แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ทางด้านระบบเทคโนโลยีสารสนเทศ
(ร่าง)

วิทยาลัยเชียงราย

พ.ศ.๒๕๖๘

โดย
กลุ่มงานบริการเทคโนโลยีสารสนเทศ
วิทยาลัยเชียงราย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๘

ที่มาและความสำคัญ

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕ กำหนดให้หน่วยงานของหน่วยงาน ต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงานนั้น

เพื่อให้ระบบเทคโนโลยีและสารสนเทศของวิทยาลัยเชียงราย หรือต่อไปนี้เรียกว่า "วิทยาลัย" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้ระบบเทคโนโลยีและสารสนเทศในลักษณะที่ไม่ถูกต้องหรือการถูกคุกคามจากภัยต่าง ๆ วิทยาลัยจึงได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดให้มีมาตรฐาน แนวทางและขั้นตอนปฏิบัติให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕

วัตถุประสงค์

(๑) เพื่อจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ อันส่งผลให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของวิทยาลัย

(๒) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ โดยมีการปรับปรุงอย่างต่อเนื่องให้ทันกับการพัฒนาทางด้านเทคโนโลยี

(๓) เพื่อกำหนดมาตรฐานแนวทางปฏิบัติให้บุคลากรวิทยาลัยและผู้เกี่ยวข้องมีความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของวิทยาลัย

(๔) เพื่อเผยแพร่นโยบายให้บุคลากรภายในวิทยาลัยทุกคนรับทราบและจะต้องถือปฏิบัติตาม นโยบายอย่างเคร่งครัด

(๕) เพื่อกำหนดให้ ต้องมีการตรวจสอบและประเมินผลการดำเนินงานไม่น้อยกว่า ๑ ครั้งต่อปี

ขอบเขตของนโยบาย

(๑) การเข้าถึงทรัพยากรสารสนเทศของวิทยาลัย ต้องมีระบบควบคุมและตรวจสอบได้ภายใต้ กรอบกฎหมาย และต้องใช้เพื่อกิจกรรมและภารกิจของวิทยาลัยเท่านั้น

(๒) ระบบสารสนเทศที่มีระดับชั้นความลับ ต้องมีระบบป้องกันการเข้าถึงและการแก้ไขโดยไม่ได้ รับอนุญาต

(๓) ข้อมูลที่มีความสำคัญต่อภารกิจงานของวิทยาลัย จะต้องมีการปกป้องไม่ให้เกิดความเสียหาย ถูกทำลาย หรือดัดแปลงแก้ไข

(๔) วิทยาลัยจะสร้างความตระหนักให้กับบุคลากรทุกระดับเห็นความสำคัญในเรื่องความมั่นคง ปลอดภัยอย่างต่อเนื่อง

(๕) แผนปฏิบัติงานด้านความมั่นคงปลอดภัยของวิทยาลัย จะต้องสามารถปรับเปลี่ยนให้ สอดคล้องกับปัญหาความมั่นคงปลอดภัยและเทคโนโลยีได้อย่างเหมาะสม

องค์ประกอบของนโยบาย ประกอบด้วย

(๑) คำนิยาม

(๒) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(๓) นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

- การเข้าถึงระบบสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
- การควบคุมการเข้าถึงเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ
- การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
- การปฏิบัติงานจากภายนอกวิทยาลัย
- แนวทางปฏิบัติในการใช้งานระบบอินเทอร์เน็ต
- แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ (Social Media)
- แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์
- ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

(๔) การจัดทำระบบสำรองข้อมูล

(๕) การตรวจสอบและประเมินความเสี่ยง

ผู้รับผิดชอบความมั่นคงปลอดภัยข้อมูล

(๑) การบริหารด้านนโยบาย

กลุ่มงานเทคโนโลยีสารสนเทศ มีหน้าที่จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยภายใต้การกำกับของรองอธิการบดีที่กำกับดูแล / หัวหน้ากลุ่มงานบริการเทคโนโลยีสารสนเทศ และจะต้องทบทวนนโยบายฉบับนี้อย่างน้อยปีละ ๑ ครั้ง และนำเสนอให้รองอธิการบดีพิจารณาให้ความเห็นชอบก่อนประกาศใช้ และนโยบายความมั่นคงปลอดภัยให้อยู่ในความดูแลของกลุ่มงานบริการเทคโนโลยีสารสนเทศ โดยมีหน้าที่ดังนี้

- จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
- จัดทำข้อเสนอแนะและกำหนดข้อปฏิบัติที่ทำให้เกิดความร่วมมือระหว่างผู้ใช้ระบบและผู้กำกับดูแลเพื่อให้มั่นใจว่าระบบสารสนเทศของวิทยาลัยมีความมั่นคงปลอดภัย
- มีการทบทวน ปรับปรุงนโยบายและข้อปฏิบัติด้านความมั่นคงปลอดภัยตามความเหมาะสม และได้รับความเห็นชอบจากผู้อำนวยการ

- มีการตรวจสอบ การควบคุมที่มีประสิทธิภาพสำหรับข้อมูลที่มีความสำคัญของวิทยาลัย

(๒) ผู้กับกับดูแล

ผู้กำกับดูแล หมายถึง กลุ่มงานบริการเทคโนโลยีสารสนเทศ ซึ่งได้รับมอบหมายให้ทำหน้าที่ดูแลระบบสารสนเทศของวิทยาลัย โดยให้มีการควบคุมการเข้าถึงระบบสารสนเทศ การจัดหาหรือให้มีระบบป้องกันภัย ตลอดจนการเฝ้าระวัง ตรวจจับ วิเคราะห์ และจัดทำรายงานที่เกี่ยวกับการฝ่าฝืนระบบรักษาความมั่นคงปลอดภัยที่อาจเกิดกับระบบสารสนเทศของวิทยาลัย

(๓) บุคลากร

บุคลากรของวิทยาลัย มีสิทธิ์ใช้ทรัพยากรสารสนเทศภายใต้ข้อกำหนด ดังนี้

- บุคลากรจะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยฉบับนี้อย่างเคร่งครัด
- บุคลากรต้องใช้ทรัพยากรสารสนเทศตามนโยบายที่อนุญาตให้ใช้งาน
- บุคลากรมีหน้าที่ตรวจสอบข้อมูลอย่างสม่ำเสมอ เพื่อมั่นใจว่าข้อมูลสำคัญในเครื่องคอมพิวเตอร์ภายใต้ความรับผิดชอบมีความมั่นคงปลอดภัย
- บุคลากรต้องปฏิบัติตามคำแนะนำด้านความมั่นคงปลอดภัยสำหรับคอมพิวเตอร์ที่อยู่ภายใต้ความรับผิดชอบ

(๔) บุคคลภายนอก/หน่วยงานภายนอก

บุคคลภายนอก/หน่วยงานภายนอกทั่วไปไม่ได้รับสิทธิ์เข้าใช้ทรัพยากรสารสนเทศของ วิทยาลัย ยกเว้น ได้รับอนุญาตเป็นกรณีเฉพาะภายใต้ระเบียบของวิทยาลัย

การฝ่าฝืนนโยบาย

กรณีตรวจพบว่ามีการฝ่าฝืนนโยบายความมั่นคงปลอดภัยของวิทยาลัย ให้ผู้ดูแลระบบรายงานเหตุการณ์ฝ่าฝืนนั้นกับหัวหน้ากลุ่มงานบริการเทคโนโลยีสารสนเทศ/รองอธิการบดีที่กำกับดูแล ภารกิจหากการละเมิดนั้นขัดต่อกฎหมายให้ประสานงานภารกิจอำนวยการเพื่อดำเนินการตามระเบียบของวิทยาลัยและรายงานต่อรองอธิการบดี

มาตรการดำเนินการ

ผู้ดูแลระบบมีอำนาจในการตัดการเชื่อมต่อของเครื่องคอมพิวเตอร์ที่ถูกตรวจพบว่าเป็นต้นเหตุของการละเมิดมาตรการความมั่นคงปลอดภัย หรือตรวจพบว่าเป็นจุดเสี่ยงของความมั่นคงปลอดภัยต่อระบบสารสนเทศของวิทยาลัย โดยจะต้องรายงานให้หัวหน้ากลุ่มงานบริการเทคโนโลยีสารสนเทศทราบก่อนดำเนินการ ในกรณีที่ร้ายแรงให้หัวหน้ากลุ่มงานบริการเทคโนโลยีสารสนเทศรายงานเสนอต่อผู้บริหารเพื่อพิจารณาโทษทางวินัยหรือทางกฎหมาย

กฎหมายที่เกี่ยวข้อง

การใช้สารสนเทศและการตรวจสอบสารสนเทศตามนโยบายความมั่นคงปลอดภัยจะต้องสอดคล้องกับกฎหมายดังต่อไปนี้

- กฎหมายธุรกรรมอิเล็กทรอนิกส์ พ.ศ.๒๕๔๕
- กฎหมายลิขสิทธิ์ พ.ศ.๒๕๓๗๖

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ประกอบด้วย

“วิทยาลัย” (College) หมายความว่า วิทยาลัยเชียงราย

“ระบบคอมพิวเตอร์” (Computer System) หมายความว่า อุปกรณ์อิเล็กทรอนิกส์หรือชุดอุปกรณ์อิเล็กทรอนิกส์ใด ๆ ที่มีการเชื่อมการทำงานเข้าด้วยกันโดยการกำหนดคำสั่งชุดคำสั่งหรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติซึ่งได้แก่ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และอุปกรณ์รอบข้าง (Peripheral) ต่าง ๆ ในการเข้ารับหรือป้อนข้อมูล (Input) นำออกหรือแสดงผลข้อมูล (Output) และบันทึกหรือเก็บข้อมูล (Store and Record)

“ระบบเครือข่าย” (Network System) หมายความว่า การนำคอมพิวเตอร์หลาย ๆ เครื่องมาต่อพ่วงกันเพื่อให้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของวิทยาลัยเช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ระบบอินเทอร์เน็ต” (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆของวิทยาลัยเข้ากับเครือข่ายอินเทอร์เน็ตสากล

“ระบบเทคโนโลยีสารสนเทศ” (Information Technology System) หมายความว่า ระบบงานของวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่วิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผนการบริหารการสนับสนุนการให้บริการการพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบเช่นระบบคอมพิวเตอร์ระบบเครือข่ายโปรแกรมข้อมูลและสารสนเทศเป็นต้น

“สารสนเทศ” (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลขข้อความหรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจและอื่นๆ

“ระบบสารสนเทศ” (Information System) หมายความว่า ระบบของการจัดเก็บประมวลผล ข้อมูลโดยอาศัยบุคคลและเทคโนโลยีสารสนเทศในการดำเนินการ เพื่อให้ได้สารสนเทศที่เหมาะสมกับงาน หรือภารกิจแต่ละอย่าง

“เครื่องคอมพิวเตอร์” (Computer) หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

“ผู้ใช้งาน” (User) หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน/บริหารจัดการ/ดูแลรักษาระบบเทคโนโลยีสารสนเทศของวิทยาลัย โดยการให้สิทธิ์และหน้าที่ขึ้นอยู่กับ นโยบายของวิทยาลัยโดยกำหนดไว้ดังนี้

“ผู้บริหาร” (Executive) หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของวิทยาลัย

“ผู้ดูแลระบบ” (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บริหารให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“บุคลากร” (Personnel) หมายความว่า เจ้าหน้าที่ ลูกจ้างตามสัญญาจ้างของวิทยาลัย

“หน่วยงานภายนอก” (Outside Organization) หมายความว่า บุคคล องค์กรหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของวิทยาลัย โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

"สิทธิ์ของผู้ใช้งาน" (User Authorization) หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นใดที่อนุญาตให้ผู้ใช้งานเกี่ยวข้องกับระบบสารสนเทศของวิทยาลัย

"สินทรัพย์" (Asset) หมายความว่า ข้อมูล ระบบข้อมูลและทรัพย์สินด้านเทคโนโลยีสารสนเทศ ของวิทยาลัยเช่นเครื่องคอมพิวเตอร์อุปกรณ์ระบบเครือข่ายซอฟต์แวร์ลิขสิทธิ์เป็นต้น

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" (Information Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับหน่วยงานภายนอก

"ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด(Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ(Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจ คาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคง ปลอดภัยถูกคุกคาม

"สื่อสังคมออนไลน์" (Social Media) หมายความว่า สื่ออิเล็กทรอนิกส์ที่ทำให้ผู้ใช้แสดงความเป็นตัวตนของตนเอง เพื่อที่จะมีปฏิสัมพันธ์หรือแบ่งปันข้อมูลกับบุคคลอื่น ได้แก่ Facebook, Twitter และWeblog เป็นต้น

"จดหมายอิเล็กทรอนิกส์" (E-mail) หมายความว่า การรับส่งข้อความหรือข่าวสารจากบุคคลหนึ่งไปยังบุคคลอื่น ๆ โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกันข้อมูลที่ส่งจะเป็นได้ ทั้งตัวอักษรภาพถ่ายภาพกราฟิกภาพเคลื่อนไหวและเสียงซึ่งมาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

"รหัสผ่าน" (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"บัญชีผู้ใช้บริการ" (Account) หมายความว่า รายชื่อผู้ได้รับสิทธิ์ใช้งานเครื่องคอมพิวเตอร์และบริการต่าง ๆ ในระบบเครือข่ายของวิทยาลัย

"โปรแกรมประสงค์ร้าย" (Malware) หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือ ข้อมูลอิเล็กทรอนิกส์ที่ที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายให้ แก่ระบบคอมพิวเตอร์หรือระบบเครือข่ายเช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

"ชื่อเครื่องคอมพิวเตอร์" (Computer Name) หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์ซึ่งสามารถบ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์เครื่องใดในระบบเครือข่าย

"สื่อบันทึกพกพา" (Portable Recorder)หมายความว่าสื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูลได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

"การตั้งค่าระบบ" (Configuration) หมายความว่าค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software)

"เลขที่อยู่ไอพี" (IP Address) หมายความว่าตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่ายซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกันโดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วนที่คั่น ด้วยเครื่องหมายจุด (.)

"เลขที่อยู่ไอพีสาธารณะ (Public IP Address)" หมายความว่าเลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงานหรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากันหรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

"แบนด์วิดท์ (Bandwidth)" หมายความว่าปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบเป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่งและเป็นการบอกถึง ความเร็วในการรับส่งข้อมูล

"ชื่อผู้ใช้" (Username) หมายความว่าชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งาน

"ลงบันทึกเข้า" (Login) หมายความว่ากระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้(Username) และรหัสผ่าน (Password) ให้ถูกต้อง

"ลงบันทึกออก" (Logout) หมายความว่ากระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

"อัพเดท" (Update) หมายความว่า การปรับปรุงข้อมูลด้านต่างๆของสารสนเทศให้ทันสมัยอยู่เสมอ

"ช่องโหว่ ของระบบหรือโปรแกรม" (Vulnerability) หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตโดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรมทำให้มีการอาศัยขอบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

"ไฟล์ที่สามารถประมวลผลได้" (Executable file) หมายความว่าไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันทีเช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ในขณะที่ ไฟล์ข้อมูลอื่นๆจะเป็นไฟล์ข้อมูลประกอบ

"การเข้ารหัส" (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

"ไฟร์วอลล์" (Firewall) หมายความว่า อุปกรณ์ฮาร์ดแวร์/ซอฟต์แวร์ ที่ช่วยป้องกันการบุกรุกจากบุคคลภายนอกเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย

"การพิสูจน์ยืนยันตัวตน" (Authentication) หมายความว่าขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ ตัวตนของผู้ใช้บริการระบบทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

ส่วนที่ ๑

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงศูนย์ข้อมูลและคอมพิวเตอร์ของวิทยาลัย ซึ่งเป็นห้องควบคุมระบบเครื่องคอมพิวเตอร์แม่ข่ายอุปกรณ์ระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศโดยพิจารณาตามความสำคัญของอุปกรณ์ซึ่งจะมีผลบังคับใช้กับผู้ใช้ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของวิทยาลัย

ข้อปฏิบัติการใช้งานศูนย์ข้อมูลและคอมพิวเตอร์

๑) ภายในห้องศูนย์ข้อมูลและคอมพิวเตอร์มีการจำแนกและกำหนดพื้นที่ของเครื่องคอมพิวเตอร์ แม่ข่ายอุปกรณ์เครือข่ายระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมโดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒) จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกันโดยการกำหนดพื้นที่ ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) ซึ่งติดตั้งในตู้ Rack ภายในห้องศูนย์ข้อมูลและคอมพิวเตอร์

๓) ต้องกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายโดยมีการบันทึกเวลา เข้า-ออก พื้นที่ห้องอย่างเป็นระบบ

๔) บุคคลภายนอกเข้ามาติดต่อต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้องและเจ้าหน้าที่ที่รับผิดชอบจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๕) มีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารปีละ ๑ ครั้ง เป็นอย่างน้อย

๖) บุคลากรอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่จะต้องได้รับอนุญาตจากหัวหน้าภารกิจเทคโนโลยีสารสนเทศและการสื่อสารก่อน

การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๓) จัดเก็บบันทึกรายการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบ หรือประเมินในภายหลัง

๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุง อุปกรณ์ดังกล่าว

๕) ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในวิทยาลัย

๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การนำทรัพย์สินออกนอกวิทยาลัย (Removal of Property)

๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกวิทยาลัย

๒) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกวิทยาลัย

๓) เมื่อมีการนำอุปกรณ์ส่งคืนให้ทำการตรวจสอบความครบถ้วน และความสมบูรณ์ของอุปกรณ์ที่ยืมไป รวมถึงความสอดคล้องของระยะเวลาที่ได้บันทึกขอยืม

๔) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกวิทยาลัยเพื่อเป็นหลักฐาน ป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกวิทยาลัย (Security of equipment Off-premises)

๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของ วิทยาลัย ออกไปใช้งานเช่นการขนส่งการเกิดอุบัติเหตุกับอุปกรณ์

๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของวิทยาลัยไว้โดยลำพังในที่สาธารณะ

๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ส่วนที่ ๒
การเข้าถึงและควบคุมการใช้งานสารสนเทศ
(Access Control)

๑. การเข้าถึงระบบสารสนเทศ

เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของวิทยาลัยและเพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องได้แก่ผู้บริหารผู้ใช้งานผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับวิทยาลัยได้รับทราบเข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัดโดยตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สินการจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องเช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิมอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของวิทยาลัยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บริหาร

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหารเช่นข้อมูลนโยบายข้อมูลยุทธศาสตร์และคำรับรองข้อมูลบุคลากรข้อมูลงบประมาณการเงินและบัญชีเป็นต้น
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการเช่นข้อมูลดัชนีเศรษฐกิจการค้า ข้อมูลการค้าระหว่างประเทศของไทยข้อมูลเศรษฐกิจการค้าจังหวัดเป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับคือ

- ข้อมูลที่มีระดับความสำคัญมาก
- ข้อมูลที่มีระดับความสำคัญปานกลาง

- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย ในกรณีที่มีผู้ต้องการข้อมูล สมศ. จะพิจารณาเป็นรายกรณีไป

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๕) การกำหนดเวลาที่ได้เข้าถึง

(๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirementsfor Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ

(๑) มีการควบคุมการเข้าถึงสารสนเทศโดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ตารางแสดงลำดับชั้นความลับและระดับความสำคัญของสารสนเทศ สมศ.

ระดับ ความลับ ความสำคัญ	ทั่วไป	ลับ	ลับที่สุด
มาก	• บทสรุปผู้บริหารฯ • สัญญาจ้างโครงการต่าง ๆ	• ผลประเมินคุณภาพการศึกษา	• รหัสผ่านของระบบคอมพิวเตอร์วิทยาลัยทุกระบบ • เงินเดือน บุคลากร เจ้าหน้าที่
ปานกลาง	• รายชื่อคณะกรรมการบริหาร • รายชื่อคณะกรรมการประเมิน • รายชื่อคณะกรรมการบริหาร • รายงานประจำปี	• ข้อมูลการบริหาร	• ผลประเมินประจำปีรายบุคคล
น้อย	• ประกาศ/รายงานผลการจัดซื้อจัดจ้าง • คำรับรองการปฏิบัติงานประจำปีงบประมาณ • สื่อสิ่งพิมพ์ ที่สามารถเปิดเผยได้	• ข้อมูลส่วนบุคคลเจ้าหน้าที่	• ข้อมูลเอกสารลับจัดเก็บใน ระบบสารบรรณวิทยาลัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการและควบคุมการเข้าถึงระบบสารสนเทศให้สามารถใช้ได้เฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อเป็นการป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อยดังนี้

๒.๑ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งานเพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๒ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่องต่อไปนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศและให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานหรือจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคลไม่ซ้ำซ้อนกัน

(๓) การกำหนดชื่อผู้ใช้งาน (Username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษร ตัวแรกของนามสกุลหากซ้ำให้เพิ่มอักษรตัวที่สองหรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานอื่น

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้ เท่าที่จำเป็น

(๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบและ/หรือความต้องการทางธุรกิจ

(๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

(๗) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการลาออกเปลี่ยนตำแหน่งโอนย้ายหรือสิ้นสุดการจ้าง เป็นต้น

๒.๓ มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษและสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงดังนี้

(๑) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

(๓) การมอบหมายสิทธิต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๔ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุมดังนี้

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราวต้องยากต่อการเดาและต้องมีความแตกต่างกัน

(๓) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยโดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ในการจัดส่งรหัสผ่านและผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราวและควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่ จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๒ ครั้งหรือเมื่อมีการเปลี่ยนแปลงเช่นมีการลาออกเปลี่ยนตำแหน่งโอนย้ายหรือสิ้นสุดการจ้างเป็นต้น

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผยการล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศมีข้อปฏิบัติอย่างน้อยดังนี้

๓.๑ มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งานเพื่อให้สามารถกำหนดรหัสผ่านการใช้งานรหัสผ่านและการเปลี่ยนหัสผ่านที่มีคุณภาพดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ควรกำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษรโดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลขและสัญลักษณ์เข้าด้วยกัน

(๔) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตนหรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกันหรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงานหลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ตนใช้งาน

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๕) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแลดังนี้

(๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งานเพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งานหรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๕) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาทีและต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๖) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตอย่างน้อยดังนี้

๔.๑ การใช้บริการเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึงโดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญเช่นระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้นโดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจาก ผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

(๒) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูลโดยจะต้องมี วิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงเช่นการใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB Token ที่มีความสามารถ PKI เป็นต้น

(๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนสำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานอย่างน้อย ๑ วิธี

(๔) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตให้มีการตรวจสอบผู้ใช้งานด้วย

๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน การเข้าถึงดังนี้

(๑) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(๒) มีการควบคุมการใช้งานอย่างเหมาะสม

(๓) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้ งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งานโดยแบ่งออกเป็น ๒ เครือข่ายคือเครือข่ายสำหรับผู้ใช้งานภายในและเครือข่ายสำหรับผู้ใช้งานภายนอก

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุอุปกรณ์เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

๔.๗ การควบคุมการเข้าใช้งานระบบจากภายนอก กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในวิทยาลัยเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของวิทยาลัยต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานเช่นรหัสผ่านหรือวิธีการเข้ารหัสเป็นต้น

(๓) วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้ากลุ่มงานบริการเทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

(๔) ก่อนการให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับวิทยาลัยอย่างเพียงพอและต้องได้รับอนุญาตจากหัวหน้าภารกิจ เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบที่ได้รับมอบหมายอย่างเป็นทางการ

(๕) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๖) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิด port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๔.๘ การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก ผู้ใช้ระบบเมื่อจะเข้าใช้งานระบบจะต้องผ่านการพิสูจน์ตัวตนจากระบบของวิทยาลัย ดังนี้

- แสดงชื่อผู้ใช้งาน (Username)
- ใส่รหัสผ่าน (Password)

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตโดยมีแนวปฏิบัติดังนี้

๕.๑ ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่อง คอมพิวเตอร์ของหน่วยงาน

๕.๒ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยการเข้าถึงระบบปฏิบัติการจะต้อง ควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัยโดยมีแนวปฏิบัติดังนี้

(๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การ เข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจ สร้างความเสียหายให้กับระบบได้

๕.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึงโดยมีแนวปฏิบัติดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของวิทยาลัย

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติมเช่น Smart Card

๕.๔ การบริหารจัดการรหัสผ่าน (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพเมื่อได้ดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ ดำเนินการดังนี้

(๑) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๖ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (SessionTime-out)

(๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อยหากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาทีตามความเหมาะสมเพื่อป้องกันการเข้าถึ ข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๕.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือ โปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูงเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้นเช่นกำหนดให้ใช้งานได้ ๓ ช.ม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

(๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๓) กำหนดให้ระบบสารสนเทศเช่นระบบงานที่มีความสำคัญสูงระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกวิทยาลัย) เป็นต้นมีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศของวิทยาลัย และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก ซึ่งอาจสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้ หยุดชะงัก อีกทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของวิทยาลัยได้อย่างถูกต้อง

แนวปฏิบัติ

๖.๑ ผู้ดูแลระบบต้องมีการกำหนดการลงทะเบียนการใช้งานของผู้ใช้งานในระบบใหม่ของ วิทยาลัย ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างให้ชัดเจน เพื่อให้มีสิทธิต่าง ๆในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน

๖.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบงานภายใน วิทยาลัย จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบตามสายบังคับบัญชา รวมถึงมีการทบทวนสิทธิอย่างสม่ำเสมอ

๖.๓ มีการกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงาน เมื่อมีผู้ใช้งานไม่มีการใช้งานระบบเกินกว่า ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Log in เข้าใช้งานระบบอีกครั้ง

๖.๔ จะต้องมีการบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังนี้

(๑) กำหนดการเปลี่ยนแปลงการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือ ยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการให้บุคคลอื่น หรือการส่งผ่านจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๓) กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

(๔) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๖.๕ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส(Encryption) ที่เป็นมาตรฐานสากลเช่น SSL VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของวิทยาลัยเช่นส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนเป็นต้น

๗. การปฏิบัติงานจากภายนอกวิทยาลัย (Teleworking)

๗.๑ ต้องมีการกำหนดมาตรการและการเตรียมการต่างๆ ที่จำเป็นก่อนซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกลก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๗.๒ ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในองค์กรก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๗.๓ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกลเพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานของวิทยาลัย

๗.๔ ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศของวิทยาลัยในสถานที่ดังกล่าว

๗.๕ ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของวิทยาลัยรวมทั้งมาตรการควบคุมการใช้บริหารเครือข่ายไร้สายสายที่บ้าน

๗.๖ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของวิทยาลัยจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์กรต้องการ

๗.๗ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกลการจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๗.๘ วิทยาลัยไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของวิทยาลัยจากระยะไกลถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยวิทยาลัย

๗.๙ วิทยาลัยต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าวชั้นความลับซองข้อมูลที่อนุญาตให้ใช้งานได้และระบบงานและบริการต่างๆ ของวิทยาลัยที่อนุญาตให้เข้าถึงได้จากระยะไกล

๗.๑๐ วิทยาลัยต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงานและการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๘. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๘.๑ ผู้ดูแลระบบคอมพิวเตอร์ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่วิทยาลัยจัดสรรไว้เท่านั้นเช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากกลุ่มเทคโนโลยีและสารสนเทศเป็นลายลักษณ์อักษร

๘.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

๘.๓ ต้องกำหนดให้มีการทำ Update Patch และ HotFix อย่างสม่ำเสมอโดยสามารถ Download Patch และ HotFix ต่าง ๆ จากเว็บไซต์ Microsoft เพื่อแก้ปัญหาช่องโหว่

๘.๔ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๘.๕ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของวิทยาลัยเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่นเว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม

๘.๖ ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของวิทยาลัย

๘.๗ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับวิทยาลัย

๘.๘ ผู้ใช้ ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของวิทยาลัยที่ยังไม่ได้ประกาศหรือยังไม่ได้รับอนุญาตผ่านอินเทอร์เน็ต

๘.๙ ผู้ใช้ต้องไม่กระทำการดาวน์โหลดหรือนำเข้าข้อมูลตามที่ระบุไว้ดังนี้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชังหรือได้รับความอับอาย

(๒) ข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อผู้อื่นหรือวิทยาลัย

(๓) ข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชน ทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตาม (๑) (๒) (๓) หรือ (๔)

๙. แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ (Social Media)

๙.๑ ผู้ใช้สามารถใช้งานสื่อสังคมออนไลน์ในช่วงนอกเวลาทำการเท่านั้น ยกเว้นกรณีการใช้งานเพื่อ ภารกิจของวิทยาลัย

๙.๒ การคัดลอก เลียนข้อความใด ๆ จากสื่อสังคมออนไลน์ พึงได้รับการอนุญาตจากเจ้าของข้อความนั้น ๆ ตามแต่กรณี กรณีจำเป็นเพื่อประโยชน์ในการเผยแพร่ข้อมูล ผู้ใช้ ต้องอ้างอิงถึงแหล่งที่มาของ ข้อความและข่าวสารนั้น โดยรับรู้ถึงสิทธิ /ลิขสิทธิ์ขององค์กรหรือบุคคลผู้เป็นเจ้าของข้อมูลดังกล่าว

๙.๓ ผู้ใช้ไม่เผยแพร่หรือส่งต่อข้อความ รูปภาพ วีดิโอที่อาจทำให้ผู้อื่นเสียหายและไม่ควรใช้ถ้อยคำหยาบคายอนาจาร ดูหมิ่น ส่อเสียด เสียดสี ให้ร้ายผู้อื่นในทางเสียหายหรือสร้างความแตกแยกในสังคม

๙.๔ ผู้ใช้ พึงตระหนักเสมอว่าการโพสต์ข้อความหรือแสดงความคิดเห็นให้เผยแพร่บนสื่อสังคม ออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ดังนั้นผู้เผยแพร่ต้องรับผิดชอบ ทั้งด้านสังคมและกฎหมาย

๑๐. แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สามารถสนับสนุนการปฏิบัติงานของวิทยาลัยเป็นไปอย่างถูกต้องสะดวกรวดเร็วทันสถานการณ์มีประสิทธิภาพและประสิทธิผลและเพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรมีความเป็นมาตรฐานอยู่ในกรอบของกฎหมายระเบียบคำสั่งข้อบังคับของวิทยาลัย แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๑๐.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของวิทยาลัยให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิ การเข้าใช้งานอย่างสม่ำเสมอ

๑๐.๒ ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของวิทยาลัย

๑๐.๓ สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบ จดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๑๐.๔ รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

๑๐.๕ ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน๓ครั้ง

๑๐.๖ ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการล็อกเอ้าท์ออกจากหน้าจอ ตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้เช่น ๑๕ นาทีเมื่อต้องการเข้าใช้งาน ต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๑๐.๗ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๐.๘ ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดเช่นควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๑๐.๙ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อวิทยาลัย หรือละเมิดสิทธิสร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรม

๑๐.๑๐ ผู้ใช้ไม่ควรใช้ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านรับส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑๐.๑๑ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของวิทยาลัยเพื่อการปฏิบัติงานตามภารกิจของ วิทยาลัยเท่านั้น

๑๐.๑๒ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรทำการล็อกเอ้าท์ออกจาก ระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๑๐.๑๓ ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำ การตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

๑๐.๑๔ ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๐.๑๕ ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมข้อมูลอัน อาจทำให้เสียชื่อเสียงของวิทยาลัยทำให้เกิดความแตกแยกโดยผ่านทางจดหมายอิเล็กทรอนิกส์

๑๐.๑๖ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อ จดหมายอิเล็กทรอนิกส์

๑๐.๑๗ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บ แฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๐.๑๘ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ ระบบจดหมายอิเล็กทรอนิกส์

๑๑. ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์ (Terms of Use and Disclaimer)

ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์จะต้องไม่กระทำการอันละเมิดต่อกฎหมายระเบียบคำสั่งข้อบังคับคำแนะนำอย่างน้อยดังต่อไปนี้

- พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๑
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔
- พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐
- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔
- ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗
- ระเบียบรักษาความปลอดภัยด้านการสื่อสาร พ.ศ.๒๕๒๕

๑๑.๑ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอเล็กทรอนิกส์ของวิทยาลัยจะต้องใช้จดหมายอิเล็กทรอนิกส์สำหรับการปฏิบัติงานตามภารกิจของวิทยาลัยเท่านั้น

๑๑.๒ ห้ามใช้จดหมายอิเล็กทรอนิกส์ของวิทยาลัยเพื่อประกอบธุรกิจ หรือแสวงหาผลประโยชน์ ส่วนตน

๑๑.๓ ห้ามใช้บริการนี้ไปในการเผยแพร่อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใด ๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์

๑๑.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของวิทยาลัยในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการความปลอดภัย ข้อมูล ข่าวสารลับของทางราชการ

๑๑.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของวิทยาลัย เพื่อการเผยแพร่ข้อมูลข่าวสาร หรือ ภาพเสียงข้อความที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๑๑.๖ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบหรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือวิทยาลัย

๑๑.๗ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)

๑๑.๘ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบเช่น

(๑) การสร้างจดหมายลูกโซ่ (Chain Mail)

(๒) การส่งจดหมายจำนวนมาก (Spam Mail)

(๓) การส่งจดหมายต่อเนื่อง (Letter Bomb)

(๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๑๑.๙ ห้ามผู้ใช้บริการกระทำการใดๆที่อาจจะนำมาซึ่งความเสื่อมเสียหรือก่อให้เกิดความเสียหาย แก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของวิทยาลัย

๑๑.๑๐ ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคลหรือหน่วยงานของจดหมายอิเล็กทรอนิกส์ เป็นไว้เป็นความลับ

๑๑.๑๑ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของวิทยาลัย

๑๑.๑๒ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอก วิทยาลัยจะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูลข่าวสาร ตามที่วิทยาลัยกำหนด

๑๑.๑๓ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) และรหัสผ่าน(Password) ของหน่วยหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันทีโดย รหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

๑๑.๑๔ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์วิทยาลัยหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์ จะต้องศึกษาคู่มือการใช้งานระเบียบปฏิบัติคำแนะนำและข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมาย อิเล็กทรอนิกส์ของวิทยาลัยได้อย่างถูกต้อง

๑๑.๑๕ กรณีได้รับการร้องเรียนร้องขอหรือพบเหตุอันไม่ชอบด้วยกฎหมายขอสงวนสิทธิ์ที่จะทำการยกเลิกหรือระงับบริการแก่สมาชิกนั้นๆเป็นการชั่วคราวเพื่อทำการสอบสวนและตรวจสอบหาสาเหตุของมูลเหตุนั้นๆ

๑๑.๑๖ การกระทำใดๆที่เกี่ยวกับการเผยแพร่ทั้งในรูปแบบของอีเมลและ/หรือโฮมเพจของ ผู้ใช้บริการให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการทั้งนี้ วิทยาลัยไม่มีส่วนเกี่ยวข้อง ใดๆทั้งสิ้น

ส่วนที่ ๓
การจัดทำระบบสำรองข้อมูล
(Backup Policy)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Computer Server) และอุปกรณ์เชื่อมโยงระบบเครือข่ายและเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิด ความเสียหายต่อระบบสารสนเทศของวิทยาลัยให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

แนวปฏิบัติงานการสำรองข้อมูลและระบบคอมพิวเตอร์

๑) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูลของวิทยาลัย

๒) การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูลได้แก่เวลาเริ่มต้นและสิ้นสุดชื่อผู้สำรองชนิดของข้อมูลที่บันทึก

๓) มีขั้นตอนการปฏิบัติการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้องทั้งด้านระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศโดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๔) การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นรวมทั้งวิธีการที่ใช้แก้ไขด้วย

๕) ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ

๖) ให้ผู้ดูแลระบบคอมพิวเตอร์กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูลโดยรูปแบบการสำรองข้อมูลมี ๒ ลักษณะได้แก่ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๗) การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญโดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๘) นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

ข้อปฏิบัติเกี่ยวกับการสำรองข้อมูล

ผู้ดูแลระบบคอมพิวเตอร์ต้องทำการสำรองข้อมูลแต่ละรายการและจะต้องทำการตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพตามรายละเอียดตามตารางความถี่การสำรองข้อมูลนั้นถูกต้องสมบูรณ์ หรือไม่

ตารางความถี่ในการสำรองข้อมูลของวิทยาลัย

ที่	**รายการ**	**ข้อมูลที่ต้องสำรอง**	**ความถี่ในการสำรองข้อมูล**
๑.	Mail Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ๊อกซ์	๑ ครั้งต่อสัปดาห์ และนำสื่อบันทึกข้อมูลเก็บนอกสถานที่
๒	Web Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ๊อกซ์	ข้อมูลเผยแพร่บนเว็บไซต์ ๑ครั้งต่อสัปดาห์ และนำสื่อบันทึกข้อมูลเก็บนอก สถานที่
๓	File Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในเมล์บ๊อกซ์	๑ ครั้งต่อสัปดาห์ และนำสื่อบันทึกข้อมูล เก็บนอกสถานที่
๔	Proxy Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในระบบ	๑ ครั้งต่อสัปดาห์ และนำสื่อบันทึกข้อมูลเก็บนอกสถานที่
๕	Database Servers	ค่า Configure	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลในฐานข้อมูลของ ระบบที่สำคัญ	๑ ครั้งต่อสัปดาห์และนำสื่อบันทึกข้อมูล เก็บนอกสถานที่
๖	Server ระบบงานของวิทยาลัย	ค่า Configure/ซอฟต์แวร์	ก่อนและหลังการเปลี่ยนแปลง
		ข้อมูลของระบบ	๑ ครั้งต่อสัปดาห์และนำสื่อบันทึกข้อมูลเก็บนอกสถานที่

หมายเหตุ ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบคอัพแบบ Full Backup

การกู้คืนระบบ

๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบคอมพิวเตอร์ดำเนินการแก้ไขรายงานผลการแก้ไข พร้อมทั้งบันทึกและให้สรุปผลการปฏิบัติงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ

๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันทีพร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๔) ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

๕) การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน

และภัยพิบัติที่อาจเกิด ขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ต้องมอบหมายให้เจ้าหน้าที่ที่เกี่ยวข้อง ดำเนินการดังต่อไปนี้

๑) กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสำคัญสูง

๒) กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๓) ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๔) จัดทำแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสำคัญสูง

๕) ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสาหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔
การตรวจสอบและประเมินความเสี่ยง
(Risk Assessment)

วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัย ด้านสารสนเทศ

ข้อปฏิบัติการประเมินความเสี่ยง

กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลและสารสนเทศให้ปฏิบัติตามกระบวนการ PDCA ดังต่อไปนี้

การกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

๑) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาจากลักษณะการดำเนินงานวิทยาลัยสถานที่ตั้งทรัพย์สินและเทคโนโลยีที่ใช้

๒) กำหนดนโยบายความมั่นคงปลอดภัยเพื่อให้ครอบคลุมตามขอบเขตที่กำหนดไว้

๓) กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงสำหรับทรัพย์สินด้านสารสนเทศของวิทยาลัย

๔) ประเมินความเสี่ยงกำหนดทางเลือกในการจัดการกับความเสี่ยงและกำหนดมาตรการลดความเสี่ยง

๕) จัดทำเอกสาร Statement of Applicability

การดำเนินการกับระบบบริหารจัดการความมั่นคงปลอดภัย (Do)

๑) จัดทำแผนการลดความเสี่ยง

๒) ปฏิบัติตามแผนการลดความเสี่ยงที่ได้กำหนดไว้

๓) กำหนดแผนการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยเพื่อใช้ในการติดตามภาพรวมของการบริหารจัดการความมั่นคงปลอดภัยของวิทยาลัย

๔) จัดทำและดำเนินการตามแผนงานและสร้างความตระหนักเพื่อให้ความรู้และสร้างความตระหนักแก่บุคลากรทั้งหมดที่อยู่ในขอบเขตเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพประสิทธิผลรวมทั้งมีความมั่นคงปลอดภัย

๕) บริหารจัดการการดำเนินงานและการใช้ทรัพยากรต่างๆ ภายในขอบเขตเพื่อให้เป็นไปตาม นโยบายความมั่นคงปลอดภัยของวิทยาลัย

๖) จัดทำขั้นตอนปฏิบัติและ/หรือกำหนดมาตรการที่จำเป็นสำหรับการติดตามและบริหาร จัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident Management Procedures and Controls) รวมทั้งกำหนดให้ผู้ที่เกี่ยวข้องให้ปฏิบัติตามโดยเคร่งครัด

การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check)

๑) ดำเนินการตามขั้นตอนปฏิบัติและมาตรการในการเฝ้าระวังและติดตาม (ที่กำหนดไว้ใน นโยบายความมั่นคงปลอดภัย) เพื่อตรวจหาข้อผิดพลาดจากการประมวลผล, ตรวจหาการละเมิดหรือความ พยายามในการละเมิดความมั่นคงปลอดภัย, ตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น, ตรวจสอบว่าการดำเนินการจัดการกับเหตุการณ์การละเมิดความมั่นคงปลอดภัยที่ได้ดำเนินการไปแล้วได้ผล หรือไม่เป็นต้น

๒) ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอโดยอย่างน้อยนำสิ่งต่างๆดังนี้มาทบทวนด้วยเช่นผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย, เหตุการณ์ด้าน ความมั่นคงปลอดภัยที่เกิดขึ้น, ผลจากการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย, คำแนะนำและผลตอบกลับ (Feedback)จากผู้ที่เกี่ยวข้อง

๓) ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอโดยดูว่าแผนการวัดความสัมฤทธิ์ผลฯเป็นไปตามเปูาหมายหรือตัวชี้วัดที่กำหนดไว้ในแผนหรือไม่

๔) ทบทวนผลการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้งทบทวนระดับความเสี่ยงที่ยังเหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ตามการเปลี่ยนแปลงต่างๆที่เกิด อาทิ เทคโนโลยีที่ใช้ภัยคุกคามที่มีการระบุเพิ่มเติมหรือเปลี่ยนแปลงเป็นต้น

๕) ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนด

๖) บันทึกข้อมูลการดำเนินการและเหตุการณ์ต่างๆ ซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่างๆ ในนโยบายความมั่นคงปลอดภัยให้ผู้ดูแลระบบคอมพิวเตอร์บันทึกหลักฐานการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเหล่านั้นไว้เพื่อให้สามารถตรวจสอบได้ในภายหลัง

การทบทวนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (Act)

ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามผลของการเฝ้าระวังติดตามและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยเช่นการปรับปรุงนโยบายความมั่งคงปลอดภัยการจัดการหรือแก้ไข ความไม่สอดคล้องกับนโยบายความมั่นคงปลอดภัยการกำหนดมาตรการเพิ่มเติมเพื่อลดการเกิดขึ้นของ เหตุการณ์ด้านความมั่นคงปลอดภัยที่เคยเกิดขึ้นแล้วการปฏิบัติตามแผนการลดความเสี่ยงการปฏิบัติตาม แผนด้านความมั่นคงปลอดภัยการปฏิบัติตามคำแนะนำและผลตอบกลับจากผู้ที่เกี่ยวข้องเป็นต้น

การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศต้องดำเนินการดังต่อไปนี้

๑) มีการบริหารความเสี่ยงเพื่อกำจัดป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒) มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับ ระบบสารสนเทศ (IT Contingency Plan)

๓) มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูลเช่นระบบ Anti Virus ระบบไฟฟูาสำรองเป็นต้น

๔) มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

๕) ต้องมีการทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปีอย่างน้อยปีละ ๑ ครั้ง

๖) ต้องมีการตรวจสอบและประเมินความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี