

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน  
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ  
สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร

ลำดับชั้นเอกสาร	เอกสารภายใน
วันที่มีผลบังคับใช้	1 เมษายน 2569
เวอร์ชันเอกสาร	1.0
เจ้าของเอกสาร	กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร

## การควบคุมเอกสาร และการอนุมัติ

### ข้อมูลการควบคุมเอกสาร

ชื่อเอกสาร	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร
รหัสเอกสาร	DLICT-01
รุ่น	1.0
ลำดับชั้น	เอกสารภายใน
สถานะ	ประกาศใช้
วันที่มีผลบังคับใช้	1 เมษายน 2569
ความถี่ของการทบทวน	รายปี

### การอนุมัติและมอบอำนาจ

เอกสารฉบับนี้ได้รับการอนุมัติอย่างเป็นทางการและได้รับอนุญาตให้ใช้งานภายในหน่วยงาน

บทบาท	ชื่อ / ตำแหน่ง	วิธีการอนุมัติ	วันที่
ผู้จัดทำ	นายกฤษดา เบ็นกาเสมอ นักวิชาการคอมพิวเตอร์ปฏิบัติการ นายจรัสสิน ศรีสังข์ นักวิชาการคอมพิวเตอร์	-	27 มีนาคม 2569
ผู้ทบทวน	นางสาวนิรติศัย สิทธิรักษ์ รอง ผอ.สพม.พิจิตร	ตรวจสอบ	31 มีนาคม 2569
ผู้อนุมัติ	นายสิงห์เพชร สุทธิ ผอ.สพม.พิจิตร	ลงนาม	31 มีนาคม 2569

## ประวัติการเปลี่ยนแปลง

เวอร์ชัน	วันที่	รายละเอียดการเปลี่ยนแปลง
0.1	12 มีนาคม 2569	ร่างนโยบาย
1.0	31 มีนาคม 2569	อนุมัติการใช้นโยบาย

## สารบัญ

หน้า

การควบคุมเอกสาร และการอนุมัติ .....	ก
ประวัติการเปลี่ยนแปลง .....	ข
สารบัญ .....	ค
<b>1. บททั่วไป .....</b>	<b>1</b>
1.1 หลักการ.....	1
1.2 วัตถุประสงค์ .....	1
1.3 ขอบเขต .....	1
1.4 การทบทวนและการปรับปรุง .....	2
1.5 การอ้างอิง.....	2
<b>2. การกำกับดูแลและอำนาจหน้าที่ตามนโยบาย .....</b>	<b>3</b>
2.1 โครงสร้างการกำกับดูแล .....	3
2.2 บทบาทและความรับผิดชอบ.....	3
2.3 กลไกการบริหารความเสี่ยงและการควบคุมภายใน .....	6
2.4 การกำกับดูแลผู้ให้บริการภายนอก.....	6
2.5 การปฏิบัติตามนโยบาย การตรวจสอบ และการรายงานผล .....	6
2.6 ข้อยกเว้นและการยอมรับความเสี่ยง .....	6
2.7 การบังคับใช้และบทลงโทษ.....	7
<b>3. ข้อกำหนดนโยบาย .....</b>	<b>8</b>
3.1 การระบุ (Identify).....	8
3.2 การป้องกัน (Protect) .....	8
3.3 การตรวจจับ .....	10
3.4 การตอบสนอง (Respond).....	10
3.5 การฟื้นฟู (Recover).....	11



# 1. บททั่วไป

## 1.1 หลักการ

นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ฉบับนี้เป็นส่วนหนึ่งของกรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์โดยรวมของสำนักงานเขตพื้นที่การศึกษา (สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร) และให้มีผลบังคับใช้กับหน่วยงานภายใน สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร บุคลากร หรือบุคคลภายนอกที่เกี่ยวข้องซึ่งเข้าถึง หรือใช้งานระบบสารสนเทศ เครือข่ายอุปกรณ์ และข้อมูลของ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดกรอบการกำกับดูแล หลักการ และข้อกำหนดขั้นต่ำของการป้องกัน ตรวจสอบ ตอบสนอง และฟื้นฟูจากภัยคุกคามทางไซเบอร์ รวมถึงเพื่อเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร ลดความเสี่ยงจากเหตุการณ์ที่อาจกระทบต่อภารกิจ การให้บริการสาธารณะ และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย ทั้งนี้ นโยบายต้องสื่อสารอย่างทั่วถึงและนำไปปฏิบัติได้จริง เพื่อคุ้มครองหน่วยงานจากเหตุการณ์ที่เกิดจากความไม่ตั้งใจและการโจมตีโดยเจตนา รวมถึงให้สอดคล้องกับกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง

## 1.2 วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดทิศทางและข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ของ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร เพื่อคุ้มครองระบบสารสนเทศ ข้อมูล และบริการที่สนับสนุนภารกิจด้านการศึกษา โดยมีวัตถุประสงค์ ดังนี้

1.2.1 เพื่อคุ้มครองข้อมูลและบริการของ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ให้คงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและความพร้อมใช้งานตลอดวงจรชีวิตของข้อมูล

1.2.2 เพื่อกำหนดมาตรการในการป้องกัน ตรวจสอบ ตอบสนอง และฟื้นฟูจากภัยคุกคามทางไซเบอร์ ลดโอกาสเกิดเหตุและลดผลกระทบต่อภารกิจ และการให้บริการสาธารณะ

1.2.3 เพื่อเสริมสร้างบทบาท หน้าที่ ความรับผิดชอบ และความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรและผู้เกี่ยวข้อง

1.2.4 เพื่อให้การดำเนินงานสอดคล้องกับกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้องของหน่วยงานของรัฐ รวมถึงการประสานงานและการรายงาน

## 1.3 ขอบเขต

นโยบายฉบับนี้ให้ใช้บังคับกับ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร รวมถึงผู้บริหาร ข้าราชการ พนักงานราชการ เจ้าหน้าที่ลูกจ้าง ผู้รับจ้าง ตลอดจนบุคคลภายนอกหรือคู่สัญญาที่มีการแลกเปลี่ยนข้อมูล ให้บริการ รับบริการหรือเข้าถึง และใช้งานระบบและเทคโนโลยีของหน่วยงานตามข้อตกลงหรือสัญญา

นโยบายฉบับนี้ครอบคลุมทรัพย์สินทั้งหมดของ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ไม่ว่าจะทรัพย์สินดังกล่าวจะตั้งอยู่หรือถูกโฮสต์ 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 การปรับปรุงหรือการเปลี่ยนแปลงต่อไปนี้อาจส่งผลต่อการออกแบบและเนื้อหาของนโยบายต้องนำมาพิจารณาประกอบ ได้แก่

1.4.1 การเปลี่ยนแปลงพันธกิจ และ / หรือวัตถุประสงค์ของสำนักงานเขตพื้นที่การศึกษา

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

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร กำหนดให้มีโครงสร้างการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูล เพื่อให้การดำเนินงานเป็นไปตามนโยบายนี้ อย่างเป็นเอกภาพ ตรวจสอบได้ และสอดคล้องกับภารกิจและข้อกำหนดที่เกี่ยวข้อง

### 2.2 บทบาทและความรับผิดชอบ

กำหนดบทบาทและความรับผิดชอบของผู้เกี่ยวข้องตามนโยบายนี้อย่างชัดเจน ครอบคลุม อย่างน้อย ดังนี้

บทบาท	ความรับผิดชอบ
ผู้บริหารระดับสูง (ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษา)	<ol style="list-style-type: none"><li>กำหนดทิศทางและอนุมัตินโยบาย แผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลของหน่วยงาน</li><li>อนุมัติกรอบบริหารความเสี่ยงระดับหน่วยงานมอบหมายกลไกกำกับดูแล</li><li>จัดสรรทรัพยากรและงบประมาณให้เพียงพอตามความเสี่ยงและความสำคัญของบริการหรือข้อมูล</li><li>กำกับติดตามผลการดำเนินงาน รับทราบรายงานความเสี่ยง ข้อค้นพบ และสั่งการแก้ไข รวมถึงกำกับการตัดสินใจเมื่อเกิดเหตุการณ์รุนแรง/วิกฤต</li></ol>
ผู้บริหารเทคโนโลยีสารสนเทศ (รองผู้อำนวยการสำนักงานเขตพื้นที่การศึกษา ที่ดูแลกลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร)	<ol style="list-style-type: none"><li>กำกับให้ดำเนินการตามมาตรการด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลในระบบและโครงสร้างพื้นฐานเป็นไปตามนโยบายของหน่วยงาน</li><li>กำกับดำเนินการควบคุมที่สำคัญให้มีประสิทธิผลและสามารถตรวจสอบได้</li><li>จัดสรรและบริหารทรัพยากรด้านเทคโนโลยี เครื่องมือ และบุคลากรให้เพียงพอต่อการปฏิบัติงานตามภารกิจ</li><li>กำกับติดตามระดับความเสี่ยงไซเบอร์ ผลการประเมิน/ตรวจประเมินและสถานะการแก้ไข</li><li>รายงานสถานะการดำเนินงาน ประเด็นสำคัญ และความเสี่ยงระดับสูงหรือระดับวิกฤตต่อผู้บริหาร</li></ol>
ผู้ดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (ผู้อำนวยการ กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและ	<ol style="list-style-type: none"><li>จัดทำ ทบทวน ประกาศใช้ และติดตามการปฏิบัติตามนโยบาย/มาตรฐาน/แนวปฏิบัติที่จำเป็นให้สอดคล้องกฎหมายและข้อกำหนด</li><li>ดูแลทะเบียนความเสี่ยงให้เป็นปัจจุบัน ระบุเจ้าของความเสี่ยง มาตรการจัดการ และติดตามสถานะการดำเนินการ</li><li>กำหนดช่องทางแจ้งเหตุ ระดับความรุนแรง และดำเนินการรับแจ้งคัดกรอง ยกระดับไปยังผู้เกี่ยวข้องตามกรอบเวลา</li></ol>

บทบาท	ความรับผิดชอบ
การสื่อสาร หรือนักวิชาการคอมพิวเตอร์)	<ol style="list-style-type: none"> <li>4. ให้ความเห็นด้านความมั่นคงปลอดภัยก่อนขึ้นใช้งานจริงสำหรับการเปลี่ยนแปลงระบบ/การเชื่อมต่อภายนอกที่สำคัญ</li> <li>5. รายงานสถานะความเสี่ยง เหตุการณ์ต่อผู้บังคับบัญชาตามรอบ และจัดเก็บหลักฐานให้ตรวจสอบย้อนกลับได้</li> </ol>
ผู้ดูแลระบบ/ผู้ดูแลเครือข่าย/ผู้ดูแลฐานข้อมูล (เจ้าหน้าที่รับผิดชอบให้ดูระบบที่เกี่ยวข้อง)	<ol style="list-style-type: none"> <li>1. กำกับดูแลให้ระบบ/โครงสร้างพื้นฐาน/ฐานข้อมูลในความรับผิดชอบมีความมั่นคงปลอดภัย สอดคล้องนโยบาย มาตรฐาน และแนวปฏิบัติของหน่วยงาน</li> <li>2. อนุมัติและกำกับกำหนดยุทธศาสตร์ การเข้าถึงตามหลักเท่าที่จำเป็นต่อหน้าที่ และจำเป็นต้องรู้ โดยร่วมกับเจ้าของข้อมูล/เจ้าของระบบ และทบทวนสิทธิ์ตามรอบที่กำหนด</li> <li>3. กำกับกำหนดยุทธศาสตร์เริ่มต้นด้านความมั่นคงปลอดภัยและการตั้งค่าควบคุมด้านความมั่นคงปลอดภัยที่เกี่ยวข้องให้คงสภาพตามมาตรฐาน</li> <li>4. ติดตามการจัดการช่องโหว่และแพตช์ รวมถึงการสำรองข้อมูล/ระบบ และการกู้คืน ให้เป็นไปตามแผนและรอบเวลาที่กำหนด</li> <li>5. ดำเนินการติดตั้งและตั้งค่า ระบบ เครือข่าย ฐานข้อมูลตาม Secure Baseline และมาตรฐานของหน่วยงาน รวมถึงปิดหรือจำกัดบริการที่ไม่จำเป็น และเปิดใช้การตั้งค่าความมั่นคงปลอดภัยที่กำหนด</li> <li>6. ดำเนินการเปลี่ยนแปลงระบบตามกระบวนการบริหารการเปลี่ยนแปลง ได้รับอนุมัติ รวมถึงการประเมินผลกระทบ การย้อนกลับ และการบันทึกหลักฐาน</li> <li>7. ดำเนินการบำรุงรักษาความมั่นคงปลอดภัยและติดตามการบันทึกเหตุการณ์/เฝ้าระวัง ให้เป็นไปตามแผนที่เกี่ยวข้อง พร้อมเก็บรักษาบันทึกตามระยะเวลาที่กำหนด</li> <li>8. เฝ้าระวัง ตรวจสอบ และรายงานเหตุผิดปกติ/เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ผ่านช่องทางที่หน่วยงานกำหนด และให้ความร่วมมือในการตอบสนองเหตุการณ์ตามแผนตอบสนองภัยคุกคามทางไซเบอร์</li> </ol>
ผู้ดูแลผู้ให้บริการภายนอก	<ol style="list-style-type: none"> <li>1. กำกับดูแลความสัมพันธ์กับผู้ให้บริการภายนอกให้เป็นไปตามนโยบายของหน่วยงานและข้อกำหนดตามสัญญา</li> <li>2. ประสานการประเมินความเสี่ยงของผู้ให้บริการภายนอกก่อนเริ่มให้บริการและทบทวนตามระยะเวลาที่กำหนด</li> <li>3. กำกับจัดการสิทธิ์การเข้าถึงของผู้ให้บริการภายนอกให้เหมาะสม และจำเป็นต่อการปฏิบัติงาน</li> </ol>

บทบาท	ความรับผิดชอบ
	4. ประสานการจัดการเหตุการณ์ที่เกี่ยวข้องกับผู้ให้บริการภายนอกให้เป็นไปตามกระบวนการ ช่องทาง และกรอบเวลาที่กำหนด
หน่วยตรวจสอบภายใน	<ol style="list-style-type: none"> <li>1. ตรวจสอบประเมินความเพียงพอและประสิทธิผลของการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลตามนโยบายมาตรฐาน และข้อกำหนดที่เกี่ยวข้อง โดยยึดหลักความเป็นอิสระและตรวจสอบได้</li> <li>2. จัดทำรายงานผลการตรวจประเมิน ข้อค้นพบ และข้อเสนอแนะต่อผู้บริหาร/คณะกรรมการกำกับ พร้อมติดตามความคืบหน้าการแก้ไขของแผนปรับปรุง จนปิดประเด็นตามกำหนด</li> <li>3. ทวนสอบความครบถ้วนของเอกสารและหลักฐาน และความสอดคล้องของกระบวนการ เช่น การบริหารความเสี่ยง การจัดการข้อบกพร่อง การจัดการเหตุการณ์ และการทดสอบแผนความต่อเนื่อง/แผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์</li> <li>4. ประสานการตรวจสอบร่วม/การตรวจจากหน่วยงานภายนอกตามที่เกี่ยวข้อง และสนับสนุนให้หน่วยงานปรับปรุงกระบวนการควบคุมอย่างต่อเนื่อง</li> </ol>
ผู้ประสานงานเหตุความมั่นคงปลอดภัย	<ol style="list-style-type: none"> <li>1. ทำหน้าที่เป็นจุดประสานงานหลักระหว่างสำนักงานเขตพื้นที่การศึกษา และสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในการรับแจ้งเหตุ เปิดบันทึกเหตุการณ์ และจัดเก็บข้อมูลเหตุการณ์ให้ครบถ้วนตามแบบฟอร์ม/ระบบที่หน่วยงานกำหนด พร้อมทั้งติดตามและปรับปรุงข้อมูลให้เป็นปัจจุบัน</li> <li>2. ประสานการควบคุมสถานการณ์และการสื่อสารระหว่างเหตุการณ์ ติดตามความคืบหน้าการดำเนินงาน และสนับสนุนการประสานการตัดสินใจเพื่อจำกัดผลกระทบ โดยให้การสื่อสารเป็นไปอย่างเป็นทางการ ปลอดภัย และสอดคล้องกับการจัดชั้นความลับของข้อมูล และการคุ้มครองข้อมูลส่วนบุคคล</li> <li>3. รวบรวมและจัดการหลักฐานและบันทึกที่เกี่ยวข้อง จัดทำรายงานสถานการณ์และสรุปผลการดำเนินการ รวมทั้งประสานการกู้คืนบริการตามแผนความต่อเนื่อง/แผนกู้คืน และการทบทวนหลังเหตุการณ์เพื่อปรับปรุงกระบวนการและติดตามการแก้ไขจนแล้วเสร็จตามที่กำหนด</li> </ol>

บทบาท	ความรับผิดชอบ
บุคลากรทุกคน/ ผู้ใช้งาน	<ol style="list-style-type: none"> <li>1. ปฏิบัติตามนโยบาย มาตรฐาน และกฎการใช้งานระบบของหน่วยงาน รวมถึงใช้ระบบและข้อมูล</li> <li>2. เข้ารับการอบรม ทดสอบความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลตามที่กำหนด</li> <li>3. ปฏิบัติตามแนวทางด้านความปลอดภัยในการทำงานประจำวัน</li> <li>4. แจ้งเหตุผิดปกติหรือเหตุการณ์ต้องสงสัยด้านความมั่นคงปลอดภัย/การละเมิดข้อมูลโดยทันทีผ่านช่องทางที่กำหนด และให้ความร่วมมือในการตอบสนอง</li> </ol>

### 2.3 กลไกการบริหารความเสี่ยงและการควบคุมภายใน

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องจัดให้มีกลไกการบริหารความเสี่ยงและการควบคุมภายในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างเป็นระบบ โดยต้องดำเนินการระบุ ประเมิน จัดการ และติดตามความเสี่ยงอย่างต่อเนื่อง รวมทั้งกำหนดมาตรการควบคุมที่เหมาะสมตามระดับความเสี่ยง ทั้งนี้ ต้องมีการอนุมัติความเสี่ยงคงเหลือ การจัดเก็บหลักฐานประกอบ และการทบทวนผลตามรอบระยะเวลาที่กำหนด

### 2.4 การกำกับดูแลผู้ให้บริการภายนอก

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องกำกับดูแลผู้ให้บริการภายนอกหรือคู่สัญญาที่เข้าถึง ประมวลผล หรือโฮสต์ข้อมูลและระบบของ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร โดยต้องกำหนดหลักเกณฑ์การคัดเลือกและการประเมินความเสี่ยง กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลไว้ในสัญญา ควบคุมสิทธิการเข้าถึงตามความจำเป็น และติดตามตรวจสอบการปฏิบัติตามอย่างสม่ำเสมอ ทั้งนี้ ต้องกำหนดให้ผู้ให้บริการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและปฏิบัติตามมาตรการที่ สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร กำหนด

### 2.5 การปฏิบัติตามนโยบาย การตรวจสอบ และการรายงานผล

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องจัดให้มีการติดตามและตรวจสอบการปฏิบัติตามนโยบายและมาตรการที่เกี่ยวข้องอย่างต่อเนื่อง รวมถึงการประเมินผลและการตรวจสอบภายในหรือภายนอกตามความจำเป็น ทั้งนี้ ต้องกำหนดช่องทางและรอบระยะเวลาการรายงานผลต่อผู้บริหาร พร้อมจัดทำและเก็บรักษาหลักฐาน เพื่อสนับสนุนการตรวจสอบและการปรับปรุงแก้ไขอย่างเหมาะสม

### 2.6 ข้อยกเว้นและการยอมรับความเสี่ยง

การขอข้อยกเว้นจากการปฏิบัติตามนโยบายต้องจัดทำเป็นลายลักษณ์อักษร และอย่างน้อยต้องระบุเหตุผลความจำเป็น ผลการประเมินความเสี่ยงและผลกระทบ รวมถึงมาตรการควบคุมทดแทน และแผนเยียวยา โดยให้เสนอเพื่อพิจารณาอนุมัติตามสายการบังคับบัญชาที่หน่วยงานกำหนด ร่วมกับเจ้าของ

ระบบหรือเจ้าของข้อมูล และผู้เกี่ยวข้องที่จำเป็น ทั้งนี้ ข้อยกเว้นต้องกำหนดระยะเวลาที่มีผลและวันสิ้นสุดไว้  
อย่างชัดเจน และต้องทบทวนก่อนครบกำหนด

กรณีที่มีการละเว้นการปฏิบัติโดยมิได้รับอนุมัติอย่างเป็นทางการ ให้ถือเป็นการไม่ปฏิบัติตาม  
ตามข้อกำหนด (Noncompliance) และให้ดำเนินการตามระเบียบและมาตรการบังคับใช้ของหน่วยงานต่อไป

## 2.7 การบังคับใช้และบทลงโทษ

บุคลากรทุกประเภทต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศ คำสั่ง และนโยบาย  
ของสำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์  
รวมถึงต้องให้ความร่วมมือและปฏิบัติตามคำสั่งของผู้บังคับบัญชาที่ชอบด้วยกฎหมาย หากมีการฝ่าฝืน  
หรือไม่ปฏิบัติตามนโยบายและมาตรการควบคุมที่กำหนด ให้ดำเนินการตามกระบวนการตรวจสอบข้อเท็จจริง  
ของหน่วยงาน และอาจถูกดำเนินการตามความเหมาะสม

### 3. ข้อกำหนดนโยบาย

เพื่อกำหนดกรอบและข้อกำหนดขั้นต่ำด้านความมั่นคงปลอดภัยสารสนเทศสำหรับ สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร เพื่อให้การบริหารจัดการและการปฏิบัติงานด้านเทคโนโลยีสารสนเทศเป็นไป อย่างเป็นระบบ มีความปลอดภัย และสอดคล้องกับพันธกรณีตามกฎหมาย ระเบียบ ข้อบังคับ และข้อกำหนดที่เกี่ยวข้อง โดยกำหนดแนวทางการดำเนินงานให้ครอบคลุมตามด้านของ NIST Cybersecurity Framework ดังนี้

#### 3.1 การระบุ (Identify)

##### 3.1.1 การกำกับดูแลและการกำกับติดตาม

สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ต้องจัดให้มีการกำกับดูแล ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อบริหารจัดการความเสี่ยงและปฏิบัติให้เป็นไปตามพันธกรณี ที่เกี่ยวข้องตามที่กฎหมาย ระเบียบข้อบังคับ หรือข้อกำหนดที่ใช้บังคับกำหนดไว้ ทั้งนี้ต้องกำหนด และมอบหมายความรับผิดชอบด้านการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติ ตามข้อกำหนดให้ชัดเจน

##### 3.1.2 การบริหารจัดการความเสี่ยง

สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ต้องดำเนินการระบุ ประเมิน และ บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อคุ้มครองการให้บริการและข้อมูลสารสนเทศ ของ สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ทั้งนี้ ก่อนอนุญาตให้บุคคลภายนอกเข้าถึงระบบหรือ ข้อมูลของ สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ต้องพิจารณาความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ อาจเกิดจากบุคคลภายนอกดังกล่าวประกอบการตัดสินใจ

##### 3.1.3 การบริหารความเสี่ยงจากผู้ให้บริการภายนอก

สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ต้องระบุ ประเมิน และบริหารความ เสี่ยงจากผู้ให้บริการภายนอก โดยดำเนินการประเมินความมั่นคงปลอดภัยก่อนเริ่มว่าจ้าง/ใช้งาน และทบทวนเป็นระยะตามที่กำหนด

##### 3.1.4 การบริหารจัดการทรัพย์สินและการกำหนดค่า

สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ต้องจัดทำและดูแล ให้มีทะเบียนทรัพย์สินของ สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ต้องทำให้มั่นใจ ว่าทรัพย์สินดังกล่าวได้รับการกำหนดค่าและบำรุงรักษาอย่างเหมาะสมเพื่อคุ้มครองสารสนเทศ

#### 3.2 การป้องกัน (Protect)

##### 3.2.1 การจำแนกประเภทข้อมูลและการจัดการข้อมูล

สำนักงานเขตพื้นที่ การศึกษามัธยมศึกษาพิจิตร ต้องดำเนินการให้มีการจำแนกประเภท ข้อมูล และจัดให้มีการบริหารจัดการข้อมูลให้สอดคล้องกับระดับความอ่อนไหวของข้อมูล แต่ละประเภท ทั้งนี้ ต้องจัดให้มีมาตรการคุ้มครองข้อมูลเพื่อป้องกันการเข้าถึง การเปิดเผย การเปลี่ยนแปลง

แก้ไข หรือการสูญหายโดยมิได้รับอนุญาต และให้เป็นไปตามแนวปฏิบัติที่เกี่ยวข้องเพื่อให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับสำนักงานเขตพื้นที่การศึกษา

### 3.2.2 ข้อมูลส่วนบุคคล

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องคุ้มครองข้อมูลส่วนบุคคลจากการเข้าถึง การใช้ หรือการเปิดเผยโดยไม่ได้รับอนุญาต ทั้งนี้ ข้อมูลส่วนบุคคลต้องถูกนำไปใช้เฉพาะเพื่อวัตถุประสงค์ของภารกิจของหน่วยงานที่ได้รับอนุญาตเท่านั้น

### 3.2.3 การบริหารจัดการตัวตนและสิทธิ์การเข้าถึง

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องอนุญาตให้เข้าถึงระบบและข้อมูลได้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น ทั้งนี้ การให้สิทธิ์การเข้าถึงต้องได้รับการอนุมัติก่อนดำเนินการจัดสรรสิทธิ์ และต้องเพิกถอนหรือยกเลิกสิทธิ์เมื่อไม่มีความจำเป็นต้องใช้สิทธิ์ดังกล่าวต่อไป

### 3.2.4 ความมั่นคงปลอดภัยเครือข่าย

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องคุ้มครองเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาตและจากกิจกรรมที่เป็นอันตราย ทั้งนี้ การเข้าถึงเครือข่ายต้องถูกควบคุมอย่างเหมาะสม เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

### 3.2.5 ความมั่นคงปลอดภัยอุปกรณ์ปลายทาง

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องคุ้มครองอุปกรณ์ปลายทางจากการถูกโจมตีและจากการใช้งานโดยไม่ได้รับอนุญาต ทั้งนี้ ต้องมีการบริหารจัดการอุปกรณ์ปลายทางอย่างเป็นระบบ เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

### 3.2.6 ความมั่นคงปลอดภัยระบบคลาวด์

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องคุ้มครองระบบและข้อมูลที่โฮสต์อยู่บนระบบคลาวด์จากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานโดยมิชอบ และการสูญหาย ทั้งนี้ ให้ใช้บริการคลาวด์ได้เฉพาะบริการที่ได้รับการอนุมัติให้ใช้ เพื่อการดำเนินงานตามภารกิจของหน่วยงานเท่านั้น

### 3.2.7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องคุ้มครองสถานที่ อุปกรณ์ และโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานจากการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และภัยคุกคามจากสภาพแวดล้อม ทั้งนี้ ต้องควบคุมการเข้าถึงทางกายภาพต่อพื้นที่ที่มีทรัพย์สินสารสนเทศให้อยู่ภายใต้มาตรการที่เหมาะสม

### 3.2.8 การสร้างความตระหนักและการฝึกอบรมบุคลากร

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องทำให้มั่นใจว่าบุคลากรมีความเข้าใจและปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ ต้องจัดให้มีการฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร

### 3.2.9 การพัฒนาและการจัดหาเทคโนโลยี

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัยเมื่อมีการจัดหา พัฒนา หรือปรับเปลี่ยนเทคโนโลยี ทั้งนี้ เทคโนโลยีที่จะนำไปใช้งานเพื่อสนับสนุนการดำเนินงานของภารกิจต้องได้รับการอนุมัติให้ใช้งานก่อนจึงจะนำไปติดตั้งหรือปรับใช้ได้

### 3.2.10 วิศวกรรมและสถาปัตยกรรมที่มั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องออกแบบและพัฒนาระบบโดยคำนึงถึงประเด็นด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ทั้งนี้ ต้องพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัย เมื่อจัดทำหรือปรับเปลี่ยนสถาปัตยกรรมของระบบ

### 3.2.11 การพัฒนาแอปพลิเคชันอย่างมั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องดำเนินการพัฒนาและบำรุงรักษาแอปพลิเคชันตามแนวทางและมาตรฐานการพัฒนาแอปพลิเคชันอย่างมั่นคงปลอดภัย เช่น OWASP เพื่อช่วยลดช่องโหว่และความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศ และเพิ่มระดับความปลอดภัยของระบบสารสนเทศ

## 3.3 การตรวจจับ (Detection)

### 3.3.1 การตรวจสอบกิจกรรมความมั่นคงปลอดภัย

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องจัดให้มีการบันทึกกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อสนับสนุนความรับผิดชอบและการตรวจสอบย้อนกลับ ทั้งนี้ บันทึกการตรวจสอบต้องได้รับการคุ้มครองจากการเข้าถึงหรือการเปลี่ยนแปลงแก้ไข โดยไม่ได้รับอนุญาต

### 3.3.2 การบริหารจัดการภัยคุกคาม

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องระบุและดำเนินการจัดการภัยคุกคามที่อาจส่งผลกระทบต่อสารสนเทศและบริการของ สำนักงานเขตพื้นที่การศึกษาประถมศึกษาพิจิตร เขต 2 ทั้งนี้ ต้องนำข้อมูลข่าวกรองด้านภัยคุกคามมาใช้ เพื่อลดโอกาสเกิดและลดผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัย

### 3.3.3 การบริหารจัดการช่องโหว่และการเยียวยา/การแก้ไข

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องระบุและดำเนินการแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยอย่างทันทั่วทั้งที่ ทั้งนี้ การดำเนินการแก้ไขและการเยียวยาต้องจัดลำดับความสำคัญเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย

## 3.4 การตอบสนอง (Respond)

### 3.4.1 การวางแผน การแจ้งเหตุ และการประสานงานในการตอบสนองเหตุการณ์

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องจัดให้มีแผนและขั้นตอนการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ครอบคลุมการจำแนกประเภทเหตุการณ์ ระดับ

ความรุนแรง การยกระดับ และการกำหนดบทบาทหน้าที่ของผู้เกี่ยวข้อง รวมถึงต้องกำหนดช่องทาง และกระบวนการแจ้งเหตุ/รายงานเหตุ เพื่อให้การสื่อสารเป็นไปอย่างรวดเร็ว

#### **3.4.2 การเยียวยา การแก้ไข และการปรับปรุงหลังเหตุการณ์**

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องดำเนินการเยียวยา/แก้ไขตามลำดับ ความสำคัญโดยคำนึงถึงความเสี่ยงและผลกระทบ เพื่อจำกัดความเสียหายและทำให้บริการที่สำคัญกลับสู่ สภาวะปกติได้โดยเร็ว ทั้งนี้ ภายหลังจากเหตุการณ์ต้องมีการสรุปบทเรียนและปรับปรุงแผน กระบวนการ มาตรการควบคุม และเอกสารที่เกี่ยวข้องอย่างต่อเนื่อง

### **3.5 การฟื้นฟู (Recover)**

#### **3.5.1 การตอบสนองเหตุการณ์และความต่อเนื่องในการดำเนินงาน**

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพิจิตร ต้องคงไว้ซึ่งความสามารถในการกู้คืน บริการที่จำเป็นและคุ้มครองสารสนเทศได้อย่างต่อเนื่อง โดยจัดให้มีแผนความต่อเนื่อง ในการดำเนินงานและแผนกู้คืนระบบ/บริการที่เหมาะสมกับภารกิจและความสำคัญของบริการ