.2 Good Practice Guidelines 2018 Edition

เป็นแนวปฏิบัติเกี่ยวกับการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management) ที่จัดทำขึ้นโดย Business Continuity Institute (BCI) โดยรวบรวมรายละเอียดเชิงเทคนิคและประสบการณ์จากการปฏิบัติจริง เพื่อใช้เป็นแนวทางสำหรับผู้ปฏิบัติงาน ที่ปรึกษา และผู้ตรวจสอบด้านการบริหารความต่อเนื่องทางธุกิจ โดย Good Practice Guidelines 2018 Edition แบ่งเนื้อหาออกเป็น 6 หัวข้อใหญ่ ๆ ได้แก่

3.1.2.1 นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ และการบริหารโครงการพัฒนาระบบบริหารความต่อเนื่องทางธุรกิจ (BCM Policy and Program Management)

3.1.2.2 การปลูกฝังการบริหารจัดการความต่อเนื่องทางธุรกิจในวัฒนธรรมองค์กร (Embedding BCM in the Organization's Culture)

3.1.2.3 การศึกษาและทำความเข้าใจองค์กร (Understanding the Organization)

3.1.2.4 การกำหนดกลยุทธ์ในการสร้างความต่อเนื่องทางธุรกิจ (Determining BCM Strategy)

3.1.2.5 การพัฒนาและนำไปปฏิบัติ (Developing and Implementing a BCM Response)

3.1.2.6 การทดสอบและฝึกซ้อม การบำรุงรักษา และการทบทวนการเตรียมการ (Exercising, Maintaining and Reviewing)

3.2 ข้อกำหนดสำหรับการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

3.2.1 การวิเคราะห์ผลกระทบทางธุรกิจและการประเมินความเสี่ยง

ขั้นตอนการวิเคราะห์ผลกระทบด้านการดำเนินงาน และประเมินความเสี่ยง เพื่อประเมินผลกระทบจากการหยุดชะงักของการดำเนินงานที่สำคัญมีดังนี้

3.2.1.1 การวิเคราะห์ผลกระทบด้านการดำเนินงาน (Business Impact Analysis: BIA) กำหนดให้ต้องทำการวิเคราะห์ผลกระทบต่อการดำเนินงานตามภารกิจ การปฏิบัติงานของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อระบุกระบวนการ/กิจกรรมที่สำคัญ (Critical Activities) ซึ่งหากมีการหยุดชะงักเกิดขึ้น อาจจะส่งผลกระทบต่อการดำเนินงาน โดยจะต้องพิจารณาเพื่อจัดลำดับความเร่งด่วน ที่ต้องได้รับการฟื้นฟูให้กลับคืนสู่สภาวะปกติ ซึ่งการวิเคราะห์ผลกระทบด้านการดำเนินงานจะต้องพิจารณาผลกระทบให้ครอบคลุมในด้านต่าง ๆ เช่น ด้านการเงิน ด้านผู้ปฏิบัติงาน ด้านชื่อเสียง และด้านกฎหมาย ข้อกำหนด เป็นต้น

3.2.1.2 การวิเคราะห์ความต้องการในการดำเนินงานอย่างต่อเนื่อง กำหนดให้ต้องรวบรวมข้อมูลเกี่ยวกับทรัพยากรที่จำเป็นสำหรับการดำเนินการอย่างต่อเนื่องในระดับที่ยอมรับได้ ทั้งในด้านบุคลากรและทักษะ สถานที่ปฏิบัติงาน เทคโนโลยี ข้อมูลและสารสนเทศ อุปกรณ์และวัสดุสิ้นเปลือง และผู้ให้บริการหลักไปพร้อมกับการวิเคราะห์ผลกระทบด้านการดำเนินงาน (Business Impact Analysis: BIA) เพื่อใช้เป็นข้อมูลในการจัดทำแผนความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Plan: IT BCP)

3.2.1.3 การประเมินความเสี่ยง (Risk Assessment: RA) ทำการประเมินความเสี่ยง (Risk Assessment: RA) โดยการระบุภัยคุกคามที่อาจส่งผลให้การปฏิบัติงานเกิดการหยุดชะงัก จุดบอดของกระบวนการ (Single Point of Failure) วิเคราะห์และประเมินผลความเสี่ยง ตลอดจนการปรับปรุงกระบวนการเพื่อลดโอกาสและผลกระทบของภัยคุกคามดังกล่าว โดยต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อเกิดการเปลี่ยนแปลงที่สำคัญทั้งปัจจัยที่มาจากภายใน และภายนอกที่อาจจะส่งผลกระทบต่อสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เช่น ระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย การสูญเสียบุคลากรสำคัญทั้งชั่วคราวหรือถาวร หรือการเกิดความเสียหายจากภัยธรรมชาติต่าง ๆ เป็นต้น

3.2.2 การกำหนดเป้าหมายในการกู้คืนการดำเนินงาน

3.2.2.1 การกำหนดกรอบช่วงเวลาในการกำหนดกลยุทธ์การเรียกคืนการดำเนินงานที่เหมาะสม ซึ่งประกอบด้วยค่าช่วงเวลาต่าง ๆ ดังนี้

1) ค่าช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD)
2) ระยะเวลาเป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Time Objective: RTO)
3) เป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Point Objective: RPO)
4) โดยการกำหนดค่าต่าง ๆ ข้างต้นนั้น ต้องสอดคล้องกับความต้องการของการดำเนินงาน ความต้องการของผู้มีส่วนได้ส่วนเสีย และต้องขอความเห็นชอบจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเพื่อการเรียนการสอน

3.2.2.2 การเลือกกลยุทธ์ในการสร้างความต่อเนื่องด้านการดำเนินงาน จะต้องคำนึงถึงทรัพยากรที่ใช้ในการดำเนินงาน โดยกำหนดแนวทางในการลดผลกระทบของเหตุการณ์ที่ทำให้ทรัพยากรที่ใช้ดำเนินงานได้รับความเสียหาย ไม่สามารถใช้งานได้ มีไม่เพียงพอกับความต้องการ โดยมีทรัพยากรที่ได้มีความสำคัญดังนี้

1) สถานที่ (Premise/Site/Facility)
2) บุคลากร (People)
3) เทคโนโลยี (Technology)
4) ข้อมูลสำคัญ (Information)
5) ผู้ส่งมอบหรือผู้รับจ้าง (Supplier/Outsource)
6) เครื่องมือ/เครื่องจักร
7) วัสดุและอุปกรณ์

3.2.3 การจัดทำแผนความต่อเนื่องทางธุรกิจ

จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อรองรับการหยุดชะงักของกระบวนการ/กิจกรรมหลัก ในปฏิบัติงานตามภารกิจและพันธกิจของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยมีรายละเอียดอย่างน้อยดังนี้

3.2.3.1 มาตรการป้องกันหรือลดผลกระทบจากการหยุดชะงักของการปฏิบัติงาน

3.2.3.2 ขั้นตอนการกู้คืนการดำเนินงาน เพื่อให้กระบวนการ/กิจกรรมหลักให้สามารถกลับมาดำเนินการได้ตามปกติในระยะเวลาที่กำหนดไว้

3.2.3.3 รายละเอียดทรัพยากรที่จำเป็นสำหรับการดำเนินงานอย่างต่อเนื่อง ทั้งด้านบุคลากรและทักษะ สถานที่ปฏิบัติงาน เทคโนโลยี ข้อมูลและเอกสารวัสดุอุปกรณ์ และผู้ส่งมอบ/ผู้รับจ้าง/ผู้จัดหา/ผู้ให้บริการหลัก (เช่น เครื่องมือ เครื่องจักร ระบบสารสนเทศ วัสดุและอุปกรณ์ เป็นต้น)

3.2.3.4 รายละเอียดการสื่อสารกับผู้ที่เกี่ยวข้องทั้งภายในและภายนอก โดยระบุรายชื่อ หมายเลขโทรศัพท์ทั้งของข้าราชการ บุคลากร เจ้าหน้าที่ ผู้ให้บริการ หน่วยงานกำกับดูแล และสื่อที่สำคัญ ทั้งนี้ ข้อมูลในส่วนนี้จำเป็นต้องปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

3.2.3.5 รายละเอียดสถานที่ปฏิบัติงานสำรอง โดยสถานที่ปฏิบัติงานสำรองควรมีระยะห่างจากสถานที่ปฏิบัติงานหลักพอที่จะไม่ได้รับผลกระทบจากอุบัติการณ์หรือภัยพิบัติเดียวกัน เพื่อป้องกันเหตุการณ์ที่มีผลกระทบในวงกว้าง

3.2.4 การเผยแพร่และฝึกอบรม

การเผยแพร่และการฝึกอบรมนั้น สามารถแบ่งออกเป็น 2 ส่วนได้ ดังนี้

3.2.4.1 การเผยแพร่ความรู้ และการสร้างความตระหนักเกี่ยวกับการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ ให้แก่บุคลากรทุกระดับ เพื่อทำให้เกิดความรู้ความเข้าใจและความตระหนักถึงความจำเป็นและความสำคัญของการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

3.2.4.2 การเผยแพร่แผนความต่อเนื่องด้านการดำเนินงาน (Business Continuity Plan: BCP) โดยแบ่งออกเป็น 2 กลุ่ม ดังนี้

1) การฝึกอบรมให้แก่บุคลากรระดับผู้อำนวยการสำนักและผู้อำนวยการกลุ่ม เพื่อให้เข้าใจบทบาทหน้าที่และความรับผิดชอบในการจัดทำแผนต่าง ๆ รวมถึงการนำมาใช้ในการปฏิบัติกรณีเกิดอุบัติการณ์หรือภัยพิบัติ
2) การฝึกอบรมให้แก่บุคลากรระดับปฏิบัติการของแต่ละหน่วยงานเพื่อให้มีความรู้ความเข้าใจและสามารถปฏิบัติตามแผนความต่อเนื่องด้านเทคโนโลยีสารสนเทศ เมื่อมีการประกาศใช้

3.2.5 การทดสอบแผนความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

การทดสอบควรมีรายละเอียดครอบคลุมประเด็นอย่างน้อย ได้แก่ วัตุประสงค์และขอบเขตของการทดสอบสถานการณ์จำลองที่ใช้ทดสอบ ระยะเวลาในการทดสอบ ขั้นตอนการอพยพบุคลากร แผนการสื่อสาร การสำรองและเรียกคืนข้อมูลที่สำคัญ ความพร้อมของสถานที่ปฏิบัติงานสำรองและการกลับสู่สภาวะปกติ ทั้งนี้ ควรมีการประเมินผลการทดสอบโดยเปรียบเทียบกับเป้าหมายที่กำหนดไว้

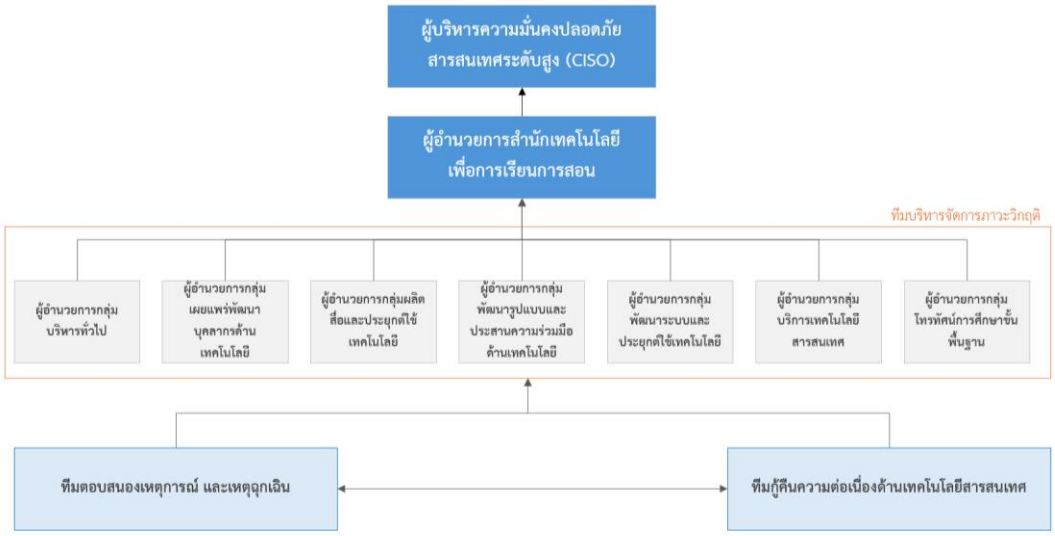
โดยการทดสอบอาจใช้วิธีการทดสอบแบบการสอบทานขั้นตอนการปฏิบัติจากเอกสารหรือการทดสอบแบบเสมือนจริงตามความเหมาะสมหรืออย่างน้อยปีละ 1 ครั้ง

3.2.6 การทบทวนและปรับปรุงแผนความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

เพื่อทำให้แผนความต่อเนื่องด้านการดำเนินงานมีความทันสมัยอยู่เสมอจะต้องมีการทบทวนและปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อกระบวนการ/กิจกรรมหลักในการปฏิบัติงาน รวมถึงทรัพยากรที่ใช้ในการดำเนินงานของกระบวนการ/กิจกรรมเหล่านั้น มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. โครงสร้างการกำกับดูแลการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

เพื่อให้การกำกับดูแลการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศสามารถบรรลุตามวัตถุประสงค์ จึงได้กำหนดให้มีโครงสร้างการกำกับดูแลการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ



4.1 บทบาทหน้าที่ความรับผิดชอบ

4.1.1 ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้รับการแต่งตั้ง โดยมีหน้าที่ดังต่อไปนี้

4.1.1.1 ให้การสนับสนุนทรัพยากรในการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

4.1.1.2 พิจารณาให้ความเห็นชอบต่อนโยบายการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

4.1.1.3 ติดตามสถานะของเหตุการณ์และความคืบหน้าในการดำเนินการต่าง ๆ อย่างต่อเนื่อง

4.1.1.4 สั่งการให้สิ้นสุดสภาวะฉุกเฉิน

4.1.1.5 กำกับ ดูแล และควบคุมการดำเนินการ การบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศให้เป็นไปตามนโยบายที่กำหนด

4.1.1.6 ให้ความเห็นชอบในการกำหนดขอบเขตการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ การะบุกระบวนการ/กิจกรรมหลัก การกำหนดระยะเวลาเป้าหมายในการฟื้นฟู การกำหนดกลยุทธ์สำหรับรองรับการดำเนินงานอย่างต่อเนื่อง

4.1.2 ผู้อำนวยการสำนักเทคโนโลยีเพื่อการเรียนการสอน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้รับการแต่งตั้ง โดยมีหน้าที่แทนกรณีผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO) ไม่อยู่/ไม่สามารถปฏิบัติงานได้

4.1.3 ทีมบริหารจัดการภาวะวิกฤต ประกอบไปด้วยผู้อำนวยการกลุ่มต่าง ๆ ของสำนักเทคโนโลยีเพื่อการเรียนการสอน ที่มีอำนาจการตัดสินใจต่อการดำเนินกิจกรรมของกลุ่มต่าง ๆ ที่เกี่ยวข้องกับกระบวนการบริหารจัดการความต่อเนื่องด้านเทคโนโลยีสารสนเทศ โดยมีหน้าที่ดังต่อไปนี้

4.1.3.1 ดำเนินการทบทวนการตอบสนองและกิจกรรมสนับสนุนภารกิจและพันธกิจ

4.1.3.2 กำหนดลำดับความสำคัญสำหรับการพัฒนากลยุทธ์เพื่อตอบสนองต่อผลที่อาจเกิดขึ้นโดยเฉพาะ

4.1.3.3 ตัดสินใจการดำเนินงานสำหรับการตอบสนองข้ามกลุ่ม หรือสำนักอื่น ๆ (ถ้ามี)

4.1.3.4 กำหนดกลยุทธ์การสื่อสารสำหรับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่สำคัญ

4.1.3.5 รับผิดชอบในการดูแล ตรวจสอบ และจัดการภัยพิบัติและการดำเนินการกู้คืนทั้งหมด

4.1.3.6 ให้คำแนะนำและตัดสินใจเพื่อสนับสนุนการดำเนินการกู้คืน

4.1.3.7 ให้การสนับสนุน ข้อมูล และคำแนะนำในการตัดสินใจสำหรับการดำเนินการกู้คืนจากมุมมองของกลุ่มของตน

4.1.3.8 ประกาศภาวะฉุกเฉินอย่างเป็นทางการ และเห็นชอบให้ใช้งานแผนความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

4.1.3.9 สั่งการให้สิ้นสุดสภาวะฉุกเฉิน

4.1.4 ทีมตอบสนองเหตุการณ์ และเหตุฉุกเฉิน ประกอบไปด้วยตัวแทนจากกลุ่มงานภายในสำนักงานเทคโนโลยีสารสนเทศเพื่อการเรียนการสอน และตัวแทนจากหน่วยงานที่เกี่ยวข้องหลัก โดยต้องทำหน้าที่สืบสวนเบื้องต้นเมื่อเกิดเหตุการณ์ ยกตัวอย่างเช่น กลุ่มบริการเทคโนโลยีสารสนเทศและการสื่อสาร สำนักเทคโนโลยีเพื่อการเรียนการสอน และสำนักอื่น ๆ ภายในสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยมีหน้าที่ดังต่อไปนี้

4.1.4.1 วิเคราะห์ประเมินความเสียหายเบื้องต้น

4.1.4.2 ยกระดับเหตุการณ์และผลการประเมินความเสียหายให้ทีมบริหารจัดการภาวะวิกฤต

4.1.4.3 ประสานงานการจัดตารางเวลาของบุคลากรในระหว่างกิจกรรมการกู้คืนและทำหน้าที่เป็นจุดศูนย์กลางสำหรับการสื่อสารภัยพิบัติทั้งหมด

4.1.4.4 การเข้าร่วมสอบถามผู้มีส่วนได้ส่วนเสียที่ได้รับผลกระทบ

4.1.4.5 ประสานงานการจัดหาและจัดส่งอุปกรณ์ทดแทนไปยังไซต์การกู้คืนสำรองต่าง ๆ

4.1.4.6 ช่วยเหลือในการพัฒนาและจัดเตรียมการเคลมประกัน

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