ประกาศโรงเรียนมหิดลวิทยานุสรณ์
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
โรงเรียนมหิดลวิทยานุสรณ์ พ.ศ. ๒๕๖๐

ตามมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา ๓๕ วรรคหนึ่งแห่งพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๔ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษรและทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอนั้น ผู้อำนวยการโรงเรียนมหิดลวิทยานุสรณ์จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า **“ ประกาศโรงเรียนมหิดลวิทยานุสรณ์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงเรียนมหิดลวิทยานุสรณ์ พ.ศ. ๒๕๖๐ ”**

ข้อ ๒ ประกาศนี้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ในประกาศ

๓.๑ โรงเรียน หมายถึง โรงเรียนมหิดลวิทยานุสรณ์

๓.๒ หน่วยงาน หมายถึง สาขาวิชา ฝ่ายงาน หรือหน่วยงานที่เรียกชื่อเป็นอย่างอื่นในสังกัดโรงเรียน

๓.๓ หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงเรียนอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของโรงเรียนโดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๓.๔ ผู้บริหารสูงสุด หมายถึง ผู้อำนวยการโรงเรียน

๓.๕ ผู้บริหารด้านเทคโนโลยีสารสนเทศ หมายถึง ผู้อำนวยการโรงเรียนหรือผู้ที่ผู้อำนวยการโรงเรียนมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของโรงเรียน

๓.๖ ผู้ดูแลระบบ (system administrator) หมายถึง บุคคลที่ได้รับมอบหมายจากผู้บริหารด้านเทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย ไม่ว่าส่วนหนึ่งส่วนใด

๓.๗ ผู้ใช้งาน (user) หมายถึง ครู เจ้าหน้าที่ นักเรียนของโรงเรียน รวมถึงบุคคลหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์หรือระบบเครือข่ายของโรงเรียน

๓.๘ บัญชีผู้ใช้ (user account) หมายถึง ชื่อผู้ใช้และรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียน

๓.๙ ชื่อผู้ใช้ (username) หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบ คอมพิวเตอร์และระบบเครือข่ายที่ได้กำหนดสิทธิ์การใช้งานไว้

๓.๑๐ รหัสผ่าน (password) หมายถึง กลุ่มตัวอักษรหรือตัวเลขหรืออักขระที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล สารสนเทศ และระบบเทคโนโลยีสารสนเทศของโรงเรียน

๓.๑๑ สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๓.๑๒ การเข้าถึงและการควบคุมการเข้าใช้งาน หมายถึง การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๑๓ การพิสูจน์ยืนยันตัวตน (authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ

๓.๑๔ ลงบันทึกเข้า (login) หมายถึง กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์หรือระบบเครือข่าย

๓.๑๕ ลงบันทึกออก (logout) หมายถึง กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์หรือ ระบบเครือข่าย

๓.๑๖ สินทรัพย์ (asset) หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับโรงเรียน

๓.๑๗ อุปกรณ์คอมพิวเตอร์ หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์ โดยอาจใช้ทำหน้าที่เป็นอุปกรณ์สื่อสาร หรือใช้บันทึกข้อมูล เป็นต้น

๓.๑๘ สื่อบันทึกข้อมูล หมายถึง สื่อทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ CD, DVD, flash drive, handy drive, thumb drive, hard drive, portable hard drive, โทรศัพท์มือถือ กล้องถ่ายรูปดิจิตอล กล้องวิดีโอ เครื่องบันทึกเสียงหรือกระดาษ เป็นต้น

๓.๑๙ เจ้าของข้อมูล หมายถึง ผู้ที่ได้รับมอบอำนาจจากผู้บริหารสูงสุดให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นสูญหาย

๓.๒๐ ข้อมูล (data) หมายถึง ข้อเท็จจริงที่เป็นตัวเลข ข้อความ ภาพ เสียง วิดีโอ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๓.๒๑ การเข้ารหัส (encryption) หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๓.๒๒ WEP (wired equivalent privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย โดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล

๓.๒๓ WPA (wi-fi protected access) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๓.๒๔ สารสนเทศ (information) หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

๓.๒๕ ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓.๒๖ ระบบเครือข่าย (network system) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ององค์กรได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น

๓.๒๖.๑ ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๓.๒๖.๒ ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๓.๒๗ ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

๓.๒๘ จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบรับส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยีสารสนเทศ ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพนิ่ง ภาพกราฟิก ภาพเคลื่อนไหวและเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ ผ่านมาตรฐานการรับส่ง เช่น SMTP,POP3 และ IMAP เป็นต้น

๓.๒๙ VPN (Virtual private network) หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓.๓๐ ไฟร์วอลล์ (firewall) หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย

๓.๓๑ อุปกรณ์กระจายสัญญาณไร้สาย (access point) หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๓.๓๒ SSID (service set identifier) หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๓.๓๓ MAC Address (media access control address) หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่มากับอีเทอร์เน็ตการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน

๓.๔๐ ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

๓.๔๑ การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงเรียน

๓.๔๒ ระบบสำรอง (disaster recovery site : DR site) หมายถึง ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็นสามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

๓.๔๓ การสำรองข้อมูล (backup) หมายถึง การสำเนาข้อมูลต่าง ๆ เก็บไว้ในอีกหน่วยความจำหนึ่ง (media or storage) เพื่อเป็นการป้องกันเมื่อเกิดความเสียหายของระบบคอมพิวเตอร์หรือของข้อมูลในหน่วยความจำที่ใช้งานอยู่

๓.๔๔ การกู้คืนข้อมูล (data recovery) หมายถึง การฟื้นคืนสภาพข้อมูลที่ได้รับความเสียหายในระบบคอมพิวเตอร์ให้สามารถใช้งานได้จากสื่อบันทึกที่สำรองข้อมูลไว้ เช่น ฐานข้อมูลระบบงานคอมพิวเตอร์ เป็นต้น

๓.๔๕ อัพเดท (update) หมายถึง การปรับปรุงข้อมูลด้านต่าง ๆ ของระบบเทคโนโลยีสารสนเทศให้ทันสมัยอยู่เสมอ

๓.๔๖ ช่องโหว่ (vulnerability) หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๔๗ โปรแกรมประสงค์ร้าย (malware) หมายถึง ชุดคำสั่งหรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย ได้แก่ ไวรัสคอมพิวเตอร์ (computer virus) สปายแวร์ (spyware) หนอน (worm) ม้าโทรจัน (trojan horse) ฟิชชิง (phishing) หรือจดหมายลูกโซ่ (mass mailing) เป็นต้น

๓.๔๘ ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบเทคโนโลยีสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๓.๔๙ เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓.๕๐ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของโรงเรียนถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ องค์ประกอบของนโยบาย

ส่วนที่ ๑ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์อุปกรณ์เครือข่ายและระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของระบบเทคโนโลยีสารสนเทศและข้อมูล โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและสื่อสารของโรงเรียน

ส่วนที่ ๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงเรียนและป้องกันการ

บุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยี สารสนเทศและการสื่อสารของโรงเรียนได้อย่างถูกต้อง

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาตรวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงเรียนได้อย่างถูกต้อง

ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานเพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศและบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียน เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

ส่วนที่ ๕ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงเรียน โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายในลักษณะแบบ VLAN

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการเพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศเพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงเรียนและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงเรียนได้อย่างถูกต้อง

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless LAN) ของโรงเรียน โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึง

อย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

ส่วนที่ ๙ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันความเสี่ยงต่อการเข้าถึงข้อมูล การถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาตจากการใช้บริการจากหน่วยงานภายนอกและเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงเรียนเป็นไปอย่างมั่นคงปลอดภัย ให้กำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก

ส่วนที่ ๑๐ ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของโรงเรียนถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

ส่วนที่ ๑๑ การสำรองและกู้คืนข้อมูล เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูลและการกู้คืนระบบ (backup and recovery) โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างสมบูรณ์ ถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

ส่วนที่ ๑๒ การใช้งานจดหมายอิเล็กทรอนิกส์เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของโรงเรียนสามารถสนับสนุนการปฏิบัติงานและการบริหารงานของโรงเรียนเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผลและเพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของโรงเรียนและหน่วยงานเป็นมาตรฐาน อยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับของโรงเรียน

ส่วนที่ ๑๓ ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของโรงเรียนสามารถสนับสนุนการปฏิบัติงานของโรงเรียนเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและเพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของโรงเรียนและหน่วยงานเป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของโรงเรียน

ส่วนที่ ๑๔ การตรวจสอบและประเมินความเสี่ยง เพื่อให้มีมาตรการในการตรวจสอบประเมินควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑๕ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ ความเข้าใจและ

ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ข้อ ๕ ตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงาน (internal auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ ๖ การสร้างความรู้ ความเข้าใจให้กับผู้ใช้งานโดยจัดอบรมให้ความรู้เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศ รวมทั้งมาตรการการเข้าถึงจากผู้ซึ่งไม่ได้รับการอนุญาต

ข้อ ๗ การกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พ.ร.บ. ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๘ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ ได้แก่ องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้อำนวยการโรงเรียนเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๙ ให้สาขาวิชาวิทยาการคอมพิวเตอร์เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้และทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงเรียน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๐ จัดให้มีระบบเทคโนโลยีสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ข้อ ๑๑ รายละเอียดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงเรียนให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ เดือนตุลาคม พ.ศ. ๒๕๖๐

(รองศาสตราจารย์ ดร. วิวัฒน์ เรืองเลิศปัญญากุล)
ผู้อำนวยการโรงเรียนมหิดลวิทยานุสรณ์

เอกสารแนบท้ายประกาศ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑

การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์

(Computing System Control Room Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวของกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์ระบบเครือข่ายและเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งก่อให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของโรงเรียน โดยกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๓. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ผู้ดูแลห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายมีแนวทางปฏิบัติดังนี้

๓.๑ ต้องตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายอย่างเคร่งครัด

๓.๒ ต้องขออนุญาตผู้บริหารสูงสุดกำหนดสิทธิการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายให้แก่บุคคลที่ปฏิบัติหน้าที่ที่เกี่ยวข้องภายในโดยจัดทำเป็นลายลักษณ์อักษร

๓.๓ ต้องจัดทำระบบเก็บบันทึกการเข้าออกห้องควบคุมระบบคอมพิวเตอร์

๓.๔ กรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย ต้องมีการควบคุมอย่างเคร่งครัด โดยเจ้าหน้าที่ศูนย์คอมพิวเตอร์

๓.๕ จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายเป็นประจำ และปรับปรุงสิทธิการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายอย่างน้อยปีละครั้ง

ส่วนที่ ๒
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงเรียนและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงักและทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๒.๓ เจ้าของข้อมูล

๓. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลสารสนเทศ

๓.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๓.๔ ผู้ดูแลระบบต้องจัดให้มีระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ ดังนี้

๓.๔.๑ จัดทำบัญชีสินทรัพย์ระบบเทคโนโลยีสารสนเทศ เพื่อจำแนกกลุ่มของของระบบหรือการทำงาน เพื่อกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๓.๔.๒ จัดทำบัญชีการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๔.๓ ตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๔.๔ ระงับการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เมื่อตรวจพบการละเมิดความปลอดภัย

๓.๕ ผู้ดูแลระบบต้องควบคุมให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๔. ข้อกำหนดเกี่ยวกับการกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๔.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งาน สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น และการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ที่ได้รับอนุญาต

๔.๒ เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๔.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๔.๔ การขอสิทธิในการเข้าสู่ระบบจะต้องมีการทำเป็นเอกสารและมีการลงนามอนุมัติ เอกสารดังกล่าวและต้องมีการจัดเก็บไว้เป็นหลักฐานด้วย

๕. ข้อกำหนดเกี่ยวกับประเภทข้อมูลลำดับชั้นความลับของข้อมูล

๕.๑ ประเภทข้อมูล

๕.๑.๑ ข้อมูลทั่วไปและข่าวสารของโรงเรียน เป็นข้อมูลทั่วไป บุคคลทั่วไปสามารถเข้าถึงได้ โดยผ่านเว็บไซต์ของโรงเรียน

๕.๑.๒ ข้อมูลระบบงานบุคลากร เป็นข้อมูลส่วนบุคคล ไม่เปิดเผยให้บุคคลภายนอกทราบ สามารถเข้าถึงได้ โดยผ่านระบบงานบริหารงานบุคคล มีการกำหนดสิทธิการเข้าถึงข้อมูล

๕.๑.๓ ข้อมูลระบบงานวิชาการ เป็นข้อมูลภายใน ใช้สื่อสารภายในระหว่างบุคลากรที่ได้รับสิทธิเท่านั้น สามารถเข้าถึงได้ โดยผ่านระบบงานวิชาการ มีการกำหนดสิทธิการเข้าถึงข้อมูล

๕.๑.๔ ข้อมูลระบบงานกิจการนักเรียน เป็นข้อมูลภายใน ใช้สื่อสารภายในระหว่างบุคลากรที่ได้รับสิทธิเท่านั้น สามารถเข้าถึงได้ โดยผ่านระบบงานกิจการนักเรียน มีการกำหนดสิทธิการเข้าถึงข้อมูล

๕.๑.๕ ข้อมูลระบบงานอาคารสถานที่และยานพาหนะ เป็นข้อมูลภายใน ใช้สื่อสารภายในระหว่างบุคลากรที่ได้รับสิทธิเท่านั้น สามารถเข้าถึงได้ โดยผ่านระบบงานอาคารสถานที่และยานพาหนะ มีการกำหนดสิทธิการเข้าถึงข้อมูล

๕.๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบถือว่า

เป็นแนวทางที่เหมาะสมที่ในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๕.๒.๑ การกำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสารกำหนดไว้ ๓ ระดับ ได้แก่ ลับ ลับมาก ลับที่สุดและมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสารและการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

๕.๒.๒ การควบคุมเอกสารโดยกำหนดให้มีมาตรการควบคุมต่าง ๆ คือการจัดทำทะเบียนการตรวจสอบการจัดทำเอกสารการสำเนาและการแปลการโอนการรับ การส่ง การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉินเวลาสูญหายรวมถึงการเปิดเผยข้อมูลในเอกสาร

๕.๓ กำหนดระดับชั้นการเข้าถึงระบบเทคโนโลยีสารสนเทศ ดังนี้

๕.๓.๑ ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

๕.๓.๒ ผู้ดูแลระบบ มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่

๕.๓.๓ บุคลากรของโรงเรียน เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้

๕.๓.๔ ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลทั่วไปและข่าวสารของโรงเรียน ผ่านเว็บไซต์ของโรงเรียน เท่านั้น ไม่สามารถเขียน แก้ไข และลบข้อมูลได้

๕.๔ ระยะเวลาการเข้าใช้งาน สามารถเข้าถึงได้ ๒๔ ชั่วโมง ทุกวัน

๕.๕ ช่องทางการเข้าถึง

๕.๕.๑ ผ่านระบบเครือข่ายของโรงเรียน

๕.๕.๒ ผ่านระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ต

๕.๕.๓ ผ่านระบบตรวจสอบสิทธิการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียน

๖. การบริหารจัดการการเข้าถึงของผู้ใช้

๖.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของโรงเรียนเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น และต้องกำหนดให้มียกเลิกสิทธิการใช้งานเมื่อลาออกไปต้องทำภายใน ๗ วันหรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน

๖.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๖.๓ การบริหารจัดการบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

๖.๓.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในส่วนที่ ๓“การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๖.๓.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ในส่วนที่ ๓ “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

๖.๓.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้หมายถึงผู้ใช้ที่มีสิทธิสูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๖.๓.๓.๑ ได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้น ๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

๖.๓.๓.๒ ควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

๖.๓.๓.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๖.๔ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๖.๔.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับให้กับข้อมูลวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๖.๔.๒ เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้งเพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๖.๔.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๖.๔.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะต้องทำการเข้ารหัสที่เป็นมาตรฐานสากล

๗. กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศของโรงเรียนในแต่ละประเภทดังนี้

๗.๑ ข้อมูลนักเรียน หน่วยงานหลักคือ ฝ่ายวิชาการ

๗.๒ ข้อมูลบุคลากร หน่วยงานหลักคือ ฝ่ายอำนวยการ

๗.๓ ข้อมูลการเงินและบัญชี หน่วยงานหลักคือ ฝ่ายคลังและพัสดุ

๗.๔ ข้อมูลทางการศึกษา ขึ้นอยู่กับสาขาวิชาที่โรงเรียนมอบหมายเป็นหน่วยงานหลัก

๗.๕ ข้อมูลทางการบริหาร ขึ้นอยู่กับฝ่ายที่โรงเรียนมอบหมายเป็นหน่วยงานหลัก

๗.๖ ข้อมูลการจราจรทางคอมพิวเตอร์ ศูนย์คอมพิวเตอร์

๗.๗ การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของโรงเรียน

๘. การควบคุมการปรับปรุงเปลี่ยนแปลง

๘.๑ การปรับปรุงเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการดังนี้

๘.๑.๑ พิจารณาวางแผนดำเนินการปรับปรุงเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการปรับปรุงเปลี่ยนแปลง

๘.๑.๒ แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการปรับปรุงเปลี่ยนแปลงนั้นๆ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง

๘.๑.๓ ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการปรับปรุงเปลี่ยนแปลง

๘.๒ ต้องจัดเก็บซอร์สโค้ดและไลบรารี่ของระบบสารสนเทศทั้งเวอร์ชั่นปัจจุบันและเวอร์ชั่นเก่าไว้ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

๙ การกำหนดการใช้งานตามภารกิจ

๙.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

๙.๑.๑ นักเรียน จะให้สิทธิทันทีที่มีสภาพเป็นนักเรียนและหมดสิทธิเมื่อพ้นสภาพนักเรียนไปแล้ว ๙๐ วัน

๙.๑.๒ บุคลากร จะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นบุคลากร

๙.๑.๓ ผู้บริหาร จะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิเมื่อพ้นสภาพการเป็นผู้บริหาร

๙.๑.๔ บุคคลภายนอก ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

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

เพื่อกำหนดมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งานมิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาตรวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ผู้ดูแลระบบ

๓. การแบ่งกลุ่มบัญชีผู้ใช้

บัญชีผู้ใช้ระบบเทคโนโลยีสารสนเทศของโรงเรียนจัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของโรงเรียน 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 นักเรียนใหม่ทุกคนจะได้รับบัญชีผู้ใช้ตามข้อมูลที่ฝ่ายวิชาการกำหนด

๔.๒ ครูผู้สอน, เจ้าหน้าที่, อาจารย์พิเศษ จะได้รับบัญชีผู้ใช้ตามข้อมูลที่งานบุคคลกำหนด

๔.๓ บัญชีผู้ใช้งานกลุ่มผู้บริหาร ศูนย์คอมพิวเตอร์จะเพิ่มสิทธิของกลุ่มผู้บริหารให้กับบัญชีในกรณีมีบัญชีใช้งานเดิมอยู่แล้ว กรณีเป็นการเปิดบัญชีใหม่ผู้บริหารจะได้รับบัญชีผู้ใช้งานหลังจากเจ้าหน้าที่งานบุคคลส่งข้อมูลให้กับศูนย์คอมพิวเตอร์เพื่อนำเข้าสู่ระบบ

๔.๔ บุคคลอื่น ๆ ที่โรงเรียนมอบสิทธิให้ ได้แก่ ผู้ทรงคุณวุฒิของสาขาวิชา/ฝ่ายงาน, นักเรียน/ครูจากโครงการแลกเปลี่ยน, บริษัทผู้เข้าดำเนินการโครงการต่าง ๆ สามารถลงทะเบียนขอบัญชีผู้ใช้ มีขั้นตอนดังนี้

๔.๔.๑ สาขาวิชา/ฝ่ายงานผู้เกี่ยวข้องกับบุคคลอื่น ๆ ที่ โรงเรียนมอบสิทธิให้ดาวน์โหลดแบบฟอร์ม ศค.๐๖ จากเว็บไซต์ศูนย์คอมพิวเตอร์ โดยกรอกข้อมูลให้ครบถ้วน และนำบันทึกข้อความหรือหนังสือที่ผ่านการขออนุญาตจากผู้บริหารติดต่อที่ศูนย์คอมพิวเตอร์

๔.๔.๒ ศูนย์คอมพิวเตอร์จะออกบัญชีผู้ใช้ให้ ตามข้อมูลที่ระบุ และแจ้งผู้รับผิดชอบทางอีเมลที่ระบุไว้ในแบบฟอร์ม

๔.๔.๓ ผู้รับผิดชอบของสาขาวิชา/ฝ่ายงาน จะต้องรับผิดชอบความเสียหายใด ๆ ที่จะเกิดจากการใช้งานบัญชีผู้ใช้ที่ศูนย์คอมพิวเตอร์ออกให้

๔.๔.๔ หากต้องการเปลี่ยนแปลงผู้รับผิดชอบบัญชีผู้ใช้ ให้แจ้งศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษรลงนามโดยหัวหน้าสาขาวิชา/ฝ่ายงาน โดยระบุผู้รับผิดชอบเดิมและชื่อผู้รับผิดชอบใหม่พร้อมบัญชีผู้ใช้และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

๔.๔.๕ หากต้องการยกเลิกบัญชีผู้ใช้ ให้แจ้งศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษรลงนามโดยหัวหน้าสาขาวิชา/ฝ่ายงาน ระบุชื่อผู้รับผิดชอบและจำนวนบัญชีผู้ใช้ที่ต้องการยกเลิก

๔.๔.๖ บัญชีผู้ใช้งานจะถูกยกเลิกตามวันเวลาที่ระบุในแบบฟอร์มหากต้องการขยายเวลาให้แจ้งศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษรลงนามโดยหัวหน้าสาขาวิชา/ฝ่ายงาน ระบุชื่อผู้รับผิดชอบ และจำนวนบัญชีผู้ใช้ที่ต้องการขยายเวลา

๕. การจัดการสิทธิของผู้ใช้งาน

๕.๑ เมื่อบุคลากรในสาขาวิชา/ฝ่ายงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิการใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิออกจากระบบทันที

๕.๒ การแจ้งขอใช้สิทธิ/เปลี่ยนแปลงสิทธิในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบเทคโนโลยีสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น มีขั้นตอนดังนี้

๕.๒.๑ ลงชื่อโดยหัวหน้าสาขาวิชา/ฝ่ายงานที่ขอใช้

๕.๒.๒ ส่งถึงผู้บริหาร

๕.๒.๓ สาขาวิชา/ฝ่ายงานสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๕.๓ ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๕.๔ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอและต้องได้รับการอนุมัติจากผู้บริหาร โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา ดังนี้

๕.๔.๑ ควบคุมการใช้งานอย่างเข้มงวด โดยผู้ดูแลระบบต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๕.๔.๒ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๕.๔.๓ ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

๖. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๖.๑ ผู้ดูแลระบบเป็นผู้กำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๖.๒ ผู้ดูแลระบบเป็นผู้กำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๖.๓ ผู้ดูแลระบบจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง

๖.๔ ผู้ดูแลระบบกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการคาดเดา

๖.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะหรือทุกครั้งที่มีการแจ้งเตือนหรือบังคับให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ

๖.๖ ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันที เมื่อเลิกใช้งานระบบหรือไม่อยู่หน้าจอเป็นเวลานาน

๖.๗ กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธิการใช้งานชั่วคราวจนกว่าจะดำเนินการเปลี่ยนรหัสผ่านเป็นที่เรียบร้อย

๗. การทบทวนสิทธิการเข้าถึง

๗.๑ ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๗.๒ บัญชีผู้ใช้จะหมดอายุ ดังนี้

๗.๒.๑ กรณีบุคลากร หมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของโรงเรียน ยกเว้น ผู้เกษียณอายุราชการซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ตและเว็บเมลเท่านั้น

๗.๒.๒ กรณีนักเรียน หมดอายุหลังพ้นสภาพการเป็นนักเรียน ๙๐ วัน แต่จะเปลี่ยนสภาพเป็นนักเรียนเก่าโดยอัตโนมัติ ซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าเว็บเมลและระบบฐานข้อมูลศิษย์เก่าเท่านั้น

๗.๒.๓ กรณีที่ไม่ใช่บุคลากรของโรงเรียน หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี

ส่วนที่ ๔
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities Policy)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการการปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนมหิดลวิทยานุสรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. ผู้รับผิดชอบ

๒.๑ ผู้ใช้งาน

๓. การใช้งานรหัสผ่าน (password use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศต้องปฏิบัติตามข้อกำหนดการใช้งานรหัสผ่านดังนี้

๓.๑ ตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น

๓.๒ ไม่เปิดเผยรหัสผ่านของตนเอง

๓.๓ จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๓.๔ เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๓.๕ ต้องตั้งรหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษร หรือเกินกว่าขั้นต่ำกำหนดไว้

๓.๖ ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๓.๗ ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๓.๘ หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน ได้แก่ 123, abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน ได้แก่ 111, aaa

๓.๙ ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่สื่อถึงตัวผู้ใช้งาน ได้แก่ ชื่อ นามสกุล ชื่อเล่น

๓.๑๐ เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่โรงเรียนกำหนด

๓.๑๑ เปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๓.๑๒ เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการลงบันทึกเข้าสู่ระบบงาน

๓.๑๓ ไม่บันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้เพื่อความสะดวกของตนเองเมื่อทำการลงบันทึกเข้าในภายหลัง

๓.๑๔ ไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น

๓.๑๕ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

๔. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

๔.๑ ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน

๔.๒ ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ใช้งานชั่วคราว

๔.๓ ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๔.๔ ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์คอมพิวเตอร์ทุกเครื่อง ต้องตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๕. การจัดวางและการป้องกันอุปกรณ์

๕.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้รับอนุญาต

๕.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

๕.๓ ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณที่มีระบบสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว ได้แก่ การตรวจสอบระดับอุณหภูมิ ความชื้นว่าอยู่ในระดับปกติหรือไม่

๖. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy)

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึก ข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานดังนี้

๖.๑ ผู้ใช้งานต้องจัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคงปลอดภัย

๖.๒ เครื่องคอมพิวเตอร์ต้องมีกลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๖.๓ ต้องป้องกันการใช้งานและควบคุมทรัพย์สิน ดังนี้

๖.๓.๑ ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันทรัพย์สินของโรงเรียน

๖.๓.๒ ลงชื่อออกจากระบบทันทีเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๖.๓.๓ จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

๖.๓.๔ ล็อคเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งาน

๖.๔ สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖.๕ โปรแกรมต่าง ๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของโรงเรียน เป็นโปรแกรมที่โรงเรียนได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมและนำไปติดตั้งบนคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน เพราะเป็นการกระทำที่ผิดกฎหมาย

๖.๖ ต้องลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

๗. การป้องกันโปรแกรมประสงค์ร้าย (malware)

๗.๑ ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๗.๒ ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๗.๓ ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านระบบเครือข่าย หรือ สื่อบันทึกข้อมูลทุกครั้ง

๘. การเข้ารหัสข้อมูลที่เป็นความลับ

ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ 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 5220.22-M, NIST 800-88

ส่วนที่ ๕
การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงเรียน 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 โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของโรงเรียน

๓.๑.๒ โรงเรียนไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความต้องการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุกเข้าสู่บัญชีผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว โรงเรียนไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๓.๑.๔ ห้ามไม่ให้ผู้ใดเข้าใช้งานโดยไม่ได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของโรงเรียน

๓.๑.๕ โรงเรียนให้บัญชีผู้ใช้งานเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้ และห้ามมิให้บุคคลใดใช้บัญชีผู้ใช้งานของบุคคลอื่นแม้ว่าจะได้รับอนุญาตจากเจ้าของบัญชีแล้วก็ตาม

๓.๑.๖ บัญชีผู้ใช้งานที่โรงเรียนให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งานนั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๑.๗ บัญชีผู้ใช้งานและแฟ้มทั้งหมดที่อยู่บนอุปกรณ์คอมพิวเตอร์และระบบเครือข่าย ถือเป็นสินทรัพย์ของโรงเรียน โรงเรียนอนุญาตให้ใช้งานเพื่อประโยชน์ทางวิชาการและการสนับสนุนทางวิชาการเท่านั้น

๓.๒ ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๓.๒.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงได้เพียงบริการที่ได้รับอนุญาตเท่านั้น

๓.๒.๒ ผู้ดูแลระบบต้องกำหนดระบบเทคโนโลยีสารสนเทศที่ต้องควบคุมการเข้าถึงโดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๓.๒.๓ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงานต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานได้ ดังนี้

๓.๒.๓.๑ การเข้าสู่ระบบจากภายนอกหน่วยงาน ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานที่จะเข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ทำการพิสูจน์ยืนยันตัวตน ด้วยชื่อผู้ใช้งานและรหัสผ่านทุกครั้ง ผ่านระบบเครือข่ายเสมือน SSL VPN (Secure Sockets Layer virtual private network)

๔. การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

ผู้ดูแลระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔.๑ ผู้ดูแลระบบต้องจัดทำแผนผังระบบเครือข่ายและใช้หมายเลขไอพีแอดเดรสในการระบุอุปกรณ์บนระบบเครือข่าย

๔.๒ ผู้ดูแลระบบต้องควบคุมการใช้งานอย่างเหมาะสมและจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ โดยผู้ที่ได้รับอนุญาตให้เข้าใช้งานจะต้องพิสูจน์ยืนยันตัวตนด้วยชื่อผู้ใช้งานและรหัสผ่านทุกครั้ง ผ่านทางหมายเลขไอพีแอดเดรสที่อนุญาต ซึ่งจะต้องได้มาจากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server)

๔.๓ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องในโรงเรียนจะต้องลงทะเบียนกับศูนย์คอมพิวเตอร์

๔.๔ อุปกรณ์ใด ๆ ที่นำมาเชื่อมต่อกับเครือข่าย ต้องได้รับการอนุมัติจากผู้บริหารสูงสุด และผ่านทางผู้บริหารด้านเทคโนโลยีสารสนเทศ

๕. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕.๑ ผู้ดูแลระบบต้องกำหนดการเปิดปิด พอร์ต-อุปกรณ์เครือข่ายตามความจำเป็นและจำกัดการเข้าถึงเครือข่ายที่ใช้ร่วมกัน

๕.๒ ผู้ใช้งานที่ต้องการเปิดพอร์ต ต้องทำบันทึกขออนุมัติจากผู้บริหารด้านเทคโนโลยีสารสนเทศ พร้อมแนบโครงการและระบุเหตุผลความจำเป็น

๕.๓ ผู้ดูแลระบบดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย

๕.๔ ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

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 ตรวจสอบการเชื่อมต่อเครือข่าย

๗.๒ จำกัดสิทธิความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย อนุญาตให้เชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๗.๓ ระบุอุปกรณ์เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๗.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

๗.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๘. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจดังนี้

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 ๖
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 ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจออัตโนมัติเพื่อทำการล็อคหน้าจอทุกครั้งที่ไม่มีการใช้งาน และต้องกำหนดรหัสผ่านเพื่อเข้าใช้งาน

๓.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๕ ผู้ใช้งานต้องลงบันทึกออกทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓.๖ ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนการเข้าสู่ระบบจะเสร็จสมบูรณ์

๓.๗ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓.๘ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง command line

๔. การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication)

๔.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน

๔.๒ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้งการยืนยันว่าเป็นผู้ใช้งานที่ระบุถึง

๔.๓ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศเพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาดผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๔.๔ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ของเครื่องคอมพิวเตอร์และระบบเครือข่ายเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๕ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่ายหรือจ่ายแจกให้ผู้อื่น

๔.๖ ผู้ใช้งานจะต้องลงบันทึกเข้าโดยใช้บัญชีผู้ใช้ของตนเอง

๕. การบริหารจัดการรหัสผ่าน (password management system)

ระบบบริหารจัดการรหัสผ่านต้องสามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๕.๑ ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเองที่เว็บเมลของโรงเรียน

๕.๒ ผู้ใช้งานต้องตั้งรหัสผ่านตามข้อกำหนดการใช้งานรหัสผ่านของโรงเรียน

๕.๓ ระบบบริหารจัดการรหัสผ่านต้องสามารถตรวจสอบความถูกต้องของรหัสผ่านตามข้อกำหนดการใช้งานรหัสผ่านของโรงเรียน

๕.๔ ระบบบริหารจัดการรหัสผ่านต้องให้ผู้ใช้งานยืนยันรหัสผ่านเพื่อตรวจสอบความถูกต้อง

๖. การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities)

การใช้งานโปรแกรมอรรถประโยชน์ต้องจำกัดและควบคุมการใช้งานสำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

๖.๑ จำกัดสิทธิการเข้าถึงการใช้โปรแกรมอรรถประโยชน์

๖.๒ กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๖.๓ ห้ามผู้ใช้งานติดตั้งโปรแกรมอรรถประโยชน์โดยไม่ได้รับอนุญาตหรือละเมิดลิขสิทธิ์

๗. การยุติการใช้งานระบบเทคโนโลยีสารสนเทศเมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง (session time-out)

กำหนดให้มีการยุติการใช้งานระบบเทคโนโลยีสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้น

๘. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (limitation of connection time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบเทคโนโลยีสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๘.๑ การเชื่อมต่อระบบเทคโนโลยีสารสนเทศสำหรับระบบเทคโนโลยีสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง กำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

๘.๒ กำหนดให้ระบบสารเทคโนโลยีสนเทศที่มีความสำคัญสูงและระบบเทคโนโลยีสารสนเทศที่มีการใช้งานในสถานที่ที่มีความเสี่ยง มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๗
การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ
(Application and Information Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงเรียนและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๓. การจำกัดการเข้าถึงสารสนเทศ (information access control)

๓.๑ ผู้ดูแลระบบต้องกำหนดให้มีขั้นตอนปฏิบัติในการลงทะเบียนบุคลากรใหม่ของโรงเรียนเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอยู่เสมอ

๓.๓ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำงานข้อมูลแต่ละประเภทชั้นความลับดังต่อไปนี้

๓.๓.๑ ต้องกำหนดบัญชีผู้ใช้เพื่อใช้ในการตรวจสอบตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓.๓.๒ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓.๓.๓ ต้องกำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๔. การจัดการกับระบบที่ไวต่อการรบกวน

๔.๑ ข้อปฏิบัติสำหรับระบบซึ่งไวต่อการรบกวน

๔.๑.๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อโรงเรียน ได้แก่

๔.๑.๑.๑ ระบบบริหารจัดการงานบุคคล ซึ่งดูแลรับผิดชอบโดยฝ่ายอำนวยการ

๔.๑.๑.๒ ระบบบริหารจัดการงานวิชาการ ซึ่งดูแลรับผิดชอบโดยฝ่ายวิชาการ

๔.๑.๑.๓ ระบบการเงิน ซึ่งดูแลรับผิดชอบโดยฝ่ายคลังและพัสดุ

ซึ่งจะได้รับการแยกออกจากระบบงานอื่น ๆ ของโรงเรียน

๔.๑.๒ ควบคุมสภาพแวดล้อมของระบบ โดยมีห้องควบคุมแยกเป็นสัดส่วน

๔.๑.๓ ต้องกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

๔.๒ ต้องควบคุมการเข้าถึงผ่านอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกดังนี้

๔.๒.๑ ต้องกำหนดสิทธิและขอบเขตการทำงาน ชนิดของงาน และระบบงาน

๔.๒.๒ ต้องกำหนดระยะเวลาการเข้าถึงและจัดให้มีการควบคุมการปฏิบัติงานและปรับปรุงสิทธิหลังจากการปฏิบัติงาน

๕. ข้อปฏิบัติในการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

เพื่อป้องกันสารสนเทศจากความเสี่ยงจากการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๕.๑ ตรวจสอบความพร้อมของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๕.๒ เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

๕.๓ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืน

๕.๔ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๕.๕ ต้องจัดให้มีการสร้างความตระหนักเพื่อระมัดระวังและป้องกันการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๕.๖ ผู้ดูแลระบบต้องกำหนดให้มีการป้องกันข้อมูลที่สำรองไว้ในอุปกรณ์จากการถูกขโมย สูญหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

๖. ข้อปฏิบัติสำหรับการปฏิบัติงานจากภายนอกหน่วยงาน (teleworking)

๖.๑ ผู้ใช้งานที่ปฏิบัติงานจากภายนอกหน่วยงานต้องผ่านระบบการพิสูจน์ยืนยันตัวตน ด้วยชื่อผู้ใช้งานและรหัสผ่านทุกครั้งผ่านระบบเครือข่ายเสมือน SSL VPN (Secure Sockets Layer virtual private network)

๖.๒ ผู้ดูแลระบบต้องจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้สำหรับผู้ปฏิบัติงานจากระยะไกล ยกเว้นอุปกรณ์ที่โรงเรียนอนุญาตให้ใช้งานได้

๖.๓ ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ ระบบงานและบริการต่าง ๆ ของโรงเรียนที่อนุญาตให้เข้าถึงได้จากระยะไกล

๖.๔ ผู้ดูแลระบบต้องยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๗. ข้อปฏิบัติการควบคุมการใช้บริการงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT outsourcing)

๗.๑ การคัดเลือกผู้ให้บริการ

๗.๑.๑ มีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบ รัดกุม และเป็นที่น่าเชื่อถือ

๗.๑.๒ มีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

๗.๒ การควบคุมผู้ให้บริการ

๗.๒.๑ ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๗.๒.๒ กำหนดให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๗.๒.๓ กำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข กำหนดให้มีขั้นตอนในการตรวจรับงานของผู้ให้บริการอย่างชัดเจน

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 เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าเกิดขึ้นในระบบเครือข่ายไร้สาย

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ต้องได้รับอนุญาตจากผู้บริหารสูงสุดตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน

๓.๔ ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน

๓.๕ ผู้ดูแลระบบต้องเปลี่ยนค่าปริยาย SSID ที่ถูกกำหนดมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สายมาใช้งาน

๓.๖ ผู้ดูแลระบบต้องแยก SSID ของผู้ใช้งานที่เป็นบุคลากรของโรงเรียน และผู้ใช้งานตามโครงการทางวิชาการต่าง ๆ ที่โรงเรียนดำเนินการจัดขึ้น โดยควบคุมสิทธิและระยะเวลาในการเข้าถึงระบบเครือข่ายไร้สาย

๓.๗ ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อผู้ใช้งานและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อผู้ใช้งานและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๓.๘ ผู้ดูแลระบบต้องใช้ระบบพิสูจน์ตัวตนและการเข้ารหัสข้อมูลระหว่างอุปกรณ์ปลายทางและอุปกรณ์กระจายสัญญาณไร้สาย

๓.๙ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ตและฐานข้อมูลภายในต่าง ๆ ของโรงเรียน

ส่วนที่ ๙
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Third Party Access Control Policy)

๑. วัตถุประสงค์

เพื่อป้องกันความเสี่ยงจากหน่วยงานภายนอกต่อการเข้าถึงข้อมูล การแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต และเพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนเป็นไปอย่างมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๒.๓ เจ้าของโครงการ

๓. ข้อปฏิบัติ

๓.๑ กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

๓.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอก

๓.๒.๑ หน่วยงานภายนอกที่ต้องการสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงเรียนต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บริหารสูงสุด

๓.๒.๒ จัดทำแบบฟอร์มสำหรับให้หน่วยงานภายนอกระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ มีรายละเอียดอย่างน้อยดังนี้

(๑) เหตุผลในการขอใช้

(๒) ระยะเวลาในการใช้

(๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๔) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓.๒.๓ หน่วยงานภายนอกที่ทำงานให้กับโรงเรียนต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของโรงเรียน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓.๒.๔ โรงเรียนต้องพิจารณาการประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศที่เข้าไปปฏิบัติงาน

๓.๒.๕ ผู้ดูแลระบบต้องกำหนดการเข้าถึงข้อมูลโดยหน่วยงานภายนอกเฉพาะบุคคลที่จำเป็นเท่านั้น

๓.๒.๖ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของโรงเรียนให้มีความมั่นคงปลอดภัยทั้งด้านการรักษาความลับ การรักษาความถูกต้องของข้อมูล และการรักษาความพร้อมที่จะให้บริการ

๓.๒.๗ โรงเรียนมีสิทธิตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าโรงเรียนสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๓.๒.๘ หน่วยงานภายนอกที่ทำงานให้กับโรงเรียนต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง

๓.๒.๙ หลังส่งมอบโครงการจากหน่วยงานภายนอก ผู้ดูแลระบบต้องดำเนินการเปลี่ยนรหัสผ่านทันที

ส่วนที่ ๑๐
ความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต
(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของโรงเรียนมหิดลวิทยานุสรณ์ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. ผู้รับผิดชอบ

๒.๑ ผู้ใช้งาน

๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราว์เซอร์ (web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการแก้ปัญหาช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์

๓.๒ ผู้ใช้ต้องทำการ update patch และ hot fix อย่างสม่ำเสมอโดยสามารถ download patch และ hot fix ต่าง ๆ จากเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่

๓.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการตรวจสอบไวรัส (virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๓.๔ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเตอร์เน็ตของโรงเรียนเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๓.๕ ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของโรงเรียน

๓.๖ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับโรงเรียน

๓.๗ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของโรงเรียนที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

๓.๘ ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดที่จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

๓.๙ หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๔. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๔.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่โรงเรียนจัดสรรไว้เท่านั้น

ส่วนที่ ๑๑
การสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

๑. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติสำหรับการสำรองข้อมูลและการกู้คืนระบบ โดยผู้ดูแลระบบสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ดูแลระบบ

๓. ข้อปฏิบัติ

๓.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานสำรองข้อมูลและจัดทำระบบสารสนเทศสำรอง

๓.๒ ผู้ดูแลระบบมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้ในกรณีที่ไม่สามารถปฏิบัติงานได้

๓.๓ ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสมพร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูลสถานที่จัดเก็บ โดยรูปแบบการสำรองข้อมูลอาจแบ่งได้เป็นการสำรองข้อมูลแบบเต็มและการสำรองข้อมูลแบบส่วนต่าง

๓.๔ ผู้ดูแลระบบต้องทำบันทึก รายละเอียดการสำรองข้อมูลได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

๓.๕ ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๓.๖ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหา รายงานต่อหัวหน้าสาขาวิชาวิทยาการคอมพิวเตอร์

๓.๗ ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นรวมทั้งวิธีการที่ใช้แก้ไขด้วย

๓.๘ ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนของการสำรองข้อมูลโดยเคร่งครัด

๓.๙ ผู้ดูแลระบบต้องทำการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมความพร้อม กรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๔. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

๔.๑ ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่อย่างน้อยดังนี้

ที่	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Mail servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลใน Mail box	เดือนละครั้ง
๒	Web servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลเผยแพร่บนเว็บไซต์	เดือนละครั้ง
๓	Database servers	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของระบบ	เดือนละครั้ง
๔	Firewall server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๕	DNS Server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๖	DHCP Server	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๗	server อื่น ๆ	ค่า configure	ก่อนและหลังการเปลี่ยนแปลง
๘	ระบบ MIS	ข้อมูลนักเรียน, ข้อมูลการศึกษา	เดือนละครั้ง
๙	ระบบงานห้องสมุด	ข้อมูลการยืม-คืน	สัปดาห์ละครั้ง
		ข้อมูลหนังสือ	เดือนละครั้ง
๑๐	ระบบบันทึกข้อมูลเข้า-ออกหอพัก	ข้อมูลการเข้า-ออกหอพัก	สัปดาห์ละครั้ง
๑๑	ระบบงานคลังและพัสดุ	การเบิกจ่ายพัสดุ	สัปดาห์ละครั้ง
		ข้อมูลพัสดุ	เดือนละครั้ง
๑๒	ระบบงานบุคคล	บันทึกการเข้างาน	สัปดาห์ละครั้ง
		ข้อมูลบุคลากร	เดือนละครั้ง

๔.๒ ผู้ดูแลระบบต้องทำการเก็บรักษาข้อมูลที่สำรองอย่างน้อย ๑ ชุดแยกสถานที่กัน เพื่อความมั่นคงปลอดภัย และใช้งานได้อย่างต่อเนื่อง

๔.๓ ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการสำรองข้อมูลตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๕. การกู้คืนระบบ (data recovery)

๕.๑ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายจะต้องทำการทดสอบการกู้คืนข้อมูลเป็นระยะ เพื่อให้แน่ใจได้ว่า การสำรองข้อมูลนั้นทำได้อย่างครบถ้วนสมบูรณ์แล้ว

๕.๒ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข แล้วรายงานสรุปผลการปฏิบัติงานต่อหัวหน้าสาขาวิชาวิทยาการคอมพิวเตอร์หรือผู้ที่ได้รับมอบหมายจากหัวหน้าสาขาวิชาวิทยาการคอมพิวเตอร์ทราบ

๕.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (latest update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๕.๔ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันทีพร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๖. การจัดทำแผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ (IT contingency plan)

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ ต้องกำหนดบุคลากรที่เกี่ยวข้องและดำเนินการดังต่อไปนี้

๖.๑ กำหนดแผนเตรียมความพร้อม และกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติ

๖.๒ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๖.๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๖.๔ จัดทำแผนรับมือกับเหตุภัยพิบัติเพื่อให้สามารถกู้คืนระบบเทคโนโลยีสารสนเทศ ที่เสียหายให้สามารถใช้งานได้โดยเร็ว

๖.๕ ทดสอบการปฏิบัติตามแผนอย่างน้อยปีละ ๑ ครั้งโดยการจำลองสถานการณ์

๖.๖ ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๒
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail Policy)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของโรงเรียนสามารถสนับสนุนการปฏิบัติงานและการบริหารงานของโรงเรียนเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของโรงเรียนเป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับของโรงเรียน

๒. ผู้รับผิดชอบ

๒.๑ ผู้ใช้งาน

๒.๒ ผู้ดูแลระบบ

๓. ข้อปฏิบัติสำหรับผู้ใช้งาน

๓.๑ ผู้ใช้งานต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๓.๒ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อโรงเรียนหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของโรงเรียน

๓.๓ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งาน และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตนเอง

๓.๔ ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการทำงานในภารกิจของโรงเรียนเท่านั้น

๓.๕ ลงบันทึกออกจากระบบจดหมายอิเล็กทรอนิกส์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

๓.๖ ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดทุกครั้งเพื่อตรวจสอบไวรัสคอมพิวเตอร์

๓.๗ ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๘ ไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมอันอาจทำให้เสียชื่อเสียงของโรงเรียนหรือข้อมูลที่ทำให้เกิดความแตกแยกในหน่วยงาน

๓.๙ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๓.๑๐ ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ

๔. ข้อปฏิบัติสำหรับผู้ดูแลระบบ

๔.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนให้เหมาะสมกับการเข้าใช้บริการและหน้าที่ความรับผิดชอบของผู้ใช้งาน และทบทวนสิทธิการเข้าใช้งานอย่างน้อยปีละ ๑ ครั้ง

๔.๒ ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ต้องทำการบันทึกออกจากหน้าจอเพื่อตัดการใช้งานจากผู้ใช้งานเมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้

ส่วนที่ ๑๓
ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์
(Terms of Use and Disclaimer)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของโรงเรียนสามารถสนับสนุนการปฏิบัติงานของโรงเรียนให้เป็นไปอย่างถูกต้อง สะดวกรวดเร็ว ทันสถานการณ์ และมีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของโรงเรียนเป็นมาตรฐานอยู่ในกรอบของกฎหมาย 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.๒๕๕๐

๓.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

๓.๑.๓ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐

๓.๑.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๓.๑.๕ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗

๓.๑.๖ ข้อตกลงเงื่อนไขการใช้บริการที่โรงเรียนกำหนด

๓.๒ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ของโรงเรียนจะต้องใช้จดหมายอิเล็กทรอนิกส์นี้เพื่อผลประโยชน์ของโรงเรียน

๓.๓ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน

๓.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือกระทำการใด ๆ ที่ก่อให้เกิดความเสียหายต่อสถาบันชาติ ศาสนา และพระมหากษัตริย์

๓.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนในการประกอบอาชญากรรมทางคอมพิวเตอร์หรือการกระทำใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับของทางราชการ

๓.๖ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อการเผยแพร่ข้อมูลข่าวสาร หรือภาพ เสียง ข้อความที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๗ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของโรงเรียนเพื่อแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบหรือสร้างความเสื่อมเสียหรือเสียหายต่อผู้อื่นหรือโรงเรียน

๓.๘ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (impersonation)

๓.๙ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

(๑) การสร้างจดหมายลูกโซ่ (chain mail)

(๒) การส่งจดหมายจำนวนมาก (spam mail)

(๓) การส่งจดหมายต่อเนื่อง (letter bomb)

(๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๓.๑๐ ห้ามผู้ใช้งานกระทำการใด ๆ ที่อาจสร้างความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของโรงเรียน

๓.๑๑ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของโรงเรียนหรือทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของโรงเรียน

๓.๑๒ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานภายนอกจะต้องเข้ารหัสข้อมูลอย่างเหมาะสมตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่โรงเรียนกำหนด

๓.๑๓ ที่อยู่จดหมายอิเล็กทรอนิกส์และรหัสผ่านของบุคคลหรือหน่วยงานจะต้องเก็บรักษาไว้เป็นความลับ หากสงสัยว่ารั่วไหลจะต้องเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา

๓.๑๔ ผู้ใช้งานหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจ เพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของโรงเรียนได้อย่างถูกต้อง

๓.๑๕ กรณีได้รับการร้องเรียนหรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอให้สงวนสิทธิ์ที่จะยกเลิกหรือระงับบริการแก่ผู้ใช้งานนั้น ๆ เป็นการชั่วคราว เพื่อทำการสอบสวนและตรวจสอบหาสาเหตุของมูลเหตุนั้น ๆ

๓.๑๖ การกระทำใด ๆ ที่เกี่ยวกับการเผยแพร่ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์หรือเว็บไซต์ของผู้ใช้งาน ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้งานนั้น ศูนย์คอมพิวเตอร์โรงเรียนมหิดลวิทยานุสรณ์ ไม่มีส่วนเกี่ยวข้องใด ๆ

ส่วนที่ ๑๔
การตรวจสอบและประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการตรวจสอบ ประเมิน ควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๒.๒ ผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบจากภายนอก (external auditor)

๒.๓ ผู้ดูแลระบบ

๓. ข้อปฏิบัติ

๓.๑ ตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓.๒ ตรวจสอบและประเมินความเสี่ยง โดยคณะกรรมการหรือหน่วยงานหรือบุคคลที่โรงเรียนเห็นสมควร เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๓ การรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลจำเป็นต้องคำนึงถึงหลายด้านหลายมิติ แต่ละด้านก็มีความจำเป็นในการตรวจสอบและประเมินความเสี่ยงแตกต่างกัน โดยให้มี การดำเนินการดังต่อไปนี้

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 การตรวจสอบและประเมินด้านผลกระทบและความต่อเนื่องของการปฏิบัติภารกิจ

๓.๓.๑๑ การตรวจสอบและประเมินด้านการปฏิบัติตามกฎหมายและสัญญา

๓.๔ ระบุความเสี่ยง เหตุการณ์ความเสี่ยง และผลกระทบให้สอดคล้องตามแผนบริหาร ความเสี่ยงของโรงเรียนดังนี้

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) ไวรัสคอมพิวเตอร์ (computer virus) ระบบไฟฟ้าขัดข้อง ความเสียหายจากเพลิงไหม้การโจรกรรมและการขโมยอุปกรณ์คอมพิวเตอร์

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 จัดทำหลักเกณฑ์นโยบายกฎระเบียบในการใช้เครื่องคอมพิวเตอร์และเครือข่ายของโรงเรียน

ส่วนที่ ๑๕
การสร้างความตระหนัก
ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ศูนย์คอมพิวเตอร์

๓. ข้อปฏิบัติ

๓.๑ จัดอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายที่เข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการจัดอบรมของโรงเรียน

๓.๒ จัดทำคู่มือการใช้งานระบบเทคโนโลยีสารสนเทศอย่างปลอดภัยและเผยแพร่ทางเว็บไซต์ภายใน (Intranet) ของโรงเรียน

๓.๓ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยวิธีการติดประกาศประชาสัมพันธ์ เผยแพร่ข้อมูลผ่านจอประชาสัมพันธ์ เผยแพร่ผ่านเว็บไซต์

๓.๔ กำกับติดตามประเมินผลและสำรวจความต้องการของผู้ใช้บริการ