นโยบายการรักษาความปลอดภัย ระบบเทคโนโลยีสารสนเทศ

โรงเรียนพบพระวิทยาคม

สำนักงานเขตพื้นที่การศึกษามัธยมศึกษา ตาก กระทรวงศึกษาธิการ

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ โรงเรียนพบพระวิทยาคม สพม.ตาก

โรงเรียนพบพระวิทยาคม ต่อไปนี้เรียกว่า “สถานศึกษา” มีนโยบายให้ระบบเทคโนโลยีสารสนเทศ เป็นปัจจัยสำคัญที่ช่วยสนับสนุนนโยบายการพัฒนาธุรกิจอย่างยั่งยืนไปกับสิ่งแวดล้อมและสังคมของ องค์กรเพื่อรองรับการตอบสนองต่อความคาดหวังและความต้องการของผู้มีส่วนได้เสีย โดยเฉพาะการมีแนวปฏิบัติมีเครื่องมือมีมาตรฐานที่ใช้ดำเนินการที่ทันสมัย มีประสิทธิภาพ และมีความปลอดภัยสอดคล้องตามมาตรฐานสากล เพื่อให้การดำเนินการใดๆ ด้านเทคโนโลยีสารสนเทศของ โรงเรียนพบพระวิทยาคม มีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนข้อมูลและสินทรัพย์สารสนเทศของสถานศึกษาได้รับการดูแลรักษาอย่างเหมาะสม โดยคำนึงถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศและด้านความ มั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นมาตรการในการรักษาความลับความถูกต้องครบถ้วนสมบูรณ์และความพร้อมใช้ต่อการดำเนินงานอย่างเหมาะสม รวมถึงสอดคล้องกับข้อบังคับ กฎระเบียบกฎหมายด้านความมั่นคง ปลอดภัยสารสนเทศจึงได้กำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศไว้ดังนี้

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

กำหนดให้นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศมีรายละเอียด ดังนี้

1) **การตรวจสอบและประเมินความเสี่ยง** มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา จัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยงและการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่สถานศึกษายอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

2) **การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ** จัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์สถานศึกษา โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถ จัดสรรทรัพยากร ได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

3) **การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ**

3.1) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ ผู้ดูแลระบบสารสนเทศของสถานศึกษากำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับการควบคุมเข้าถึงและ การใช้งานระบบสารสนเทศของสถานศึกษาให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับ ชั้นความลับของข้อมูล

รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความ เสียหายให้แก่ข้อมูลของสถานศึกษา

3.2) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องกำหนดมาตรการป้องกัน ควบคุมการใช้งาน และการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศ และอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐาน ที่สนับสนุนการทำงานของระบบสารสนเทศของสถานศึกษา ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

3.3) การจัดการข้อมูลสารสนเทศและการรักษาความลับ

(1) การจำแนกประเภททรัพย์สินสารสนเทศ มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องกำหนดแนวทางการจัดหมวดหมู่ ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับ ให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับสถานศึกษา มาร่วมพิจารณา การกำหนด ชั้นความลับที่เหมาะสม รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนว ทางการดำเนินงานที่กำหนดไว้

(2) การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องจัดทำระบบสารสนเทศสำรอง ที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบ สารสนเทศที่สำคัญ รวมทั้งจัดทำแผน รองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์ เพื่อให้ สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียม ความพร้อมกรณี ฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการ ดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบ สารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่ สามารถ ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์และให้มีการทดสอบสภาพพร้อมใช้งานของ ระบบสารสนเทศ ระบบสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

(3) การควบคุมการเข้ารหัสข้อมูล มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องกำหนดมาตรการการเข้ารหัสลับ ข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยง ที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้รวมทั้ง ติดตามให้มีการปฏิบัติให้เป็น ไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

3.4) การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

(1) การควบคุมการใช้งานของผู้ใช้งาน มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษาต้องจัดให้มีการควบคุมการใช้งาน ทรัพย์สินสารสนเทศและระบบสารสนเทศ ดังนี้

1. กำหนดมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องกำหนดให้ผู้ใช้งาน เข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่ รหัสผ่าน และให้ ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์โดย ทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มี การล็อคหน้าจอเครื่อง คอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน หรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม

2. กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกสถานศึกษา มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องกำหนดให้มีมาตรการที่ เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภท พกพา โดยพิจารณา จากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของ สถานศึกษา รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกสถานศึกษา

3. กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน มอบหมายให้ดูแลระบบสารสนเทศของสถานศึกษา ต้องจัดทำขั้นตอนปฏิบัติงาน และมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้ง ซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และ กำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบน เครื่องคอมพิวเตอร์ของ สถานศึกษา อย่างเป็นลายลักษณ์อักษร และปรับปรุง ให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายใน สถานศึกษา รับทราบและปฏิบัติตาม

(2) การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องจัดทำข้อกำหนดและกรอบ การปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ มีความมั่นคงปลอดภัยโดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับ ดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงาน ด้านเทคโนโลยีสารสนเทศ

3.5) การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

(1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่าย คอมพิวเตอร์ มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องควบคุม กำกับให้มีการบริหาร จัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคง ปลอดภัย และควบคุมให้มีการกำหนด คุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และ ความต้องการด้านการบริหาร จัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่าย คอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบ

เครือข่ายผลกระทบ ทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

(2) การควบคุมการรับส่งข้อมูลสารสนเทศมอบหมายให้ดูแลระบบสารสนเทศของสถาน ศึกษา ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในสถานศึกษา และระหว่าง สถานศึกษา กับหน่วยงานภายนอกโดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

1. ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการ แลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของ ข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูล สารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในสถานศึกษา รวมทั้งบริษัทในกลุ่มบริษัท บางจากฯ และระหว่างสถานศึกษากับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

2. ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทาง อิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์(E-Mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โ ดยข้อความทาง อิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

3. หัวหน้าการบริหารงานทั้ง 4 ฝ่ายต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ ปฏิบัติงานให้สถานศึกษามีการทำ สัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของสถานศึกษา อย่างเป็นลายลักษณ์อักษร

3.6) การป้องกันภัยคุกคามต่อระบบสารสนเทศ

(1) การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องกำหนดมาตรการสำหรับการ ตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สิน จากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

(2) การบริหารจัดการช่องโหว่ทางเทคนิค มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา ต้องควบคุมให้ระบบสารสนเทศของ สถานศึกษา ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้น ได้โดยให้เป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

1. จัดให้มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อ กับระบบเครือข่ายภายนอก (Untrusted Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่ รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบของสถานศึกษา (Risk and School Impact Analysis) ดังนี้

1.1.กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อย ทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ

1.2.กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 5 ปี

2. จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มี ความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมี นัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไข และป้องกัน

3. จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้อง ครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์(Cyber Security Drill)

3.7) การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ มอบหมายให้ดูแลระบบสารสนเทศของ สถานศึกษา จัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลด ความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตาม ข้อตกลงที่กำหนดไว้ 4) การกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของ หน่วยงานที่สอดคล้องกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ได้ประกาศใช้งาน และ ดำเนินการประกาศให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตาม มาตรฐานการรักษา ความปลอดภัยระบบเทคโนโลยีสารสนเทศได้ และต้องกำหนดผู้รับผิดชอบตามมาตรฐานการรักษาความปลอดภัย ระบบเทคโนโลยีสารสนเทศดังกล่าวให้ชัดเจน โดยมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ของ สถานศึกษา 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 กำหนดให้มีการทบทวนนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอยาง น้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ทั้งนี้ฝ่ายเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้อง ต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลง

6) การเผยแพร่นโยบาย ข้าราชการครูและบุคลากรทางการศึกษา มีหน้าที่รับผิดชอบโดยการประกาศให้ทราบและเผยแพร่นโยบาย เหล่านี้รวมทั้งทำการ สนับสนุน ตอบสนอง นโยบายของสถานศึกษา

7) การรายงาน ให้มีการรายงานการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึง ระเบียบและข้อกำหนดใดๆ ต่อคณะกรรมการของสถานศึกษา อย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีเหตุการณ์ใดๆ ซึ่ง อาจส่งผลกระทบต่อการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึงระเบียบ และข้อกำหนดอย่างมีนัยสำคัญ เช่น ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใดๆ แก่ สถานศึกษาหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายการรักษาความ ปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดที่สถานศึกษา กำหนดไว้ทั้งนี้ผู้อำนวยการ สถานศึกษาเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

8) บทบังคับใช้ นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศนี้ให้ใช้บังคับกับ ข้าราชการครูและบุคลากร ทางการศึกษา พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของ โรงเรียนบ้านห้วยน้ำพุรวมถึงบุคคลภายนอกและหน่วยงานภายนอกที่เข้ามารับบริการบริการภายในสถานศึกษาโดยมีผลบังคับใช้ตั้งแต่วันถัดจากวัน ประกาศเป็นต้นไป