ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร

ลำดับชั้นเอกสาร	:	เอกสารภายใน
วันที่บังคับใช้	:	มีนาคม ๒๕๖๙
เวอร์ชันเอกสาร	:	๐.๑
เจ้าของเอกสาร	:	กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร

ลำดับชั้นเอกสาร	เอกสารภายใน
วันที่บังคับใช้	มีนาคม ๒๕๖๙
เวอร์ชันเอกสาร	๐.๑
เจ้าของเอกสาร	**กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร**

การควบคุมเอกสาร และการอนุมัติ

ข้อมูลการควบคุมเอกสาร

ชื่อเอกสาร	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร
รหัสเอกสาร	
รุ่น	V0.1
ลำดับชั้น	เอกสารภายใน
สถานะ	-
วันที่มีผลบังคับใช้	มีนาคม ๒๕๖๙
ความถี่ของการทบทวน	รายปี

การอนุมัติและมอบอำนาจ

เอกสารฉบับนี้ได้รับการอนุมัติอย่างเป็นทางการและได้รับอนุญาตให้ใช้งานภายในหน่วยงาน

บทบาท	ชื่อ / ตำแหน่ง	วิธีการอนุมัติ	วันที่
ผู้จัดทำ	**นางสาววิภาวดี เหล็มเต๊ะ** **ผู้อำนวยการกลุ่มนโยบายและแผน** **และปฏิบัติหน้าที่ผู้อำนวยการกลุ่มDLICT**		**๑๐ มีนาคม ๒๕๖๙**
ผู้ทบทวน	**นายไตรรัตน์ เอี่ยมพันธ์** **รองผู้อำนวยการสำนักงานเขตพื้นที่การศึกษา** **ประถมศึกษากรุงเทพมหานคร** **(รับผิดชอบดูแลกลุ่มDLICT)**		**๑๑ มีนาคม ๒๕๖๙**
ผู้อนุมัติ	**นายชาญณรงค์ หวานใจ** **รองผู้อำนวยการสำนักงานเขตพื้นที่การศึกษา** **รักษาราชการแทน ผู้อำนวยการสำนักงานเขต** **พื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร**		**๑๒ มีนาคม ๒๕๖๙**

ประวัติการเปลี่ยนแปลง

เอกสารฉบับนี้ได้รับการอนุมัติอย่างเป็นทางการและได้รับอนุญาตให้ใช้งานภายในหน่วยงาน

เวอร์ชัน	วันที่	รายละเอียดเปลี่ยนแปลง
๐.๑	๑๐ มีนาคม ๒๕๖๙	ร่างนโยบาย
๑.๐	๑๒ มีนาคม ๒๕๖๙	อนุมัติการใช้นโยบาย

สารบัญ

หน้า

๑. บททั่วไป

๑.๑ หลักการ

นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ฉบับนี้เป็นส่วนหนึ่งของกรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์โดยรวมของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร และให้มีผลบังคับใช้กับหน่วยงานภายใน สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร บุคลากร หรือบุคคลภายนอกที่เกี่ยวข้องซึ่งเข้าถึง หรือใช้งานระบบสารสนเทศ เครือข่าย อุปกรณ์ และข้อมูลของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดกรอบการกำกับดูแล หลักการ และข้อกำหนดขั้นต่ำของการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุมคามทางไซเบอร์ รวมถึงเพื่อเสริมสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร ลดความเสี่ยงจากเหตุการณ์ที่อาจกระทบต่อภารกิจการให้บริการสาธารณะ และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย ทั้งนี้ นโยบายต้องสื่อสารอย่างทั่วถึงและนำไปปฏิบัติได้จริง เพื่อคุ้มครองหน่วยงานจากเหตุการณ์ที่เกิดจากความไม่ตั้งใจและการโจมตีโดยเจตนา รวมถึงให้สอดคล้องกับกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

๑.๒ วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดทิศทางและข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร เพื่อคุ้มครองระบบสารสนเทศ ข้อมูลและบริการ ที่สนับสนุนภารกิจด้านการศึกษาโดยมีวัตถุประสงค์ ดังนี้

๑.๒.๑ เพื่อคุ้มครองข้อมูลและบริการของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ให้คงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและความพร้อมใช้งานตลอดวงจรชีวิตของข้อมูล

๑.๒.๒ เพื่อกำหนดมาตรการให้การป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุมคามทางไซเบอร์ ลดโอกาสเกิดเหตุและลดผลกระทบต่อภารกิจ และการให้บริการสาธารณะ

๑.๒.๓ เพื่อเสริมสร้างบทบาท หน้าที่ ความรับผิดชอบ และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรและผู้เกี่ยวข้อง

๑.๒.๔ เพื่อให้การดำเนินงานสอดคล้องกับกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้องของหน่วยงานของรัฐ รวมถึงการประสานงานและการรายงาน

๑.๓ ขอบเขต

นโยบายฉบับนี้ให้ใช้บังคับกับสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร รวมถึงผู้บริหาร ข้าราชการ พนักงานราชการ เจ้าหน้าที่ ลูกจ้าง ผู้รับจ้าง ตลอดจนบุคคลภายนอกหรือคู่สัญญาที่มีการแลกเปลี่ยนข้อมูล ให้บริการ รับบริการ หรือเข้าถึง และใช้งานระบบและเทคโนโลยีของหน่วยงานตามข้อตกลงหรือสัญญา

นโยบายฉบับนี้ครอบคลุมทรัพย์สินทั้งหมดของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ไม่ว่าทรัพย์สินดังกล่าวจะตั้งอยู่ หรือถูกโฮสต์ ณ สถานที่ของหน่วยงาน ณ สถานที่ของผู้ให้บริการภายนอก ศูนย์ข้อมูล หรือสถานที่อื่นใดที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อย ดังนี้

๑.๓.๑ ทรัพย์สินสารสนเทศ เช่น ข้อมูลผู้เรียน ข้อมูลบุคลากร ข้อมูลการบริหาร ฐานข้อมูลเอกสารและสื่อบันทึกข้อมูล

๑.๓.๒ ทรัพย์สินซอฟต์แวร์ เช่น ระบบสารสนเทศเพื่อการศึกษา แอปพลิเคชัน โปรแกรมและซอร์สโค้ดที่หน่วยงานพัฒนา หรือว่าจ้างพัฒนา

๑.๓.๓ ทรัพย์สินทางกายภาพ เช่น อาคารสถานที่ ห้องแม่ข่าย อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์จัดเก็บข้อมูล

๑.๓.๔ บริการที่สนับสนุนการดำเนินงาน เช่น ไฟฟ้า ระบบสื่อสาร เครือข่ายอินเทอร์เน็ต บริการคลาวด์ และบริการเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

๑.๔ การทบทวนและการปรับปรุง

นโยบายฉบับนี้ต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง และ/หรือเมื่อมีการเปลี่ยนแปลงสาระสำคัญ เพื่อให้มีความเหมาะสมและมีประสิทธิผลอย่างต่อเนื่อง ทั้งนี้ การปรับปรุงหรือมีการเปลี่ยนแปลงต่อไปนี้ ซึ่งอาจส่งผลต่อการออกแบบและเนื้อหาของนโยบายต้องนำมาพิจารณาประกอบ ได้แก่

๑.๔.๑ การเปลี่ยนแปลงพันธกิจ และ/หรือวัตถุประสงค์ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร

๑.๔.๒ ประเด็นหรือภัยคุกคามที่เกิดขึ้นใหม่ แนวโน้มภัยคุมคามล่าสุด ช่องโหว่ และมาตรการตอบโต้ที่เกี่ยวข้อง

๑.๔.๓ กฎหมาย ระเบียบ ข้อกำหนด หรือคำวินิจฉัยของศาลที่เกี่ยวข้อง ซึ่งมีต่อการดำเนินงานของหน่วยงาน

๑.๕ การอ้างอิง

นโยบายฉบับนี้จัดทำให้สอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง ต่อไปนี้

๑.๕.๑ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๕.๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑.๕.๓ National Institute of Standard and Technology, Special Publication ๘๐๐-๕๓ Revision ๕, Security and Privacy Controls for Information Systems and Organizations, กันยายน ๒๐๒๐

๒. การกำกับดูแลและอำนาจหน้าที่ตามนโยบาย

๒.๑ โครงสร้างการกำกับดูแล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร กำหนดให้มีโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูล เพื่อให้การดำเนินงานเป็นไปตามนโยบายนี้อย่างเป็นเอกภาพ ตรวจสอบได้ และสอดคล้องกับภารกิจและข้อกำหนดที่เกี่ยวข้อง

๒.๒ บทบาทและความรับผิดชอบ

กำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องตามนโยบายนี้อย่างชัดเจน ครอบคลุมอย่างน้อยดังนี้

บทบาท	ความรับผิดชอบ
ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร	๑. กำหนดทิศทางและอนุมัตินโยบาย แผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลของหน่วยงาน ๒. อนุมัติกรอบบริหารความเสี่ยงระดับหน่วยงานมอบหมายกลไกกำกับดูแล ๓. จัดสรรทรัพยากรและงบประมาณให้เพียงพอตามความเสี่ยงและความสำคัญของบริการหรือข้อมูล ๔. กำกับติดตามผลการดำเนินงาน รับทราบรายงานความเสี่ยง ข้อค้นพบและสั่งการแก้ไข รวมถึงกำกับการตัดสินใจเมื่อเกิดเหตุการณ์รุนแรง/วิกฤต
รองผู้อำนวยการสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร (ดูแลกลุ่มDLICT)	๑. กำกับให้ดำเนินการตามมาตรการด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลในระบบและโครงสร้างพื้นฐานเป็นไปตามนโนบายของหน่วยงาน ๒. กำกับการดำเนินการควบคุมที่สำคัญให้มีประสิทธิผลและสามารถตรวจสอบได้ ๓. จัดสรรทรัพยากรด้านเทคโนโลยี เครื่องมือ และบุคลากรให้เพียงพอต่อการปฏิบัติงานตามภารกิจ ๔. กำกับติดตามระดับความเสี่ยงไซเบอร์ ผลการประเมิน/ตรวจประเมินและสถานการณ์แก้ไข ๕. รายงานสถานการณ์ดำเนินงาน ประเด็นสำคัญ และความเสี่ยงระดับสูงหรือระดับวิกฤตต่อผู้บริหาร
ผู้อำนวยการกลุ่มDLICT	๑. จัดทำ ทบทวน ประกาศใช้ และติดตามการปฏิบัติตามนโยบาย/มาตรฐาน/แนวปฏิบัติที่จำเป็นให้สอดคล้องกฎหมายและข้อกำหนด ๒. ดูแลทะเบียนความเสี่ยงให้เป็นปัจจุบัน ระบุเจ้าของความเสี่ยง มาตรการจัดการ และติดตามสถานะการดำเนินการ ๓. กำหนดช่องทางแจ้งเหตุ ระดับความรุนแรง และดำเนินการรับแจ้ง คัดกรองยกระดับไปยังผู้เกี่ยวข้องตามกรอบเวลา ๔. ให้ความเห็นด้านความมั่นคงปลอดภัยก่อนขึ้นใช้งานจริงสำหรับการเปลี่ยนแปลงระบบ/การเชื่อต่อภายนอกที่สำคัญ ๕. รายงานสถานะความเสี่ยง เหตุการณ์ต่อผู้บังคับบัญชาตามรอบและจัดเก็บหลักฐานให้ตรวจสอบย้อนกลับได้

บทบาท	ความรับผิดชอบ
ผู้ดูแลระบบ/ผู้ดูแลเครือข่าย/ผู้ดูแลฐานข้อมูล (เจ้าหน้าที่รับผิดชอบดูระบบที่เกี่ยวข้อง)	๑. กำกับดูแลให้ระบบ/โครงการพื้นฐาน/ฐานข้อมูลในความรับผิดชอบมีความมั่นคงปลอดภัย สอดคล้องกับนโยบาย มาตรฐาน และแนวปฏิบัติของหน่วยงาน ๒. อนุมัติและกำกับการกำหนดสิทธิ์การเข้าถึงตามหลักเท่าที่จำเป็นต่อหน้าที่และจำเป็นต้องรู้ โดยร่วมกับเจ้าของข้อมูล/เจ้าของระบบและทบทวนสิทธิ์ตามรอบที่กำหนด ๓. กำกับการกำหนดค่าเริ่มต้นด้านความมั่นคงปลอดภัยและการตั้งค่าควบคุมด้านความมั่นคงปลอดภัยที่เกี่ยวข้องให้คงสภาพตามมาตรฐาน ๔. ติดตามการจัดการช่องโหว่และแพตช์ รวมถึงการสำรองข้อมูล/ระบบและการกู้คืน ให้เป็นไปตามแผนและรอบเวลาที่กำหนด ๕. ดำเนินการติดตั้งและตั้งค่า ระบบ เครือข่าย ฐานข้อมูลตาม Secure Baseline และมาตรฐานของหน่วยงาน รวมถึงปิดหรือจำกัดบริการที่ไม่จำเป็น และเปิดใช้การตั้งค่าความมั่นคงปลอดภัยที่กำหนด ๖. ดำเนินการเปลี่ยนแปลงระบบตามกระบวนการบริหารเปลี่ยนแปลงได้รับอนุมัติ รวมถึงการประเมินผลกระทบ การย้อนกลับ และการบันทึกหลักฐาน ๗. ดำเนินการบำรุงรักษาความมั่นคงปลอดภัยและติดตามการบันทึกเหตุการณ์/เฝ้าระวัง ให้เป็นไปตามแผนที่เกี่ยวข้อง พร้อมเก็บรักษาบันทึกตามระยะเวลาที่กำหนด ๘. เฝ้าระวัง ตรวจพบ และรายงานเหตุผิดปกติ/เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านช่องทางที่หน่วยงานกำหนด และให้ความร่วมมือในการตอบสนองเหตุการณ์ตามแผนตอบสนองภัยคุมคามทางไซเบอร์
ผู้ดูแลผู้ให้บริการภายนอก	๑. กำกับดูแลความสัมพันธ์กับผู้ให้บริการภายนอกให้เป็นไปตามนโยบายของหน่วยงานและข้อกำหนดตามสัญญา ๒. ประสานการประเมินความเสี่ยงของผู้ให้บริการภายนอกก่อนเริ่มให้บริการและทบทวนตามระยะเวลาที่กำหนด ๓. กำกับการจัดการสิทธิ์การเข้าถึงของผู้ให้บริการภายนอกให้เหมาะสมและจำเป็นต่อการปฏิบัติงาน ๔. ประสานการจัดเหตุการณ์ที่เกี่ยวข้องกับผู้ให้บริการภายนอกให้เป็นไปตามกระบวนการ ช่องทาง และกรอบเวลาที่กำหนด
หน่วยตรวจสอบภายใน	๑. ตรวจประเมินความเพียงพอและประสิทธิผลของการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลตามนโยบาย มาตรฐาน และข้อกำกับที่เกี่ยวข้อง โดยยึดหลักความเป็นอิสระและตรวจสอบได้ ๒. จัดทำรายงานผลการตรวจประเมิน ข้อค้นพบ และข้อเสนอแนะต่อผู้บริหาร/คณะกรรมการกำกับ พร้อมติดตามความคืบหน้าการแก้ไขของแผนปรับปรุงจนปิดประเด็นตามกำหนด ๓. ตรวจสอบความครบถ้วนของเอกสารและหลักฐาน และความสอดคล้องของกระบวนการ เช่น การบริหารความเสี่ยง การจัดการข้อยกเว้น การจัดการเหตุการณ์ และการทดสอบแผนความต่อเนื่อง/แผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์

บทบาท	ความรับผิดชอบ
	๔. ประสานการตรวจสอบร่วม/การตรวจจากหน่วยงานภายนอกตามที่เกี่ยวข้อง และสนับสนุนให้หน่วยงานปรับปรุงกระบวนการควบคุมอย่างต่อเนื่อง
ผู้ประสานงานเหตุความมั่นคงปลอดภัย	๑. ทำหน้าที่เป็นจุดประสานงานหลักระหว่างสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร และสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในการรับแจ้งเหตุ เปิดบันทึกเหตุการณ์ และจัดเก็บข้อมูลเหตุการณ์ให้ครบถ้วนตามแบบฟอร์ม/ระบบที่หน่วยงานกำหนด พร้อมทั้งติดตามและปรับปรุงข้อมูลให้เป็นปัจจุบัน ๒. ประสานการควบคุมสถานการณ์และการสื่อสารระหว่างเหตุการณ์ติดตามความคืบหน้าการดำเนินงาน และสนับสนุนการประสานการติดสินใจเพื่อจำกัดผลกระทบ โดยให้การสื่อสารเป็นไปอย่างเป็นทางการ ปลอดภัย โดยให้การสื่อสารเป็นไปอย่างเป็นทางการ ปลอดภัย และสอดคล้องกับการจัดชั้นความลับของข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล ๓. รวบรวมและจัดการหลักฐานและบันทึกที่เกี่ยวข้อง จัดทำรายงานสถานการณ์และสรุปผลการดำเนินการ รวมทั้งประสานการกู้คืนบริการตามแผนความต่อเนื่อง/แผนกู้คืน และการทบทวนหลังเหตุการณ์เพื่อปรับปรุงกระบวนการและติดตามการแก้ไขจนเสร็จตามที่กำหนด ๔. ติดตามการจัดการช่องโหว่และแพตช์ รวมถึงการสำรองข้อมูล/ระบบและการกู้คืน ให้เป็นไปตามแผนและรอบเวลาที่กำหนด
บุคลากรทุกคน/ผู้ใช้งาน	๑. ปฏิบัติตามนโยบาย มาตรฐาน และกฎการใช้งานระบบของหน่วยงาน รวมถึงใช้ระบบและข้อมูล ๒. เข้ารับการอบรม ทดสอบความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลตามที่กำหนด ๓. ปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยในการทำงานประจำวัน ๔. แจ้งเหตุผิดปกติหรือเหตุการณ์ต้องสงสัยด้านความมั่นคงปลอดภัย/การละเมิดข้อมูลโดยทันทีผ่านช่องทางที่กำหนด และให้ความร่วมมือในการตอบสนอง

๒.๓ กลไกการบริหารความเสี่ยงและการควบคุมภายใน

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องจัดให้มีกลไกการบริหารความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างเป็นระบบ โดยต้องดำเนินการระบุ ประเมิน จัดการ และติดตามความเสี่ยงอย่างต่อเนื่อง รวมทั้งกำหนดมาตรการควบคุมที่เหมาะสมตามระดับความเสี่ยง ทั้งนี้ ต้องมีการอนุมัติความเสี่ยงคงเหลือ การจัดเก็บหลักฐานประกอบ และการทบทวนผลตามรอบระยะเวลาที่กำหนด

๒.๔ การกำกับดูแลผู้ให้บริการภายนอก

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องกำกับดูแลผู้ให้บริการภายนอกหรือคู่สัญญาที่เข้าถึง ประมวลผล หรือโฮสต์ข้อมูลและระบบของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร โดยกำหนดหลักเกณฑ์การคัดเลือกและการประเมินความเสี่ยง กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลไว้ในสัญญา ควบคุมสิทธิการเข้าถึงตามความจำเป็นและติดตามตรวจสอบการปฏิบัติตามอย่างสม่ำเสมอ ทั้งนี้ ต้องกำหนดให้ผู้ให้บริการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและปฏิบัติตามมาตรการที่สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร กำหนด

๒.๕ การปฏิบัติตามนโยบาย การตรวจสอบ และการรายงานผล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องจัดให้มีการติดตามและตรวจสอบการปฏิบัติตามนโยบายและมาตรการที่เกี่ยวข้องอย่างต่อเนื่อง รวมถึงการประเมินผลและการตรวจสอบภายในหรือภายนอกตามความจำเป็น ทั้งนี้ ต้องกำหนดช่องทางและรอบระยะเวลาการรายงานผลต่อผู้บริหาร พร้อมจัดทำและเก็บรักษาหลักฐาน เพื่อสนับสนุนการตรวจสอบและการปรับปรุงแก้ไขอย่างเหมาะสม

๒.๖ ข้อยกเว้นและการยอมรับความเสี่ยง

การขอข้อยกเว้นจากการปฏิบัติตามนโยบายต้องจัดทำเป็นลายลักษณ์อักษร และอย่างน้อยต้องระบุเหตุผลความจำเป็น ผลการประเมินความเสี่ยงและผลกระทบ รวมถึงมาตรการควบคุมทดแทนและแผนเยียวยา โดยให้เสนอเพื่อพิจารณาอนุมัติตามสายบังคับบัญชาที่หน่วยงานกำหนด ร่วมกับเจ้าของระบบหรือเจ้าของข้อมูล และผู้เกี่ยวข้องที่จำเป็น ทั้งนี้ ข้อยกเว้นต้องกำหนดระยะเวลามีผลและสิ้นสุดไว้อย่างชัดเจน และต้องทบทวนก่อนครบกำหนด

ทั้งนี้ที่มีการละเว้นการปฏิบัติโดยมิได้รับอนุมัติอย่างเป็นทางการ ให้ถือเป็นการไม่ปฏิบัติตามข้อกำหนด (Noncompliance) และให้ดำเนินการตามระเบียบและมาตรการบังคับใช้ของหน่วยงานต่อไป

๒.๗ การบังคับใช้บทลงโทษ

บุคลากรทุกประเภทต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศ คำสั่ง และนโยบายของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงต้องให้ความร่วมมือและปฏิบัติตามคำสั่งของผู้บังคับบัญชาที่ชอบด้วยกฎหมาย หากมีการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการควบคุมที่กำหนด ให้ดำเนินการตามกระบวนการตรวจสอบข้อเท็จจริงของหน่วยงาน และอาจถูกดำเนินการตามความเหมาะสม

๓. ข้อกำหนดนโยบาย

เพื่อกำหนดกรอบและข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศสำหรับ สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร เพื่อให้การบริหารจัดการและการปฏิบัติงานด้านเทคโนโลยีสารเทศเป็นไปอย่างเป็นระบบ มีความปลอดภัยและสอดคล้องกับพันธกรณีตามกฎหมาย ระเบียบ ข้อบังคับและข้อกำหนดที่เกี่ยวข้อง โดยกำหนดแนวทางการดำเนินงานให้ครอบคลุมตามด้านของ NIST Cybersecurity Framework ดังนี้

๓.๑ การระบุ (Identify)

๓.๑.๑ การกำกับดูแลและการกำกับติดตาม

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องจัดให้มีการกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อบริหารจัดการความเสี่ยงและปฏิบัติให้เป็นไปตามพันธกรณีที่เกี่ยวข้องตามกฎหมาย ระเบียบข้อบังคับ หรือข้อกำหนดที่ใช้บังคับกำหนดไว้ ทั้งนี้ต้องกำหนดและมอบหมายความรับผิดชอบต้านการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศและปฏิบัติตามข้อกำหนดให้ชัดเจน

๓.๑.๒ การบริหารจัดการความเสี่ยง

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องดำเนินการระบุ ประเมินและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อคุ้มครองการให้บริการและข้อมูลสารสนเทศของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ทั้งนี้ ก่อนอนุญาตให้บุคคลภายนอกเข้าถึงระบบหรือข้อมูลของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องพิจารณาความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดจากบุคคลภายนอกดังกล่าวประกอบการตัดสินใจ

๓.๑.๓ การบริหารความเสี่ยงจากผู้ให้บริการภายนอก

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องระบุ และบริหารความเสี่ยงจากผู้ให้บริการภายนอก โดยดำเนินการประเมินความมั่นคงปลอดภัยก่อนเริ่มว่าจ้าง/ใช้งาน และทบทวนเป็นระยะเวลาที่กำหนด

๓.๑.๔ การบริหารจัดการทรัพย์สินและการกำหนดค่า

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องจัดและดูแลให้มีทะเบียนทรัพย์สินของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร และต้องทำให้มั่นใจว่าทรัพย์สินดังกล่าวได้รับการกำหนดค่าและบำรุงรักษาอย่างเหมาะสมเพื่อคุ้มครองสารสนเทศ

๓.๒ การป้องกัน (Protect)

๓.๒.๑ การจำแนกประเภทข้อมูลและการจัดการข้อมูล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องดำเนินการให้มีการจำแนกประเภทข้อมูล และจัดให้มีการบริหารจัดการข้อมูลให้สอดคล้องกับระดับความอ่อนไหวของข้อมูลแต่ละประเภท ทั้งนี้ ต้องจัดให้มีมาตรการคุ้มครองข้อมูล เพื่อป้องกันการเข้าถึง การเปิดเผย การเปลี่ยนแปลงแก้ไข หรือการสูญหายโดยมิได้รับอนุญาต และให้เป็นไปตามแนวปฏิบัติที่เกี่ยวข้องเพื่อให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำหรับสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร

๓.๒.๒ ข้อมูลส่วนบุคคล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องคุ้มครองข้อมูลส่วนบุคคลจากการเข้าถึง การใช้ หรือการเปิดเผยโดยไม่ได้รับอนุญาต ทั้งนี้ ข้อมูลส่วนบุคคลต้องถูกนำไปใช้เฉพาะเพื่อวัตถุประสงค์ของภารกิจหน่วยงานที่ได้รับอนุญาตเท่านั้น

๓.๒.๓ การบริหารจัดการตัวตนและสิทธิ์การเข้าถึง

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องอนุญาตให้เข้าถึงระบบและข้อมูลได้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น ทั้งนี้ การให้สิทธิ์เข้าถึงต้องได้รับอนุมัติก่อนดำเนินการจัดสรรสิทธิ์ และต้องเพิกถอนหรือยกเลิกสิทธิ์เมื่อไม่มีความจำเป็นต้องใช้สิทธิ์ดังกล่าวต่อไป

๓.๒.๔ ความมั่นคงปลอดภัยเครือข่าย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องคุ้มครองเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาตและจากกิจกรรมที่เป็นอันตราย ทั้งนี้ การเข้าถึงเครือข่ายต้องถูกควบคุมอย่างเหมาะสม เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

๓.๒.๕ ความมั่นคงปลอดภัยอุปกรณ์ปลายทาง

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องคุ้มครองอุปกรณ์ปลายทางจากการถูกโจมตีและจากการใช้งานโดยไม่ได้รับอนุญาต ทั้งนี้ ต้องมีการบริหารจัดการอุปกรณ์ปลายทางอย่างเป็นระบบ เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

๓.๒.๖ ความมั่นคงปลอดภัยระบบคลาวด์

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องคุ้มครองระบบและข้อมูลที่โฮสต์อยู่บนระบบคลาวด์จากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานโดยมิชอบ และการสูญหาย ทั้งนี้ ให้ใช้บริการคลาวด์ได้เฉพาะบริการที่ได้รับการอนุมัติให้ใช้เพื่อการดำเนินงานตามภารกิจของหน่วยงานนั้น

๓.๒.๗ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องคุ้มครองสถานที่ อุปกรณ์และโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานจากการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และภัยคุกคามจากสภาพแวดล้อม ทั้งนี้ ต้องควบคุมการเข้าถึงทางกายภาพต่อพื้นที่ที่มีทรัพย์สินสารสนเทศให้อยู่ภายใต้มาตรการที่เหมาะสม

๓.๒.๘ การสร้างความตระหนักและการฝึกอบรมบุคลากร

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องทำให้มั่นใจว่าบุคลากรมีความเข้าใจและปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ ต้องจัดให้มีการฝึกอบรมและสร้างความตระหนักด้านความมั่นคลปลอดภัยสารสนเทศแก่บุคลากร

๓.๒.๙ การพัฒนาและการจัดหาเทคโนโลยี

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องพิจารณาข้อกำหนดด้านความมั่นคลปลอดภัยเมื่อมีการจัดหา พัฒนา หรือปรับเปลี่ยนเทคโนโลยี ทั้งนี้ เทคโนโลยีที่จะนำไปใช้งานเพื่อสนับสนุนการดำเนินงานของภารกิจต้องได้รับการอนุมัติให้ใช้งานก่อนจึงจะนำไปติดตั้งหรือปรับใช้ได้

๓.๒.๑๐ วิศวกรรมและสถาปัตยกรรมที่มั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องออกแบบและพัฒนาระบบโดยคำนึงถึงประเด็นด้านความมั่นคงปลอดภัยเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ทั้งนี้ ต้องพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัย เมื่อจัดทำหรือปรับเปลี่ยนสถาปัตยกรรมของระบบ

๓.๒.๑๑ การพัฒนาแอปพลิเคชันอย่างมั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องดำเนินการพัฒนาและบำรุงรักษาแอปพลิเคชันตามแนวทางและมาตรฐานการพัฒนาแอปพลิเคชันอย่างมั่นคงปลอดภัย เช่น OWASP เพื่อช่วยลดช่องโหว่และความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศ และเพิ่มระดับความปลอดภัยของระบบสารสนเทศ

๓.๓ การตรวจจับ (Detection)

๓.๓.๑ การตรวจสอบกิจกรรมความมั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องจัดให้มีการบันทึกกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อสนับสนุนความรับผิดชอบและการตรวจสอบย้อนกลับ ทั้งนี้ บันทึกการตรวจสอบต้องได้รับการคุ้มครองจากการเข้าถึงหรือการเปลี่ยนแปลงแก้ไข โดยไม่ได้รับอนุญาต

๓.๓.๒ การบริหารจัดการภัยคุกคาม

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องระบุและดำเนินการจัดการภัยคุกคามที่อาจส่งผลกระทบต่อสารสนเทศและบริการของสำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ทั้งนี้ ต้องนำข้อมูลข่าวกรองด้านภัยคุกคามมาใช้ เพื่อลดโอกาสเกิดและลดผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัย

๓.๓.๓ การบริหารจัดการช่องโหว่และการเยียวยา/การแก้ไข

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องระบุและดำเนินงานแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยอย่างทันท่วงที ทั้งนี้ การดำเนินการแก้ไขและการเยียวยาต้องจัดลำดับความสำคัญ เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

๓.๔ การตอบสนอง (Respond)

๓.๔.๑ การวางแผน การแจ้งเหตุ และการประสานงานในการตอบสนองเหตุการณ์

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องจัดให้มีแผนและขั้นตอนการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ครอบคลุมการจำแนกประเภทเหตุการณ์ ระดับความรุนแรง การยกระดับ และการกำหนดบทบาทหน้าที่ของผู้เกี่ยวข้อง รวมถึงต้องกำหนดช่องทางและกระบวนการแจ้งเหตุ/รายงานเหตุ เพื่อให้การสื่อสารเป็นไปอย่างรวดเร็ว

๓.๔.๒ การบริหารจัดการภัยคุกคาม

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องดำเนินการเยียวยา/แก้ไขตามลำดับความสำคัญโดยคำนึงถึงความเสี่ยงและผลกระทบ เพื่อจำกัดความเสียหายและทำให้บริการที่สำคัญกลับสู่ภาวะปกติโดยเร็ว ทั้งนี้ ภายหลังเหตุการณ์ต้องมีการสรุปบทเรียนและปรับปรุงแผน กระบวนการ มาตรการควบคุม และเอกสารที่เกี่ยวข้องอย่างต่อเนื่อง

๓.๕ การฟื้นฟู (Recover)

๓.๕.๑ การตอบสนองเหตุการณ์และความต่อเนื่องในการดำเนินงาน

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร ต้องคงไว้ซึ่งความสามารถในการกู้คืนบริการที่จำเป็นและคุ้มครองสารสนเทศได้อย่างต่อเนื่อง โดยจัดให้มีแผนความต่อเนื่องในการดำเนินงานและแผนกู้คืนระบบ/บริการที่เหมาะสมกับภารกิจและความสำคัญของบริการ

สำนักงานเขตพื้นที่การศึกษาประถมศึกษากรุงเทพมหานคร