# ประกาศมหาวิทยาลัยพะเยา

เรื่อง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยพะเยา พ.ศ. ๒๕๖๙

---

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับตามมาตรา ๔๔ มาตรา ๔๕ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ อาศัยอำนาจตามความในมาตรา ๓๓ แห่งพระราชบัญญัติมหาวิทยาลัยพะเยา พ.ศ. ๒๕๕๓ จึงออกประกาศไว้ดังนี้

**ข้อ ๑** ประกาศนี้ เรียกว่า “ประกาศมหาวิทยาลัยพะเยา เรื่อง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยพะเยา พ.ศ. ๒๕๖๙”

**ข้อ ๒** ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

**ข้อ ๓** ให้ยกเลิก

(๑) ประกาศมหาวิทยาลัยพะเยา เรื่อง นโยบายการให้บริการและการใช้งานระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย

(๒) ประกาศมหาวิทยาลัยพะเยา เรื่อง นโยบายการให้บริการและการใช้งานระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย (ฉบับที่ ๒)

**ข้อ ๔** ในประกาศนี้

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยพะเยา

“อธิการบดี” หมายความว่า อธิการบดีมหาวิทยาลัยพะเยา

“ส่วนงาน” หมายความว่า ส่วนงานตามมาตรา ๗ แห่งพระราชบัญญัติมหาวิทยาลัยพะเยา พ.ศ. ๒๕๕๓

“หัวหน้าส่วนงาน”...

“หัวหน้าส่วนงาน” หมายความว่า หัวหน้าส่วนงานตามมาตรา ๗ แห่งพระราชบัญญัติมหาวิทยาลัยพะเยา พ.ศ. ๒๕๕๓

“หน่วยงานภายใน” หมายความว่า หน่วยงานภายในของส่วนงานตามมาตรา ๗ แห่งพระราชบัญญัติมหาวิทยาลัยพะเยา พ.ศ. ๒๕๕๓

“ผู้อำนวยการ” หมายความว่า ผู้อำนวยการกอง ผู้อำนวยการศูนย์ ของหน่วยงานภายใน

“หัวหน้างาน” หมายความว่า หัวหน้าหน่วยตรวจสอบภายใน และหัวหน้าศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์

“ผู้ใช้งาน” หมายความว่า พนักงานมหาวิทยาลัย ลูกจ้าง นิสิตมหาวิทยาลัยพะเยา นักเรียนโรงเรียนสาธิตมหาวิทยาลัยพะเยา และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศและทรัพยากรเทคโนโลยีสารสนเทศของมหาวิทยาลัยได้

“ศูนย์” หมายความว่า ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร และศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์

**ข้อ ๕** นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย

หมวด ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หมวด ๔ นโยบายการสร้างความตระหนักด้านความปลอดภัยสารสนเทศ

**ข้อ ๖** ให้หัวหน้าส่วนงาน ผู้อำนวยการ และหัวหน้างานเป็นผู้รับผิดชอบในการกำกับดูแลการดำเนินงานของส่วนงาน และหน่วยงานภายในให้สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัย

**ข้อ ๗** ให้ศูนย์เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนปรับปรุงให้สอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้องให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง และแจ้งให้ผู้ใช้งานส่วนงาน และหน่วยงานภายในทราบทุกครั้ง

**ข้อ ๘** นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย เพื่อใช้เป็นแนวปฏิบัติในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง รายละเอียดตามเอกสารแนบท้ายประกาศนี้ จึงให้หัวหน้าส่วนงาน ผู้อำนวยการ หัวหน้างาน และผู้ใช้งานปฏิบัติตามประกาศนี้อย่างเคร่งครัด

ข้อ ๙ ให้อธิการบดี...

**ข้อ ๙** ให้อธิการบดีรักษาการตามประกาศนี้ กรณีที่มีปัญหาเกี่ยวกับการบังคับใช้หรือการปฏิบัติตามประกาศนี้ อธิการบดีมีอำนาจตีความและวินิจฉัยชี้ขาด การตีความและการวินิจฉัยให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๑๐ เมษายน พ.ศ. ๒๕๖๙

(รองศาสตราจารย์ ดร.สุภกร พงศบางโพธิ์)
อธิการบดีมหาวิทยาลัยพะเยา

**เอกสารแนบท้ายประกาศมหาวิทยาลัยพะเยา**
**เรื่อง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ**
**มหาวิทยาลัยพะเยา พ.ศ. ๒๕๖๙**

# คำนำ

ระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นกลไกสำคัญในการขับเคลื่อนภารกิจด้านการเรียนการสอน การวิจัย การบริหารจัดการ และการให้บริการของมหาวิทยาลัยพะเยา การรักษาความมั่นคงปลอดภัยของสารสนเทศจึงเป็นปัจจัยสำคัญที่ส่งผลต่อความน่าเชื่อถือและความต่อเนื่องของการให้บริการของมหาวิทยาลัย ประกอบกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและทวีความรุนแรงมากขึ้นทั้งในประเทศและต่างประเทศ มหาวิทยาลัยจึงตระหนักถึงความจำเป็นในการกำหนดกรอบนโยบาย มาตรการและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศให้เป็นระบบ มีมาตรฐานและสอดคล้องกับบริบทของมหาวิทยาลัย

มหาวิทยาลัยพะเยาจึงได้จัดทำนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศฉบับนี้ขึ้น เพื่อใช้เป็นกรอบการดำเนินงานระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยให้มีประสิทธิผล สามารถบริหารจัดการความเสี่ยงด้านสารสนเทศได้อย่างเหมาะสมและตรวจสอบได้ และสอดคล้องกับกฎหมายต่าง ๆ ที่เกี่ยวข้อง

# สารบัญ


๑. วัตถุประสงค์ ..... ๑

๒. คำนิยาม ..... ๑

๓. ขอบเขตการให้บริการระบบเทคโนโลยีสารสนเทศ ..... ๔

๔. องค์ประกอบของนโยบายและแนวปฏิบัติ ..... ๖

หมวดที่ ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ..... ๗

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) ..... ๗

ส่วนที่ ๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility) ..... ๘

ส่วนที่ ๓ การใช้สื่อสังคมออนไลน์ (Social Network) ..... ๑๑

ส่วนที่ ๔ การบริหารจัดการทรัพย์สิน (Asset Management) ..... ๑๓

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control) ..... ๑๔

ส่วนที่ ๖ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control) ..... ๑๕

ส่วนที่ ๗ การควบคุมการเข้าโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control) ..... ๑๖

ส่วนที่ ๘ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-mail) ..... ๑๗

ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook) ..... ๑๘

ส่วนที่ ๑๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ..... ๑๙

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล ..... ๒๐

ส่วนที่ ๑ การรักษาความปลอดภัย ..... ๒๐

ส่วนที่ ๒ การสำรองข้อมูล (Backup) ..... ๒๐

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ..... ๒๒

ส่วนที่ ๑ การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Management) ..... ๒๒

หมวด ๔ นโยบายการสร้างความตระหนักด้านความปลอดภัยสารสนเทศ ..... ๒๓

ส่วนที่ ๑ การสร้างความตระหนักด้านความปลอดภัยสารสนเทศ ..... ๒๓

# นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยพะเยา

## ๑. วัตถุประสงค์

เพื่อกำหนดแนวทางในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศภายในมหาวิทยาลัย ให้มีความปลอดภัย เชื่อถือได้ และสามารถให้บริการระบบสารสนเทศได้อย่างต่อเนื่อง รวมทั้งเพื่อลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศและข้อมูลของมหาวิทยาลัย นโยบายและแนวปฏิบัติฉบับนี้จัดทำขึ้นให้สอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ รวมทั้งสอดคล้องกับบริบทของมหาวิทยาลัยและผลการประเมินความเสี่ยงของระบบสารสนเทศตามข้อกำหนดมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อกำหนดนโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับบริบทมหาวิทยาลัย เพื่อให้ระบบสารสนเทศและข้อมูลของมหาวิทยาลัยมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

๒. เพื่อสร้างความเข้าใจและความตระหนักในการใช้งานระบบสารสนเทศอย่างปลอดภัยแก่ผู้บริหาร พนักงานมหาวิทยาลัย ลูกจ้าง นิสิตมหาวิทยาลัยพะเยา และนักเรียนโรงเรียนสาธิตมหาวิทยาลัยพะเยา รวมถึงผู้รับจ้างหรือผู้ที่ปฏิบัติงานให้กับมหาวิทยาลัยพะเยา

๓. เพื่อกำหนดแนวทางปฏิบัติสำหรับผู้ดูแลระบบสารสนเทศ เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการเฝ้าระวัง ติดตาม และดูแลด้านความมั่นคงปลอดภัยอย่างเหมาะสม สอดคล้องกับข้อกำหนดมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒

## ๒. คำนิยาม

๑) **มหาวิทยาลัย** หมายความว่า มหาวิทยาลัยพะเยา

๒) **ระบบสารสนเทศ** หมายความว่า ระบบที่ให้บริการข้อมูลสารสนเทศของมหาวิทยาลัยพะเยา ได้แก่ เว็บไซต์ เว็บแอปพลิเคชัน ระบบฐานข้อมูล เป็นต้น ที่ให้บริการทั้งภายในและภายนอกมหาวิทยาลัย

๓) **ทรัพยากร** หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ เครื่องมือสื่อสาร และข้อมูลสารสนเทศของมหาวิทยาลัย ภายใต้การกำกับดูแลของศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร

๔) **โครงสร้างพื้นฐานทางสารสนเทศ** หมายความว่า การให้บริการระบบสารสนเทศ ได้แก่ ระบบเครือข่ายระบบคอมพิวเตอร์ (Hardware/Software) คลาวด์ (Cloud) จดหมายอิเล็กทรอนิกส์ เป็นต้น

๕) **ผู้ใช้งาน** หมายความว่า พนักงานมหาวิทยาลัย ลูกจ้าง นิสิตมหาวิทยาลัยพะเยา นักเรียนโรงเรียนสาธิตมหาวิทยาลัยพะเยา และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศและทรัพยากรเทคโนโลยีสารสนเทศของมหาวิทยาลัยได้

๖) **ผู้ดูแลระบบสารสนเทศส่วนกลาง** หมายความว่า บุคลากรของศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร ที่ทำหน้าที่กำกับดูแลโครงสร้างพื้นฐานทางสารสนเทศที่อยู่ในความรับผิดชอบของศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร

๗) **ผู้ดูแลระบบสารสนเทศ** หมายความว่า บุคลากรของส่วนงานและหน่วยงานภายใน ที่ทำหน้าที่กำกับดูแลระบบสารสนเทศของส่วนงานและหน่วยงานภายใน

๘) **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย

๙) **การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control)** หมายความว่า การกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อควบคุมการเข้าใช้งานระบบสารสนเทศ เช่น การให้สิทธิหรือการมอบอำนาจให้ผู้ใช้งานเพื่อเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตการเข้าถึงสำหรับบุคคลภายนอก

๑๐) **ความมั่นคงปลอดภัยไซเบอร์ (Cyber and Information Security)** หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและข้อมูล รวมทั้งคุณสมบัติอื่นที่เกี่ยวข้อง ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบในการดำเนินการ (Accountability) การไม่สามารถปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) รวมถึงการป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง การใช้งาน การเปิดเผย การขัดขวาง การเปลี่ยนแปลง การสูญหาย ความเสียหาย การถูกทำลาย หรือการล่วงรู้โดยมิชอบ

๑๑) **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัย

๑๒) **สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบสารสนเทศของมหาวิทยาลัยถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๑๓) **หน่วยงานภายนอก** หมายความว่า องค์กรหรือหน่วยงานที่มหาวิทยาลัยอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของมหาวิทยาลัย โดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความปลอดภัยและความลับของข้อมูลของมหาวิทยาลัย

**๑๔) ข้อมูลคอมพิวเตอร์** หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง ที่อยู่ในระบบคอมพิวเตอร์ ซึ่งอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ รวมถึงข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

**๑๕) สารสนเทศ (Information)** หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

**๑๖) ระบบเครือข่าย (Network System)** หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบสารสนเทศต่าง ๆ ของมหาวิทยาลัย ได้ เช่น ระบบเครือข่ายสาย (LAN) ระบบเครือข่ายไร้สาย (Wireless Lan) และระบบอินเทอร์เน็ต (Internet)

**๑๗) เจ้าของข้อมูล (Data Owner)** หมายความว่า บุคคลที่ได้รับมอบอำนาจให้เป็นผู้รับผิดชอบในการบริหารจัดการข้อมูลของระบบงาน โดยมีหน้าที่กำกับดูแลความถูกต้องและความมั่นคงปลอดภัยของข้อมูล รวมถึงเป็นผู้รับผิดชอบต่อผลกระทบที่เกิดขึ้นหากข้อมูลสูญหายหรือถูกทำลาย

**๑๘) เจ้าของข้อมูลส่วนบุคคล (Data Subject)** หมายความว่า บุคคลธรรมดาที่ข้อมูลส่วนบุคคลสามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

**๑๙) รหัสผ่าน (Password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

**๒๐) ชุดคำสั่งไม่พึงประสงค์ (Malicious Software)** หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

**๒๑) ระยะเวลาเป้าหมายในการกู้คืนสภาพระบบ (Recovery Time Objective: RTO)** หมายความว่า ระยะเวลาสูงสุดที่กำหนดขึ้นเพื่อกู้คืนระบบสารสนเทศให้กลับมาพร้อมใช้งานตามปกติ

**๒๒) ระยะเวลาเป้าหมายในการกู้คืนข้อมูล (Recovery Point Objective: RPO)** หมายความว่า ระยะเวลาสูงสุดที่ยอมรับได้ให้เกิดการสูญเสียข้อมูลเมื่อเกิดเหตุขัดข้องหรือภัยพิบัติ

**๒๓) ความมั่นคงปลอดภัยทางด้านกายภาพ (Physical Security)** หมายความว่า การจัดให้มีนโยบาย มาตรการหลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

## ๓. ขอบเขตการให้บริการระบบเทคโนโลยีสารสนเทศ

๑. บริการบัญชีผู้ใช้งาน (ชื่อผู้ใช้งานและรหัสผ่าน) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล และกำหนดสิทธิการเข้าใช้งานระบบเทคโนโลยีสารสนเทศที่มหาวิทยาลัยจัดเตรียมไว้ให้

๒. บริการการเชื่อมต่อผ่านสายสัญญาณเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ระบบเครือข่ายแบบสาย (LAN Cable) และระบบสายใยแก้วนำแสง (Fiber Optic Cable) เพื่อใช้ในการเข้าถึงบริการสารสนเทศและบริการอินเทอร์เน็ต

๓. บริการการเชื่อมต่อแบบไร้สาย (Wi-Fi) เพื่อใช้เข้าถึงระบบเครือข่ายคอมพิวเตอร์ บริการสารสนเทศ และบริการอินเทอร์เน็ต โดยมีบริการดังต่อไปนี้

๓.๑ Fahmui-WiFi สำหรับใช้งานบนเครื่องคอมพิวเตอร์หรืออุปกรณ์ส่วนบุคคล โดยต้องใช้งานร่วมกับบัญชีผู้ใช้งานของมหาวิทยาลัย

๓.๒ UP-WiFi สำหรับใช้งานบนเครื่องคอมพิวเตอร์หรืออุปกรณ์ส่วนบุคคลที่ไม่รองรับการเชื่อมต่อ Fahmui-WiFi โดยต้องใช้งานร่วมกับบัญชีผู้ใช้งานของมหาวิทยาลัย

๓.๓ UP-WiFi-Guest สำหรับการจัดโครงการภายในมหาวิทยาลัยในบริเวณที่มีสัญญาณระบบเครือข่ายไร้สาย เพื่อให้บริการอินเทอร์เน็ตแก่ผู้เข้าร่วมโครงการที่เป็นบุคคลภายนอก

๓.๔ Fahmui-IOT สำหรับอุปกรณ์ที่ต้องการเชื่อมต่ออินเทอร์เน็ต เช่น โทรทัศน์ ตู้เย็น เครื่องซักผ้า พัดลม Android Box หรือ Apple TV เป็นต้น โดยต้องลงทะเบียนอุปกรณ์ก่อนใช้งานด้วยบัญชีผู้ใช้งานของมหาวิทยาลัย

๓.๕ eduroam เป็นบริการเครือข่ายโรมมิ่งเพื่อการศึกษาและการวิจัย สำหรับนิสิตและบุคลากรของสถาบันการศึกษาที่เป็นสมาชิกเครือข่าย เพื่ออำนวยความสะดวกในการใช้งานเครือข่ายอินเทอร์เน็ตเมื่อเดินทางไปเยือนสถาบันสมาชิกทั้งในประเทศและต่างประเทศ โดยสามารถเข้าใช้งานได้ด้วยบัญชีผู้ใช้งานของมหาวิทยาลัย

๔. บริการระบบเครือข่ายอินเทอร์เน็ต (Internet) เป็นบริการโครงสร้างพื้นฐานสำหรับการเชื่อมต่อและใช้งานบริการพื้นฐานบนอินเทอร์เน็ต เช่น Website, Video Online, Social Media, Application Online และ Search Engine เป็นต้น

๕. บริการสื่อสารด้วยจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นบริการรับ-ส่งข้อมูลผ่านจดหมายอิเล็กทรอนิกส์ที่มหาวิทยาลัยจัดเตรียมไว้ เพื่อใช้ในการติดต่อสื่อสารและสนับสนุนการดำเนินงานตามพันธกิจของมหาวิทยาลัย ส่วนงาน และหน่วยงานภายใน

๖. บริการซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง ฟรีซอฟต์แวร์ หรือซอฟต์แวร์แบบเปิดเผยรหัส (Open-source software) ซึ่งเป็นซอฟต์แวร์พื้นฐานที่สนับสนุนการเรียนการสอนและการปฏิบัติงาน

๗. บริการเครื่องคอมพิวเตอร์แม่ข่ายเสมือนและชื่อโดเมน สำหรับให้บริการส่วนงานและหน่วยงานภายใน เพื่อจัดทำเว็บไซต์ เว็บแอปพลิเคชัน ระบบฐานข้อมูล และการเผยแพร่ข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์หรือระบบเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย

๘. บริการสำรองและกู้คืนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน เพื่อสำรองข้อมูลและลดความเสี่ยงจากการสูญหายของข้อมูล โดยมีการสำรองข้อมูลอย่างน้อยทุก ๒๔ ชั่วโมง หรือตามระดับความสำคัญของระบบที่ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสารกำหนด รวมทั้งรองรับการกู้คืนระบบเมื่อได้รับการร้องขอจากเจ้าของระบบหรือผู้ดูแลระบบสารสนเทศ

๙. บริการเครื่องคอมพิวเตอร์ลูกข่าย (Client) ได้แก่ เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) หรือเครื่องคอมพิวเตอร์แบบพกพา (Notebook) ที่จัดเตรียมไว้สำหรับการใช้งาน ดังนี้

๙.๑ เครื่องคอมพิวเตอร์สำหรับใช้งานภายในห้องเรียนส่วนกลางของมหาวิทยาลัย ได้แก่ ห้องเรียนทั่วไป และห้องเรียนคอมพิวเตอร์

๙.๒ เครื่องคอมพิวเตอร์สำหรับใช้งานในสำนักงาน สำหรับพนักงานมหาวิทยาลัยและลูกจ้าง

๙.๓ เครื่องคอมพิวเตอร์สำหรับให้บริการผู้ใช้งาน ณ สถานที่ของส่วนงาน หรือหน่วยงานภายในเพื่อให้ผู้รับบริการสามารถเข้าใช้งานระบบสารสนเทศได้ทันที

๑๐. บริการพื้นที่จัดเก็บข้อมูลสำหรับการเรียนการสอน การวิจัย และการปฏิบัติงานของพนักงานมหาวิทยาลัย ลูกจ้าง นิสิตมหาวิทยาลัย และนักเรียนโรงเรียนสาธิตมหาวิทยาลัยพะเยา ดังนี้

๑๐.๑ พื้นที่จัดเก็บข้อมูลส่วนบุคคลบนระบบคลาวด์ ใช้สำหรับจัดเก็บข้อมูลส่วนบุคคลของพนักงานมหาวิทยาลัย ลูกจ้าง นิสิตมหาวิทยาลัย และนักเรียนโรงเรียนสาธิตมหาวิทยาลัยพะเยา

๑๐.๒ พื้นที่จัดเก็บข้อมูลเพื่อสนับสนุนการเรียนการสอน ใช้สำหรับจัดเก็บและแลกเปลี่ยนข้อมูลระหว่างผู้สอนและผู้เรียนในแต่ละรายวิชาตามหลักสูตรที่มหาวิทยาลัยกำหนด ผ่านระบบ Microsoft Teams โดยกองบริการการศึกษามีหน้าที่ในการจัดสรรพื้นที่ของแต่ละรายวิชา ได้แก่ การสร้าง การแก้ไข และการลบ

๑๐.๓ พื้นที่จัดเก็บข้อมูลเพื่อสนับสนุนการปฏิบัติงาน ใช้สำหรับจัดเก็บและแลกเปลี่ยนข้อมูลระหว่างผู้ใช้งานในส่วนงานและหน่วยงานภายใน

## ๔. องค์ประกอบของนโยบายและแนวปฏิบัติ

หมวดที่ ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติดังนี้

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

ส่วนที่ ๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

ส่วนที่ ๓ การใช้สื่อสังคมออนไลน์ (Social Network)

ส่วนที่ ๔ การบริหารจัดการทรัพย์สิน (Asset Management)

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ส่วนที่ ๖ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ส่วนที่ ๗ การควบคุมการเข้าโปรแกรมประยุกต์ หรือแอปพลิเคชัน และระบบสารสนเทศ (Application and Information access control)

ส่วนที่ ๘ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

ส่วนที่ ๑๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

หมวดที่ ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล มีแนวปฏิบัติดังนี้

ส่วนที่ ๑ การรักษาความปลอดภัย

ส่วนที่ ๒ การสำรองข้อมูล (Backup)

หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีแนวปฏิบัติดังนี้

ส่วนที่ ๑ การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Management)

หมวดที ๔ นโยบายการสร้างความตระหนักด้านความปลอดภัยสารสนเทศ มีแนวปฏิบัติดังนี้

ส่วนที่ ๑ การสร้างความตระหนักด้านความปลอดภัยสารสนเทศ

## หมวดที่ ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มาตรการควบคุมและป้องกันการเข้าใช้งานสารสนเทศ เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของมหาวิทยาลัย และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และทำให้ตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

**วัตถุประสงค์**

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ และการมอบอำนาจของส่วนงาน หน่วยงานภายใน และผู้ปฏิบัติงานที่เกี่ยวข้อง

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

**ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)**

๑.๑ ผู้ดูแลระบบสารสนเทศส่วนกลาง เป็นผู้กำหนดสิทธิการเข้าใช้งานระบบเครือข่ายและโครงสร้างพื้นฐานทางสารสนเทศของมหาวิทยาลัยแก่ผู้ใช้งาน โดยผู้ดูแลระบบสารสนเทศส่วนกลางต้องจัดทำแนวปฏิบัติและมาตรการในการควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของมหาวิทยาลัยให้มีความมั่นคงปลอดภัย รวมทั้งจัดทำบัญชีรายชื่อผู้ได้รับสิทธิการเข้าถึงโครงสร้างพื้นฐานทางสารสนเทศ

๑.๒ ผู้ดูแลระบบสารสนเทศ เป็นผู้กำหนดสิทธิการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศของส่วนงานและหน่วยงานภายใน โดยผู้ดูแลระบบสารสนเทศต้องจัดทำแนวปฏิบัติและมาตรการในการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย พร้อมทั้งจัดทำบัญชีรายชื่อผู้ได้รับสิทธิ

๑.๓ หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย หรือผู้ใช้งานที่ต้องการขอสิทธิพิเศษในการเข้าใช้งานระบบสารสนเทศนอกเหนือจากสิทธิที่กำหนด ต้องขออนุญาตเป็นลายลักษณ์อักษรต่ออธิการบดีหรือผู้ที่ได้รับมอบอำนาจจากอธิการบดี

๑.๔ ให้ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศทบทวนสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และปรับปรุงสิทธิให้เป็นปัจจุบัน

๑.๕ การยกเลิกหรือสิ้นสุดการให้บริการระบบเครือข่ายและบริการโครงสร้างพื้นฐานทางสารสนเทศแก่ผู้ใช้งาน

๑) กรณีผู้ใช้งานที่เป็นนิสิตมหาวิทยาลัยและนักเรียนโรงเรียนสาธิตมหาวิทยาลัย เมื่อพ้นสภาพการเป็นนิสิตมหาวิทยาลัยหรือนักเรียนของโรงเรียนสาธิตมหาวิทยาลัยแล้ว จะสิ้นสุดสิทธิการใช้บริการโครงสร้างพื้นฐานทางสารสนเทศ โดยมีรายละเอียดดังนี้

๑.๑) กรณีพ้นสภาพเนื่องจากจบการศึกษาตามที่กำหนด ให้สามารถใช้งานระบบสารสนเทศที่จัดทำไว้เพื่อสนับสนุนศิษย์เก่าต่อไปได้ตามระยะเวลา นโยบาย และวัตถุประสงค์การให้บริการของแต่ละระบบ

๑.๒) กรณีพ้นสภาพเนื่องจากเสียชีวิต ลาออก หรือไม่จบการศึกษาตามที่หลักสูตรกำหนด ให้สิ้นสุดสิทธิการใช้บริการโครงสร้างพื้นฐานทางสารสนเทศทั้งหมด

๒) กรณีผู้ใช้งานเป็นพนักงานมหาวิทยาลัยและลูกจ้าง เมื่อพ้นสภาพการเป็นพนักงานมหาวิทยาลัยและลูกจ้างแล้ว จะสิ้นสุดสิทธิการใช้งานโครงสร้างพื้นฐานทางสารสนเทศทั้งหมด

๓) การยกเลิกหรือสิ้นสุดการให้บริการโครงสร้างพื้นฐานทางสารสนเทศ จะดำเนินการภายหลังจากการพ้นสภาพเป็นเวลา ๓๐ วัน เพื่อให้ผู้ใช้งานสามารถสำรองข้อมูลของตนเองได้

๑.๖ ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ในการตรวจสอบและระงับการใช้งานของผู้ใช้งาน หากพบเหตุการณ์ด้านความมั่นคงปลอดภัยหรือการใช้งานที่เป็นการฝ่าฝืนต่อประกาศฉบับนี้ที่ส่งผลกระทบให้เกิดความเสียหายต่อโครงสร้างพื้นฐานทางสารสนเทศ ระบบเครือข่าย ระบบสารสนเทศ ข้อมูลสารสนเทศ และทรัพย์สินของมหาวิทยาลัยหรือของผู้ใช้งานอื่น ๆ ให้ประสานศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการสืบสวน และพิจารณาให้ระงับการให้บริการ หรือระงับการเชื่อมต่อเข้าระบบของผู้ใช้งาน เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ที่เป็นต้นเหตุของปัญหา

ทั้งนี้ ให้ศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์รายงานผลการตรวจสอบเหตุการณ์ที่อาจก่อให้เกิดปัญหาด้านความมั่นคงปลอดภัย ความเสถียรภาพของโครงสร้างพื้นฐานทางสารสนเทศ ระบบสารสนเทศ หรือการกระทำที่ขัดต่อนโยบาย หรือกฎหมายที่เกี่ยวข้อง ต่อมหาวิทยาลัย

**ส่วนที่ ๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)**

๒.๑ หน้าที่และความรับผิดชอบของผู้ใช้งานโครงสร้างพื้นฐานทางระบบสารสนเทศ มีดังต่อไปนี้

๑) ผู้ใช้งานต้องลงทะเบียนเพื่อใช้งานระบบยืนยันตัวตนแบบหลายปัจจัย MFA (Multi Factor Authentication) ที่ https://go.up.ac.th/MFA

๒) ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีความยาวไม่น้อยกว่า ๙ ตัวอักษร โดยต้องประกอบด้วยอักษรภาษาอังกฤษตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ อย่างน้อย ๑ ตัวอักษร

๓) หากผู้ใช้งานมีการกรอกรหัสผ่านเพื่อเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัยผิดเกินจำนวนครั้งที่กำหนด ระบบจะระงับการลงชื่อเข้าใช้งานชั่วคราวจนกว่าจะครบระยะเวลาที่กำหนด และระบบสามารถเพิ่มช่วงระยะเวลาการระงับการเข้าใช้งานได้ หากยังพบว่ามีการกรอกรหัสผ่านผิดซ้ำ

๔) ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศต้องกำหนดรหัสผ่านสำหรับการใช้งานระบบสารสนเทศให้มีความยาวไม่น้อยกว่า ๑๒ ตัวอักษร โดยต้องประกอบด้วยอักษรภาษาอังกฤษตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ อย่างน้อย ๑ ตัวอักษร

๔.๑) กรณีระบบสารสนเทศไม่รองรับระบบยืนยันตัวตนแบบหลายปัจจัย MFA (Multi - Factor Authentication) ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศ ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๖ เดือน หรือเมื่อระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๔.๒) กรณีระบบสารสนเทศรองรับระบบยืนยันตัวตนแบบหลายปัจจัย MFA (Multi - Factor Authentication) ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศต้องลงทะเบียนเพื่อใช้งานระบบยืนยันตัวตนแบบหลายปัจจัย MFA ที่ https://go.up.ac.th/MFA

๕) รหัสผ่านเป็นข้อมูลเฉพาะบุคคล ผู้ใช้งานต้องเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ หากมีผู้อื่นล่วงรู้และนำไปใช้งานในทางที่ผิด เจ้าของรหัสผ่านไม่สามารถปฏิเสธความรับผิดชอบได้ เว้นแต่มีผลการสอบสวนจากตัวแทนของมหาวิทยาลัยหรือเจ้าพนักงานที่เกี่ยวข้องว่าไม่ใช่ความผิดของผู้ใช้งาน

๖) ผู้ใช้งานควรหลีกเลี่ยงการใช้โปรแกรมหรือระบบบันทึกรหัสผ่านอัตโนมัติ (Save Password)

๗) ห้ามจดหรือบันทึกรหัสผ่านในสถานที่ที่ง่ายต่อการสังเกตเห็น

๘) ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล รวมทั้งเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศอื่นใด ที่อาจเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ

๙) ผู้ใช้งานที่มีสิทธิเข้าถึงข้อมูล ต้องเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลอย่างปลอดภัย และไม่อนุญาตให้บุคคลใดละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น เว้นแต่กรณีที่มหาวิทยาลัยมีความจำเป็นต้องตรวจสอบข้อมูล หรือมีเหตุอันควรเชื่อว่าข้อมูลดังกล่าวเกี่ยวข้องกับมหาวิทยาลัย ซึ่งมหาวิทยาลัยสามารถแต่งตั้งผู้มีหน้าที่ตรวจสอบข้อมูลดังกล่าวได้โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

๑๐) มหาวิทยาลัยไม่เปิดให้บริการการใช้งานโปรแกรมประเภท Peer-to-Peer (รูปแบบการเชื่อมต่อเครือข่ายที่อุปกรณ์หรือคอมพิวเตอร์แต่ละเครื่องสามารถทำหน้าที่เป็นทั้งผู้ให้บริการและผู้ใช้บริการได้โดยตรงโดยไม่ผ่านเซิร์ฟเวอร์กลาง) เช่น บิทเทอร์เรนท์ (BitTorrent), อีมูล (eMule) เป็นต้น

๑๑) กรณีที่ผู้ใช้งานจำเป็นต้องติดต่อสื่อสารผ่านบริการจดหมายอิเล็กทรอนิกส์เกี่ยวกับงานตามพันธกิจของมหาวิทยาลัย ส่วนงานหรือหน่วยงานภายใน รวมถึงข้อมูลข่าวสารที่มีความสำคัญหรือ

เป็นความลับ ผู้ใช้งานต้องใช้บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยเท่านั้น (ชื่อโดเมน @up.ac.th) ยกเว้นการติดต่อสื่อสารส่วนบุคคล สามารถใช้บริการจดหมายอิเล็กทรอนิกส์ของผู้ให้บริการอื่นได้

๑๒) ผู้ใช้งานต้องรับผิดชอบในการดูแลและบำรุงรักษาฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลหรือสารสนเทศใด ๆ ที่อยู่ในความรับผิดชอบของตน รวมถึงเครื่องคอมพิวเตอร์ส่วนบุคคล อุปกรณ์ต่อพ่วง และทรัพยากรบนระบบเครือข่ายอื่น ๆ ที่มหาวิทยาลัยจัดสรรให้ ยกเว้นทรัพยากรที่มีการใช้งานร่วมกันหลายบุคคลและอยู่ภายใต้การกำกับดูแลของศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร

๑๓) ห้ามผู้ใช้งานนำฮาร์ดแวร์หรือซอฟต์แวร์มาติดตั้งในโครงสร้างพื้นฐานทางสารสนเทศของมหาวิทยาลัยโดยไม่ได้รับอนุญาต หากเกิดความเสียหายต่อโครงสร้างพื้นฐานทางสารสนเทศ อันเนื่องมาจากการติดตั้ง เปลี่ยนแปลง ทำซ้ำ หรือต่อเติมฮาร์ดแวร์หรือซอฟต์แวร์ดังกล่าว ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายนั้น

๑๔) ผู้ใช้งานต้องรับผิดชอบในการรับ ส่ง หรือจัดเก็บข้อมูลอันเป็นความลับ โดยการใช้งาน Share File หรือ Share Drive อย่างปลอดภัย เช่น การกำหนดรหัสผ่านเพื่อเข้าถึงข้อมูล การกำหนดสิทธิการเข้าถึงเฉพาะผู้ที่เกี่ยวข้อง หรือการส่งรหัสผ่านผ่านช่องทางอื่นแยกจากไฟล์ข้อมูล

๑๕) ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสารจะติดตั้งซอฟต์แวร์ป้องกันไวรัส (Anti-virus) บนเครื่องคอมพิวเตอร์ระบบปฏิบัติการ Microsoft Windows ที่มหาวิทยาลัยให้บริการ ผู้ใช้งานต้องเปิดใช้งานระบบสแกนไวรัส (Scan virus) และปรับปรุงซอฟต์แวร์ (Update patch) ให้เป็นปัจจุบันอย่างสม่ำเสมอ รวมถึงตรวจสอบเครื่องคอมพิวเตอร์ที่มหาวิทยาลัยจัดสรรให้และเครื่องคอมพิวเตอร์ส่วนตัวที่นำมาเชื่อมต่อกับโครงสร้างพื้นฐานทางสารสนเทศของมหาวิทยาลัย เพื่อให้มั่นใจว่าอุปกณ์มีความปลอดภัยและปราศจากไวรัส หนอนคอมพิวเตอร์ โทรจัน สปายแวร์ หรือซอฟต์แวร์ที่ไม่พึงประสงค์

๑๖) ผู้ใช้งานต้องตั้งค่าการล็อกหน้าจออัตโนมัติ (Auto Screen Lock) หากไม่มีการใช้งานหน้าจอเกิน ๑๕ นาที

๒.๒ การใช้งานโครงสร้างพื้นฐานทางสารสนเทศ ไม่อนุญาตให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

๑) ใช้งานโครงสร้างพื้นฐานทางสารสนเทศเพื่อกระทำสิ่งที่ผิดกฎหมาย ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๒) ใช้บัญชีผู้ใช้งานของผู้อื่นในการเข้าใช้งานระบบสารสนเทศ

๓) ใช้งานโครงสร้างพื้นฐานทางสารสนเทศและระบบสารสนเทศที่ตนไม่มีสิทธิการเข้าถึง

๔) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง ทำซ้ำ หรือเพิ่มเติมข้อมูลหรือสารสนเทศของผู้อื่นโดยมิชอบ

๕) ปลอมแปลงตัวตนในระบบเครือข่ายเพื่อเข้าใช้งานแทนผู้ใช้งานอื่นโดยมิชอบ

๖) เผยแพร่ข้อมูลหรือสารสนเทศที่เป็นเท็จ ผิดกฎหมาย หรือดำเนินการใด ๆ ที่ก่อให้เกิดความเสียหายแก่ผู้อื่นหรือมหาวิทยาลัย

๗) เผยแพร่หรือจัดเก็บข้อมูลที่มีลักษณะลามก อนาจาร หรือขัดต่อศีลธรรมอันดี

๘) เผยแพร่ภาพ ภาพตัดต่อ เติมแต่ง หรือดัดแปลงภาพของบุคคลอื่นด้วยวิธีการใด ๆ ที่อาจทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๙) ใช้ทรัพยากรหรือบริการของโครงสร้างพื้นฐานทางสารสนเทศเพื่อประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน

๑๐) กระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่น

๑๑) ใช้วิธีการใด ๆ ที่ทำให้การสื่อสารข้อมูลเกิดความล่าช้าหรือถูกรบกวน จนโครงสร้างพื้นฐานทางสารสนเทศ ทรัพยากร หรือบริการใด ๆ ของมหาวิทยาลัยไม่สามารถทำงานได้ตามปกติ

๑๒) ทำลาย หรือพยายามทำลายระบบรักษาความปลอดภัยของโครงสร้างพื้นฐานทางสารสนเทศ

๑๓) ลักลอบนำฮาร์ดแวร์หรือซอฟต์แวร์มาเชื่อมต่อกับระบบเครือข่ายโดยไม่ได้รับอนุญาต และส่งผลให้เกิดความเสียหายต่อระบบเครือข่ายหรือทรัพยากรอื่น ๆ ของมหาวิทยาลัย

๑๔) ใช้งานโครงสร้างพื้นฐานทางสารสนเทศในลักษณะที่ขัดต่อนโยบาย กฎ ระเบียบ หรือข้อบังคับของมหาวิทยาลัย หรือขัดต่อกฎหมายของรัฐ

**ส่วนที่ ๓ การใช้สื่อสังคมออนไลน์ (Social Network)**

๓.๑ “สื่อสังคมออนไลน์” หมายความว่า สื่อหรือช่องทางอิเล็กทรอนิกส์เพื่อการติดต่อสื่อสารและแลกเปลี่ยนข้อมูลระหว่างกัน โดยใช้เทคโนโลยีสารสนเทศที่เน้นการสร้างและเผยแพร่เนื้อหาระหว่างผู้ใช้งานด้วยกัน (Creation and Exchange of User-generated Content) หรือสนับสนุนการสื่อสารสองทาง รวมถึงการนำเสนอและเผยแพร่ภาพ เนื้อหาและข้อมูลต่าง ๆ สู่สาธารณะด้วยตนเอง ซึ่งนิยมเรียกเป็นภาษาอังกฤษว่า Social Media หรือ Social Network โดยรวมถึงสื่อดังต่อไปนี้

๑) กระดานข่าว (Web board หรือ Online Forums)

๒) เครือข่ายสังคมออนไลน์ (Social Networking Services) เช่น Facebook, WhatsApp, Instagram, LinkedIn เป็นต้น

๓) ระบบส่งข้อความทันที (Instant Messaging) เช่น WhatsApp, Facebook Messenger, Line

๔) สื่อสำหรับการเผยแพร่และแลกเปลี่ยนเนื้อหา ในรูปแบบภาพนิ่ง เสียง วีดิทัศน์ หรือแฟ้มข้อมูล รวมถึงบริการพื้นที่จัดเก็บข้อมูลบนเครือข่ายอินเทอร์เน็ต (Photo-sharing, Audio-sharing, Video Sharing, File-sharing และ Online Storage Services) เช่น Flickr, Podcast, YouTube, Instagram, Dropbox, Google Drive, Microsoft OneDrive เป็นต้น

๕) บล็อก (Blogs) เช่น WordPress, Blogger และไมโครบล็อก (Microblogs) เช่น X (Twitter)

๖) เว็บไซต์สำหรับการสร้างและแก้ไขเนื้อหาร่วมกัน (Wikis) เช่น Wikipedia

๗) เกมออนไลน์หรือโลกเสมือนที่มีผู้ใช้งานร่วมกันจำนวนมาก (Multi-user Virtual Environments)

๘) สื่ออิเล็กทรอนิกส์หรือสื่อออนไลน์อื่น ที่มีลักษณะเดียวกันหรือคล้ายคลึงกัน ซึ่งจัดทำขึ้นเพื่อเป็นช่องทางสื่อสารระหว่างบุคคล กลุ่มบุคคล หรือต่อสาธารณะ

๓.๒ แนวปฏิบัติในการใช้งานสื่อสังคมออนไลน์

๑) ผู้ใช้งานต้องตระหนักถึงหน้าที่ตามกฎหมายในการรักษาความลับ (Confidentiality) และความเป็นส่วนตัว (Privacy) ของเจ้าของข้อมูล และหลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลที่เชื่อมโยงกับมหาวิทยาลัยเพื่อการใช้งานสื่อสังคมออนไลน์ส่วนบุคคล เช่น การใช้อีเมลของมหาวิทยาลัยในการลงทะเบียนบัญชีส่วนบุคคล

๒) การเปิดเผยข้อมูลส่วนบุคคล แม้จะได้รับความยินยอมจากของเจ้าของข้อมูลหรือผู้แทนโดยชอบธรรม หรือเป็นไปตามที่กฎหมายกำหนดแล้วก็ตาม ผู้ใช้งานต้องพิจารณาถึงผลกระทบอย่างรอบคอบเพื่อมิให้เกิดความเสียหายต่อเจ้าของข้อมูล ผู้ใช้งาน มหาวิทยาลัย และสาธารณประโยชน์

๓) ผู้ใช้งานต้องเคารพศักดิ์ศรีความเป็นมนุษย์ และหลีกเลี่ยงการกระทำหรือการเผยแพร่เนื้อหาที่เป็นการละเมิดสิทธิส่วนบุคคล หรือส่งผลให้ผู้อื่นได้รับความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือถูกคุกคามกลั่นแกล้ง (Cyberbullying)

๔) ผู้ใช้งานควรศึกษาเงื่อนไขและข้อตกลงการให้บริการ (Terms of Service) ของผู้ให้บริการสื่อสังคมออนไลน์แต่ละประเภทก่อนใช้งาน

๕) ผู้ใช้งานต้องกำหนดค่าความเป็นส่วนตัว (Privacy Settings) เพื่อจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคล และควรแยกบัญชีสื่อสังคมออนไลน์ระหว่างการใช้งานส่วนตัวและการปฏิบัติงานออกจากกัน พร้อมตรวจสอบความถูกต้องเหมาะสมของเนื้อหาที่เผยแพร่อย่างสม่ำเสมอ

๖) การขอความยินยอมเพื่อเปิดเผยข้อมูลส่วนบุคคล ต้องแจ้งวัตถุประสงค์ รูปแบบ ช่องทางและผลกระทบจากการเปิดเผยข้อมูลให้ทราบอย่างชัดเจน โดยเปิดโอกาสให้เจ้าของข้อมูลซักถามและให้ความยินยอมโดยสมัครใจ

๗) ในกรณีมีความจำเป็นต้องเปิดเผยข้อมูล ผู้ใช้งานต้องดำเนินการปกปิดข้อมูลที่สามารถระบุตัวตน เช่น ชื่อ-นามสกุล หรือหมายเลขประจำตัวประชาชน เป็นต้น

๘) ห้ามเผยแพร่ภาพนิ่งหรือวีดิทัศน์ที่ไม่เหมาะสม หรือภาพที่อาจก่อให้เกิดความเข้าใจผิด ดูหมิ่นเหยียดหยาม ลามกอนาจาร หรือแสดงความรุนแรง ที่นำมาซึ่งความเสียหายต่อบุคคล ไม่ว่าภาพนั้นจะสามารถระบุตัวตนได้หรือไม่ก็ตาม

๙) ห้ามใช้สื่อสังคมออนไลน์ในการโฆษณา แอบอ้าง หรือใช้ตราสัญลักษณ์ของมหาวิทยาลัยเพื่อประโยชน์ส่วนตน หรือยินยอมให้ผู้อื่นนำไปใช้ในทางที่ขัดต่อประมวลจริยธรรม ข้อบังคับทางวิชาชีพ หรือกฎหมาย

๑๐) ผู้ใช้งานควรหลีกเลี่ยงการแสดงความคิดเห็นในประเด็นที่ละเอียดอ่อน หรือประเด็นที่อาจก่อให้เกิดความขัดแย้งในสังคม เช่น เรื่องเกี่ยวกับสถาบันหลักของชาติ ศาสนา หรือทัศนคติทางการเมือง

๑๑) การใช้สื่อสังคมออนไลน์ต้องไม่กระทบต่อการปฏิบัติงานตามหน้าที่ หรือเป็นอุปสรรคต่อการให้บริการของมหาวิทยาลัย รวมถึงต้องรักษามาตรฐานการให้บริการตามที่กำหนด

๑๒) ผู้ใช้งานต้องตระหนักว่าข้อมูลที่เผยแพร่บนสื่อสังคมออนไลน์สามารถถูกนำไปใช้ต่อโดยผู้อื่นได้อย่างรวดเร็วและไม่สามารถลบออกได้อย่างถาวร จึงต้องคำนึงถึงความถูกต้องและความเหมาะสมก่อนการเผยแพร่ทุกครั้ง

๑๓) ผู้ใช้งานต้องหลีกเลี่ยงการใช้ถ้อยคำที่ไม่สุภาพ ก้าวร้าว หรือไม่เหมาะสมในการสื่อสารผ่านช่องทางออนไลน์

๑๔) เมื่อสิ้นสุดการใช้งาน ผู้ใช้งานต้องออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันการลักลอบเข้าถึงบัญชีโดยบุคคลอื่นที่ไม่ได้รับอนุญาต

**ส่วนที่ ๔ การบริหารจัดการทรัพย์สิน (Asset Management)**

๔.๑ ศูนย์ข้อมูลกลาง (Data Center) เป็นสถานที่สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และ/หรืออุปกรณ์บริหารจัดการระบบเครือข่าย ซึ่งถือเป็นพื้นที่ควบคุมการเข้าถึงโดยเด็ดขาด ห้ามบุคคลใดเข้าถึงพื้นที่ดังกล่าวก่อนได้รับอนุญาตจากผู้ดูแลระบบสารสนเทศส่วนกลาง

๔.๒ การนำอุปกรณ์หรือชิ้นส่วนใดออกจากศูนย์ข้อมูลกลาง (Data Center) จะต้องได้รับอนุญาตจากผู้ดูแลระบบสารสนเทศส่วนกลางก่อนดำเนินการทุกครั้ง

๔.๓ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์ใด ๆ มาเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยเพื่อวัตถุประสงค์ในการประกอบธุรกิจส่วนตัว หรือกระทำการใด ๆ ที่ผิดกฎหมาย

๔.๔ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์ โดยไม่ได้รับอนุญาต และต้องไม่เข้าถึงใช้งาน หรือลบแฟ้มข้อมูลของผู้อื่นโดยมิชอบ

๔.๕ ผู้ใช้งานต้องดำเนินการทำลายข้อมูลสำคัญ ที่จัดเก็บอยู่ในอุปกรณ์สื่อบันทึกข้อมูลหรือแฟ้มข้อมูลก่อนการจำหน่ายหรือการกำจัดอุปกรณ์ดังกล่าว และต้องใช้เทคนิคในการลบข้อมูลแบบถาวรหรือการเขียนข้อมูลทับบนข้อมูลสำคัญก่อนอนุญาตให้ผู้อื่นนำอุปกรณ์ไปใช้งานต่อ เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบ โดยให้พิจารณาวิธีการทำลายข้อมูลตามประเภทของสื่อบันทึกข้อมูล ดังนี้

| **ประเภทสื่อข้อมูล** | **วิธีการทำลาย** |
|---|---|
| กระดาษ | ใช้เครื่องทำลายเอกสาร |
| Flash Drive | - ลบข้อมูลโดยใช้วิธีที่ไม่สามารถกู้คืนได้<br>- ใช้วิธีทุบหรือบดให้เสียหาย |
| CD/DVD | หั่นเป็นชิ้นเล็ก หรือใช้เครื่องทำลายเอกสาร |
| ฮาร์ดดิสก์ | - ลบข้อมูลโดยใช้วิธีที่ไม่สามารถกู้คืนได้<br>- ใช้วิธีทุบหรือบดให้เสียหาย |

๔.๖ ผู้ใช้งานต้องรับผิดชอบดูแลทรัพย์สินที่มหาวิทยาลัยมอบหมายให้ใช้งาน เสมือนเป็นทรัพย์สินของตนเอง โดยรายการทรัพย์สิน (Asset List) รวมถึงการรับหรือส่งคืนทรัพย์สิน จะต้องมีการบันทึกและตรวจสอบทุกครั้ง โดยมีหลักเกณฑ์การตรวจสอบดังนี้

๑) ในกรณีที่ทรัพย์สินอยู่ในความรับผิดชอบของศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร ให้ผู้ดูแลระบบสารสนเทศส่วนกลางเป็นผู้ตรวจสอบ

๒) ในกรณีที่ทรัพย์สินอยู่ในความรับผิดชอบของส่วนงานและหน่วยงานภายใน ให้ผู้ดูแลระบบสารสนเทศเป็นผู้ตรวจสอบ

๔.๗ กรณีการนำทรัพย์สินไปใช้งานนอกสถานที่ ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงาน หรือผู้อำนวยการ หรือหัวหน้างาน โดยผู้ใช้งานมีหน้าที่ดูแลรักษาทรัพย์สินให้ปลอดภัยจากการโจรกรรม และต้องป้องกันไม่ให้ข้อมูลภายในของมหาวิทยาลัยรั่วไหล

๔.๘ ผู้ใช้งานต้องรับผิดชอบชดใช้ค่าเสียหาย ในกรณีที่ทรัพย์สินที่ชำรุดหรือสูญหายตามมูลค่าของทรัพย์สินนั้น หากตรวจสอบพบว่าความเสียหายดังกล่าวเกิดจากความประมาทของผู้ใช้งาน

๔.๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์พกพาของมหาวิทยาลัยไปใช้งาน เว้นแต่ได้รับอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงาน หรือผู้อำนวยการ หรือหัวหน้างาน และเมื่อสิ้นสุดภารกิจการใช้งาน ผู้ใช้งานต้องดำเนินการเปลี่ยนรหัสผ่านเข้าใช้งานเครื่องคอมพิวเตอร์

๔.๑๐ ผู้ใช้งานมีสิทธิใช้ทรัพย์สินและระบบสารสนเทศที่มหาวิทยาลัยจัดเตรียมไว้ให้เพื่อวัตถุประสงค์ในการดำเนินงานตามภารกิจของมหาวิทยาลัยเท่านั้น ห้ามนำทรัพย์สินหรือระบบดังกล่าวไปใช้ในกิจกรรมที่ไม่เกี่ยวข้อง หรือกิจกรรมที่อาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัย

๔.๑๑ ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔.๑๐ ให้ถือเป็นความรับผิดชอบส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อผลกระทบและความเสียหายที่เกิดขึ้นทั้งหมดแต่เพียงผู้เดียว

**ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)**

๕.๑ ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตเท่านั้น โดยการเข้าสู่ระบบเครือข่ายภายในมหาวิทยาลัยผ่านระบบอินเทอร์เน็ต ผู้ใช้งานต้องลงชื่อเข้าใช้งาน (Login) เพื่อแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และต้องพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่านที่ถูกต้องก่อนเข้าใช้งานทุกครั้ง

๕.๒ การเชื่อมต่อจากภายนอกมหาวิทยาลัยผ่านระบบเครือข่ายเสมือน (Virtual Private Network: VPN) สงวนสิทธิ์เฉพาะผู้ที่ได้รับอนุญาตเป็นลายลักษณ์อักษรเท่านั้น จึงจะสามารถเชื่อมต่อเข้าสู่เครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ (User Authentication for External Connections)

๕.๓ ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศ มีหน้าที่จัดเก็บข้อมูลการขอเชื่อมต่อระบบเครือข่าย โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๑) ข้อมูลเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ขอใช้บริการ รวมถึง IP Address และสถานที่ติดตั้ง

๒) การกำหนดและจำกัดสิทธิผู้ใช้งาน (Access Control) ที่สามารถเข้าถึงอุปกรณ์โครงสร้างพื้นฐานทางสารสนเทศ

๓) กรณีอุปกรณ์ที่มีการเชื่อมต่อจากภายนอก ต้องระบุหมายเลขประจำตัวอุปกรณ์หรือข้อมูลอุปกรณ์ เพื่อใช้ตรวจสอบสิทธิในการเชื่อมต่อเข้าสู่ระบบเครือข่ายภายใน

๔) อุปกรณ์ระบบเครือข่ายต้องสามารถตรวจสอบและบันทึก IP Address ของทั้งต้นทางและปลายทางได้

๕) มีมาตรการรักษาความปลอดภัยเพื่อมิให้หน่วยงานภายนอกสามารถตรวจสอบหรือตรวจพบ IP Address ภายในเครือข่ายของมหาวิทยาลัยได้

๕.๔ ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศต้องควบคุมและป้องกันการเข้าถึงพอร์ต (Port) หรือการปรับเปลี่ยนค่ากำหนดของระบบ โดยกำหนดสิทธิการเข้าถึงผ่านระบบ Firewall

๕.๕ ห้ามผู้ใดทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือดำเนินการใด ๆ ต่ออุปกรณ์ระบบเครือข่ายส่วนกลางของมหาวิทยาลัย ได้แก่ อุปกรณ์จัดเส้นทาง (Router), อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หรืออุปกรณ์ที่เชื่อมต่ออื่น ๆ โดยไม่ได้รับอนุญาต หากมีความประสงค์จะดำเนินการดังกล่าว ต้องแจ้งต่อผู้ดูแลระบบสารสนเทศส่วนกลางเพื่อพิจารณาอนุมัติก่อนทุกครั้ง

๕.๖ ระบบเครือข่ายของมหาวิทยาลัยที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอกต้องดำเนินการผ่านระบบ Firewall และอุปกรณ์ป้องกันการบุกรุกที่มีประสิทธิภาพ และต้องมีคุณสมบัติในการตรวจจับและป้องกันซอฟต์แวร์ที่ไม่พึงประสงค์ (Malware Detection)

๕.๗ ผู้ดูแลระบบสารสนเทศส่วนกลางต้องติดตั้งและบริหารจัดการระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection/Prevention System: IDS/IPS) โดยใช้ Firewall หรือระบบรักษาความปลอดภัยเครือข่ายที่มีประสิทธิภาพ เพื่อตรวจสอบพฤติกรรมการใช้งานที่ผิดปกติ การบุกรุก หรือการเปลี่ยนแปลงระบบเครือข่ายโดยผู้ที่ไม่มีสิทธิเข้าถึง

**ส่วนที่ ๖ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)**

๖.๑ ผู้ดูแลระบบสารสนเทศส่วนกลางมีหน้าที่รับผิดชอบในบริหารจัดการ ติดตั้ง และกำหนดค่าการทำงานของระบบ Firewall ของมหาวิทยาลัยให้มีความมั่นคงปลอดภัย

๖.๒ การกำหนดค่าเริ่มต้นของระบบ Firewall ต้องตั้งค่าเป็นการปฏิเสธการเชื่อมต่อทั้งหมด (Deny All) และเปิดให้บริการเฉพาะกรณีที่ได้รับอนุญาตเท่านั้น หากมีการเปลี่ยนแปลงค่าที่มีนัยสำคัญ ต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร

๖.๓ บริการหรือเส้นทางการเชื่อมต่ออินเทอร์เน็ตที่ไม่ได้รับอนุญาตตามนโยบาย ต้องถูกปิดกั้น (Block) โดยระบบ Firewall และการขอยกเว้นหรือเปลี่ยนแปลงต้องได้รับความเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

๖.๔ ผู้ดูแลระบบสารสนเทศส่วนกลางต้องกำหนดค่าพารามิเตอร์ (Parameter) การให้บริการและการเชื่อมต่อที่ได้รับอนุญาต และต้องบันทึกการเปลี่ยนแปลงการตั้งค่าของระบบ Firewall ทุกครั้งในเอกสารหรือแบบฟอร์มการร้องขอการเปลี่ยนแปลงหรือแก้ไขระบบ

๖.๕ ต้องกำหนดมาตรการป้องกันการเข้าถึงระบบ Firewall จากผู้ที่ไม่ได้รับอนุญาต โดยจำกัดสิทธิการเข้าถึงเฉพาะ IP Address ที่ได้รับอนุญาตเท่านั้น

๖.๖ การควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) และโปรแกรมสำหรับการใช้งาน

๑) ผู้ใช้งานที่ได้รับสิทธิการเข้าถึงโครงสร้างพื้นฐานทางสารสนเทศ สามารถดาวน์โหลดและติดตั้งโปรแกรมที่มหาวิทยาลัยจัดเตรียมไว้ให้ในอุปกรณ์ของตนเองได้ตามเงื่อนไขลิขสิทธิ์ของแต่ละโปรแกรม

๒) ห้ามผู้ใช้งานปรับแต่ง แก้ไข หรือดัดแปลงโปรแกรมที่มหาวิทยาลัยจัดเตรียมไว้โดยไม่ได้รับอนุญาต

๖.๗ การควบคุมการใช้งานโปรแกรมสำหรับการเรียนการสอน

๑) ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ในการติดตั้งโปรแกรมสำหรับการเรียนการสอนในห้องเรียนของมหาวิทยาลัยเท่านั้น

๒) โปรแกรมที่ติดตั้งเพื่อใช้ในการเรียนการสอน ต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

๖.๘ การควบคุมการใช้งานซอฟต์แวร์ (Software) ซอฟต์แวร์ที่มหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นทรัพยากรที่จำเป็นต่อการปฏิบัติงาน ผู้ใช้งานต้องไม่ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟต์แวร์ดังกล่าวเพื่อนำไปใช้งานที่อื่น

๖.๙ การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-out) ต้องกำหนดให้มีการตัดการเชื่อมต่อหรือสิ้นสุดการใช้งานโดยอัตโนมัติ เมื่อไม่มีการใช้งานระบบภายในระยะเวลาไม่เกิน ๘ ชั่วโมง สำหรับระบบสารสนเทศที่มีความเสี่ยงสูง ให้กำหนดระยะเวลาการตัดการเชื่อมต่อที่สั้นลงตามความเหมาะสม

**ส่วนที่ ๗ การควบคุมการเข้าโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control)**

๗.๑ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานให้อยู่ในความรับผิดชอบของผู้ดูแลระบบสารสนเทศ โดยต้องได้รับอนุมัติจากหัวหน้าส่วนงาน หรือผู้อำนวยการ หรือหัวหน้างานก่อนดำเนินการทุกครั้ง และต้องปฏิบัติตามกระบวนการบริหารการเปลี่ยนแปลง (Change Management)

๗.๒ ผู้ดูแลระบบสารสนเทศต้องดำเนินการจัดเก็บซอร์สโค้ด (Source Code) ไลบรารี (Library) และเอกสารที่เกี่ยวข้องกับซอฟต์แวร์ระบบงานไว้ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) และต้องมีระบบสำรองข้อมูล (Backup) เพื่อป้องกันการสูญหาย ความเสียหาย หรือการถูกทำลาย

๗.๓ มหาวิทยาลัยให้ความสำคัญต่อทรัพย์สินทางปัญญา ซอฟต์แวร์ทุกประเภทที่ใช้ภายในมหาวิทยาลัยต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากตรวจพบการกระทำความผิด ให้ถือเป็นความรับผิดชอบส่วนบุคคลของผู้ใช้งานนั้น

๗.๔ กรณีผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์มีการทำงานผิดปกติ หรือมีแนวโน้มว่าจะติดไวรัสหรือมัลแวร์ ผู้ใช้งานต้องระงับการเชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่ายของมหาวิทยาลัย และต้องแจ้งผู้ดูแลระบบสารสนเทศเพื่อดำเนินการแก้ไขทันที

๗.๕ ห้ามผู้ใดเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อทรัพย์สิน ข้อมูล หรือระบบสารสนเทศของมหาวิทยาลัย

**ส่วนที่ ๘ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)**

๘.๑ พนักงานมหาวิทยาลัย ลูกจ้าง นิสิตมหาวิทยาลัย และนักเรียนโรงเรียนสาธิตมหาวิทยาลัยพะเยา จะได้รับสิทธิการใช้งานจดหมายอิเล็กทรอนิกส์ส่วนบุคคลของมหาวิทยาลัย โดยสิทธิดังกล่าวจะสิ้นสุดลงเมื่อผู้ใช้งานพ้นสภาพการเป็นพนักงานมหาวิทยาลัย ลูกจ้าง นิสิตมหาวิทยาลัย หรือนักเรียนโรงเรียนสาธิตมหาวิทยาลัยพะเยา

๘.๒ กรณีส่วนงานและหน่วยงานภายใน มีความประสงค์ใช้งานจดหมายอิเล็กทรอนิกส์ที่เป็นชื่อเฉพาะเพื่อการติดต่อสื่อสารหรือการประชาสัมพันธ์ ต้องแจ้งความจำนงเพื่อขออนุมัติจากผู้อำนวยการศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสารก่อนดำเนินการ

๘.๓ เมื่อสิ้นสุดการใช้งานระบบจดหมายอิเล็กทรอนิกส์ในแต่ละครั้ง ผู้ใช้งานต้องออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบ

๘.๔ การส่งข้อมูลที่มีชั้นความลับผ่านจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานไม่ควรระบุข้อมูลสำคัญไว้ในหัวข้อจดหมาย (Subject) และควรเข้ารหัสไฟล์ข้อมูล (Encryption) ก่อนการจัดส่ง รวมทั้งต้องตรวจสอบที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail) ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งข้อมูลผิดพลาด

๘.๕ ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam mail)

๘.๖ ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๘.๗ ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาเป็นการละเมิดต่อกฎหมาย หรือละเมิดสิทธิส่วนบุคคลของผู้อื่น

๘.๘ ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสหรือมัลแวร์ไปยังบุคคลอื่นโดยเจตนา

๘.๙ ผู้ใช้งานต้องระบุชื่อผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งออกจากระบบของมหาวิทยาลัย

๘.๑๐ ผู้ใช้งานควรสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่สำคัญตามความจำเป็นอย่างสม่ำเสมอ

๘.๑๑ ผู้ใช้งานต้องตรวจสอบเอกสารแนบ (Attachment) ก่อนการเปิดใช้งานทุกครั้ง โดยการแสกนด้วยโปรแกรมป้องกันไวรัส เพื่อป้องกันการเปิดไฟล์ประเภทที่ประมวลผลได้ (Executable File) เช่น .exe, .com, .bat, .ps๑ เป็นต้น

๘.๑๒ ผู้ใช้งานควรหลีกเลี่ยงการเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ รวมถึงข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จักหรือไม่สามารถระบุตัวตนได้

๘.๑๓ ผู้ใช้งานต้องไม่ใช้ถ้อยคำที่ไม่สุภาพ หรือส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาไม่เหมาะสม หรือมีข้อมูลที่อาจก่อให้เกิดความเสียหายต่อชื่อเสียงของมหาวิทยาลัย หรือก่อให้เกิดความแตกแยกภายในมหาวิทยาลัย

๘.๑๔ ผู้ใช้งานควรตรวจสอบกล่องจดหมาย (Inbox) อย่างสม่ำเสมอ และควรจัดเก็บจดหมายอิเล็กทรอนิกส์เท่าที่จำเป็น โดยการลบข้อมูลที่ไม่จำเป็นออกจากระบบ เพื่อลดการใช้พื้นที่ระบบจดหมายอิเล็กทรอนิกส์ส่วนกลาง

๘.๑๕ ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จำเป็นต้องใช้อ้างอิงในระยะยาวจัดเก็บไว้ในอุปกรณ์ส่วนบุคคลที่ปลอดภัย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และไม่ควรจัดเก็บจดหมายอิเล็กทรอนิกส์ที่ไม่จำเป็นไว้ในกล่องจดหมาย (Inbox)

**ส่วนที่ ๙ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)**

๙.๑ แนวทางปฏิบัติของการใช้งานทั่วไป

๑) เครื่องคอมพิวเตอร์แบบพกพาที่มหาวิทยาลัยจัดสรรให้ใช้งานถือเป็นทรัพย์สินของมหาวิทยาลัย ผู้ใช้งานมีหน้าที่ดูแลรักษาให้อยู่ในสภาพพร้อมใช้งานเสมอ และห้ามดัดแปลง แก้ไข หรือเปลี่ยนแปลงส่วนประกอบของเครื่องโดยไม่ได้รับอนุญาต

๒) ผู้ใช้งานต้องเคลื่อนย้ายและจัดเก็บอุปกรณ์ด้วยความระมัดระวังในสภาพแวดล้อมที่เหมาะสม เพื่อป้องกันความเสียหายจากการกระแทก ความร้อน หรือความชื้น ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยและความพร้อมใช้งานของข้อมูลและระบบสารสนเทศ

๓) ซอฟต์แวร์ที่ติดตั้งบนเครื่องต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและได้รับอนุญาตจากมหาวิทยาลัยเท่านั้น ห้ามคัดลอก ดัดแปลง หรือนำไปใช้งานในลักษณะที่ละเมิดลิขสิทธิ์ หรือให้ผู้อื่นใช้งานโดยไม่ได้รับอนุญาต

๔) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหายหรือการโจรกรรม โดยต้องดำเนินการล็อกตัวเครื่องหรือจัดเก็บในที่ปลอดภัยทุกครั้งเมื่อไม่ได้ใช้งาน และต้องไม่วางเครื่องทิ้งไว้ในพื้นที่สาธารณะหรือในลักษณะที่เสี่ยงต่อการถูกโจรกรรม

๙.๒ การควบคุมการเข้าถึงระบบปฏิบัติการ

ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่มีความมั่นคงปลอดภัยสำหรับการเข้าใช้งานระบบปฏิบัติการ โดยต้องเก็บรักษารหัสผ่านไว้เป็นความลับ และออกจากระบบ (Log out) หรือล็อกหน้าจอ (Log Screen) ทันทีเมื่อสิ้นสุดการใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบ

**ส่วนที่ ๑๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)**

๑๐.๑ ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศ มีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อจัดเก็บข้อมูลที่สามารถรักษาความถูกต้อง ครบถ้วน และความแท้จริงของข้อมูลได้ พร้อมทั้งสามารถระบุตัวบุคคลที่เข้าถึงข้อมูลดังกล่าวได้ โดยมีการกำหนดระดับชั้นความลับเพื่อควบคุมการเข้าถึง

ทั้งนี้ ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศต้องกำหนดการเทียบเวลาของอุปกรณ์ระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย โดยกำหนดค่าอ้างอิงจากแหล่งเวลามาตรฐาน (NTP Server) เป็น th.pool.ntp.org

๑๐.๒ ผู้ดูแลระบบสารสนเทศส่วนกลางต้องรับผิดชอบในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Logs) บันทึกการปฏิบัติงานของผู้ใช้งาน (Transaction Logs) และบันทึกการใช้งานของผู้ดูแลระบบ (Admin Logs) โดยต้องเก็บรักษาข้อมูลดังกล่าวไว้เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน

๑๐.๓ ผู้ดูแลระบบสารสนเทศต้องรับผิดชอบในการจัดเก็บบันทึกการปฏิบัติงานของผู้ใช้งาน (Transaction Logs) และบันทึกการใช้งานของผู้ดูแลระบบ (Admin Logs) โดยต้องเก็บรักษาข้อมูลดังกล่าวไว้เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน

๑๐.๔ ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมายมีสิทธิในการเข้าถึงข้อมูล Log เพื่อวัตถุประสงค์ในการตรวจสอบและรักษาความมั่นคงปลอดภัยเท่านั้น ไม่มีสิทธิการแก้ไขข้อมูลหรือเปลี่ยนแปลงข้อมูล Log และห้ามเปิดเผยข้อมูล Log ต่อบุคคลภายนอก เว้นแต่กรณีที่มีความจำเป็นเพื่อใช้ประกอบการดำเนินการทางกฎหมาย ซึ่งต้องได้รับอนุมัติจากอธิการบดีก่อนดำเนินการ

## หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

**วัตถุประสงค์**

๑) เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยสามารถให้บริการได้อย่างต่อเนื่องและมีความพร้อมใช้งาน

๒) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และบทบาทความรับผิดชอบของผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศในการปฏิบัติงาน

๓) เพื่อสร้างความตระหนักรู้ให้ผู้ใช้งานปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศได้อย่างถูกต้อง

**แนวทางปฏิบัติ**

**ส่วนที่ ๑ การรักษาความปลอดภัย**

กำหนดให้ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศ มีหน้าที่รักษาความมั่นคงปลอดภัยของข้อมูล ดังนี้

๑.๑ การรักษาความลับ (Confidential) มีการรักษาความลับหรือปกปิดข้อมูลและสารสนเทศจากบุคคลที่ไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าผู้ที่ได้รับอนุญาตเท่านั้นจึงจะมีสิทธิ์ข้าถึงข้อมูลได้ โดยใช้เทคนิคหรือมาตรการควบคุม เช่น การเข้ารหัสข้อมูล เป็นต้น

๑.๒ การรักษาความถูกต้องครบถ้วน (Integrity) มีการรักษาความถูกต้องครบถ้วนของข้อมูลและสารสนเทศ สามารถตรวจสอบได้ว่าไม่มีการเปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ถูกต้องจากผู้ที่ไม่ได้รับอนุญาต เพื่อให้ข้อมูลและสารสนเทศนั้นสามารถนำไปใช้ประโยชน์ได้อย่างถูกต้องและสมบูรณ์

๑.๓ ความพร้อมใช้งาน (Availability) มีการบริหารจัดการให้ข้อมูลและสารสนเทศให้สามารถเข้าถึงหรือเรียกใช้งานได้ทันทีเมื่อผู้ใช้งานที่ได้รับอนุญาตต้องการ หรือตามกรอบระยะเวลาในการให้บริการที่มหาวิทยาลัย ส่วนงาน และหน่วยงานภายในกำหนด

**ส่วนที่ ๒ การสำรองข้อมูล (Backup)**

๒.๑ ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศ ต้องดำเนินการสำรองข้อมูลและระบบสารสนเทศที่มีความสำคัญต่อการดำเนินงานของมหาวิทยาลัย เพื่อให้ข้อมูลและระบบสารสนเทศมีความพร้อมใช้งาน โดยต้องดำเนินการดังต่อไปนี้

๑) กำหนดประเภทของข้อมูลสำคัญ และจัดทำแผนการสำรองข้อมูลอย่างเหมาะสม สอดคล้องกับระยะเวลาสูงสุดที่ยอมรับได้หากข้อมูลสูญเสีย (Recovery Point Objective: RPO)

๒) จัดทำแผนและดำเนินการทดสอบการกู้คืนข้อมูล (Restore) อย่างสม่ำเสมอ เพื่อยืนยันความสมบูรณ์ของข้อมูลสำรองและความสามารถในการนำข้อมูลกลับมาใช้งาน

๒.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Business Continuity Plan: BCP) เพื่อรองรับเหตุการณ์ที่ส่งผลกระทบต่อการให้บริการระบบสารสนเทศ เช่น ความเสี่ยง วิกฤต หรือภัยพิบัติ โดยต้องมีการทบทวนและปรับปรุงแผน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่มีนัยสำคัญ

๒.๓ ต้องดำเนินการทดสอบความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองข้อมูล และซ้อมแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่มีนัยสำคัญ เพื่อประเมินความสามารถในการกู้คืนระบบให้กลับมาให้บริการได้ตามระยะเวลาที่กำหนด (Recovery Time Objective: RTO)

## หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

**วัตถุประสงค์**

๑) เพื่อระบุ ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ รวมทั้งสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดการณ์ได้

๒) เพื่อป้องกัน ลด หรือควบคุมระดับความเสี่ยงให้อยู่ในระดับที่มหาวิทยาลัยยอมรับได้

๓) เพื่อกำหนดแนวทางในการดำเนินการเมื่อเกิดเหตุการณ์หรือความเสี่ยงที่อาจส่งผลกระทบต่อข้อมูลและระบบสารสนเทศของมหาวิทยาลัย

**แนวทางปฏิบัติ**

**ส่วนที่ ๑ การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Management)**

ผู้ดูแลระบบสารสนเทศส่วนกลางและผู้ดูแลระบบสารสนเทศ ต้องดำเนินการประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยต้องรายงานผลการประเมินความเสี่ยงต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

แนวทางในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

๑) กำหนดเกณฑ์การประเมินความเสี่ยง (Risk Criteria)

๒) ระบุและประเมินความเสี่ยง (Risk Assessment)

๓) จัดลำดับความสำคัญของความเสี่ยง (Risk Prioritization)

๔) กำหนดมาตรการเพื่อลดความเสี่ยง และจัดทำแผนจัดการความเสี่ยง (Risk Treatment Plan)

๕) ติดตามความเสี่ยงที่ยังคงเหลือ (Residual Risk)

๖) รายงานผลการประเมินความเสี่ยงต่อที่ประชุมทบทวนฝ่ายบริหาร

## หมวด ๔ นโยบายการสร้างความตระหนักด้านความปลอดภัยสารสนเทศ

**วัตถุประสงค์**

๑) เพื่อเสริมสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศ และส่งเสริมให้ผู้ใช้งานตระหนักถึงความสำคัญของการใช้งานระบบสารสนเทศอย่างปลอดภัย และเป็นไปตามกฎหมายที่เกี่ยวข้อง

๒) เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดจากพฤติกรรมของผู้ใช้งานและป้องกันความเสียหายต่อระบบสารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัย

**แนวทางปฏิบัติ**

**ส่วนที่ ๑ การสร้างความตระหนักด้านความปลอดภัยสารสนเทศ**

๑) จัดให้มีการอบรมด้านความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานมหาวิทยาลัยและลูกจ้างอย่างน้อยปีละ ๑ ครั้ง โดยต้องมีเนื้อหาครอบคลุมนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย ภัยคุกคามรูปแบบใหม่ และแนวทางปฏิบัติที่ถูกต้อง พร้อมทั้งมีการวัดผลการเรียนรู้ (Assessment)

๒) ส่งเสริมการเผยแพร่ข้อมูลข่าวสาร แนวทางปฏิบัติ และคำเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ ผ่านช่องทางต่าง ๆ เพื่อสร้างความตื่นตัวในการเฝ้าระวัง

๓) ดำเนินการตรวจติดตามภายใน (Internal Audit) เพื่อประเมินการปฏิบัติตามนโยบาย และติดตามอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident) ที่เกิดขึ้น เพื่อนำมาเป็นกรณีศึกษาในปรับปรุงเนื้อหาการสร้างความตระหนักรู้