ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2

ลำดับชั้นเอกสาร	เอกสารภายใน
วันที่มีผลบังคับใช้	2569-03-13
เวอร์ชันเอกสาร	0.1
เจ้าของเอกสาร	กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร

การควบคุมเอกสาร และการอนุมัติ

ข้อมูลการควบคุมเอกสาร

ชื่อเอกสาร	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2
รหัสเอกสาร	
รุ่น	V0.1
ลำดับชั้น	เอกสารภายใน
สถานะ	ฉบับอนุมัติ
วันที่มีผลบังคับใช้	2569-03-13
ความถี่ของการทบทวน	รายปี

การอนุมัติและมอบอำนาจ

เอกสารฉบับนี้ได้รับการอนุมัติอย่างเป็นทางการและได้รับอนุญาตให้ใช้งานภายในหน่วยงาน

บทบาท	ชื่อ / ตำแหน่ง	ลงนาม	วันที่
ผู้จัดทำ	นายภัทรชัย มุกดาสนิท		18 มี.ค. 2569
ผู้ทบทวน	นายสยาม นำเจริญ		18 มี.ค. 69
ผู้อนุมัติ	นายอภิลักษณ์ ธีราลักษณ์สกุล		20 มี.ค. 69

ประวัติการเปลี่ยนแปลง

เวอร์ชัน	วันที่	รายละเอียดการเปลี่ยนแปลง
0.1	2569-03-13	ร่างนโยบาย
1.0	2569-03-18	อนุมัติการใช้นโยบาย

สารบัญ

หน้า

1. บททั่วไป

1.1 หลักการ

นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ฉบับนี้เป็นส่วนหนึ่งของกรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์โดยรวมของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยอง เขต 2 และให้มีผลบังคับใช้กับหน่วยงานภายในสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 บุคลากร หรือบุคคลภายนอกที่เกี่ยวข้องซึ่งเข้า ถึงหรือใช้งานระบบสารสนเทศเครือข่าย อุปกรณ์ และข้อมูลของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยอง เขต 2

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดกรอบการกำกับดูแล หลักการ และข้อกำหนดขั้นต่ำของการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคามทางไซเบอร์ รวมถึงเพื่อเสริมสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร ลดความเสี่ยงจากเหตุการณ์ที่อาจกระทบต่อภารกิจการให้บริการสาธารณะ และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย ทั้งนี้ นโยบายต้องสื่อสารอย่างทั่วถึงและนำไปปฏิบัติได้จริง เพื่อคุ้มครองหน่วยงานจากเหตุการณ์ที่เกิดจากความไม่ตั้งใจและการโจมตีโดยเจตนรวมถึงให้สอดคล้องกับกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

1.2 วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดทิศทางและข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยอง เขต 2 เพื่อคุ้มครองระบบสารสนเทศ ข้อมูล และบริการที่สนับสนุนภารกิจด้านการศึกษา
โดยมีวัตถุประสงค์ ดังนี้

1.2.1 เพื่อคุ้มครองข้อมูลและบริการของสานักงานเขตพื้นที่การศึกษาประถมศึกษาระยอง เขต 2 ให้คงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและความพร้อมใช้งานตลอดวงจรชีวิตของข้อมูล

1.2.2 เพื่อกำหนดมาตรการในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคามทางไซเบอร์ ลดโอกาสเกิดเหตุและลดผลกระทบต่อภารกิจ และการให้บริการสาธารณะ

1.2.3 เพื่อเสริมสร้างบทบาท หน้าที่ ความรับผิดชอบ และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรและผู้เกี่ยวข้อง

1.2.4 เพื่อให้การดำเนินงานสอดคล้องกับกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติที่เกี่ยว

1.3 ขอบเขต

นโยบายฉบับนี้ให้ใช้บังคับกับสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 รวมถึงผู้บริหาร ข้าราชการ พนักงานราชการ เจ้าหน้าที่ลูกจ้าง ผู้รับจ้าง ตลอดจนบุคคลภายนอกหรือคู่สัญญาที่มีการแลกเปลี่ยนข้อมูล ให้บริการ รับบริการหรือเข้าถึง และใช้งานระบบและเทคโนโลยีของหน่วยงานตามข้อตกลงหรือสัญญา

นโยบายฉบับนี้ครอบคลุมทรัพย์สินทั้งหมดของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยอง เขต 2 ไม่ว่าทรัพย์สินดังกล่าวจะตั้งอยู่หรือถูกโฮสต์ ณ สถานที่ของหน่วยงาน หรืออยู่ ณ สถานที่ของผู้ให้บริการภายนอก ศูนย์ข้อมูล หรือสถานที่อื่นใดที่เกี่ยวข้อง โดยครอบคลุมอย่างน้อย ดังนี้

1.3.1 ทรัพย์สินสารสนเทศ เช่น ข้อมูลผู้เรียน ข้อมูลบุคลากร ข้อมูลการบริหาร ฐานข้อมูล เอกสาร และสื่อบันทึกข้อมูล

1.3.2 ทรัพย์สินซอฟต์แวร์ เช่น ระบบสารสนเทศเพื่อการศึกษา แอปพลิเคชัน โปรแกรม และซอร์สโค้ดที่หน่วยงานพัฒนา หรือว่าจ้างพัฒนา

1.3.3 ทรัพย์สินทางกายภาพ เช่น อาคารสถานที่ ห้องแม่ข่าย อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์จัดเก็บข้อมูล

1.3.4 บริการที่สนับสนุนการดำเนินงาน เช่น ไฟฟ้า ระบบสื่อสาร เครือข่ายอินเทอร์เน็ต บริการคลาวด์ และบริการเทคโนโลยีสารสนเทศอื่นที่เกี่ยวข้อง

1.4 การทบทวนและการปรับปรุง

นโยบายฉบับนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และ/หรือเมื่อมีการเปลี่ยนแปลงสาระสำคัญ เพื่อให้มีความเหมาะสมและมีประสิทธิผลอย่างต่อเนื่อง ทั้งนี้ การปรับปรุงหรือการเปลี่ยนแปลงต่อไปนี้ ซึ่งอาจส่งผลต่อการออกแบบและเนื้อหาของนโยบายต้องนำมาพิจารณาประกอบ ได้แก่

1.4.1 การเปลี่ยนแปลงพันธกิจ และ/หรือวัตถุประสงค์ของสานักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2

1.4.2 ประเด็นหรือภัยคุกคามที่เกิดขึ้นใหม่ แนวโน้มภัยคุกคามล่าสุด ช่องโหว่ และมาตรการตอบโต้ที่เกี่ยวข้อง

1.4.3 กฎหมาย ระเบียบ ข้อกำหนด หรือคำวินิจฉัยของศาลที่เกี่ยวข้อง ซึ่งมีผลต่อการดำเนินงานของหน่วยงาน

1.5 การอ้างอิง

นโยบายฉบับนี้จัดทำให้สอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง ต่อไปนี้

1.5.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.5.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.5.3 National Institute of Standard and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, กันยายน 2020

2. การกำกับดูแลและอำนาจหน้าที่ตามนโยบาย

2.1 โครงสร้างการกำกับดูแล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 กำหนดให้มีโครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูล เพื่อให้การดำเนินงานเป็นไปตามนโยบายนี้อย่างเป็นเอกภาพ ตรวจสอบได้ และ สอดคล้องกับภารกิจและข้อกำหนดที่เกี่ยวข้อง

2.2 บทบาทและความรับผิดชอบ

กำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องตามนโยบายนี้อย่างชัดเจน ครอบคลุมอย่างน้อย ดังนี้

บทบาท	ความรับผิดชอบ
ผู้บริหารระดับสูง (ผอ.เขต)	1. กำหนดทิศทางและอนุมัตินโยบาย แผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลของหน่วยงาน 2. อนุมัติกรอบบริหารความเสี่ยงระดับหน่วยงานมอบหมายกลไกกำกับดูแล 3. จัดสรรทรัพยากรและงบประมาณให้เพียงพอตามความเสี่ยงและความสำคัญของบริการหรือข้อมูล 4. กำกับติดตามผลการดำเนินงาน รับทราบรายงานความเสี่ยง ข้อค้นพบ และสั่งการแก้ไข รวมถึงกำกับการตัดสินใจเมื่อเกิดเหตุการณ์รุนแรง/วิกฤต
ผู้บริหารเทคโนโลยีสารสนเทศ (รอง ผอ.เขต ที่ดูแลกลุ่มงาน DLICT)	1. กำกับให้ดำเนินการตามมาตรการด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลในระบบและโครงสร้างพื้นฐานเป็นไปตามนโยบายของหน่วยงาน 2. กำกับการดำเนินการควบคุมที่สำคัญให้มีประสิทธิผลและสามารถตรวจสอบได้ 3. จัดสรรและบริหารทรัพยากรด้านเทคโนโลยี เครื่องมือ และบุคลากรให้เพียงพอต่อการปฏิบัติงานตามภารกิจ 4. กำกับติดตามระดับความเสี่ยงไซเบอร์ ผลการประเมิน/ตรวจประเมิน และสถานะการแก้ไข 5. รายงานสถานะการดำเนินงาน ประเด็นสำคัญ และความเสี่ยงระดับสูงหรือระดับวิกฤตต่อผู้บริหาร
ผู้ดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (ผอ.กลุ่มงาน DLICT หรือนักวิชาการคอมพิวเตอร์)	1. จัดทำ ทบทวน ประกาศใช้ และติดตามการปฏิบัติตามนโยบาย/มาตรฐาน/แนวปฏิบัติที่จำเป็นให้สอดคล้องกฎหมายและข้อกำหนด 2. ดูแลทะเบียนความเสี่ยงให้เป็นปัจจุบัน ระบุเจ้าของความเสี่ยง มาตรการจัดการ และติดตามสถานะการดำเนินการ 3. กำหนดช่องทางแจ้งเหตุ ระดับความรุนแรง และดำเนินการรับแจ้ง คัดกรอง ยกระดับไปยังผู้เกี่ยวข้องตามกรอบเวลา

บทบาท	ความรับผิดชอบ
	4. ให้ความเห็นด้านความมั่นคงปลอดภัยก่อนขึ้นใช้งานจริงสำหรับการเปลี่ยนแปลงระบบ/การเชื่อมต่อภายนอกที่สำคัญ 5. รายงานสถานะความเสี่ยง เหตุการณ์ต่อผู้บังคับบัญชาตามรอบ และจัดเก็บหลักฐานให้ตรวจสอบย้อนกลับได้
ผู้ดูแลระบบ/ผู้ดูแลเครือข่าย/ผู้ดูแลฐานข้อมูล (เจ้าหน้าที่รับผิดชอบดูระบบที่เกี่ยวข้อง)	1. กำกับดูแลให้ระบบ/โครงสร้างพื้นฐาน/ฐานข้อมูลในความรับผิดชอบมีความมั่นคงปลอดภัย สอดคล้องนโยบาย มาตรฐาน และแนวปฏิบัติของหน่วยงาน 2. อนุมัติและกำกับการกำหนดสิทธิ์การเข้าถึงตามหลักเท่าที่จำเป็นต่อหน้าที่และจำเป็นต้องรู้ โดยร่วมกับเจ้าของข้อมูล/เจ้าของระบบ และทบทวนสิทธิ์ตามรอบที่กำหนด 3. กำกับการกำหนดค่าเริ่มต้นด้านความมั่นคงปลอดภัยและการตั้งค่าควบคุมด้านความมั่นคงปลอดภัยที่เกี่ยวข้องให้คงสภาพตามมาตรฐาน 4. ติดตามการจัดการช่องโหว่และแพตช์ รวมถึงการสำรองข้อมูล/ระบบและการกู้คืน ให้เป็นไปตามแผนและรอบเวลาที่กำหนด 5. ดำเนินการติดตั้งและตั้งค่า ระบบ เครือข่าย ฐานข้อมูลตาม Secure Baseline และมาตรฐานของหน่วยงาน รวมถึงปิดหรือจำกัดบริการที่ไม่จำเป็น และเปิดใช้การตั้งค่าความมั่นคงปลอดภัยที่กำหนด 6. ดำเนินการเปลี่ยนแปลงระบบตามกระบวนการบริหารการเปลี่ยนแปลงได้รับอนุมัติ รวมถึงการประเมินผลกระทบ การย้อนกลับ และการบันทึกหลักฐาน 7. ดำเนินการบำรุงรักษาความมั่นคงปลอดภัยและติดตามการบันทึกเหตุการณ์/เฝ้าระวัง ให้เป็นไปตามแผนที่เกี่ยวข้อง พร้อมเก็บรักษาบันทึกตามระยะเวลาที่กำหนด 8. เฝ้าระวัง ตรวจพบ และรายงานเหตุผิดปกติ/เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านช่องทางที่หน่วยงานกำหนด และให้ความร่วมมือในการตอบสนองเหตุการณ์ตามแผนตอบสนองภัยคุกคามทางไซเบอร์
ผู้ดูแลผู้ให้บริการภายนอก	1. กำกับดูแลความสัมพันธ์กับผู้ให้บริการภายนอกให้เป็นไปตามนโยบายของหน่วยงานและข้อกำหนดตามสัญญา 2. ประสานการประเมินความเสี่ยงของผู้ให้บริการภายนอกก่อนเริ่มให้บริการและทบทวนตามระยะเวลาที่กำหนด 3. กำกับการจัดการสิทธิ์การเข้าถึงของผู้ให้บริการภายนอกให้เหมาะสมและจำเป็นต่อการปฏิบัติงาน

บทบาท	ความรับผิดชอบ
	4. ประสานการจัดการเหตุการณ์ที่เกี่ยวข้องกับผู้ให้บริการภายนอกให้เป็นไปตามกระบวนการ ช่องทาง และกรอบเวลาที่กำหนด
หน่วยตรวจสอบภายใน	1. ตรวจประเมินความเพียงพอและประสิทธิผลของการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลตามนโยบาย มาตรฐาน และข้อกำกับที่เกี่ยวข้อง โดยยึดหลักความเป็นอิสระและตรวจสอบได้ 2. จัดทำรายงานผลการตรวจประเมิน ข้อค้นพบ และข้อเสนอแนะต่อผู้บริหาร/คณะกรรมการกำกับ พร้อมติดตามความคืบหน้าการแก้ไขของแผนปรับปรุง จนปิดประเด็นตามกำหนด 3. ทวนสอบความครบถ้วนของเอกสารและหลักฐาน และความสอดคล้องของกระบวนการ เช่น การบริหารความเสี่ยง การจัดการข้อยกเว้น การจัดการเหตุการณ์ และการทดสอบแผนความต่อเนื่อง/แผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ 4. ประสานการตรวจสอบร่วม/การตรวจจากหน่วยงานภายนอกตามที่เกี่ยวข้อง และสนับสนุนให้หน่วยงานปรับปรุงกระบวนการควบคุมอย่างต่อเนื่อง
ผู้ประสานงานเหตุความมั่นคงปลอดภัย	1. ทำหน้าที่เป็นจุดประสานงานหลักระหว่างสำนักงานเขตพื้นที่การศึกษาและสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในการรับแจ้งเหตุ เปิดบันทึกเหตุการณ์ และจัดเก็บข้อมูลเหตุการณ์ให้ครบถ้วนตามแบบฟอร์ม/ระบบที่หน่วยงานกำหนด พร้อมทั้งติดตามและปรับปรุงข้อมูลให้เป็นปัจจุบัน 2. ประสานการควบคุมสถานการณ์และการสื่อสารระหว่างเหตุการณ์ ติดตามความคืบหน้าการดำเนินงาน และสนับสนุนการประสานการตัดสินใจเพื่อจำกัดผลกระทบ โดยให้การสื่อสารเป็นไปอย่างเป็นทางการ ปลอดภัย และสอดคล้องกับการจัดชั้นความลับของข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล 3. รวบรวมและจัดการหลักฐานและบันทึกที่เกี่ยวข้อง จัดทำรายงานสถานการณ์และสรุปผลการดำเนินการ รวมทั้งประสานการกู้คืนบริการตามแผนความต่อเนื่อง/แผนกู้คืน และการทบทวนหลังเหตุการณ์เพื่อปรับปรุงกระบวนการและติดตามการแก้ไขจนแล้วเสร็จตามที่กำหนด

บทบาท	ความรับผิดชอบ
บุคลากรทุกคน/ ผู้ใช้งาน	1. ปฏิบัติตามนโยบาย มาตรฐาน และกฎการใช้งานระบบของหน่วยงาน รวมถึงใช้ระบบและข้อมูล 2. เข้ารับการอบรม ทดสอบความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลตามที่กำหนด 3. ปฏิบัติตามแนวทางด้านความปลอดภัยในการทำงานประจำวัน 4. แจ้งเหตุผิดปกติหรือเหตุการณ์ต้องสงสัยด้านความมั่นคงปลอดภัย/การละเมิดข้อมูลโดยทันทีผ่านช่องทางที่กำหนด และให้ความร่วมมือในการตอบสนอง

2.3 กลไกการบริหารความเสี่ยงและการควบคุมภายใน

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 จัดให้มีกลไกการบริหารความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างเป็นระบบ โดยต้องดำเนินการระบุ ประเมิน จัดการ และติดตาม ความเสี่ยงอย่างต่อเนื่อง รวมทั้งกำหนดมาตรการควบคุมที่เหมาะสมตามระดับความเสี่ยง ทั้งนี้ ต้องมีการอนุมัติความเสี่ยงคงเหลือ การจัดเก็บหลักฐานประกอบและการทบทวนผลตามรอบระยะเวลาที่กำหนด

2.4 การกำกับดูแลผู้ให้บริการภายนอก

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 กำกับดูแลผู้ให้บริการภายนอกหรือคู่สัญญาที่เข้าถึงประมวลผล หรือ โฮสต์ข้อมูลและระบบของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 โดยต้องกำหนดหลักเกณฑ์การคัดเลือกและการประเมิน ความเสี่ยง กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลไว้ในสัญญา ควบคุมสิทธิการเข้าถึงตาม ความจำเป็น และติดตามตรวจสอบการปฏิบัติตามอย่างสม่ำเสมอ ทั้งนี้ ต้องกำหนด ให้ผู้บริการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและปฏิบัติตามมาตรการที่สานักงานเขตพื้นที่การศึกษาประถมศึกษาระยอง เขต 2 กำหนด

2.5 การปฏิบัติตามนโยบาย การตรวจสอบ และการรายงานผล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ต้องจัดให้มีการติดตามและตรวจสอบการปฏิบัติตามนโยบายและมาตร การที่เกี่ยวข้องอย่างต่อเนื่อง รวมถึงการประเมินผลและการตรวจสอบภายในหรือภายนอกตามความจำเป็น ทั้งนี้ ต้องกำหนดช่องทางและรอบระยะเวลาการรายงานผลต่อผู้บริหาร พร้อมจัดทำและเก็บรักษาหลักฐาน เพื่อสนับสนุนการตรวจสอบและการปรับปรุงแก้ไขอย่างเหมาะสม

2.6 ข้อยกเว้นและการยอมรับความเสี่ยง

การขอข้อยกเว้นจากการปฏิบัติตามนโยบายต้องจัดทำเป็นลายลักษณ์อักษร และอย่างน้อยต้องระบุเหตุผลความจำเป็น ผลการประเมินความเสี่ยงและผลกระทบ รวมถึงมาตรการควบคุมทดแทนและแผนเยียวยา โดยให้เสนอเพื่อพิจารณาอนุมัติตามสายการบังคับบัญชาที่หน่วยงานกำหนด ร่วมกับเจ้าของระบบหรือเจ้าของข้อมูล และผู้เกี่ยวข้องที่จำเป็น ทั้งนี้ ข้อยกเว้นต้องกำหนดระยะเวลามีผลและวันสิ้นสุดไว้อย่างชัดเจน และต้องทบทวนก่อนครบกำหนด

กรณีที่มีการละเว้นการปฏิบัติโดยมิได้รับอนุมัติอย่างเป็นทางการ ให้ถือเป็นการไม่ปฏิบัติตามข้อกำหนด (Noncompliance) และให้ดำเนินการตามระเบียบและมาตรการบังคับใช้ของหน่วยงานต่อไป

2.7 **การบังคับใช้และบทลงโทษ**

บุคลากรทุกประเภทต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศ คำสั่ง และนโยบายของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงต้องให้ความร่วมมือและปฏิบัติตามคำสั่งของผู้บังคับบัญชาที่ชอบด้วย กฎหมาย หากมีการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการควบคุมที่กำหนด ให้ดำเนินการตามกระบวนการตรวจสอบข้อเท็จจริงของหน่วยงาน และอาจถูกดำเนินการตามความเหมาะสม

3. ข้อกำหนดนโยบาย

เพื่อกำหนดกรอบและข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศสำหรับสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 เพื่อให้การบริหารจัดการและการปฏิบัติงานด้านเทคโนโลยีสารสนเทศเป็นไปอย่างเป็นระบบ มีความปลอดภัย และสอดคล้องกับพันธกรณีตามกฎหมายระเบียบข้อบังคับ และข้อกำหนดที่เกี่ยวข้อง โดยกำหนดแนวทางการดำเนินงานให้ครอบคลุมตาม ด้านของ NIST Cybersecurity Framework ดังนี้

3.1 การระบุ (Identify)

3.1.1 การกำกับดูแลและการกำกับติดตาม

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 จัดให้มีการกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อบริหารจัดการความเสี่ยงและปฏิบัติให้เป็นไปตามพันธกรณีที่เกี่ยวข้องตามที่กฎหมาย ระเบียบข้อบังคับหรือข้อกำหนดที่ใช้บังคับกำหนดไว้ ทั้งนี้ต้องกำหนดและมอบหมายความรับผิดชอบด้านการกำกับ ดูแลความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติตามข้อกำหนดให้ชัดเจน

3.1.2 การบริหารจัดการความเสี่ยง

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ดำเนินการระบุประเมิน และบริหารจัดการความเสี่ยงด้าน เทคโนโลยีสารสนเทศ เพื่อคุ้มครองการให้บริการและข้อมูลสารสนเทศของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ทั้งนี้ ก่อนอนุญาตให้ บุคคลภายนอกเข้าถึงระบบหรือข้อมูลของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ต้องพิจารณาความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิด จากบุคคลภายนอกดังกล่าวประกอบการตัดสินใจ

3.1.3 การบริหารความเสี่ยงจากผู้ให้บริการภายนอก

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ระบุ ประเมิน และบริหารความเสี่ยงจากผู้ให้บริการภายนอก โดยดำเนินการประเมินความมั่นคงปลอดภัยก่อนเริ่มว่าจ้าง/ใช้งาน และทบทวนเป็นระยะตามที่กำหนด

3.1.4 การบริหารจัดการทรัพย์สินและการกำหนดค่า

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 จัดทำและดูแลให้มีทะเบียนทรัพย์สินขอสานักงานเขตพื้น ที่การศึกษาประถมศึกษาระยองเขต 2 และต้องทำให้มั่นใจว่าทรัพย์สินดังกล่าวได้รับการกำหนดค่าและ บำรุงรักษาอย่างเหมาะสมเพื่อคุ้มครองสารสนเทศ

3.2 การป้องกัน (Protect)

3.2.1 การจำแนกประเภทข้อมูลและการจัดการข้อมูล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ดำเนินการให้มีการจำแนกประเภทข้อมูล และจัดให้มีการ บริหารจัดการข้อมูลให้สอดคล้องกับระดับความอ่อนไหวของข้อมูลแต่ละประเภท ทั้งนี้ ต้องจัดให้มีมาตรการคุ้มครองข้อมูลเพื่อป้องกันการเข้าถึง การเปิดเผย การเปลี่ยนแปลงแก้ไขหรือการสูญหายโดยมิได้รับอนุญาต และให้เป็นไปตามแนวปฏิบัติที่เกี่ยวข้องเพื่อให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 สำหรับสำนักงานเขตพื้นที่การศึกษา

3.2.2 ข้อมูลส่วนบุคคล

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 คุ้มครองข้อมูลส่วนบุคคลจากการเข้าถึง การใช้ หรือการเปิดเผย โดยไม่ได้รับอนุญาต ทั้งนี้ ข้อมูลส่วนบุคคลต้องถูกนำไปใช้เฉพาะเพื่อวัตถุประสงค์ของภารกิจของหน่วยงานที่ได้รับอนุญาตเท่านั้น

3.2.3 การบริหารจัดการตัวตนและสิทธิ์การเข้าถึง

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 อนุญาตให้เข้าถึงระบบและข้อมูลได้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น ทั้งนี้ การให้สิทธิ์การเข้าถึงต้องได้รับการอนุมัติก่อนดำเนินการจัดสรรสิทธิ์ และต้องเพิกถอนหรือยกเลิกสิทธิ์เมื่อไม่มีความจำเป็นต้องใช้สิทธิ์ดังกล่าวต่อไป

3.2.4 ความมั่นคงปลอดภัยเครือข่าย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 คุ้มครองเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาต และจากกิจกรรมที่เป็นอันตราย ทั้งนี้ การเข้าถึงเครือข่ายต้องถูกควบคุมอย่างเหมาะสม เพื่อลดความเสี่ยง ด้านความมั่นคงปลอดภัย

3.2.5 ความมั่นคงปลอดภัยอุปกรณ์ปลายทาง

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 คุ้มครองอุปกรณ์ปลายทางจากการถูกโจมตี และจากการใช้งานโดยไม่ได้รับอนุญาต ทั้งนี้ ต้องมีการบริหารจัดการอุปกรณ์ปลายทางอย่างเป็นระบบ เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

3.2.6 ความมั่นคงปลอดภัยระบบคลาวด์

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 คุ้มครองระบบและข้อมูลที่โฮสต์อยู่บนระบบคลาวด์จากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานโดยมิชอบ และการสูญหาย ทั้งนี้ ให้ใช้บริการคลาวด์ได้เฉพาะบริการที่ได้รับ การอนุมัติให้ใช้ เพื่อการดำเนินงานตามภารกิจของหน่วยงานเท่านั้น

3.2.7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 คุ้มครองสถานที่ อุปกรณ์ และโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานจากการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และภัยคุกคามจากสภาพ แวดล้อม ทั้งนี้ ต้องควบคุมการเข้าถึงทางกายภาพต่อพื้นที่ที่มีทรัพย์สินสารสนเทศให้อยู่ภายใต้มาตรการที่เหมาะสม

3.2.8 การสร้างความตระหนักและการฝึกอบรมบุคลากร

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ทำให้มั่นใจว่าบุคลากรมีความเข้าใจและปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ ต้องจัดให้มีการฝึกอบรมและสร้างความตระหนักด้านความมั่น คงปลอดภัยสารสนเทศแก่บุคลากร

3.2.9 การพัฒนาและการจัดหาเทคโนโลยี

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 พิจารณาข้อกำหนดด้านความมั่นคงปลอดภัยเมื่อมีการจัดหา พัฒนา หรือปรับเปลี่ยนเทคโนโลยี ทั้งนี้ เทคโนโลยีที่จะนำไปใช้งานเพื่อสนับสนุนการดำเนินงานของภารกิจ ต้องได้รับการอนุมัติให้ใช้งานก่อนจึงจะนำไปติดตั้งหรือปรับใช้ได้

3.2.10 วิศวกรรมและสถาปัตยกรรมที่มั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ออกแบบและพัฒนาระบบโดยคำนึงถึงประเด็นด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ทั้งนี้ ต้องพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัยเมื่อจัดทำหรือปรับเปลี่ยนสถาปัตยกรรมของระบบ

3.2.11 การพัฒนาแอปพลิเคชันอย่างมั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ดำเนินการพัฒนาและบำรุงรักษาแอปพลิเคชันตามแนวทางและมาตรฐานการพัฒนาแอปพลิเคชันอย่างมั่นคงปลอดภัย เช่น OWAS เพื่อช่วยลดช่องโหว่และความเสี่ยงด้าน ความมั่นคงปลอดภัยของสารสนเทศ และเพิ่มระดับความปลอดภัยของระบบสารสนเทศ

3.3 การตรวจจับ (Detection)

3.3.1 การตรวจสอบกิจกรรมความมั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 จัดให้มีการบันทึกกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อสนับสนุนความรับผิดรับชอบและการตรวจสอบย้อนกลับ ทั้งนี้ บันทึกการตรวจสอบต้องได้รับการคุ้มครองจากการเข้าถึงหรือการเปลี่ยนแปลงแก้ไข โดยไม่ได้รับอนุญาต

3.3.2 การบริหารจัดการภัยคุกคาม

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ระบุและดำเนินการจัดการภัยคุกคามที่อาจส่งผลกระทบต่อ สารสนเทศและบริการของ สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยอง เขต 2 ทั้งนี้ ต้องนำข้อมูลข่าวกรองด้านภัยคุกคามมาใช้ เพื่อลดโอกาสเกิดและ ลดผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัย

3.3.3 การบริหารจัดการช่องโหว่และการเยียวยา/การแก้ไข

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ระบุและดำเนินการแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยอย่างทันท่วงที ทั้งนี้ การดำเนินการแก้ไขและการเยียวยาต้องจัดลำดับความสำคัญ เพื่อลดความเสี่ยงด้าน ความมั่นคงปลอดภัย

3.4 การตอบสนอง (Respond)

3.4.1 การวางแผน การแจ้งเหตุ และการประสานงานในการตอบสนองเหตุการณ์

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 จัดให้มีแผนและขั้นตอนการตอบสนองเหตุการณ์ด้านความมั่น คงปลอดภัยสารสนเทศที่ครอบคลุมการจำแนกประเภทเหตุการณ์ ระดับความรุนแรง การยกระดับ และการกำหนดบทบาทหน้าที่ของผู้เกี่ยวข้อง รวมถึงต้องกำหนดช่องทางและกระบวนการแจ้งเหตุ/รายงานเหตุ เพื่อให้การสื่อสารเป็นไปอย่างรวดเร็ว

3.4.2 การเยียวยา การแก้ไข และการปรับปรุงหลังเหตุการณ์

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 ดำเนินการเยียวยา/แก้ไข ตามลำดับความสำคัญโดยคำนึงถึง ความเสี่ยงและผลกระทบ เพื่อจำกัดความเสียหายและทำให้บริการที่สำคัญกลับสู่สภาวะปกติได้โดยเร็ว ทั้งนี้ ภายหลังเหตุการณ์ต้องมีการสรุปบทเรียนและปรับปรุงแผน กระบวนการ มาตรการควบคุม และเอกสารที่เกี่ยวข้องอย่างต่อเนื่อง

3.5 การฟื้นฟู (Recover)

3.5.1 การตอบสนองเหตุการณ์และความต่อเนื่องในการดำเนินงาน

สำนักงานเขตพื้นที่การศึกษาประถมศึกษาระยองเขต 2 คงไว้ซึ่งความสามารถในการกู้คืนบริการที่จำเป็นและคุ้มครองสารสนเทศได้อย่างต่อเนื่อง โดยจัดให้มีแผนความต่อเนื่องในการดำเนินงานและแผนกู้คืนระบบ/บริการที่ เหมาะสมกับภารกิจและความสำคัญของบริการ