# นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

# โรงเรียนแม่สะเรียง "บริพัตรศึกษา" สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาแม่ฮ่องสอน

โรงเรียนแม่สะเรียง "บริพัตรศึกษา" ต่อไปนี้เรียกว่า "สถานศึกษา" มีนโยบายให้ระบบเทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญที่ช่วยสนับสนุนนโยบายการพัฒนาการจัดการศึกษาอย่างยั่งยืนไปกับสิ่งแวดล้อมและสังคมขององค์กร เพื่อรองรับการตอบสนองต่อความคาดหวังและความต้องการของผู้มีส่วนได้เสีย โดยเฉพาะการมีแนวปฏิบัติ มีเครื่องมือ มีมาตรฐานที่ใช้ดำเนินการที่ทันสมัย มีประสิทธิภาพ และมีความปลอดภัยสอดคล้องตามมาตรฐานสากล

เพื่อให้การดำเนินการใดๆ ด้านเทคโนโลยีสารสนเทศของโรงเรียนแม่สะเรียง "บริพัตรศึกษา" มีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนข้อมูลและสินทรัพย์สารสนเทศของสถานศึกษาได้รับการดูแลรักษาอย่างเหมาะสม โดยคำนึงถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศและด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น มาตรการในการรักษาความลับ ความถูกต้อง ครบถ้วน สมบูรณ์และความพร้อมใช้ต่อการดำเนินงานอย่างเหมาะสม รวมถึงสอดคล้องกับข้อบังคับ กฎ ระเบียบกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ จึงได้กำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศไว้ดังนี้

## นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

กำหนดให้นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศมีรายละเอียด ดังนี้

### 1) การตรวจสอบและประเมินความเสี่ยง

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา จัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยงและการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่สถานศึกษายอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

### 2) การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

จัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์สถานศึกษา โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยี

สารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

**3) การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ**

**3.1) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ**

ผู้ดูแลระบบสารสนเทศของสถานศึกษา กำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของสถานศึกษา ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของสถานศึกษา

**3.2) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องกำหนดมาตรการป้องกัน ควบคุมการใช้งานและการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศ และอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของสถานศึกษา ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

**3.3) การจัดการข้อมูลสารสนเทศและการรักษาความลับ**

**(1) การจำแนกประเภททรัพย์สินสารสนเทศ**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องกำหนดแนวทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับสถานศึกษา มาร่วมพิจารณาการกำหนดชั้นความลับที่เหมาะสม รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้

**(2) การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการ

ดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน

**(3) การควบคุมการเข้ารหัสข้อมูล**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

**3.4) การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน**

**(1) การควบคุมการใช้งานของผู้ใช้งาน**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษาต้องจัดให้มีการควบคุมการใช้งานทรัพย์สินสารสนเทศและระบบสารสนเทศ ดังนี้

1. กำหนดมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน โดยกำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่รหัสผ่าน และให้ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มีการล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม

2. กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกสถานศึกษา โดยกำหนดให้มีมาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของสถานศึกษา รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกสถานศึกษา

3. กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน โดยจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของสถานศึกษาอย่างเป็นลายลักษณ์

อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในสถานศึกษารับทราบและปฏิบัติตาม

**(2) การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

**3.5) การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ**

**(1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม

**(2) การควบคุมการรับส่งข้อมูลสารสนเทศ**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในสถานศึกษา และระหว่างสถานศึกษากับหน่วยงานภายนอกโดยให้เป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

1. ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในสถานศึกษา และระหว่างสถานศึกษากับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

2. ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

3. หัวหน้าการบริหารงานทั้ง 4 ฝ่ายต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้สถานศึกษา มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของสถานศึกษาอย่างเป็นลายลักษณ์อักษร

**3.6) การป้องกันภัยคุกคามต่อระบบสารสนเทศ**

**(1) การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

**(2) การบริหารจัดการช่องโหว่ทางเทคนิค**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องควบคุมให้ระบบสารสนเทศของสถานศึกษาได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

1. จัดให้มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (Untrusted Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ ทั้งนี้ระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปี และระบบงานที่มีความสำคัญอื่นๆ ต้องทดสอบอย่างน้อยทุก 5 ปี

2. จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไขและป้องกัน

3. จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)

**3.7) การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ**

มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา จัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

**4) การกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ**

ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานที่สอดคล้องกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศได้ และต้องกำหนดผู้รับผิดชอบตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศดังกล่าวให้ชัดเจน โดยมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของสถานศึกษา แบ่งออกเป็น 14 ข้อ ได้แก่

1 มาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard)

2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

4 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

6 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

10 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

11 การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

14 การปฏิบัติตามข้อกำหนด (Compliance)

**5) การทบทวนนโยบาย**

กำหนดให้มีการทบทวนนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้ฝ่ายเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้อง ต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลง

**6) การเผยแพร่นโยบาย**

ข้าราชการครูและบุคลากรทางการศึกษา มีหน้าที่รับผิดชอบโดยการประกาศให้ทราบ และเผยแพร่นโยบายเหล่านี้ รวมทั้งทำการสนับสนุน ตอบสนองนโยบายของสถานศึกษา

**7) การรายงาน**

ให้มีการรายงานการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดใดๆ ต่อคณะกรรมการของสถานศึกษาอย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีเหตุการณ์ใดๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ เช่น ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่สถานศึกษาหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ทั้งนี้ผู้อำนวยการสถานศึกษาเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

**8) บทบังคับใช้**

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศนี้ให้ใช้บังคับกับข้าราชการครูและบุคลากรทางการศึกษา พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของโรงเรียนแม่สะเรียง "บริพัตรศึกษา" รวมถึงบุคคลภายนอกและหน่วยงานภายนอกที่เข้ามารับบริการภายในสถานศึกษา โดยมีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป