



แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงเรียนอนุบาลเมืองอุทัยธานี

ส่วนที่ ๑ การควบคุมการเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์ (Computing System Control Room Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือ การเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์ระบบเครือข่ายและเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มี อำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก่ไข หรือเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งก่อให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของโรงเรียน โดยกำหนดกระบวนการควบคุมการ เข้า - ออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์ และเครือข่าย

๒. ผู้รับผิดชอบ

ศูนย์คอมพิวเตอร์

๓. กระบวนการควบคุมการเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ผู้ดูแลห้องควบคุม ระบบคอมพิวเตอร์และเครือข่ายมีแนวทางปฏิบัติดังนี้

๓.๑ ต้องตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายให้ ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายอย่างเคร่งครัด

๓.๒ ต้องขออนุญาตผู้บริหารสูงสุดกำหนดสิทธิการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ให้แก่บุคคลที่ปฏิบัติหน้าที่ที่เกี่ยวข้องภายในโดยจัดทำเป็นลายลักษณ์อักษร

๓.๒ ต้องจัดทำระบบเก็บบันทึกการเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์

๓.๔ กรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องจัดทำเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์ และเครือข่าย ต้องมีการควบคุมอย่างเคร่งครัด โดยเจ้าหน้าที่ศูนย์คอมพิวเตอร์

๓.๕ จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า - ออกพื้นที่ห้องควบคุมระบบคอมพิวเตอร์และ เครือข่ายเป็นประจำ และปรับปรุงสิทธิการเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย อย่างน้อยปีละครั้ง

๓.๖ จัดให้มีกล้องวงจรปิดเพื่อบันทึกข้อมูลการเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

ส่วนที่ ๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงเรียนและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงักและทำให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๒.๓ เจ้าของข้อมูล

การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ระบบเทคโนโลยีสารสนเทศ

๓. สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่

๓.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า – ออกที่รัดกุม อนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยี สารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๓.๔ ผู้ดูแลระบบต้องจัดให้มีระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ ดังนี้

๓.๔.๑ จัดทำบัญชีสินทรัพย์ระบบเทคโนโลยีสารสนเทศ เพื่อจำแนกกลุ่มของระบบหรือการทำงาน เพื่อกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๓.๔.๒ จัดทำบัญชีการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๔.๓ ตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๔.๔ ระงับการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เมื่อตรวจพบการละเมิดความปลอดภัย ผู้ดูแลระบบต้องควบคุมให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ ต่าง ๆ และการผ่านเข้า – ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๔. ข้อกำหนดเกี่ยวกับการกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๔.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น และการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ที่ได้รับอนุญาต

๔.๒ เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงใน

การใช้งานเกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความ จำเป็นขั้นต่ำเท่านั้น

๔.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๔.๔ การขอสิทธิในการเข้าสู่ระบบจะต้องมีการทำเป็นเอกสารและมีการลงนามอนุมัติ เอกสารดังกล่าว และต้องมีการจัดเก็บไว้เป็นหลักฐานด้วย

๕.ข้อกำหนดเกี่ยวกับประเภทข้อมูลลำดับชั้นความลับของข้อมูล

๕.๑ ประเภทข้อมูล

๕.๑.๑ ข้อมูลทั่วไปและข่าวสารของโรงเรียน เป็นข้อมูลทั่วไป บุคคลทั่วไปสามารถเข้าถึงได้ โดยผ่านเว็บไซต์และช่องทางประชาสัมพันธ์อื่นของโรงเรียน

๕.๑.๒ ข้อมูลภายใน เป็นข้อมูลเฉพาะบุคลากรไม่เปิดเผยให้บุคคลภายนอกทราบ บุคลากรสามารถเข้าถึงได้ผ่านระบบอินทราเน็ตของโรงเรียน มีการกำหนดสิทธิการเข้าถึงข้อมูลเฉพาะบุคลากรภายในโรงเรียนเท่านั้น

๕.๑.๓ ข้อมูลระบบสารสนเทศ เป็นข้อมูลระบบงาน ใช้ในการปฏิบัติงานระหว่างบุคลากรที่เกี่ยวข้องกับงาน สามารถเข้าถึงได้ผ่านระบบงาน มีการกำหนดสิทธิการเข้าถึงข้อมูลเฉพาะ ผู้เกี่ยวข้องกับการทำงานเท่านั้น

๕.๑.๔ ข้อมูลเชิงบริหาร เป็นข้อมูลภายใน ใช้ในการวิเคราะห์และบริหารจัดการของผู้บริหาร สามารถเข้าถึงได้ผ่านระบบงาน มีการกำหนดสิทธิการเข้าถึงข้อมูลเฉพาะผู้บริหารเท่านั้น

การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางตามประกาศโรงเรียนมหิดลวิทยา นุสรณ์ เรื่อง

๕.๒ การกำหนดให้ข้อมูลข่าวสารลับอยู่ในชั้นความลับใด พ.ศ. ๒๕๖๐ ซึ่งระเบียบดังกล่าว เป็นมาตรการที่ละเอียดรอบคอบถือว่าเป็นแนวทางที่เหมาะสมที่ในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๕.๒.๑ การกำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสารกำหนดไว้ ๓ ระดับ ได้แก่

๕.๒.๑.๑ ลับที่สุด (TOP SECRET) ได้แก่

(ก) ต้นฉบับข้อสอบคัดเลือกนักเรียนเข้าเรียนชั้นมัธยมศึกษาปีที่ ๔

(ข) ต้นฉบับข้อทดสอบกลางภาคเรียนและปลายภาคเรียน

๕.๒.๑.๒ ลับมาก (SECRET) ได้แก่

(ก) ต้นฉบับคะแนนผลการสอบรายวิชา

(ข) ต้นฉบับข้อทดสอบย่อย

๕.๕.๑.๓ ลับ (CONFIDENTIAL) ได้แก่

(ก) คำสั่งแต่งตั้งคณะกรรมการคัดเลือกสรรหาบุคคลเป็นเจ้าหน้าที่

(ข) คำสั่งแต่งตั้งคณะกรรมการประเมินเพื่อต่อสัญญาจ้าง

(ค) คำสั่งแต่งตั้งคณะกรรมการประเมินเพื่อเลื่อนตำแหน่ง

(ง) คำสั่งเลื่อนเงินเดือน

(จ) คำสั่งการจ่ายเงินรางวัลผลการปฏิบัติงานขององค์กร

ชั้นมัธยมศึกษาปีที่ ๔

(ฉ) คำสั่งแต่งตั้งคณะกรรมการออกข้อสอบคัดเลือกนักเรียนเข้า

(ช) คำสั่งแต่งตั้งคณะกรรมการสืบข้อเท็จจริง

(ซ) คำสั่งลงโทษเจ้าหน้าที่และลูกจ้าง

(ฌ) คะแนนการประเมินผลการปฏิบัติงาน

(ญ) บัญชีเงินเดือนของเจ้าหน้าที่และลูกจ้าง

(ฎ) เงินเดือนของเจ้าหน้าที่และลูกจ้าง

(ฏ) ข้อตกลงจ้างเจ้าหน้าที่และลูกจ้างทั้งชาวไทยและต่างประเทศ

(ฐ) คำสั่งและสัญญาจ้างที่ปรึกษาประจำสาขาวิชาและฝ่าย

(ฑ) หนังสือรับรองเงินเดือน

(ฒ) กระดาษคำตอบของนักเรียน

(ณ) บันทึกการตัดคะแนนความประพฤตินักเรียน

มีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนด

ระดับชั้นความลับของเอกสารและการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตาม ความจำเป็น

๕.๒.๒ การควบคุมเอกสาร โดยกำหนดให้มีมาตรการควบคุมต่าง ๆ คือการจัดทำทะเบียน การตรวจสอบ การจัดทำเอกสาร การสำเนาการแปล การโอน การรับ การส่ง การเก็บรักษา การยืม การทำลายและการปฏิบัติในเวลาฉุกเฉินเวลาสูญหายรวมถึงการเปิดเผยข้อมูลใน เอกสาร

๕.๓ กำหนดระดับชั้นการเข้าถึงระบบเทคโนโลยีสารสนเทศ ดังนี้

๕.๓.๑ ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

๕.๓.๒ ผู้ดูแลระบบและผู้เกี่ยวข้องกับงาน มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่

๕.๓.๓ บุคลากรของโรงเรียน เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้

๕.๓.๔ ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลทั่วไปและข่าวสารของโรงเรียน ผ่านเว็บไซต์ของโรงเรียนเท่านั้น ไม่สามารถเขียน แก้ไข และลบข้อมูลได้

๕.๔ ระยะเวลาการเข้าใช้งาน สามารถเข้าถึงได้ ๒๔ ชั่วโมง ทุกวัน

๕.๕ ช่องทางการเข้าถึง

๕.๕.๑ ผ่านระบบเครือข่ายของโรงเรียน

๕.๕.๒ ผ่านระบบเครือข่ายอินเทอร์เน็ต

๕.๕.๓ ผ่านระบบตรวจสอบสิทธิการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียน

๖. การบริหารจัดการการเข้าถึงของผู้ใช้

๖.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของโรงเรียนเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นและต้องกำหนดให้มีการยกเลิกสิทธิการใช้งานเมื่อพ้นสภาพจากการเป็นบุคลากรของโรงเรียนภายใน ๗ วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน หลังจากศูนย์คอมพิวเตอร์ได้รับแจ้งข้อมูลจากหน่วยงานที่เกี่ยวข้อง

๖.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ระบบเครือข่ายไร้สายระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับอนุมัติจากเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๖.๓ การบริหารจัดการบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

๖.๓.๑

ดูแลระบบที่รับผิดชอบระบบงานนั้นๆต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในส่วนที่๓ “การบริหารจัดการการเข้าถึงของผู้ใช้งาน” การกำหนดการเปลี่ยนแปลงและการ ยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ในส่วนที่๓

“การบริหารจัดการการเข้าถึงของผู้ใช้งาน” กรณีมีความ

จำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานหมายถึงผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้น

อย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการ พิจารณาได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้น ๆ

โดยนำเสนอผู้บังคับบัญชาอนุมัติควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๖.๔.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับให้กับข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๖.๔.๒ เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของ ผู้ใช้งานเหล่านั้นทุก ๖ เดือนเป็นอย่างน้อย เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความ เหมาะสม

๖.๔.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๖.๔.๔ การรับ - ส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะต้องทำการเข้ารหัสที่เป็นมาตรฐานสากล กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศของโรงเรียนในแต่ละประเภทดังนี้

ข้อมูลนักเรียน หน่วยงานหลักคือ งานวิชาการและงานกิจการนักเรียน

ข้อมูลบุคลากร หน่วยงานหลักคือ งานบริหารทรัพยากรบุคคล

ข้อมูลการเงินและบัญชี หน่วยงานหลักคือ งานการเงินและการบัญชี

ข้อมูลทางการศึกษา ขึ้นอยู่กับสาขาวิชา/ฝ่าย/กิจกรรมที่โรงเรียนมอบหมายเป็นหน่วยงานหลัก

ข้อมูลทางการบริหารขึ้นอยู่กับหน่วยงานที่โรงเรียนมอบหมายเป็นหน่วยงานหลักในการดำเนินงาน

ข้อมูลการจราจรทางคอมพิวเตอร์หน่วยงานหลักคือศูนย์คอมพิวเตอร์การกำหนดกฎเกณฑ์เกี่ยวกับ

การอนุญาตให้เข้าถึงต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจของ โรงเรียน การควบคุมการปรับปรุงเปลี่ยนแปลง

๘.๑ การปรับปรุงเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ ดำเนินการดังนี้

๘.๑.๑ พิจารณาวางแผนดำเนินการปรับปรุงเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่

จำเป็นต้องใช้ในการปรับปรุงเปลี่ยนแปลง

๘.๑.๒ แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการปรับปรุงเปลี่ยนแปลงนั้นๆ

เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง

๘.๑.๓ ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการปรับปรุง เปลี่ยนแปลง
๘.๒ ต้องจัดเก็บซอร์สโค้ดและไลบรารีของระบบสารสนเทศทั้งเวอร์ชันปัจจุบันและเวอร์ชันเก่าไว้ใน
สถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็นการกำหนดการใช้งานตามภารกิจ
การควบคุมการเข้าถึงระบบสารสนเทศ

๙.๑.๑ นักเรียน จะให้สิทธิคนที่ที่มีสภาพเป็นนักเรียนและหมดสิทธิตามข้อกำหนดของโรงเรียน
เมื่อพ้นสภาพการเป็นนักเรียน

๙.๑.๒ บุคลากร จะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิตามข้อกำหนด
ของโรงเรียนเมื่อพ้นสภาพการเป็นบุคลากร

๙.๑.๓ ผู้บริหาร จะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิตามข้อกำหนด
ของโรงเรียนเมื่อพ้นสภาพการเป็นผู้บริหาร

๙.๑.๔ บุคคลภายนอก ได้รับอนุญาตเฉพาะระบบงานตามความจำเป็นในการปฏิบัติงานใน ช่วงเวลาที่กำหนด
๙.๒ ข้อจำกัดในการเข้าถึง

๙.๒.๑ นักเรียน เข้าถึงได้เฉพาะระบบที่ได้รับอนุญาต

๙.๒.๒ บุคลากร เข้าถึงได้ตามสิทธิเบื้องต้นและภารกิจที่ได้รับมอบหมาย

๙.๒.๓ ผู้บริหาร เข้าถึงตามสิทธิและภารกิจที่ได้รับมอบหมาย

๙.๒.๔ บุคคลภายนอก เข้าถึงได้ตามที่ได้รับอนุญาต

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งานมิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

ผู้ดูแลระบบ

๓. การแบ่งกลุ่มบัญชีผู้ใช้

บัญชีผู้ใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนจัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของโรงเรียน ต้องระบุชื่อบัญชีผู้ใช้แยกเป็นรายบุคคลที่ไม่ซ้ำซ้อนกัน โดยแบ่งกลุ่มผู้ใช้งานออกเป็น ๖ กลุ่มคือ

๓.๑ นักเรียน

๓.๒ ครูผู้สอน

๓.๓ เจ้าหน้าที่

๓.๔ อาจารย์พิเศษ

๓.๕ ผู้บริหาร

๓.๖ บุคคลอื่น ๆ ที่โรงเรียนมอบสิทธิให้

๔. การลงทะเบียนผู้ใช้งาน

๔.๑ นักเรียนจะได้รับบัญชีผู้ใช้จากหน่วยงานที่บริหารจัดการข้อมูลนักเรียน

๔.๒ ครูผู้สอนเจ้าหน้าที่อาจารย์พิเศษและที่ปรึกษาจะได้รับบัญชีผู้ใช้จากหน่วยงานที่บริหารจัดการข้อมูลบุคลากร

๔.๓ บัญชีผู้ใช้งานกลุ่มผู้บริหารศูนย์คอมพิวเตอร์จะเพิ่มสิทธิของกลุ่มผู้บริหารให้กับบัญชีในกรณีมีบัญชีใช้งานเดิมอยู่แล้ว กรณีเป็นการเปิดบัญชีใหม่ผู้บริหารจะได้รับบัญชีผู้ใช้งานหลังจากหน่วยงานที่บริหารจัดการข้อมูลบุคลากรส่งข้อมูลให้กับศูนย์คอมพิวเตอร์เพื่อนำเข้าสู่ระบบบุคคลอื่น ๆ ที่โรงเรียนมอบสิทธิให้ สามารถลงทะเบียนขอบัญชีผู้ใช้ มีขั้นตอนดังนี้

๔.๔.๑ สาขาวิชา/ฝ่ายผู้เกี่ยวข้องกับบุคคลอื่น ๆ ที่ โรงเรียนมอบสิทธิให้ดาวน์โหลดแบบฟอร์มจากเว็บไซต์ศูนย์คอมพิวเตอร์ โดยกรอกข้อมูลให้ครบถ้วนและนำบันทึกข้อความหรือหนังสือที่ผ่านการขออนุญาตจากผู้บริหารติดต่อที่ศูนย์คอมพิวเตอร์

๔.๔.๒ ศูนย์คอมพิวเตอร์จะออกบัญชีผู้ใช้ให้ตามข้อมูลที่ระบุและแจ้งผู้รับผิดชอบทางอีเมลที่ระบุ ไว้ในแบบฟอร์ม

๔.๔.๓ ผู้รับผิดชอบของสาขาวิชา/ฝ่าย จะต้องรับผิดชอบความเสียหายใด ๆ ที่เกิดจากการใช้งานบัญชีผู้ใช้ที่ศูนย์คอมพิวเตอร์ออกให้

๔.๔.๔

หากต้องการเปลี่ยนแปลงผู้รับผิดชอบบัญชีผู้ใช้ให้แจ้งศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษรลงนามโดยหัวหน้าสาขาวิชา/ฝ่ายโดยระบุชื่อผู้รับผิดชอบเดิมและชื่อผู้รับผิดชอบใหม่พร้อมบัญชีผู้ใช้และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

๔.๔.๕ หากต้องการยกเลิกบัญชีผู้ใช้ให้แจ้งศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษรลงนามโดยหัวหน้าสาขาวิชา/ฝ่าย ระบุชื่อผู้รับผิดชอบและจำนวนบัญชีผู้ใช้ที่ต้องการยกเลิก

๔.๔.๖ บัญชีผู้ใช้งานจะถูกยกเลิกตามวันเวลาที่ระบุในแบบฟอร์ม หากต้องการขยายเวลาให้แจ้งศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษรลงนามโดยหัวหน้าสาขาวิชา/ฝ่าย ระบุชื่อ ผู้รับผิดชอบ และจำนวนบัญชีผู้ใช้ที่ต้องการขยายเวลา

๕.การจัดการสิทธิของผู้ใช้งาน

๕.๑ เมื่อบุคลากรในสาขาวิชา/ฝ่าย พ้นสภาพจากการปฏิบัติหน้าที่ หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิการใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนแปลงสิทธิ ระบุหรือถอดถอนสิทธิออกจากระบบทันที

๕.๒ การแจ้งขอใช้สิทธิ/เปลี่ยนแปลงสิทธิในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบเทคโนโลยีสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผลและความจำเป็น โดยมีขั้นตอน ดังนี้

๕.๒.๑ ลงชื่อโดยหัวหน้าสาขาวิชา/ฝ่ายที่ขอใช้

๕.๒.๒ ขออนุญาตจากผู้บริหาร

๕.๒.๓ สาขาวิชา/ฝ่ายสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๕.๓ ให้อำนาจกับผู้ดูแลระบบในการระบุสิทธิ ในกรณีตรวจพบว่าการกระทำผิดตามนโยบาย การเข้าถึงและควบคุมการใช้งานสารสนเทศ

๕.๔ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้น อย่างรัดกุมและต้องได้รับการอนุญาตจากผู้บริหาร โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา ควบคุมการใช้งานอย่างเคร่งครัด โดยผู้ดูแลระบบต้องควบคุมการใช้งานเฉพาะกรณีจำเป็น เท่านั้น ระบุการใช้งานทันทีเมื่อพ้นระยะเวลาที่กำหนดหรือหมดความจำเป็นในการใช้งาน กรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

๖.การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๖.๑ ผู้ดูแลระบบเป็นผู้กำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคง ปลอดภัย

๖.๒ ผู้ดูแลระบบเป็นผู้กำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการคาดเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๖.๓ ผู้ดูแลระบบส่งบัญชีผู้ใช้และรหัสผ่านแก่หน่วยงานที่รับผิดชอบ ส่วนหน่วยงานที่รับผิดชอบส่งบัญชีผู้ใช้และรหัสผ่านให้ผู้ใช้งาน

๖.๔ ผู้ดูแลระบบกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราวและต้องเป็นรหัสผ่านที่มีความยากต่อการคาดเดา ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะ หรือ ทุกครั้งที่มีการแจ้งเตือน หรือ บังคับให้เปลี่ยนรหัสผ่าน จากผู้ดูแลระบบ

ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันที เมื่อเลิกใช้งานระบบหรือไม่ใช้งานเป็นเวลานาน

การทบทวนสิทธิการเข้าถึง

๗.๑ ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและปรับปรุงบัญชีผู้ใช้ทุก ๖ เดือนเป็นอย่างน้อย

๗.๒ บัญชีผู้ใช้จะหมดอายุ ดังนี้

๗.๒.๑ กรณีบุคลากร หมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของโรงเรียน ยกเว้น ผู้เกษียณอายุราชการซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ตและอีเมลเท่านั้น

๗.๒.๒ กรณีนักเรียน หมดอายุหลังพ้นสภาพการเป็นนักเรียน ๙๐ วัน แต่จะเปลี่ยนสภาพเป็นนักเรียนเก่า ซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอีเมลและระบบฐานข้อมูลศิษย์เก่าเท่านั้น

๗.๒.๓ กรณีที่ไม่ใช่บุคลากรของโรงเรียน หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี

ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศและบังคับใช้กับผู้ที่ใช้ระบบเทคโนโลยีสารสนเทศของโรงเรียนมหิดลวิทยา นุสรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. ผู้รับผิดชอบ

ผู้ใช้งาน

๓. การใช้งานรหัสผ่าน (password use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศต้องปฏิบัติตามข้อกำหนดการใช้งานรหัสผ่านดังนี้

๓.๑ ตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น

๓.๒ ไม่เปิดเผยรหัสผ่านของตนเอง

๓.๓ จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๓.๔ เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๓.๕ ต้องตั้งรหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษร หรือเกินกว่าขั้นต่ำที่กำหนดไว้

๓.๖ ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๓.๗ ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๓.๘ หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน ได้แก่ ๑๒๓, abcd หรือกลุ่มของตัว อักขระที่เหมือนกัน ได้แก่ ๑๑๑, aaa

๓.๙ ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่มีชื่อถึงตัวผู้ใช้งาน ได้แก่ ชื่อ นามสกุล ชื่อเล่น

๓.๑๐ เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่โรงเรียนกำหนด

๓.๑๑ เปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๓.๑๒ เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการลงบันทึกเข้าสู่ระบบงาน

๓.๑๓ ไม่บันทึกหรือจดจำรหัสผ่านของตนเองไว้เพื่อความสะดวกของตนเองเมื่อทำการลงบันทึกเข้าในภายหลัง

๓.๑๔ ไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น

๓.๑๕ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

๔. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

๔.๑ ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเลิกใช้งานระบบหรือไม่ใช้งานเป็นเวลานาน

๔.๒ ผู้ใช้งานต้องล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ใช้งานชั่วคราว

๔.๓ ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๔.๔ ผู้ใช้งานต้องใช้เวลาในการล็อกหน้าจอกรณีที่ไม่ได้ใช้งานคอมพิวเตอร์ภายใน ๑๕ นาทีและให้มีการใช้รหัสผ่านในการปลดล็อกอีกครั้ง

๕. การจัดวางและการป้องกันอุปกรณ์

๕.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้รับ อนุญาต

๕.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

๕.๓ ดำเนินการตรวจสอบ สอดส่องและดูแลสภาพแวดล้อมภายในบริเวณที่มีระบบสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว ได้แก่ การตรวจสอบระดับอุณหภูมิ ความชื้นว่าอยู่ในระดับปกติหรือไม่

๖. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึก ข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ใน ภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจาก การใช้งานดังนี้

๖.๑ ผู้ใช้งานต้องจัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศไว้ในสถานที่มั่นคง ปลอดภัย

๖.๒ เครื่องคอมพิวเตอร์ต้องมีการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๖.๓ ต้องป้องกันการใช้งานและควบคุมทรัพย์สิน ดังนี้

๖.๓.๑ ทุกคนต้องตระหนักและปฏิบัติตามใด ๆ เพื่อป้องกันทรัพย์สินของโรงเรียน

๖.๓.๒ ลงชื่อออกจากระบบทันทีเมื่อไม่ได้ใช้งาน

๖.๓.๓ จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

๖.๓.๔ ถอดหน้าจอเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งาน

๖.๔ สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมเพื่อป้องกันการ สูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖.๕ โปรแกรมต่าง ๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของโรงเรียนเป็นโปรแกรมที่โรงเรียนได้ซื้อลิขสิทธิ์มา อย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมและนำไปติดตั้งบนคอมพิวเตอร์ ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน เพราะเป็นการกระทำที่ผิดกฎหมาย

๖.๖ ต้องลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำลายหรือเปลี่ยนทดแทนหรือ จำหน่ายอุปกรณ์

๗. การป้องกันโปรแกรมประสงค์ร้าย (malware)

๗.๑ ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๗.๒ ผู้ใช้งานต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๗.๓ ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี ในการรับ - ส่ง ข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านระบบเครือข่าย หรือ สื่อบันทึกข้อมูลทุกครั้ง

๘. การเข้ารหัสข้อมูลที่เป็นความลับ

ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษา

ความลับทางราชการ พ.ศ. ๒๕๔๔

๙. มาตรการทำลายสื่อบันทึกข้อมูลที่เป็นความลับ

สื่อบันทึกข้อมูลที่ใช้ในการจัดเก็บข้อมูล หรือสำรองข้อมูล ที่มีความสำคัญขององค์กรที่เป็นความลับต้องทำลายข้อมูลเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
เอกสาร สื่อต่าง ๆ ที่เป็นกระดาษ	ใช้วิธีทำลายด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้วิธีทำลายด้วยเครื่องทำลายแผ่น CD/DVD
ฮาร์ดดิสก์ / flash drive / สารสนเทศอื่น ๆ	ให้ทำลายข้อมูลตามมาตรฐานสากล DoD ๕๒๒๐.๒๒-M, NIST ๘๐๐-๘๘ ทำลายตามแนวปฏิบัติการทำลายข้อมูล

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้เป็นความลับ มีความถูกต้องและพร้อมใช้งานอยู่เสมอ

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๒.๓ ผู้ใช้งาน

๓. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๓.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓.๒ ก่อนเข้าใช้ระบบปฏิบัติการ ผู้ใช้งานต้องใส่ชื่อผู้ใช้และรหัสผ่านทุกครั้ง

๓.๓ ผู้ใช้งานต้องตั้งค่าการล็อกหน้าจออัตโนมัติเพื่อทำการล็อกหน้าจอทุกครั้งที่ไม่มีการใช้งานและต้องกำหนดรหัสผ่านเพื่อเข้าใช้งาน

๓.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๕ ผู้ใช้งานต้องลงบันทึกออกทันทีเมื่อเลิกใช้งานหรือกรณีที่ไม่ได้ใช้งานภายใน ๑๕ นาที

๓.๖ ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนการเข้าสู่ระบบจะเสร็จสมบูรณ์

๓.๗ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓.๘ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง command line

๔ การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication)

๔.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน

๔.๒ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้และต้องมีการพิสูจน์และยืนยันตัวตนด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้งและเป็นการยืนยันยืนยันว่าเป็น ผู้ใช้งานที่ระบุถึง

๔.๓ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศเพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาดผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๔.๔ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ของเครื่องคอมพิวเตอร์และระบบเครือข่ายเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำ ของผู้อื่น

๔.๕ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่ายหรือแจกให้ผู้อื่น

๔.๖ ผู้ใช้งานจะต้องลงบันทึกเข้าโดยใช้บัญชีผู้ใช้ของตนเอง

๕. การบริหารจัดการรหัสผ่าน (password management system)

ระบบบริหารจัดการรหัสผ่านต้องสามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๕.๑ ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเองที่เว็บไซต์เปลี่ยนรหัสผ่านของโรงเรียน

๕.๒ ผู้ใช้งานต้องตั้งรหัสผ่านตามข้อกำหนดการใช้งานรหัสผ่านของโรงเรียน

๕.๓ ระบบบริหารจัดการรหัสผ่านต้องสามารถตรวจสอบความถูกต้องของรหัสผ่านตามข้อกำหนดการใช้งานรหัสผ่านของโรงเรียน

๕.๔ ระบบบริหารจัดการรหัสผ่านต้องให้ผู้ใช้งานยืนยันรหัสผ่านเพื่อตรวจสอบความถูกต้อง

๖. การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities)

การใช้งานโปรแกรมอรรถประโยชน์ต้องจำกัดและควบคุมการใช้งานสำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

๖.๑ จำกัดสิทธิการเข้าถึงการใช้โปรแกรมอรรถประโยชน์กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๖.๒ ห้ามผู้ใช้งานติดตั้งโปรแกรมอรรถประโยชน์โดยไม่ได้รับอนุญาตหรือละเมิดลิขสิทธิ์

๗. การยุติการใช้งานระบบเทคโนโลยีสารสนเทศเมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (session time-out) กำหนดให้มีการยุติการใช้งานระบบเทคโนโลยีสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลง

๘. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบเทคโนโลยีสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๘.๑ การเชื่อมต่อระบบเทคโนโลยีสารสนเทศสำหรับระบบเทคโนโลยีสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง กำหนดให้ใช้งานได้ ๔ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

๘.๒ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูงและระบบเทคโนโลยีสารสนเทศที่มีการใช้งานในสถานที่ที่มีความเสี่ยง มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control Policy)

๑ วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงเรียนและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๓. การจำกัดการเข้าถึงสารสนเทศ (information access control)

๓.๑ ผู้ดูแลระบบต้องกำหนดให้มีขั้นตอนปฏิบัติในการลงทะเบียนบุคลากรใหม่ของโรงเรียนเพื่อให้มีสิทธิ ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะ การปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้ง ต้องทบทวนสิทธิดังกล่าวอยู่เสมอ

๓.๓ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึง ข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำงานข้อมูลแต่ละประเภทชั้นความลับดังต่อไปนี้

๓.๓.๑ ต้องกำหนดบัญชีผู้ใช้เพื่อใช้ในการตรวจสอบตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นความลับของ ข้อมูล

๓.๓.๒ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๓.๓ ต้องกำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๔ การจัดการกับระบบที่ไวต่อการรบกวน

๔.๑ ข้อปฏิบัติสำหรับระบบซึ่งไวต่อการรบกวน

๔.๑.๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อโรงเรียน ได้แก่

๔.๑.๑.๑ ระบบบริหารจัดการงานบุคคล ซึ่งดูแลรับผิดชอบโดยหน่วยงานที่บริหารจัดการ ข้อมูลบุคลากร

๔.๑.๑.๒ ระบบบริหารจัดการงานวิชาการ ซึ่งดูแลรับผิดชอบโดยหน่วยงานที่บริหาร จัดการข้อมูลนักเรียน

๔.๑.๑.๓ ระบบการเงิน ซึ่งดูแลรับผิดชอบโดยหน่วยงานที่บริหารจัดการระบบการเงิน ซึ่งจะได้รับการแยกออกจากระบบงานอื่น ๆ ของโรงเรียน

๔.๑.๒ ควบคุมสภาพแวดล้อมของระบบ โดยมีห้องควบคุมแยกเป็นสัดส่วน

๔.๑.๓ ต้องกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

๔.๒ ต้องควบคุมการเข้าถึงผ่านอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกดังนี้

๔.๒.๑ ต้องกำหนดสิทธิและขอบเขตการทำงาน ชนิดของงานและระบบงาน

๔.๒.๒ ต้องกำหนดระยะเวลาการเข้าถึงและจัดให้มีการควบคุมการปฏิบัติงานและปรับปรุงสิทธิ
หลังจากการปฏิบัติงาน

๕ ข้อปฏิบัติในการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
เพื่อป้องกันสารสนเทศจากความเสียหายอันเกิดจากการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
โรงเรียนจึงมีข้อกำหนดดังนี้

๕.๑ ตรวจสอบความพร้อมของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่จะนำไปใช้งานว่าอยู่
ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๕.๒ เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้นำส่งคืนเจ้าหน้าที่
ที่รับผิดชอบทันที

๕.๓ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์
และอุปกรณ์สื่อสารเคลื่อนที่ที่รับคืน

๕.๔ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้
ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๕.๕ ต้องจัดให้มีการสร้างความตระหนักเพื่อระมัดระวังและป้องกันการใช้งานอุปกรณ์คอมพิวเตอร์และ
อุปกรณ์สื่อสารเคลื่อนที่

๕.๖ ต้องกำหนดให้มีการป้องกันข้อมูลที่สำรองไว้ในอุปกรณ์จากการถูกขโมย สูญหาย หรือเข้าถึงโดย
ไม่ได้รับอนุญาต

๖ ข้อปฏิบัติสำหรับการปฏิบัติงานจากภายนอกหน่วยงาน (teleworking)

๖.๑ ศูนย์คอมพิวเตอร์ต้องจัดเตรียมอุปกรณ์และระบบสำหรับการปฏิบัติงานจากระยะไกล

๖.๒ ผู้ใช้งานที่ปฏิบัติงานจากภายนอกหน่วยงานต้องผ่านระบบการพิสูจน์และยืนยันตัวตนด้วยชื่อ
ผู้ใช้งานและรหัสผ่านทุกครั้ง

๖.๓ ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล ชั่วโมง
การทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ ระบบงานและบริการ ต่าง ๆ
ของโรงเรียนที่อนุญาตให้เข้าถึงได้จากระยะไกล

๖.๔ ผู้ดูแลระบบต้องยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึง ระบบงาน
และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๗ ข้อปฏิบัติในการควบคุมการให้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT outsourcing)

๗.๑ การคัดเลือกผู้ให้บริการ

๗.๑.๑ มีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการและคัดเลือกผู้ให้บริการที่มีขั้นตอนการ
ปฏิบัติงานที่รอบคอบ รัดกุมและเป็นที่น่าเชื่อถือ

๗.๑.๒ มีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขต
งานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

๗.๒ การควบคุมผู้ให้บริการ

๗.๒.๑ ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่
มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความ จำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง
(production environment) ต้องมีการควบคุมหรือ

ตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๗.๒.๒ กำหนดให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๗.๒.๓ กำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข กำหนดให้มีขั้นตอนในการตรวจรับงานของผู้ให้บริการอย่างชัดเจน

ส่วนที่ ๗ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบ เทคโนโลยีสารสนเทศของโรงเรียน โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกัน

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๒.๓ ผู้ใช้งาน

๓. การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๓.๑ ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑.๑ ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรม ห้ามมิให้กระทำการใด ๆ อันส่งผลกระทบต่อการทำงานของผู้อื่น โดยผู้ใช้งานรับรองว่าหากมี การกระทำการใด ๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของโรงเรียน

๓.๑.๒ โรงเรียนไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความต้องการ ซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การให้บริการโฆษณาสินค้าหรือการเปิด บริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มีชื่อของตนโดยไม่ได้รับอนุญาต การบุกรุกเข้าสู่บัญชีผู้อื่น การเผยแพร่ข้อความใด ๆ

ที่ก่อให้เกิดความเสียหายแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว

โรงเรียนไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๓.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยไม่ได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกรานเขตหวงห้ามของโรงเรียน

๓.๑.๕ โรงเรียนให้บัญชีผู้ใช้งานเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกสิทธินี้ให้กับผู้อื่นไม่ได้ และห้ามมิให้บุคคลใดใช้บัญชีผู้ใช้งานของบุคคลอื่นแม้ว่าจะได้รับอนุญาตจาก เจ้าของบัญชีแล้วก็ตาม

๓.๑.๖ บัญชีผู้ใช้งานที่โรงเรียนให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งานนั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๑.๗ บัญชีผู้ใช้งานและแฟ้มทั้งหมดที่อยู่บนอุปกรณ์คอมพิวเตอร์และระบบเครือข่าย ถือเป็นสินทรัพย์ของโรงเรียน โรงเรียนอนุญาตให้ใช้งานเพื่อประโยชน์ทางวิชาการและการ สนับสนุนทางวิชาการเท่านั้น

๓.๒ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงได้เพียงบริการที่ได้รับอนุญาตเท่านั้น

๓.๒.๒ ผู้ดูแลระบบต้องกำหนดระบบเทคโนโลยีสารสนเทศที่ต้องควบคุมการเข้าถึงโดยระบบเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๓.๒.๓ การยืนยันตัวบุคคลสำหรับผู้ ใช้งานที่อยู่ภายนอกหน่วยงานต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน เข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานได้ ดังนี้

๓.๒.๓.๑ การเข้าสู่ระบบจากภายนอกหน่วยงาน ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานที่จะเข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ทำการพิสูจน์และยืนยัน ตัวตน ด้วยชื่อผู้ใช้งานและรหัสผ่านทุกครั้ง ผ่านระบบเครือข่ายเสมือน VPN (Virtual Private Network)

๔. การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

ผู้ดูแลระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔.๑ ผู้ดูแลระบบต้องจัดทำแผนผังระบบเครือข่ายและใช้หมายเลขไอพีแอดเดรสในการระบุอุปกรณ์บนระบบเครือข่าย

๔.๒ ผู้ดูแลระบบต้องควบคุมการใช้งานอย่างเหมาะสมและจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ โดยผู้ที่ได้รับอนุญาตให้เข้าใช้งานจะต้องพิสูจน์และยืนยันตัวตนด้วยชื่อผู้ใช้งานและรหัสผ่านทุกครั้งผ่านทางหมายเลขไอพีแอดเดรสที่อนุญาต ซึ่งจะต้องได้มาจากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server)

๔.๓ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องในโรงเรียนจะต้องลงทะเบียนกับศูนย์คอมพิวเตอร์

๔.๔ อุปกรณ์ใด ๆ ที่นำมาเชื่อมต่อกับเครือข่าย ต้องได้รับการอนุมัติจากผู้บริหารสูงสุด และผ่านทางผู้บริหารด้านเทคโนโลยีสารสนเทศ

๕. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทาง เครือข่าย

๕.๑ ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายตามความจำเป็นและจำกัดการเข้าถึงเครือข่ายที่ใช้ร่วมกัน

๕.๒ ผู้ใช้งานที่ต้องการเปิดพอร์ต ต้องทำบันทึกขออนุมัติจากผู้บริหารด้านเทคโนโลยีสารสนเทศ พร้อมแนบโครงการและระบุเหตุผลความจำเป็น

๕.๓ ผู้ดูแลระบบดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย

๕.๔ จำกัดระยะเวลาการใช้งานพอร์ตเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๖. การแบ่งแยกเครือข่าย (segregation in networks)

ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศดังนี้

๖.๑ จัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๖.๒ แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้งาน และระบบงานต่าง ๆ ของโรงเรียน

๖.๓ มีไฟร์วอลล์ควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

๗. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

ผู้ดูแลระบบต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงดังนี้

๗.๑ ระบุอุปกรณ์เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๗.๒ ตรวจสอบการใช้งานเครือข่าย

๗.๓ จำกัดสิทธิความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย อนุญาตให้เชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๗.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

๗.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๘. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน

หรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจดังนี้

๘.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขไอพี

๘.๒ กำหนดให้มีการแปลงหมายเลขเครือข่ายเพื่อแยกเครือข่ายย่อย

๘.๓ กำหนดเส้นทางการใช้งานเครือข่ายระหว่างคอมพิวเตอร์และเครือข่ายปลายทาง

๘.๔ อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

๘.๕ มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๘.๖ ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๘.๗ ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

๘.๘ ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๘.๙ ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อระงับการใช้จากเส้นทางอื่น

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สายของโรงเรียน โดยการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๓. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๑ ผู้ดูแลระบบต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายไร้สาย

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึง อย่างสม่ำเสมอ ทั้งนี้ต้องได้รับอนุญาตจากผู้บริหารสูงสุดตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน

๓.๔ ผู้ดูแลระบบต้องกำหนดค่ากำลังส่งของอุปกรณ์กระจายสัญญาณให้เหมาะสมกับพื้นที่ใช้งาน

๓.๕ ผู้ดูแลระบบต้องเปลี่ยนค่าเริ่มต้น SSID ที่ถูกกำหนดมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สายมาใช้งาน

๓.๖ ผู้ดูแลระบบต้องแยก SSID ของผู้ใช้งานที่เป็นบุคลากรของโรงเรียน และผู้ใช้งานตามโครงการทางวิชาการต่าง ๆ ที่โรงเรียนดำเนินการจัดขึ้น โดยควบคุมสิทธิและระยะเวลาในการเข้าถึงระบบ เครือข่ายไร้สาย

๓.๗ ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อผู้ใช้งานและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกชื่อผู้ใช้งานและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

๓.๘ ผู้ดูแลระบบต้องใช้ระบบพิสูจน์ตัวตนและการเข้ารหัสข้อมูลระหว่างอุปกรณ์ปลายทางและอุปกรณ์กระจายสัญญาณไร้สาย

๓.๙ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินเทอร์เน็ตและฐานข้อมูลภายในต่าง ๆ ของโรงเรียน

ส่วนที่ ๔ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy)

๑. วัตถุประสงค์

เพื่อป้องกันความเสี่ยงจากหน่วยงานภายนอกต่อการเข้าถึงข้อมูล การแก้ไขข้อมูลอย่างไม่ถูกต้องและการประมวลผลของระบบงานโดยไม่ได้รับอนุญาตและเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนเป็นไปอย่างมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๒.๓ เจ้าของโครงการ

๓. ข้อปฏิบัติ

๓.๑ กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

๓.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

๓.๒.๑ หน่วยงานภายนอกที่ต้องการสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนต้องดำเนินการขออนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารสูงสุด

๓.๒.๒ จัดทำแบบฟอร์มสำหรับให้หน่วยงานภายนอกระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ มีรายละเอียดอย่างน้อยดังนี้

๑. เหตุผลในการขอใช้

๒. ระยะเวลาในการใช้

๓. การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๔. ข้อมูล MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๕. การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓.๒.๓ หน่วยงานภายนอกที่ทำงานให้กับโรงเรียนต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของโรงเรียน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓.๒.๔ โรงเรียนต้องพิจารณาการประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศที่เข้าไปปฏิบัติงาน

๓.๒.๕ ผู้ดูแลระบบต้องกำหนดการเข้าถึงข้อมูลโดยหน่วยงานภายนอกเฉพาะบุคคลที่จำเป็น เท่านั้น

๓.๒.๕ ๖ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของโรงเรียนให้มีความมั่นคงปลอดภัยทั้งด้านการรักษาความลับ การรักษาความถูกต้องของข้อมูลและการรักษาความพร้อมที่จะให้บริการ

๓.๒.๗ โรงเรียนมีสิทธิตรวจสอบสิทธิการใช้งานของหน่วยงานภายนอกตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าโรงเรียนสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๓.๒.๘ หน่วยงานภายนอกที่ทำงานให้กับโรงเรียนต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง

๓.๒.๙ หลังส่งมอบโครงการจากหน่วยงานภายนอก ผู้ดูแลระบบต้องดำเนินการเปลี่ยนรหัสผ่าน ทันที

ส่วนที่ ๑๐ การควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Personal Data Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุม การเก็บรวบรวม การใช้ การประมวลผล การเปิดเผย การเข้าถึง และการแก้ไขข้อมูลส่วนบุคคลของโรงเรียนเป็นไปอย่างมั่นคงปลอดภัย เพื่อป้องกันความเสียหายต่อเจ้าของข้อมูล

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๒.๓ เจ้าของข้อมูล

๓. กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการควบคุม ดูแล คัดกรองข้อมูลส่วนบุคคลของโรงเรียนในแต่ละประเภทดังนี้

๓.๑ ข้อมูลนักเรียน หน่วยงานหลักคือ งานวิชาการและงานกิจการนักเรียน

๓.๒ ข้อมูลบุคลากรภายใน หน่วยงานหลักคือ งานบริหารทรัพยากรบุคคล

๓.๓ ข้อมูลบุคลากรและหน่วยงานภายนอกที่ติดต่อขอรับการบริการวิชาการ หน่วยงานหลักคือ งานบริการวิชาการ

๓.๔ ข้อมูลการเงินและบัญชี หน่วยงานหลักคือ งานการเงินและการบัญชี

๓.๕ ข้อมูลทางการศึกษา ขึ้นอยู่กับสาขาวิชา/ฝ่าย/กิจกรรม ที่โรงเรียนมอบหมายเป็นหน่วยงานหลัก

๓.๖ ข้อมูลทางการบริหาร ขึ้นอยู่กับหน่วยงานที่โรงเรียนมอบหมายเป็นหน่วยงานหลักในการดำเนินงาน

๓.๗ ข้อมูลการจราจรทางคอมพิวเตอร์ หน่วยงานหลักคือ ศูนย์คอมพิวเตอร์

๔ การเก็บรวบรวมข้อมูลส่วนบุคคล

๔.๑ หน่วยงานหลักต้องเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์การใช้งานเท่านั้น

๔.๒ หน่วยงานหลักต้องแจ้งให้เจ้าของข้อมูลทราบรายละเอียดดังต่อไปนี้เป็นอย่างน้อย

๔.๒.๑ ข้อมูลที่จัดเก็บ

๔.๒.๒ วัตถุประสงค์

๔.๒.๓ ระดับชั้นความลับของข้อมูล และหน่วยงานที่สามารถเข้าถึงข้อมูล

๔.๓ หน่วยงานหลักสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้ต้องได้รับความยินยอมจากเจ้าของข้อมูล ก่อน และแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบที่เกิดขึ้นกรณีไม่ให้ข้อมูล

๔.๔ เจ้าของข้อมูลต้องให้ข้อมูลที่ถูกต้อง สมบูรณ์ ครบถ้วน และเป็นปัจจุบัน หากเจ้าของข้อมูลให้ข้อมูลอันเป็นเท็จอาจถูกดำเนินคดีตามกฎหมาย

๕ การใช้หรือการประมวลผลข้อมูลส่วนบุคคล

๕.๑ หน่วยงานหลักต้องใช้งานข้อมูลที่จัดเก็บตามวัตถุประสงค์ หรือเกี่ยวข้องกับการวางแผนของ โรงเรียน แต่ต้องไม่เกิดความเสียหายต่อเจ้าของข้อมูล

๕.๒ หน่วยงานหลักต้องกำหนดสิทธิการเข้าถึงข้อมูลให้สอดคล้องกับระดับชั้นความลับและหน่วยงานตามที่แจ้งเจ้าของข้อมูล

๕.๓ การใช้หรือการประมวลผลใด ๆ ที่นอกเหนือจากวัตถุประสงค์ ต้องได้รับอนุญาตจากผู้บริหารสูงสุด ก่อน

๖ การเปิดเผยข้อมูลส่วนบุคคล

๖.๑ หน่วยงานหลักสามารถเปิดเผยข้อมูลก็ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูล

๖.๒ หน่วยงานหลักสามารถเปิดเผยข้อมูลเพื่อประโยชน์เกี่ยวกับการวางแผนหรืองานที่เกี่ยวข้องของโรงเรียน แต่ต้องไม่เกิดความเสียหายต่อเจ้าของข้อมูล

๖.๓ การกระทำการใด ๆ ที่เกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคล อันนำไปสู่การสร้างความเสียหายต่อเจ้าของข้อมูล ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้เปิดเผยข้อมูลแต่เพียงผู้เดียว

๖.๔ หน่วยงานภายนอกที่ต้องการสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนต้อง
ดำเนินการขออนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารสูงสุด

๗ กำหนดระดับชั้นการเข้าถึงข้อมูลส่วนบุคคล ดังนี้

๗.๑ ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

๗.๒ ผู้ดูแลระบบและผู้เกี่ยวข้องกับการงาน มีสิทธิเก็บรวบรวม ใช้หรือประมวลผล และเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมาย

๗.๓ หน่วยงานของรัฐภายนอก สามารถเข้าถึงข้อมูลได้ตามสิทธิและหน้าที่กฎหมายกำหนด

ส่วนที่ ๑๑ ความมั่นคงปลอดภัยของการใช้งานอินเทอร์เน็ต (Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของโรงเรียนอนุบาลเมืองอุทัยธานีถูกระงับ ชะลอ ชัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. ผู้รับผิดชอบ

๒.๑ ผู้ใช้งาน

๒.๒ ผู้ดูแลระบบ

๓. ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการแก้ปัญหาช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์

๓.๒ ผู้ใช้ต้องทำการอัปเดต patch และ hot fix อย่างสม่ำเสมอโดยสามารถดาวน์โหลด patch และ hot fix ต่าง ๆ จากเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่

๓.๓ ในการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัส (virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ - ส่งข้อมูลทุกครั้ง

๓.๔ ผู้ใช้ต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของโรงเรียนเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๓.๕ ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของโรงเรียน

๓.๖ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับโรงเรียน

๓.๗ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของโรงเรียนที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๓.๘ ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

๓.๙ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๔. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๔.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่โรงเรียนจัดสรรไว้เท่านั้น

ส่วนที่ ๑๒ การสำรองและกู้คืนข้อมูล

(Backup and Recovery Policy)

๑. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติสำหรับการสำรองข้อมูลและการกู้คืนระบบ โดยผู้ดูแลระบบสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น รวมทั้งผู้ใช้งานสามารถดำเนินการสำรองข้อมูลและกู้คืนข้อมูลได้

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบงาน

๒.๓ ผู้ใช้งาน

๓. ข้อปฏิบัติ

๓.๑ ผู้ดูแลระบบงานต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานสำรองข้อมูลและจัดทำระบบสารสนเทศสำรอง

๓.๒ ผู้ดูแลระบบงานมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้ในกรณีที่ไม่สามารถปฏิบัติงานได้

๓.๓ ผู้ดูแลระบบงานกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสมพร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูลสถานที่จัดเก็บ โดยรูปแบบการสำรองข้อมูลอาจแบ่งได้เป็นการสำรองข้อมูลแบบเต็ม และการสำรองข้อมูลแบบส่วนต่าง

๓.๔ ผู้ดูแลระบบงานต้องทำบันทึก รายละเอียดการสำรองข้อมูลได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๓.๕ ผู้ดูแลระบบงานต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๓.๖ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้าหน่วยงานของระบบงาน

๓.๗ ผู้ดูแลระบบงานต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นรวมทั้งวิธีการที่ใช้แก้ไข ด้วย

๓.๘ ผู้ดูแลระบบงานต้องปฏิบัติตามขั้นตอนของการสำรองข้อมูลโดยเคร่งครัด

๓.๙ ผู้ดูแลระบบงานต้องทำการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมความพร้อม กรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๓.๑๐ ผู้ใช้งานต้องพิจารณาคัดเลือกระบบสำรองข้อมูลที่เหมาะสม

๓.๑๑ ผู้ใช้งานต้องสำรองและกู้คืนข้อมูลที่จำเป็นให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

๔.๑ ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่อย่างน้อยดังนี้

ที่	ระบบ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Web servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	เดือนละครั้ง
๒	Database servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบ	เดือนละครั้ง
๓	Firewall server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๔	DNS Server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๕	DHCP Server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๖	Server อื่น ๆ	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๗	ระบบ MIS	ข้อมูลนักเรียน, ข้อมูลการศึกษา	เดือนละครั้ง
๘	ระบบงานห้องสมุด	ข้อมูลระบบงานห้องสมุด	วันละครั้ง
๙	ระบบงานหอพัก	ข้อมูลการเข้า - ออกหอพัก	สัปดาห์ละครั้ง
๑๐	ระบบงานพัสดุ	การเบิกจ่ายพัสดุ	สัปดาห์ละครั้ง
		ข้อมูลพัสดุ	เดือนละครั้ง
๑๑	ระบบงานบุคคล	บันทึกการเข้างาน	สัปดาห์ละครั้ง
		ข้อมูลบุคลากร	เดือนละครั้ง

๔.๒ ผู้ดูแลระบบงานต้องทำการเก็บรักษาข้อมูลสำรองอย่างน้อย ๑ ชุดแยกสถานที่กัน เพื่อความมั่นคงปลอดภัย และใช้งานได้อย่างต่อเนื่อง

๔.๓ ผู้ดูแลระบบงานต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการสำรองข้อมูลตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๕. การกู้คืนระบบ (data recovery)

๕.๑ ผู้ดูแลระบบงานหรือผู้ที่ได้รับมอบหมายจะต้องทำการทดสอบการกู้คืนข้อมูลเป็นระยะ เพื่อให้แน่ใจได้ว่า การสำรองข้อมูลนั้นทำได้อย่างครบถ้วนสมบูรณ์แล้ว

๕.๒ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการ แก้ไข แล้วรายงานสรุปผลการปฏิบัติงานต่อหัวหน้าหน่วยงานของระบบงาน

๕.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (latest update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๕.๔ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันทีพร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๖ การจัดทำแผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ (IT contingency plan)

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ ต้องกำหนดบุคลากรที่เกี่ยวข้องและดำเนินการดังต่อไปนี้

๖.๑ กำหนดแผนเตรียมความพร้อมและกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติ

๖.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๖.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๖.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติเพื่อให้สามารถกู้คืนระบบเทคโนโลยีสารสนเทศที่เสียหายให้สามารถใช้งานได้โดยเร็ว

๖.๕ ทดสอบการปฏิบัติตามแผนอย่างน้อยปีละ ๑ ครั้งโดยการจำลองสถานการณ์

๖.๖ ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๓ การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail Policy)

๑. วัตถุประสงค์

๑.๑. เพื่อให้การรับ – ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของโรงเรียนสามารถสนับสนุนการปฏิบัติงานและการบริหารงานของโรงเรียนให้เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผล

๑.๒. เพื่อให้การติดต่อสื่อสารโดยการรับ – ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของโรงเรียนเป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับของโรงเรียน

๒. ผู้รับผิดชอบ

๒.๑ ผู้ใช้งาน

๒.๒ ผู้ดูแลระบบ

๓. ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑ ผู้ใช้งานต้องไม่ตั้งจำจอร์หัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์ เว้นแต่เป็นอุปกรณ์ส่วนบุคคล

๓.๒ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อโรงเรียนหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรมและไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่าย ของโรงเรียน

๓.๓ ห้ามมิให้ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับ – ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการ ใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตนเอง

๓.๔ ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการทำงานในภารกิจของโรงเรียน เท่านั้น

๓.๕ ลงบันทึกออกจากระบบจดหมายอิเล็กทรอนิกส์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

๓.๖ ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดทุกครั้งเพื่อตรวจสอบไวรัสคอมพิวเตอร์

๓.๗ ไม่เปิดอ่านหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๘ ไม่ใช้ข้อความที่ไม่สุภาพหรือรับ – ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมอันอาจทำให้เสื่อมเสียชื่อเสียงของโรงเรียนหรือข้อมูลที่ทำให้เกิดความแตกแยกในหน่วยงาน

๓.๙ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๓.๑๐ ผู้ใช้งานต้องตรวจสอบกล่องจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ

๔. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๔.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนให้เหมาะสมกับการเข้าใช้บริการ หน้าที่ความรับผิดชอบของผู้ใช้งานและทบทวนสิทธิการเข้าใช้งานอย่างน้อยปีละ ๑ ครั้ง

๔.๒ ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ต้องทำการบันทึกออกจากหน้าจอเพื่อตัดการใช้งานจากผู้ใช้งานเมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้

ส่วนที่ ๑๔ ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์ (Terms of Use and Disclaimer)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับ - ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของโรงเรียนสามารถสนับสนุนการปฏิบัติงานของโรงเรียนให้เป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์และมีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ - ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของโรงเรียนเป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของโรงเรียน

๒. ผู้รับผิดชอบ

๒.๑ ผู้ใช้งาน

๓. ข้อตกลงการใช้บริการ

๓.๑ ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนจะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ และคำแนะนำ อย่างน้อยดังต่อไปนี้

๓.๑.๑ พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๓.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒

๓.๑.๓ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐

๓.๑.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๓.๑.๕ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒

๓.๑.๖ ข้อตกลงเงื่อนไขการใช้บริการที่โรงเรียนกำหนด

๓.๒ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ของโรงเรียนจะต้องใช้จดหมายอิเล็กทรอนิกส์นี้เพื่อผลประโยชน์ของโรงเรียน

๓.๓ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วน ตน

๓.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการเผยแพร่ อ้างอิง พาดพิง ดุหมิ่น หรือกระทำการใด ๆ ที่ก่อให้เกิดความเสียหายต่อสถาบันชาติ ศาสนา และพระมหากษัตริย์

๓.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนในการประกอบอาชญากรรมทางคอมพิวเตอร์หรือการกระทำใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับของทางราชการ

๓.๖ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพ เสียง ข้อความที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๗ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อแสดงความคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบหรือสร้างความเสื่อมเสียหรือเสียหายต่อผู้อื่นหรือโรงเรียน

๓.๘ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (impersonation)

๓.๙ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

๑ การสร้างจดหมายลูกโซ่ (chain mail)

๒. การส่งจดหมายจำนวนมาก (spam mail)

๓. การส่งจดหมายต่อเนื่อง (letter bomb)

๔. การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๓.๑๐ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของโรงเรียนหรือทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของโรงเรียน

๓.๑๑ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานภายนอกจะต้องเข้ารหัสข้อมูลอย่างเหมาะสมตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่ โรงเรียนกำหนด

๓.๑๒ ที่อยู่จดหมายอิเล็กทรอนิกส์และรหัสผ่านของบุคคลหรือหน่วยงานจะต้องเก็บรักษาไว้เป็นความลับ หากสงสัยว่ารั่วไหลจะต้องเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา

๓.๑๓ ผู้ใช้งานหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำและข้อตกลงเงื่อนไขให้เข้าใจ เพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของโรงเรียนได้อย่าง ถูกต้อง

๓.๑๔ กรณีได้รับการร้องเรียนหรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะยกเลิกหรือระงับบริการแก่ผู้ใช้งานเป็นการชั่วคราว เพื่อทำการสอบสวนและตรวจสอบหาสาเหตุของมูลเหตุ

๓.๑๕ การกระทำใด ๆ ที่เกี่ยวกับการเผยแพร่ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์หรือเว็บไซต์ของผู้ใช้งาน ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้งาน โรงเรียนไม่มีส่วนเกี่ยวข้อง ใด ๆ

ส่วนที่ ๑๕ ข้อตกลงการใช้งานลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature Agreement)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การใช้งานลายมือชื่ออิเล็กทรอนิกส์ในการปฏิบัติงานของโรงเรียนเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว และเป็นไปในแนวทางเดียวกัน

๑.๒ เพื่อให้การใช้งานลายมือชื่ออิเล็กทรอนิกส์สำหรับบุคลากรของโรงเรียนเป็นมาตรฐานอยู่ในกรอบ ของ กฎหมาย ระเบียบ คำสั่ง และข้อบังคับ

๒. ผู้รับผิดชอบ

เจ้าของลายมือชื่อหรือเจ้าของใบรับรองดิจิทัล

๓ ข้อตกลงการใช้บริการ

๓.๑ เจ้าของลายมือชื่อหรือเจ้าของใบรับรองดิจิทัลจะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ และคำแนะนำ อย่างน้อยดังต่อไปนี้

๓.๑.๑ พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๓.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒

๓.๑.๓ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐

๓.๑.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๓.๑.๕ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒

๓.๑.๖ ข้อตกลงเงื่อนไขการใช้บริการที่โรงเรียนกำหนด

๓.๒ เจ้าของลายมือชื่อต้องเก็บรักษาใบรับรองดิจิทัลและรหัสผ่านที่ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์ ไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น และห้ามโอนจำหน่ายหรือแจกให้ผู้อื่น

๓.๓ เจ้าของลายมือชื่อต้องลงลายมือชื่ออิเล็กทรอนิกส์ตามรูปแบบที่โรงเรียนกำหนด

๓.๔ เจ้าของลายมือชื่อต้องใช้งานใบรับรองดิจิทัลที่โรงเรียนกำหนดในการลงลายมือชื่ออิเล็กทรอนิกส์ เท่านั้น

๓.๕ เจ้าของลายมือชื่อต้องทำบันทึกข้อความเพื่อระงับการใช้งานใบรับรองดิจิทัลและขออนุมัติใบรับรองดิจิทัลใหม่ กรณีลืมรหัสผ่านหรือหากสงสัยว่าใบรับรองดิจิทัลรั่วไหล

๓.๖ เจ้าของลายมือชื่อลงลายมือชื่อในหนังสือราชการ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้น ถูกลงลายมือชื่อ โดยเจ้าของลายมือชื่อแล้ว

๓.๗ ลายมือชื่ออิเล็กทรอนิกส์ใช้ในการรับรองความถูกต้องและความครบถ้วนของหนังสือราชการ

๓.๘ ห้ามใช้ลายมือชื่ออิเล็กทรอนิกส์กับหนังสือราชการที่ไม่เกี่ยวข้องกับการดำเนินงานของโรงเรียน

๔. ข้อปฏิบัติในการใช้งานลายมือชื่ออิเล็กทรอนิกส์

๔.๑ การสร้างใบรับรองดิจิทัล ต้องใช้ข้อมูลส่วนบุคคล ซึ่งสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือ ทางอ้อม และไม่อยู่ภายใต้การควบคุมของบุคคลอื่น

๔.๒ ลายมือชื่ออิเล็กทรอนิกส์ที่ใช้สำหรับหนังสือภายใน ต้องใช้ร่วมกับใบรับรองดิจิทัลที่ออกโดย โรงเรียน หรือที่โรงเรียนกำหนดให้ใช้งานเท่านั้น

๔.๓ ลายมือชื่ออิเล็กทรอนิกส์ที่ใช้สำหรับหนังสือติดต่อกับราชการ ต้องใช้ร่วมกับใบรับรองดิจิทัลที่ออกโดย ผู้ให้บริการออกใบรับรอง

๔.๔ เจ้าของลายมือชื่อต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ ข้อตกลง และเงื่อนไขให้ เข้าใจ เพื่อใช้งานลายมือชื่ออิเล็กทรอนิกส์ได้อย่างถูกต้อง

๔.๕ การรับรองหนังสือติดต่อราชการ ต้องตรวจสอบความถูกต้องและความครบถ้วนของข้อมูลก่อนลง ลายมือชื่ออิเล็กทรอนิกส์ในหนังสือติดต่อราชการ

๔.๖ กรณีได้รับการร้องเรียนหรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์การใช้ใบรับรองและลายมือชื่ออิเล็กทรอนิกส์ชั่วคราว เพื่อตรวจสอบสาเหตุ

๔.๗ การกระทำการใด ๆ ที่เกี่ยวเนื่องกับการใช้งานใบรับรองดิจิทัลและลายมือชื่ออิเล็กทรอนิกส์ที่อยู่นอกเหนือจากข้อปฏิบัติ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของเจ้าของลายมือชื่อหรือเจ้าของใบรับรองดิจิทัลแต่เพียงผู้เดียว

ส่วนที่ ๑๖ การตรวจสอบและประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการตรวจสอบ ประเมิน ควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบจากภายนอก (external auditor)

๒.๓ ผู้ดูแลระบบ

๓. ขอบปฏิบัติ

๓.๑ ตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓.๒ ตรวจสอบและประเมินความเสี่ยง โดยคณะกรรมการหรือหน่วยงานหรือบุคคลที่โรงเรียน เห็นสมควร เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้าน สารสนเทศ

๓.๓ การรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลจำเป็นต้องคำนึงถึงหลายด้านหลายมิติ แต่ละด้านก็มีความจำเป็นในการตรวจสอบและประเมินความเสี่ยงแตกต่างกัน โดยให้มีการ ดำเนินการดังต่อไปนี้

๓.๓.๑ การตรวจสอบและประเมินนโยบาย

๓.๓.๒ การตรวจสอบและประเมินความพร้อมทางด้านโครงสร้างองค์กร

๓.๓.๓ การตรวจสอบและประเมินด้านการบริหารทรัพย์สิน (ข้อมูลและระบบสารสนเทศ)

๓.๓.๔ การตรวจสอบและประเมินด้านบุคลากร

๓.๓.๕ การตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม

๓.๓.๖ การตรวจสอบและประเมินการสื่อสารและการปฏิบัติการ

๓.๓.๗ การตรวจสอบและประเมินการควบคุมการเข้าถึง

๓.๓.๘ การตรวจสอบและประเมินด้านการพัฒนาระบบ การจัดซื้อจัดหาระบบ การดูแลระบบ

๓.๓.๙ การตรวจสอบและประเมินด้านความพร้อมรับมือกับเหตุการณ์

๓.๓.๑๐ การตรวจสอบและประเมินด้านผลกระทบและความต่อเนื่องของการปฏิบัติการกิจ

๓.๓.๑๑ การตรวจสอบและประเมินด้านการปฏิบัติตามกฎหมายและสัญญา

๓.๔ ระบุความเสี่ยง เหตุการณ์ความเสี่ยงและผลกระทบให้สอดคล้องตามแผนบริหารความเสี่ยงของโรงเรียนดังนี้

๓.๔.๑ การลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๓.๔.๒ การลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๓.๔.๓ การลงบันทึกเข้า (login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

๓.๔.๔ การลักลอบใช้รหัสผ่าน (password) ของผู้อื่นโดยไม่ได้รับอนุญาต

- ๓.๔.๕ ความผิดพลาดของเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (human error) มัลแวร์ (malware) ระบบไฟฟ้าขัดข้อง ความเสียหายจากเพลิงไหม้การโจรกรรมและการขโมย อุปกรณ์คอมพิวเตอร์
- ๓.๕ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น
- ๓.๖ การประมาณความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้
 - ๓.๖.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
 - ๓.๖.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
 - ๓.๖.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ
- ๓.๗ กำหนดมาตรการจัดการความเสี่ยง
 - ๓.๗.๑ ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT contingency plan)
 - ๓.๗.๒ จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของ โรงเรียน

ส่วนที่ ๑๗ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

ศูนย์คอมพิวเตอร์

๓. ขอบปฏิบัติ

๓.๑. จัดอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายที่เข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการจัดอบรมของโรงเรียน

๓.๒. จัดทำคู่มือการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัยและเผยแพร่ทางเว็บไซต์ภายใน (Intranet) ของโรงเรียน

๓.๓. ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยวิธีการติดประกาศประชาสัมพันธ์ เผยแพร่ข้อมูลผ่านจอประชาสัมพันธ์ เผยแพร่ผ่านเว็บไซต์

๓.๔. กำกับติดตามประเมินผลและสำรวจความต้องการของผู้ใช้บริการ