เอกสาร

การดำเนินงานตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงานของรัฐ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏเพชรบูรณ์

สารบัญ

ประกาศมหาวิทยาลัยราชภัฏเพชรบูรณ์
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร

.....

เพื่อให้การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏเพชรบูรณ์ เป็นไปตามมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๓๑ (๑) (๒) และ (๙) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ ประกอบ มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรม ทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จึงออกประกาศมหาวิทยาลัยราชภัฏเพชรบูรณ์ เรื่อง นโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร ความดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยราชภัฏเพชรบูรณ์ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร”

ข้อ ๒ ประกาศนี้ ให้ใช้บังคับเมื่อพ้น**กำหนดเก้าสิบวัน** นับตั้งแต่วันประกาศฉบับนี้ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

“**มหาวิทยาลัย**” หมายความว่า มหาวิทยาลัยราชภัฏเพชรบูรณ์

“**หน่วยงาน**” หมายความว่า คณะ สำนัก สถาบัน ตามกฎกระทรวงจัดตั้งส่วนราชการในมหาวิทยาลัยหรือจัดตั้งเป็นส่วนงานภายในมหาวิทยาลัย

“**ผู้ใช้งาน**” หมายความว่า บุคลากร นักศึกษา ลูกจ้าง ผู้ดูแลระบบหรือผู้ที่มหาวิทยาลัยอนุญาตให้ใช้สินทรัพย์ของมหาวิทยาลัย

“**สิทธิของผู้ใช้งาน**” หมายความว่า สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย หรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัย

“**สินทรัพย์**” หมายความว่า เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย และระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาขึ้นหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

“**เครื่องคอมพิวเตอร์**” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งซึ่งทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“**ห้องคอมพิวเตอร์แม่ข่าย**” หมายความว่า สถานที่ติดตั้งอุปกรณ์แม่ข่ายหรืออุปกรณ์เครือข่ายของมหาวิทยาลัยภายในมหาวิทยาลัย

“**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ**” หมายความว่า ความสามารถในการเข้าถึงระบบสารสนเทศที่ได้รับการอนุญาต จากการกำหนดสิทธิหรือได้รับมอบอำนาจในการเข้าถึงระบบ ใน

การอ่าน สร้าง สำเนา และแก้ไขสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการทางกายภาพ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การรักษาไว้ซึ่งความลับ (confidentiality) ความครบถ้วนถูกต้อง (integrity) และความพร้อมใช้ (availability) ของสารสนเทศ และระบบเครือข่าย รวมทั้ง คุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพใช้งานการให้บริการเครือข่ายสารสนเทศมหาวิทยาลัยที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“เครือข่ายสารสนเทศมหาวิทยาลัย” หมายความว่า ระบบเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย โดยมีวัตถุประสงค์การเข้าใช้งานเพื่อการบริหารงาน การบริการวิชาการการศึกษาและงานวิจัยที่เป็นพันธกิจของมหาวิทยาลัย

“ผู้ดูแลเครือข่ายสารสนเทศมหาวิทยาลัย” หมายความว่า บุคลากรที่ได้รับมอบหมายจากมหาวิทยาลัยเพื่อปฏิบัติงานให้ดูแลบริหารจัดการระบบเครือข่ายสารสนเทศ ให้พร้อมสำหรับการใช้งานของมหาวิทยาลัย

“ผู้ปฏิบัติงานระบบสารสนเทศ” หมายความว่า บุคลากรที่ได้รับมอบหมายจากหน่วยงานเพื่อทำการป้อนข้อมูล และแก้ไขข้อมูลของระบบสารสนเทศของมหาวิทยาลัย

“เครือข่ายย่อย” หมายความว่า อุปกรณ์ต่อพ่วงต่าง ๆ รวมถึงอุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในเครือข่ายสารสนเทศมหาวิทยาลัย ตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ

“ผู้ดูแลระบบเครือข่ายย่อย” หมายความว่า บุคลากรหรือลูกจ้างได้รับมอบหมายจากหัวหน้าหน่วยงาน เพื่อปฏิบัติงานให้ระบบเครือข่ายของหน่วยงานพร้อมสำหรับการใช้งานของมหาวิทยาลัย

“ผู้ใช้บริการเครือข่าย” หมายความว่า บุคคล หน่วยงานที่ต่อเชื่อมและรับบริการจากเครือข่ายสารสนเทศของมหาวิทยาลัย

“ผู้บริหารระดับสูงสุด” หมายความว่า อธิการบดีมหาวิทยาลัยราชภัฏเพชรบูรณ์ (Chief Executive Officer : CEO)

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” หมายความว่า ผู้ได้รับการแต่งตั้งโดยผู้บริหารระดับสูงสุดให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ให้มีหน้าที่ดูแลด้านความมั่นคงปลอดภัยด้านสารสนเทศ

“คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร” หมายความว่า คณะกรรมการที่ได้รับการแต่งตั้งจากมหาวิทยาลัย เพื่อทำหน้าที่ในการ

กำหนด ตรวจสอบ ทบทวน ปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“**ผู้ตรวจสอบภายใน**” หมายความว่า บุคลากรภายในมหาวิทยาลัยที่ได้รับการแต่งตั้งจากมหาวิทยาลัยเพื่อทำหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“**ผู้ตรวจสอบจากภายนอก**” หมายความว่า เป็นบุคคลภายนอกที่มีความรู้ ความสามารถทางด้านเทคโนโลยีสารสนเทศที่ได้รับเชิญเป็นผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“**บทลงโทษ**” หมายความว่า บทลงโทษที่มหาวิทยาลัยเป็นผู้กำหนดหรือบทลงโทษตามกฎหมายที่เกี่ยวข้อง

ข้อ ๔ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๕

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๖-๑๔

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่เกี่ยวข้องกับการจัดทำนโยบาย

๕.๑.๑ ผู้บริหาร บุคลากรทางด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

๕.๑.๒ จัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคง โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ และประกาศให้ผู้ใช้งานทราบรวมทั้งสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย ซึ่งต้องยึดถือปฏิบัติตามอย่างเคร่งครัดต่อไป

๕.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๕.๑.๔ ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ส่วนที่เกี่ยวข้องกับรายละเอียดของนโยบาย

๕.๒.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้ง มีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๕.๒.๒ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๕.๒.๓ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕.๒.๔ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

๖.๑ ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล เพื่อคำนึงถึงการใช้งานและความมั่นคงปลอดภัย โดยการกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานในระบบ (user registration) การตรวจสอบสิทธิในการเข้าถึงข้อมูลตามหน้าที่และความรับผิดชอบ การทบทวนสิทธิของผู้ใช้งานระบบสารสนเทศ เมื่อมีการเปลี่ยนแปลงสถานะของผู้ใช้งาน

๖.๒ กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๖.๓ กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๗. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

๗.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๗.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๗.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๗.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๗.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

๘.๑ การใช้งานรหัสผ่าน (Password Usage) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๘.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๘.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ อันได้แก่ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบ

๘.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙. ควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๙.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๙.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๙.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๙.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๙.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๙.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้ ถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๙.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐. ควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๑๐.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๑๐.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน(User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และ

เลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๑๐.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๑๐.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๑๐.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

๑๐.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑. ควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่น และสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

๑๑.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๑.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน

๑๑.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๑๑.๔ การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๒. จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๑๒.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑๒.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๒.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๒.๕ ปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๓. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ดังนี้

๑๓.๑ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) เป็นประจำอย่างน้อยปีละ ๑ ครั้ง

๑๓.๒ ในการตรวจสอบและประเมินความเสี่ยง จะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๔. ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ดังนี้

๑๔.๑ ระดับนโยบาย

๑๔.๑.๑ ให้ผู้บริหารระดับสูงสุด (CEO) เป็นผู้รับผิดชอบในการกำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย โดยมีหน้าที่กำกับ ดูแล รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้การสนับสนุนและส่งเสริมการดำเนินงานด้านสารสนเทศอย่างมีประสิทธิภาพ

๑๔.๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง(CIO) ทำหน้าที่ติดตามกำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงานผู้รับผิดชอบระดับปฏิบัติงาน กำกับดูแลให้มีการปฏิบัติ และดำเนินการตามประกาศ ฉบับนี้

๑๔.๒ ระดับปฏิบัติงาน

ผู้ดูแลระบบสารสนเทศและระบบเครือข่ายของมหาวิทยาลัย รับผิดชอบงานพัฒนาระบบเครือข่ายและสารสนเทศ ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตาม การปฏิบัติงานตามแผน การบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ ดังนี้

๑๔.๒.๑ ควบคุมการเข้า - ออก ห้องคอมพิวเตอร์แม่ข่าย (Server) ตามการกำหนดสิทธิการเข้าถึง คอมพิวเตอร์แม่ข่าย (Server)

๑๔.๒.๒ ตรวจสอบ บำรุงรักษาอุปกรณ์ และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๑๔.๒.๓ การติดตั้ง รื้อถอน ตรวจสอบการเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการในมหาวิทยาลัย

๑๔.๒.๔ ดูแลรักษาการทำงานระบบดับเพลิงของห้องคอมพิวเตอร์แม่ข่าย (Server) ให้อยู่ในสภาพพร้อมใช้งาน สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

๑๔.๒.๕ แก้ไขปัญหาที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๑๔.๒.๖ เฝ้าระวังติดตาม ตรวจสอบ วิเคราะห์ การเข้าใช้งานและการเข้าถึงระบบการทำงานของระบบสารสนเทศและระบบเครือข่ายตามสิทธิการเข้าถึงระบบ

๑๔.๒.๗ ป้องกันและแก้ไขปัญหาการถูกเจาะเข้าระบบสารสนเทศและระบบเครือข่ายโดยไม่ได้รับอนุญาต และรายงานสภาพปัญหา ให้แก่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงทราบ

๑๔.๒.๘ ตรวจสอบ ป้องกันการถูกเจาะระบบ จากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของระบบสารสนเทศและระบบเครือข่ายทั้งหมดที่ให้บริการให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๑๔.๒.๙ ตรวจสอบอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัย ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๑๔.๒.๑๐ กำหนดและแก้ไข หรือเปลี่ยนแปลงค่าคอนฟิกระบบ (Configuration) ระบบสารสนเทศ ระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

๑๔.๒.๑๑ ประสานหน่วยงานที่เกี่ยวข้องกับการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคง ปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๑๔.๒.๑๒ แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศที่เกิดจากการถูกเจาะระบบ และการถูกทำลายจากภัยคุกคาม และรายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยงฯ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

๑๔.๒.๑๓ สำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๑๔.๒.๑๔ บริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Management) ระบบสารสนเทศแต่ละระบบของมหาวิทยาลัย เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๑๔.๒.๑๕ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและ ระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

ข้อ ๑๕. ให้ผู้บริหารระดับสูงสุดเป็นผู้รักษาการตามประกาศนี้ พร้อมกับมีอำนาจออกคำสั่งและในกรณีมีปัญหาเกี่ยวกับการปฏิบัติ ให้ผู้บริหารสูงสุดเป็นผู้วินิจฉัยชี้ขาด และคำวินิจฉัยชี้ขาดให้ถือเป็นที่สุด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๔ มิถุนายน พ.ศ. ๒๕๖๐

(ผู้ช่วยศาสตราจารย์ ดร.ประยูร ลิ้มสุข)
รักษาราชการแทนอธิการบดี

แนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๑.๑ แต่ละหน่วยงานภายในมหาวิทยาลัยจะต้องจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน มีการระบุหมายเลขทรัพย์สินตามที่กองพัสดุกลางเป็นผู้กำหนด และกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) โดยจัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ เพื่อตรวจสอบสิทธิ มอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ พร้อมทั้งทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งาน (review of user access rights) โดยมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ เมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ

๑.๒.๑ การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ต้องกำหนดสิทธิ์ที่สามารถใช้งานในขอบเขตดังนี้

(๑) อ่านอย่างเดียว
(๒) สร้างข้อมูล
(๓) ลบข้อมูล
(๔) แก้ไขข้อมูล
(๕) อนุมัติ
(๖) ไม่มีสิทธิ

๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓ มีขั้นตอนในการเก็บปฏิบัติเพื่อการจัดเก็บข้อมูลโดยจัดแบ่งประเภท ความสำคัญ ลำดับชั้นความลับ และการเข้าถึงข้อมูล มีการจัดแบ่งดังนี้

๑.๓.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น

(๑) ข้อมูลสารสนเทศด้านบริหารจัดการ
(๒) ข้อมูลสารสนเทศด้านการเรียนการสอน
(๓) ข้อมูลสารสนเทศด้านการวิจัย

๑.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

(๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด
(๒) ข้อมูลที่มีระดับความสำคัญปานกลาง
(๓) ข้อมูลที่มีระดับความสำคัญน้อย

๑.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

(๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

(๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

(๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๓.๔ จัดแบ่งระดับชั้นการเข้าถึง

(๑) ระดับชั้นสำหรับผู้บริหาร เข้าถึงข้อมูลด้านการบริหารจัดการ/ควบคุม/กำหนดนโยบาย และมาตรฐานของระบบสารสนเทศของมหาวิทยาลัย

(๒) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลด้านการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและเข้าถึงผ่านระบบงาน ภายใต้มหาวิทยาลัยกำหนด

(๓) ระดับชั้นสำหรับผู้ปฏิบัติงาน เข้าถึงชั้นข้อมูลระดับการบันทึกข้อมูล ตรวจสอบข้อมูล ปรับปรุงข้อมูล และรายงานข้อมูล ภายใต้มหาวิทยาลัยกำหนด

(๔) ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงชั้นข้อมูลระดับการอ่านข้อมูลและใช้ข้อมูลภายใต้มหาวิทยาลัยกำหนด

๑.๓.๕ การกำหนดเวลาที่ได้เข้าถึง

(๑) การใช้งานระบบสามารถเข้าใช้งานได้ ๒๔ ชั่วโมง ๗ วัน

(๒) กำหนดให้ระบบสารสนเทศ มีการยุติการใช้งานโดยการออกจากระบบโดยอัตโนมัติ เมื่อไม่มีการใช้งานหรือพักหน้าจอในช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑.๓.๖ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

(๑) ผ่านระบบยืนยันตัวตนบนโปรแกรมบราวเซอร์เครือข่ายอินเตอร์เน็ต

๑.๔ ข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๑.๔.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๑.๔.๒ แนวทางการควบคุมการเข้าถึง โดยมีการแบ่งระดับชั้นและสิทธิการเข้าถึงดังนี้

(๑) ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและเข้าถึงผ่านระบบงาน รวมไปถึงวิธีการทำลายข้อมูล

(๒) ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

(๓) ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึกข้อมูล ตรวจสอบข้อมูล ปรับปรุงข้อมูลและรายงานข้อมูลตามต้องการของมหาวิทยาลัย

(๔) ระดับชั้นสำหรับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่มหาวิทยาลัยมอบให้เท่านั้น

(๕) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

(๖) ตรวจสอบและประเมินผลการใช้งานระบบสารสนเทศ

(๗) มีรายงานปัญหาและข้อเสนอแนะการใช้งานระบบสารสนเทศต่อมหาวิทยาลัยอย่างน้อยปีละ ๑ ครั้ง

(๘) ทบทวนและปรับปรุงการใช้งานให้เหมาะสมกับภาระงานในปัจจุบัน

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ มีการกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training)

๒.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๓ กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่องต่อไปนี้

๒.๓.๑ จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๒.๓.๒ มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน โดยกำหนดเป็นชื่อภาษาอังกฤษ และตัวเลข หากซ้ำกันให้เพิ่มตัวอักษรหรือตัวเลขจนกว่าจะไม่ซ้ำกับชื่อผู้อื่น

๒.๓.๓ มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือความต้องการทางการศึกษา

๒.๓.๔ จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

๒.๓.๕ มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๒.๓.๖ มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๓.๗ มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๒.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยกำหนดรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๒.๔.๑ กำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

๒.๔.๒ การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึงระบบสารสนเทศ

๒.๔.๓ ทำการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๕ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๒.๕.๑ มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย ดังนี้

(๑) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรภาษาอังกฤษ และตัวเลข เข้าด้วยกัน

(๒) ไม่กำหนดรหัสผ่านในส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดตน หรือวัน เดือน ปีเกิด หรือเบอร์โทรศัพท์ หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๒.๕.๒ การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

๒.๕.๓ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน

๒.๕.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และต้องตั้งรหัสผ่านให้เกิดความปลอดภัย ยากแก่การคาดเดา

๒.๕.๕ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

๒.๕.๖ ต้องมีการลงนามการรับรหัสผ่านเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

๒.๕.๗ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๒.๕.๘ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสถานะภาพของผู้ใช้งาน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑ มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password User) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ ดังนี้

๓.๑.๑ เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

๓.๑.๒ ตั้งรหัสผ่านที่ยากต่อการคาดเดา

๓.๑.๓ การกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษร และตัวเลข เข้าด้วยกัน

๓.๑.๔ ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๓.๑.๕ ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

๓.๑.๖ ไม่ตั้งรหัสผ่านเป็นวันเกิด ปีที่เกิด ซึ่งง่ายต่อการคาดเดา

๓.๑.๗ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๓.๑.๘ เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๓.๑.๙ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

๓.๑.๑๐ ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

๓.๑.๑๑ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๓.๑.๑๒ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๑๘๐ วัน หรือทุกครั้งที่ได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่านจากผู้ดูแลเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏเพชรบูรณ์

๓.๑.๑๓ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

๓.๑.๑๔ หลีกเลี่ยงการใช้รหัสผ่านเดิม

๓.๑.๑๕ ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน ถี่กว่าผู้ใช้งานทั่วไป

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

๓.๒.๑ มีบัญชีควบคุมอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๒.๒ อุปกรณ์ที่ไม่มีการใช้งานจะต้องนำมาเก็บไว้ในสถานที่ที่ปลอดภัย เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๒.๓ สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

๓.๒.๔ ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๓.๒.๕ ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๓.๒.๖ ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๓.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อไม่มีการใช้งาน ดังนี้

๓.๓.๑ มีมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ดังนี้ คือ

(๑) พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในให้ติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

(๒) มีระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

(๓) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบว่ายังใช้งานได้ตามปกติ

(๔) ให้มีการบันทึกวันและเวลาเข้า-ออก พื้นที่หรือบริเวณที่มีความสำคัญของผู้ที่มาเยือน

(๕) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๖) จัดเก็บบันทึกการเข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เพื่อใช้ในการตรวจสอบภายหลังเมื่อมีความจำเป็น

(๗) ผู้มาเยือนต้องติดบัตรให้เห็นชัดตลอดระยะเวลาที่อยู่บริเวณพื้นที่ใช้งานระบบ

(๘) ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของมหาวิทยาลัย

(๙) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้องที่มีความสำคัญให้น้อยที่สุด

๓.๓.๒ การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

(๑) แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ

(๒) กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ

(๓) วัฒนธรรมองค์กร

๓.๓.๓ มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๓.๓.๔ มีการกำหนดขอบเขตของการป้องกัน ดังนี้

(๑) ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน

(๒) ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

(๓) จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

(๔) ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน

(๕) ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน

(๖) ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

(๗) ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

(๘) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๓.๕ กำหนดมาตรการทำลายสื่อบันทึกข้อมูล/ข้อมูลอิเล็กทรอนิกส์ ดังนี้

อุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง มีข้อปฏิบัติดังนี้

(๑) ต้องทำลายข้อมูลสำคัญภายในอุปกรณ์บันทึกข้อมูลหรือสื่อที่ใช้สำหรับบันทึกข้อมูลก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) สื่อบันทึกข้อมูลที่เป็นประเภทจานแม่เหล็กให้ทำการ Format อุปกรณ์ดังกล่าว โดยไม่สามารถเรียกคืนกลับมาได้ตามมาตรฐาน DOD 5220.00 M หรือวิธีบดขยี้ตามมาตรฐาน ISO/IEC 27002 : 2005

(๓) สื่อบันทึกข้อมูลประเภท Optical Disk ทำลาย โดยวิธีบดขยี้ การหัก หรือเจาะรูโดยไม่สามารถเรียกข้อมูลกลับมาได้ตามมาตรฐาน ISO/IEC 27002 : 2005

(๔) สื่อบันทึกข้อมูลขนาดเล็กแบบพกพา (Flash Drive) ให้ทำการ Format อุปกรณ์ดังกล่าว โดยไม่สามารถเรียกคืนกลับมาได้ตามมาตรฐาน DOD 5220.00 M

(๕) มีกระบวนการในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ตามมาตรฐาน NSA

๓.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ตามแนวปฏิบัติข้อ ๕(๓)

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๔.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔.๑.๑ กำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

๔.๑.๒ ผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔.๑.๓ การใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๔.๑.๔ การใช้งานระบบเครือข่ายไร้สายจะต้องมีการลงทะเบียนตาม ใช้งานชื่อผู้ใช้ รหัสผ่านและสิทธ์ตามแนวปฏิบัติการเข้าถึงของผู้ใช้งาน

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

๔.๒.๑ ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องขออนุญาตและต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ซึ่งได้จากการลงทะเบียนผ่านเจ้าหน้าที่

๔.๒.๒ การลงทะเบียนเพื่อยืนยันตัวตนของผู้ใช้งาน ต้องใช้เอกสารบัตรประชาชนหรือเอกสารอื่นที่ทางราชการเป็นผู้ออกให้เท่านั้น และต้องมีกำหนดระยะเวลาการเข้าใช้งาน

๔.๒.๓ การพิสูจน์ตัวตน (Authentication) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบ โดยผู้ใช้งานต้องกรอกรหัสผ่าน(password) เพื่อยืนยันตัวบุคคล (authentication) ว่าเป็นผู้ใช้งานตัวจริง

๔.๓ การนำอุปกรณ์มาใช้บนระบบเครือข่ายของมหาวิทยาลัยต้องระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงดังนี้

๔.๓.๑ การระบุอุปกรณ์และการจัดเก็บข้อมูล

(๑) ใช้หมายเลข IP Address ในการระบุอุปกรณ์ โดยกำหนดเป็นช่วงของหมายเลข IP แยกตามประเภทของอุปกรณ์

(๒) จัดเก็บข้อมูล อุปกรณ์บนเครือข่ายโดยระบุชนิดของอุปกรณ์การใช้งาน และเก็บบันทึกในรูปแบบสื่ออิเล็กทรอนิกส์ และเอกสารแล้วนำไปเก็บไว้ในตู้นิรภัย

๔.๓.๒ มีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ ดังนี้

(๑) กำหนดบัญชีผู้ใช้และสิทธิการเข้าถึงอุปกรณ์บนอุปกรณ์เครือข่าย

(๒) ให้ใช้โปรแกรมประเภท terminal ในการเข้าถึงอุปกรณ์

(๓) ตั้งค่าความเร็วของการเข้าถึงตามคุณลักษณะของอุปกรณ์นั้น (สามารถดูได้จากคู่มือของอุปกรณ์)

(๔) เมื่อเข้าสู่อุปกรณ์แล้วระบบจะให้กรอกชื่อผู้ใช้และรหัสผ่าน

(๕) เมื่อกรอกชื่อผู้ใช้และรหัสผ่านที่ถูกต้องระบบจะยอมให้ใช้งานอุปกรณ์ตามสิทธิ์ที่ได้กำหนดไว้

(๖) เมื่อกรอกชื่อผู้ใช้และรหัสผ่านที่ไม่ถูกต้องระบบจะไม่ยอมให้เข้าใช้งานอุปกรณ์

(๗) ระบบจะให้กรอกชื่อผู้ใช้และรหัสผ่านไม่เกิน ๓ ครั้ง มิฉะนั้นระบบจะล็อคการเข้าใช้งานอุปกรณ์ เป็นเวลา ๓๐ นาที

๔.๓.๓ ควบคุมการใช้งานอย่างเหมาะสม

๔.๓.๔ จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๔.๔.๑ การปรับเปลี่ยนหรือควบคุมการเข้าถึงพอร์ตต้องทำหนังสือขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เป็นลายลักษณ์อักษร

๔.๔.๒ บันทึกและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

๔.๔.๓ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอกและมีการแบ่งแยกเครือข่ายตามแต่ละหน่วยงานและการใช้งาน (VLAN)

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๔.๖.๑ มีการตรวจสอบการเชื่อมต่อเครือข่าย เป็นประจำเพื่อตรวจหาการเชื่อมต่อที่ไม่ได้รับอนุญาต

๔.๖.๒ จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย และกลั่นกรองข้อมูลที่รับ-ส่ง โดยอาศัยกฎเกณฑ์ต่าง ๆ ที่กำหนดไว้ล่วงหน้า

๔.๖.๓ ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย ต้องกระทำผ่านไฟร์วอลล์ โดยกำหนดให้ไฟร์วอลล์อนุญาตเฉพาะการเชื่อมต่อจากภายในออกไปยังปลายทางภายนอกได้เท่านั้น

๔.๖.๔ มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย จากผู้ไม่หวังดีด้วยระบบตรวจจับผู้บุกรุก (IDS/IPS) และตรวจทาน

๔.๖.๕ ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๔.๗.๑ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๔.๗.๒ กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๔.๗.๓ กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก จะต้องสอดคล้องตามแนวปฏิบัติการควบคุมการเข้าถึงดังนี้

๔.๘.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของหน่วยงาน ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๔.๘.๒ การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายขององค์กรต้องควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๔.๘.๓ วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือบุคคลที่ได้รับมอบหมายจากมหาวิทยาลัยก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๔.๘.๔ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๔.๘.๕ มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๔.๘.๖ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวให้ตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

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

๕.๒ การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๕.๒.๑ ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๕.๒.๒ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๕.๒.๓ จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

๕.๒.๔ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕.๓ ระบบยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้เข้าใช้งานระบบ มีแนวปฏิบัติ ดังนี้

๕.๓.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๕.๓.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านการศึกษาและงานที่ต้องทำ

๕.๓.๓ สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม

๕.๔ การบริหารจัดการรหัสผ่าน (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยมีแนวปฏิบัติดังนี้

๕.๔.๑ มีระบบบริหารจัดการรหัสผ่าน ผ่านระบบเครือข่ายสารสนเทศของมหาวิทยาลัย

๕.๔.๒ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ

๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ให้จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งาน

โปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

๕.๕.๑ จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ และควบคุมไม่ให้ใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์

๕.๕.๒ กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๕.๕.๓ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๕.๕.๔ มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๕.๕.๕ กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๖ เมื่อไม่มีการใช้งานระบบสารสนเทศในระยะเวลาที่กำหนดให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out) ดังนี้

๕.๖.๑ ให้ระบบสารสนเทศทำการยุติหรือออกจากระบบโดยอัตโนมัติ เมื่อไม่มีการใช้งานเกินระยะเวลา ๑๕ นาที

๕.๖.๒ ระบบสารสนเทศใดที่มีความเสี่ยงสูง ให้ระบบยุติหรือออกจากระบบโดยอัตโนมัติ เมื่อไม่มีการใช้งานให้สั้นลงเหลือ ๑๐ นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๕.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบเครือข่าย (Limitation of Connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูงดังนี้

๕.๗.๑ จำกัดระยะเวลาการเชื่อมต่อกับระบบเครือข่าย เพื่อให้ระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง โดยให้ผู้ใช้งานระบบเครือข่ายสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดได้ไม่เกินครั้งละ ๒ ชั่วโมง

๕.๗.๒ การกำหนดช่วงเวลาการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและผู้สนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยสอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ โดยมีแนวปฏิบัติดังนี้

๖.๑.๑ กรณีมีการจ้างเหมาพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development) มีมาตรการควบคุม Outsource ดังนี้

(๑) การคัดเลือกผู้ให้บริการ

- กำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

- สัญญาต้องระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

(๒) การควบคุมผู้ให้บริการ

- จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

- มหาวิทยาลัยเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก

- ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

- ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

- กรณีผู้รับจ้างให้บริการจากภายนอก ต้องการพัฒนาระบบงานหรือให้บริการจากภายนอก ต้องให้เจ้าหน้าที่ตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะการเปิดพอร์ต remote access และปิดพอร์ต remote access ทันทีที่การให้บริการเสร็จสิ้น

๖.๑.๒ กรณีบริหารจัดการการเข้าถึงผู้ใช้งานและผู้สนับสนุนการเข้าใช้งานระบบสารสนเทศ

(๑) มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ครอบคลุมในเรื่องต่อไปนี้

- จัดทำแบบฟอร์มขอใช้ระบบสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อ ตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

- มีการระบุชื่อ นามสกุล ของผู้ใช้งาน

- มีการระบุรหัสบัญชีผู้ใช้ระบบสารสนเทศของผู้ใช้งาน

- มีการระบุ ตำแหน่ง หน่วยงานที่สังกัด และหมายเลขโทรศัพท์ติดต่อ

- มีการลงนามของผู้บังคับบัญชาของผู้ใช้งาน

- มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

- จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

- มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

- มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

(๒) การทบทวนสิทธิ์การเข้าใช้งาน ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้ระบบสารสนเทศและ ปรับปรุงบัญชีผู้ใช้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยน ตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

(๓) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

- ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

- เจ้าของข้อมูล จะต้องทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆที่ให้ไว้ยังคงมีความเหมาะสม

- วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลแต่ละชั้นความลับข้อมูล

- การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ EML Encryption

- ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่บำรุงรักษาเครื่องคอมพิวเตอร์ หรือนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๖.๒ ระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

๖.๒.๑ ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน ได้แก่ ระบบสารสนเทศเพื่อการบริหาร ระบบทะเบียนและวัดผลนักศึกษา ระบบสารบรรณอิเล็กทรอนิกส์ ซึ่งต้องได้รับการดูแลเป็นพิเศษ

๖.๒.๒ มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ โดยมีห้องปฏิบัติงานเป็นสัดส่วน และกำหนดสิทธิเฉพาะผู้มีสิทธิใช้งานเท่านั้น

๖.๒.๓ มีการควบคุมอุปกรณ์คอมพิวเตอร์ ระบบสื่อสารและการปฏิบัติงานจากภายนอกหน่วยงานที่เกี่ยวข้องกับระบบดังกล่าว ด้วยข้อกำหนดที่สามารถตั้งค่าได้บน Firewall

๖.๒.๔ มีการควบคุมในเรื่องของ ควบคุมการเข้าถึงทางกายภาพ ระบบดับเพลิงในห้องแม่ข่าย รวมถึงระบบควบคุมความชื้น หรือ ระบบต่าง ๆ ภายในห้องแม่ข่าย

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และระบบการสื่อสาร ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และระบบการสื่อสาร เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และระบบการสื่อสาร โดยมีแนวทางในการปฏิบัติแบ่งออกเป็น ๒ กลุ่ม ดังนี้

๖.๓.๑ อุปกรณ์คอมพิวเตอร์

(๑) เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้น ผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัย ได้ซื้อลิขสิทธิ์มาอย่างถูกกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ เพื่อนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัย

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยพนักงานปฏิบัติการคอมพิวเตอร์หรือนักวิชาการคอมพิวเตอร์ของแต่ละหน่วยงาน หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ทำการล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๙) การนำเครื่องคอมพิวเตอร์มาใช้กับระบบเครือข่ายของมหาวิทยาลัย ต้องยืนยันตัวตนผ่านระบบก่อนเข้าใช้งานทุกครั้ง

๖.๓.๒ อุปกรณ์สื่อสารเคลื่อนที่

(๑) เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ จะต้องยืนยันตัวตนก่อนเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต

(๒) เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ เมื่อเลิกใช้งานระบบเครือข่ายต้องออกจากระบบการยืนยันตัวตน ทุกครั้ง

(๓) ไม่อนุญาตให้เข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม หากผู้ดูแลระบบตรวจพบจะระงับสิทธิ์การเข้าใช้งาน

(๔) ไม่อนุญาตให้ผู้ใช้งานผ่านอุปกรณ์สื่อสารกระทำผิด พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายเทคโนโลยีสารสนเทศ

๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน มีแนวปฏิบัติ ดังนี้

๖.๔.๑ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

๖.๔.๒ จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้ระบบสารสนเทศซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

(๑) เหตุผลในการขอใช้

(๒) ระยะเวลาในการใช้

(๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๔) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๖.๔.๓ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

(๑) หน่วยงานภายนอกที่ทำงานให้กับมหาวิทยาลัยทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในมหาวิทยาลัยหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของ

มหาวิทยาลัย โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

(๒) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(๓) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของมหาวิทยาลัย ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๔) มหาวิทยาลัยมีสิทธิในการตรวจสอบตามสัญญาการใช้ระบบสารสนเทศ เพื่อให้มั่นใจได้ว่ามหาวิทยาลัยสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(๕) กำหนดให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๗.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้ดูแลระบบเครือข่ายสารสนเทศมหาวิทยาลัยที่ได้รับมอบหมาย

๗.๒ ผู้ดูแลระบบเครือข่ายมหาวิทยาลัย ต้องดำเนินการดังต่อไปนี้

ต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access point) ให้เหมาะสม เพื่อป้องกันการเข้าใช้งานจากบุคคลที่ไม่ได้รับอนุญาตเข้าใช้ระบบ

๗.๒.๑ ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๗.๒.๒ ต้องทำการเปลี่ยนค่าชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบ ให้เลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๗.๒.๓ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๗.๒.๔ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๗.๒.๕ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๗.๒.๖ เลือกใช้วิธีการควบคุมชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี ชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๗.๒.๗ มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๗.๒.๘ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงทราบโดยทันที

๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพต่อระบบเครือข่าย

๘.๑ ผู้ดูแลระบบเครือข่ายสารสนเทศมหาวิทยาลัย

๘.๑.๑ กำหนด และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน พื้นที่ควบคุมให้ชัดเจน และประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ แบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

๘.๑.๒ กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งาน โดยแบ่งสิทธิในการใช้งาน ดังนี้ ผู้ดูแลระบบเครือข่าย ผู้ใช้งาน ผู้ปฏิบัติงาน และผู้ใช้บริการเครือข่ายหรือบุคคลภายนอก

๘.๑.๓ ตรวจสอบระบบรักษาความมั่นคงปลอดภัยที่กำหนดไว้ สามารถควบคุมรักษาความปลอดภัยได้ครอบคลุมระบบงาน รวมถึงวิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นในสถานการณ์ปัจจุบันนั้น ๆ อย่างน้อยปีละ ๑ ครั้ง และนำเสนอรายงานผู้บริหารมหาวิทยาลัย

๘.๑.๔ มหาวิทยาลัยมีการควบคุมการเข้าออก อาคารสถานที่ โดยมีการจัดการและจัดทำเอกสารระบุสิทธิ์ของบุคลากร และบุคคลภายนอก ในการเข้าถึงสถานที่โดยแบ่งแยกได้ ดังนี้

(๑) กำหนดสิทธิผู้ใช้ที่มีสิทธิผ่านเข้าออกและลงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอกหรือผู้มาติดต่อ ต้องได้รับอนุญาตจาก ผู้ดูแลเครือข่ายสารสนเทศมหาวิทยาลัย และต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ ไม่ว่าจะเป็นบัตรประชาชน บัตรที่หน่วยงานรัฐออกให้ที่มีหมายเลขบัตรประชาชน หรือหนังสือเดินทาง แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

(๓) บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในสถานที่นั้น ๆ

(๔) เจ้าหน้าที่หรือบุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้อง และจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

(๕) บุคคลภายนอกหรือผู้ติดต่อต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ (Visitor) กับผู้ดูแลเครือข่ายสารสนเทศมหาวิทยาลัย ก่อนออกจากอาคารผู้ดูแลเครือข่ายสารสนเทศ

ต้องตรวจสอบผู้ติดต่อ และสัมภาระ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง ผู้ใช้จะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

(๖) หากมีบุคคลอื่นที่ไม่ใช่ผู้ใช้ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้าหน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่องค์กรออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

(๗) ผู้ใช้บริการเครือข่ายหรือบุคคลภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องเป็นเจ้าหน้าที่ ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

(๘) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องทำงานผิดปกติหรือหยุดการทำงาน

๘.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

๘.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๘.๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๘.๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๘.๒.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๘.๒.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๘.๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๘.๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม สำหรับระบบสารสนเทศที่สำคัญ

๘.๒.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๘.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๘.๓.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๘.๓.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๘.๓.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๘.๓.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๘.๓.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๘.๓.๖ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘.๔ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๘.๔.๑ ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๘.๔.๒ กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๘.๔.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๘.๔.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๘.๔.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๘.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

๘.๕.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน

๘.๕.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๘.๕.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๘.๖ การทำลายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

๘.๖.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะทำลายอุปกรณ์ดังกล่าว

๘.๖.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

๘.๗.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๘.๗.๒ ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๘.๗.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ในระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๙.๑.๑ ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

๙.๑.๒ ให้ผู้ดูแลระบบสารสนเทศที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

๙.๑.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๙.๑.๔ ไม่ควรติดตั้งซอร์สโค้ด คอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นๆ

๙.๑.๕ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๙.๑.๖ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๙.๑.๗ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๙.๑.๘ ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

๙.๑.๙ ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุง ก่อนที่จะเริ่มต้นทำการพัฒนา

๙.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๙.๒.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๙.๒.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๙.๓.๑ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๙.๓.๒ ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๙.๓.๓ ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๙.๓.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

๙.๔.๑ กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ให้มีการบันทึกดังต่อไปนี้

(๑) ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน

(๒) สถานที่ที่ติดตั้ง

(๓) เครื่องที่ติดตั้ง

(๔) ผู้ผลิตซอฟต์แวร์

(๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟแวร์นั้น ๆ

๙.๔.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๙.๔.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

(๑) มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(๒) ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน

(๓) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๙.๔.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๙.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

๙.๕.๑ ข้อมูลชื่อบัญชีผู้ใช้งาน

๙.๕.๒ ข้อมูลวันเวลาที่เข้าถึงระบบ

๙.๕.๓ ข้อมูลวันเวลาที่ออกจากระบบ

๙.๕.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๙.๕.๕ ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

๙.๕.๖ ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

๙.๕.๗ ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่นของระบบ

๙.๕.๘ ข้อมูลแสดงการใช้งานแอพพลิเคชัน

๙.๕.๙ ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์

๙.๕.๑๐ ข้อมูลไอพีแอดเดรสที่เข้าถึง

๙.๕.๑๑ ข้อมูลโพรโตคอลเครือข่ายที่ใช้

๙.๕.๑๒ ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

๙.๕.๑๓ ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑๐.๑ การใช้งานทั่วไป

๑๐.๑.๑ เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ผู้ใช้งาน นำไปใช้งานเป็นทรัพย์สิน

ของหน่วยงาน ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๑๐.๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๐.๑.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

๑๐.๑.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

๑๐.๑.๕ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๑๐.๑.๖ ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

๑๐.๑.๗ ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๑๐.๑.๘ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๑๐.๑.๙ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ให้ใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

๑๐.๑.๑๐ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดให้ปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๐.๑.๑๑ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๐.๑.๑๒ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑๐.๑.๑๓ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๐.๑.๑๔ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว และในที่มีความชื้น

๑๐.๑.๑๕ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย

๑๐.๑.๑๖ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๑๐.๒ การสำรองข้อมูลและการกู้คืน

๑๐.๒.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ

๑๐.๒.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๑.๑ ผู้ดูแลระบบเครือข่ายสารสนเทศของมหาวิทยาลัย ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑๑.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๑.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๑๑.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๑๑.๕ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ไม่ว่าจะเป็นการส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม หรือการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึก

๑๒. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๑๒.๑ มีการกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยดังนี้

๑๒.๑.๑ ผู้ที่ต้องการใช้งาน E-mail ของมหาวิทยาลัย ต้องกรอกแบบคำขอใช้งานเพื่อให้ผู้ดูแลระบบทำการเพิ่มบัญชีและกำหนดสิทธิการเข้าใช้งาน

๑๒.๑.๒ ผู้ใช้งานจะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลอื่น

๑๒.๑.๓ ห้ามเข้าถึง E-mail ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ E-mail และให้ถือว่าเจ้าของ e-mail เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ใน E-mail ของตน

๑๒.๑.๔ หลังการใช้งานให้ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

๑๒.๑.๕ ผู้ใช้งานจะต้องรับผิดชอบผลกระทบที่เกิดจากการใช้งานไม่ถูกต้อง

๑๒.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

๑๒.๒.๑ กำหนดสิทธิการเข้าถึงระบบของจดหมายอิเล็กทรอนิกส์

๑๒.๒.๒ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด (Password)

๑๒.๒.๓ มหาวิทยาลัยขอสงวนสิทธิ์ในการระงับ เปลี่ยนแปลง หรือยกเลิก การใช้งานตามเหตุอันสมควร

๑๓. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๓.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้ดูแลระบบเครือข่ายของมหาวิทยาลัยที่ได้รับมอบหมายแล้วเท่านั้น

๑๓.๒ การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ของระบบปฏิบัติการ

๑๓.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย และต้องไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัย เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

๑๓.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๓.๕ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑๓.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๑๓.๗ หลังการใช้งานระบบอินเทอร์เน็ตทุกครั้ง ให้ผู้ใช้งานทำการออกจากอินเตอร์เน็ต (Logout) และปิดเว็บบราวเซอร์ทุกครั้งเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๔.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้เท่านั้น

๑๔.๒ ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องตระหนักถึงความมั่นคงปลอดภัยในการใช้งานและต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับมหาวิทยาลัย อันเกิดจากการใช้งานเครือข่ายสังคมออนไลน์

๑๔.๓ ไม่อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์เพื่อเผยแพร่ข้อมูลที่เป็นความลับ และมีผลกระทบด้านชื่อเสียงต่อบุคคลอื่นหรือมหาวิทยาลัย

๑๔.๔ ให้ใช้งานเครือข่ายสังคมออนไลน์ได้เท่าที่จำเป็นโดยไม่เบียดบังเวลาปฏิบัติงาน

๑๔.๕ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบกับบุคคลอื่นหรือมหาวิทยาลัย ผู้ใช้งานต้องแจ้งต่อผู้ดูแลระบบโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

๑๕. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติ ดังต่อไปนี้

๑๕.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๑๕.๒ ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๑๕.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑๕.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

แนวปฏิบัติระบบสารสนเทศและระบบสำรองของสารสนเทศ

๑. หน่วยงานภายในมหาวิทยาลัย ต้องให้ผู้รับผิดชอบระบบสารสนเทศทุกระบบ จัดทำแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล โดยจัดระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศทั้งหมดของหน่วยงาน พร้อมจัดทำระบบสำรองและจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง ได้แก่ การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. หน่วยงานภายในมหาวิทยาลัย ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น

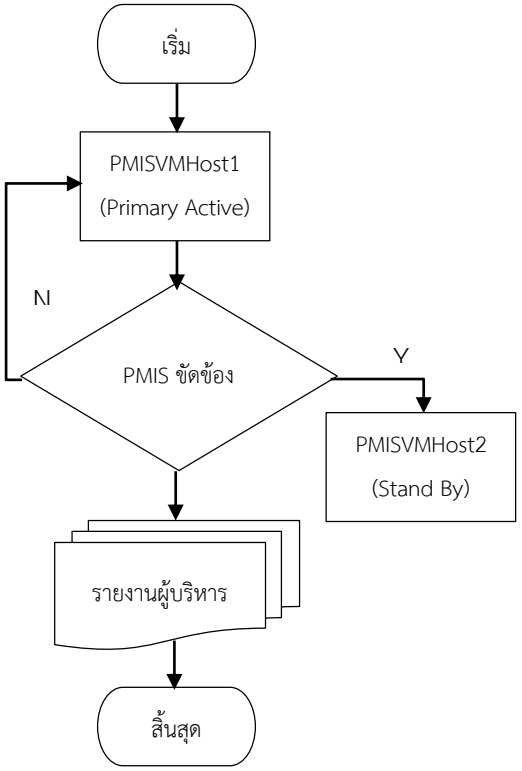
(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(๗) กำหนดเป็นแผนการสำรองระบบสารสนเทศ ดังนี้

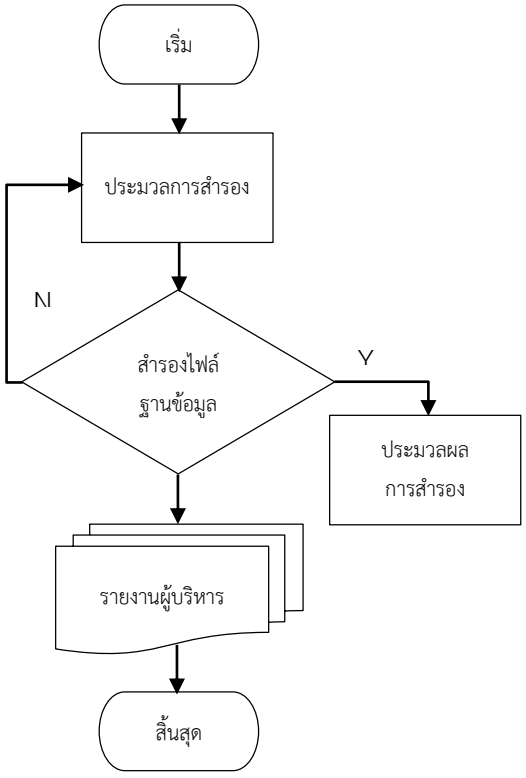
มรภ.เพชรบูรณ์	**ขั้นตอนการปฏิบัติงาน** **(Work Procedure)** ขั้นตอนการสำรองระบบสารสนเทศ	**เขียนโดย** นายไพบูลย์ กันยา **ตำแหน่ง** นักวิชาการคอมพิวเตอร์ **โทรศัพท์** ๐๕๖-๗๑๗๑๐๐ ต่อ ๒๘๓๑-๒๘๓๓ **โทรศัพท์มือถือ** ๐๘๖๐๗๗๒๘๔๖ **อนุมัติโดย** งานวิจัยและพัฒนาซอฟต์แวร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
ผู้รับผิดชอบ	**กิจกรรม**	**ผู้เกี่ยวข้อง**
นายไพบูลย์ กันยา		งานวิจัยและพัฒนาซอฟต์แวร์คอมพิวเตอร์และเครือข่าย โทรศัพท์ ๐๕๖-๗๑๗๑๐๐ ต่อ ๒๘๓๑ - ๓๓ โทรศัพท์มือถือ ๐๘๖-๐๗๗-๒๘๔๖

รายละเอียดขั้นตอนการสำรองระบบสารสนเทศ

ขั้นตอนที่	การปฏิบัติ	เวลาที่ปฏิบัติ
๑.ระบบ PMIS ทำงาน	ระบบสารสนเทศทำงานเป็นปกติระบบสารสนเทศจะทำงานอยู่ในกลุ่ม Primary Active	
๒. ระบบ PMIS ทำงานไม่เป็นปกติ	ระบบสำรองจะทำการย้าย Virtualization มายังชุดเครื่อง Stand By	ระบบย้ายโดยอัตโนมัติ
๓. รายงานผล	รายงานผลการทำงานของระบบ PMIS ต่อผู้บริหาร	๑๐ นาที

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

มรภ.เพชรบูรณ์	**ขั้นตอนการปฏิบัติงาน** **(Work Procedure)** ขั้นตอนการสำรองระบบฐานข้อมูลสารสนเทศ	**เขียนโดย** นายไพบูลย์ กันยา **ตำแหน่ง** นักวิชาการคอมพิวเตอร์ **โทรศัพท์** ๐๕๖-๗๑๗๑๐๐ ต่อ ๒๘๓๑-๓๓ **โทรศัพท์มือถือ** ๐๘๖-๐๗๗-๒๘๔๖ **อนุมัติโดย** งานวิจัยและพัฒนาซอฟต์แวร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
ผู้รับผิดชอบ	**กิจกรรม**	**ผู้เกี่ยวข้อง**
นายไพบูลย์ กันยา		งานวิจัยและพัฒนาซอฟต์แวร์คอมพิวเตอร์และเครือข่าย โทรศัพท์ ๐๕๖-๗๑๗๑๐๐ ต่อ ๒๘๓๑ - ๓๓ โทรศัพท์มือถือ ๐๘๖-๐๗๗-๒๘๔๖

การกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

ตำแหน่ง	รับผิดชอบ	หมายเลขโทรศัพท์
ผู้บริหารระดับสูงสุด (CEO) อธิการบดีมหาวิทยาลัยราชภัฏเพชรบูรณ์	กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย	ที่ทำงาน ๐๕๖๗๑๗๑๐๑
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) รองอธิการบดีฝ่ายบริหาร	ทำหน้าที่ติดตามกำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงาน	ที่ทำงาน ๐๕๖๗๑๗๑๐๒
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	ทำหน้าที่ติดตามกำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงาน	ที่ทำงาน ๐๕๖๗๑๗๑๐๐ ต่อ ๒๘๐๕
รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ฝ่ายงานวิจัยและพัฒนาซอฟต์แวร์	รับผิดชอบงานพัฒนาระบบสารสนเทศ กำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงาน	ที่ทำงาน ๐๕๖๗๑๗๑๐๐ ต่อ ๔๕๕๑ มือถือ ๐๘๖๔๐๒๘๙๒๗
รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ฝ่ายงานบริการคอมพิวเตอร์	รับผิดชอบงานพัฒนาระบบเครือข่าย กำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงาน	ที่ทำงาน ๐๕๖๗๑๗๑๐๐ ต่อ ๔๕๐๓,๒๘๐๒ มือถือ ๐๘๑๘๒๗๗๙๔๔
หัวหน้างานบริการคอมพิวเตอร์	ผู้ดูแลระบบเครือข่าย ปฏิบัติงานตามแผน และรายงานผลการดำเนินการ	ที่ทำงาน ๐๕๖๗๑๗๑๐๐ ต่อ ๒๘๔๑-๔ มือถือ ๐๘๘๑๕๑๙๙๗๘
หัวหน้างานงานวิจัยและพัฒนาซอฟต์แวร์	ผู้ดูแลระบบสารสนเทศ ปฏิบัติงานตามแผน และรายงานผลการดำเนินการ	ที่ทำงาน ๐๕๖๗๑๗๑๐๐ ต่อ ๒๘๓๑-๓ มือถือ ๐๘๒๑๖๐๖๙๙๐
นักวิชาการคอมพิวเตอร์	ปฏิบัติหน้าที่ดูแลและควบคุมการใช้งานระบบเครือข่าย	ที่ทำงาน ๐๕๖๗๑๗๑๐๐ ต่อ ๒๘๔๓ มือถือ ๐๘๖๒๐๒๓๘๓๘

ตำแหน่ง	รับผิดชอบ	หมายเลขโทรศัพท์
นักวิชาการคอมพิวเตอร์	ปฏิบัติหน้าที่ดูแลและควบคุมการใช้งานระบบสารสนเทศ	ที่ทำงาน ๐๕๖๗๑๗๑๐๐ ต่อ ๒๘๓๓ มือถือ ๐๘๖๐๗๗๒๘๔๖

๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑. จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย เพื่อตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๑.๑ แต่งตั้งคณะกรรมการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศจากผู้เชี่ยวชาญทั้งภายในและภายนอกมหาวิทยาลัย

๑.๒ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ จากคณะกรรมการในข้อ ๑.๑ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๒. แนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงอย่างน้อยดังนี้

๒.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน

๒.๒ ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

(๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

(๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

(๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๒.๔ กำหนดมาตรการจัดการความเสี่ยงด้านสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อคแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๕ ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบอย่างชัดเจน โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๒.๖ ผู้ดูแลระบบทดสอบและปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอยู่เสมอ เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

๒.๗ ผู้ดูแลระบบต้องบันทึกเหตุการณ์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อกรณีที่เหตุการณ์ที่เกิดขึ้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

แนวปฏิบัติการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของแต่ละหน่วยงาน เมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๒. จัดให้มีการทบทวนการใช้งานระบบสารสนเทศของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๓. จัดทำคู่มือและแนวปฏิบัติงานระบบสารสนเทศของแต่ละหน่วยงานทั้งในรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์

๔. มีการเผยแพร่นโยบายและแนวปฏิบัติในการใช้ระบบสารสนเทศ ระบบคอมพิวเตอร์ และนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

๒๕๕๘

แผนเตรียมความพร้อมฉุกเฉิน

(IT Contingency Plan)

มหาวิทยาลัยราชภัฏเพชรบูรณ์

พฤษภาคม ๒๕๕๘

สารบัญ

แผนเตรียมความพร้อมฉุกเฉิน

หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการปฏิบัติงานราชการ ทั้งในส่วนของการบริหารจัดการ การจัดเก็บและรวบรวมข้อมูล รวมไปถึงการประมวลผลระบบงานที่สำคัญ มหาวิทยาลัยราชภัฏเพชรบูรณ์ได้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์การ และการปฏิบัติงานของบุคลากร ซึ่งเมื่อมีการใช้งานระบบเหล่านี้ทำงานร่วมกันมากขึ้น อาจทำให้เกิดความเสี่ยงหรือโอกาสที่เกิดความเสียหาย หรือถูกรบกวนจากสถานการณ์ที่คาดไม่ถึงได้ หรืออาจเกิดจากสถานการณ์ที่เกิดขึ้นโดยบังเอิญและโดยธรรมชาติ ซึ่งสถานการณ์เหล่านี้ เรียกว่า “สถานการณ์ฉุกเฉิน (Contingency)”

มหาวิทยาลัยราชภัฏเพชรบูรณ์จำเป็นจะต้องมีการจัดทำแผนเตรียมความพร้อมฉุกเฉิน เพื่อเป็นการเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ และเพื่อให้เกิดความมั่นคงปลอดภัยและมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๕. เพื่อเป็นแนวทางการดำเนินการ กำกับข้อมูล ตรวจสอบเกี่ยวกับการบริหารจัดการ และเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงของระบบฐานข้อมูลด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏเพชรบูรณ์ให้เจ้าหน้าที่ที่เกี่ยวข้องนำไปใช้ประโยชน์

นิยามศัพท์เฉพาะ

ภัยพิบัติ หมายถึง เหตุการณ์ที่อาจเกิดจากธรรมชาติ หรือเกิดจากการกระทำของมนุษย์ที่อาจเกิดขึ้นปัจจุบันทันด่วนหรือค่อย ๆ เกิด มีผลต่อชุมชนหรือประเทศชาติ ภัยพิบัติอาจเป็นได้ทั้งเหตุการณ์ที่เกิดขึ้นตามธรรมชาติ เช่น อุทกภัย หรือเป็นเหตุการณ์ที่มนุษย์กระทำขึ้น เช่น การจลาจล หรือการชุมนุมทางการเมือง เป็นต้น

สถานการณ์ฉุกเฉิน หมายถึง สถานการณ์ทุกชนิดที่เป็นภัยต่อความมั่นคงของรัฐ กระทบกระเทือนต่อความสงบของประชาชน รวมไปถึงภัยธรรมชาติที่กระทบต่อสาธารณชน ซึ่งจะครอบคลุมตั้งแต่เกิดการกบฏ จลาจล เกิดภัยธรรมชาติ รวมทั้งเกิดสถานการณ์สงคราม

การวิเคราะห์ภัยพิบัติและสถานการณ์ฉุกเฉิน

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานของทุกหน่วยงานภายในมหาวิทยาลัยราชภัฏเพชรบูรณ์ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล การใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายและวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆการจัดทำและพัฒนาระบบเทคโนโลยีสารสนเทศในภาพรวม มุ่งหวังให้ระบบสารสนเทศช่วยในการดำเนินงานของหน่วยงานมีความสะดวกรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น แต่การนำเทคโนโลยีสารสนเทศมาใช้ย่อมมีความเสี่ยงหลายประการด้วยกัน โดยเฉพาะสถานการณ์ที่ไม่ได้คาดคิดมาก่อนเช่น ภัยธรรมชาติ อัคคีภัย ซึ่งการวางแผนเตรียมความพร้อมฉุกเฉินของระบบเทคโนโลยีสารสนเทศจึงเป็นเรื่องสำคัญและควรมีการเตรียมการที่ดี โดยหากหน่วยงานไม่มีการวางแผนเตรียมความพร้อมฉุกเฉินรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อการดำเนินงานและสร้างความเสียหายต่อหน่วยงานได้ ทั้งในด้านการพัฒนาระบบราชการ บุคลากร ความคุ้มค่าทางงบประมาณ ดังนั้นเพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินผลกระทบที่อาจจะเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏเพชรบูรณ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์ภัยพิบัติและสถานการณ์ฉุกเฉินของมหาวิทยาลัยราชภัฏเพชรบูรณ์ ได้ระบุเหตุการณ์ที่จะเกิดและผลกระทบดังต่อไปนี้

ภัยพิบัติและสถานการณ์ฉุกเฉิน	ผลกระทบ
๑. อัคคีภัย	ทำลายระบบฐานข้อมูล/เอกสาร อาคาร/สถานที่ ทรัพย์สินของทางราชการและความปลอดภัยของบุคลากร
๒. ไฟฟ้าดับ	ผู้ปฏิบัติงานและผู้รับบริการไม่สามารถเข้าถึงข้อมูลได้ อาจเกิดความเสียหายต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศซึ่งเป็นเหตุการณ์ที่มีโอกาสเกิดขึ้นบ่อยครั้ง
๓. อุทกภัย	กระบวนการหยุดชะงักผู้ปฏิบัติงานและผู้รับบริการไม่สามารถดำเนินกิจกรรมได้ทำให้ไม่สามารถบรรลุเป้าหมายตามเวลาที่กำหนดได้อาจเกิดความเสียหายต่อฐานข้อมูล และระบบเทคโนโลยีสารสนเทศ
๔. พายุ	
๕. แผ่นดินไหว	
๖. การปิดล้อมโดยกลุ่มผู้ชุมนุม	สานักงานถูกปิดกั้นช่องทางเข้า-ออก ทาให้เจ้าหน้าที่ ไม่สามารถปฏิบัติงานได้และส่งผลต่อความปลอดภัยของเจ้าหน้าที่และความเสียหายต่อทรัพย์สินของทางราชการ

จากตารางภัยพิบัติและสถานการณ์ฉุกเฉินและผลกระทบที่จะเกิดขึ้นได้นำเอามาประเมินความรุนแรงและโอกาสที่จะเกิดและจัดลำดับได้ดังนี้

ภัยพิบัติและสถานการณ์ฉุกเฉิน	ระดับคะแนน (๕)		คะแนนรวม	เรียงลำดับความสำคัญ
	โอกาส	ผลกระทบ		
๑. อัคคีภัย	๒	๕	๑๐	๒
๒. ไฟฟ้าดับ	๔	๓	๑๒	๑
๓. อุทกภัย	๑	๓	๓	๓
๔. พายุ	๑	๓	๓	๓
๕. แผ่นดินไหว	๑	๓	๓	๓
๖. การปิดล้อมโดยกลุ่มผู้ชุมนุม	๑	๓	๓	๓

จากการวิเคราะห์ผลกระทบและโอกาสที่จะเกิดขึ้นสามารถเรียงลำดับความสำคัญได้ดังนี้ ไฟฟ้าดับ และอัคคีภัย

แผนเตรียมความพร้อมฉุกเฉิน

๑. แผนเตรียมความพร้อมฉุกเฉินรองรับกรณีไฟฟ้าดับ

การดำเนินการ ณ อาคารบรรณราชนครินทร์

๑.๑ ก่อนเกิดเหตุ

๑.๑.๑ กำหนดและจัดหาอุปกรณ์ เช่น เครื่องสำรองไฟฟ้า (UPS) รองรับกรณีไฟฟ้าดับของห้องบริการเครื่องแม่ข่ายคอมพิวเตอร์

๑.๑.๒ กำหนดบุคลากรผู้รับผิดชอบในการควบคุมภาวะฉุกเฉินกรณีไฟฟ้าดับ

ผู้รับผิดชอบ	บทบาทหน้าที่
เจ้าหน้าที่ซ่อมบำรุงประจำอาคาร (นายไพโรจน์ ใจใหญ่) (นายประสงค์ อุ่นคำยี่)	- ทดสอบระบบรองรับกรณีไฟฟ้าดับ เช่น ไฟฉุกเฉิน และบันทึกเหตุการณ์ไว้ทุกครั้ง
เจ้าหน้าที่ปฏิบัติงานบริหารสำนักงาน (นายประสงค์ อุ่นคำยี่) (นางรัตนา ชมมัย)	- แจ้งการไฟฟ้าเพื่อเข้ามาตรวจสอบและแก้ไข
ฝ่ายพัฒนาระบบเครือข่าย (นายธนวัฒน์ เฉลิมพงษ์) (นายวิเศษ เกตุดี)	- ทำการสำรองข้อมูลเครื่องแม่ข่าย

๑.๑.๓ คณะ/สถาบัน/ สำนัก/ พิจารณาและจัดหาระบบสำรองไฟฉุกเฉินสำหรับคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล ตามความจำเป็น

๑.๒ ขณะเกิดเหตุ

๑.๒.๑ เมื่อเกิดไฟดับหรือไฟตกจนทำให้เครื่องตัดไฟ (เบรกเกอร์) หลัง เครื่องสำรองไฟฟ้า (UPS) จะทำงานอัตโนมัติ จะทำการจ่ายไฟสำรองให้ เครื่องคอมพิวเตอร์แม่ข่าย

๑.๒.๑ โทรแจ้งเหตุไฟฟ้าดับให้เจ้าหน้าที่ฝ่ายอาคารสถานที่ทราบ พร้อมจัดทำบันทึกนำส่งในการแจ้งเหตุ

๑.๒.๓ เจ้าหน้าที่ฝ่ายอาคารสถานที่ที่ได้รับแจ้งเหตุ เข้าทำการตรวจสอบเบื้องต้นและทำการแก้ไข หากไม่สามารถดำเนินการแก้ไขได้ โทรแจ้งการไฟฟ้าเพชรบูรณ์

๑.๒.๔. เจ้าหน้าที่ซ่อมบำรุงคอยอำนวยความสะดวกในการแก้ไข และบอกข้อมูลแผนผังไฟฟ้าในอาคาร

๑.๓ หลังเกิดเหตุ

ผู้รับผิดชอบทำการเปิดเครื่องตัดไฟ (เบรกเกอร์) หลักเพื่อใช้งานตามระบบปกติ และบันทึกการทำงานของระบบทุกครั้งที่เกิดเหตุไฟฟ้าดับ

๑.๔ การติดตามและรายงานผล

๑.๔.๑ ให้มีตรวจสอบความพร้อมการทำงานของเครื่องสำรองไฟฟ้า (UPS) ทุก ๓ เดือน

๑.๔.๒ ให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการตรวจสอบให้ผู้กำกับดูแลทราบ

๒. แผนการป้องกันและระงับอัคคีภัย

๒.๑ การป้องกันอัคคีภัย

กำหนดให้มีผู้รับผิดชอบ โดยแบ่งบทบาทหน้าที่ในการดำเนินการ ดังนี้

ผู้รับผิดชอบ	บทบาทหน้าที่
หัวหน้าสำนักงาน (นางสาวหนึ่งฤทัย บุญมี)	ดูแลเกี่ยวกับอาคารสถานที
เจ้าหน้าที่ทุกคน	การปฏิบัติและการละเว้นการปฏิบัติเพื่อป้องกันและหลีกเลี่ยงเหตุที่ก่อให้เกิดอัคคีภัย
ฝ่ายอาคารสถานที่ (นางสาวหนึ่งฤทัย บุญมี)	ตรวจสอบและกำกับ ดูแล การป้องกันอัคคีภัย

รายละเอียดบทบาทหน้าที่ของผู้รับผิดชอบแต่ละกลุ่ม คือ

๒.๑.๑ หัวหน้าสำนักงาน

(๑) จัดผังอาคารให้คำนึงถึงการเกิดอัคคีภัย

(๒) กำหนดพื้นที่ควบคุมที่อาจเกิดอัคคีภัย

(๓) กำหนดมาตรฐานการปฏิบัติงานให้ปลอดภัยจากอัคคีภัย

(๔) ควบคุมการใช้ไฟ การก่อเกิดไฟ เปลวไฟ ประกายไฟ ไฟฟ้า ความร้อน ไฟฟ้าสถิต หรือวิธีการทางานอื่นใดที่ทำให้เกิดอัคคีภัย เช่น การเชื่อม การตัด การขัด ตลอดจน การขนย้ายขนส่ง เคลื่อนย้ายสารไวไฟ ผู้อนุญาตให้มีการทำงานดังกล่าวต้องเป็นผู้ที่ได้รับมอบหมาย

(๕) มอบหมายให้มีคณะกรรมการความปลอดภัย กำหนดแผนและการดำเนินการป้องกันและระงับอัคคีภัย เช่น การฝึกอบรม การตรวจสอบ และการปรับปรุงสภาพของงาน เป็นต้น

(๖) ติดตามตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวกับการป้องกันอัคคีภัย

(๗) วางแผนระยะยาวเกี่ยวกับการป้องกันอัคคีภัย เช่น ในเรื่องการติดตั้งระบบตรวจสอบสารไวไฟหรือควันไฟ ระบบสัญญาณเตือนภัย ระบบดับเพลิงอัตโนมัติในจุดที่มีสารไวไฟหรือสารติดไฟ ได้ง่าย

(๘) กำหนดระเบียบและการควบคุมผู้รับเหมาหรือบุคคลภายนอกที่ปฏิบัติงานเกี่ยวกับการนำไฟมาใช้ หรือก่อให้เกิดเปลวไฟ ประกายไฟและความร้อน

๒.๑.๒ เจ้าหน้าที่ทุกคน

(๑) ห้ามก่อไฟในบริเวณที่หวงห้ามหรือในบริเวณควบคุมก่อนได้รับอนุญาตจาก ผู้มีหน้าที่รับผิดชอบ

(๒) ห้ามสูบบุหรี่ในบริเวณที่มีป้าย “อันตรายจากสารไวไฟหรือวัตถุระเบิด” หรือ “บริเวณที่ห้ามสูบบุหรี่” นอกจากสถานที่จัดไวเทานั้น

(๓) ห้ามทำการซ่อมแซมเครื่องจักรเครื่องมือในบริเวณที่มีสารไวไฟหรือวัสดุติดไฟได้ง่ายโดยพละการก่อนที่ช่างซ่อมและเจ้าหน้าที่ความปลอดภัยจะรวมกันจัดทำใบแจ้งซ่อมตามขั้นตอนและวิธีการที่กำหนด

(๔) การควบคุมพื้นที่ที่มีสารไวไฟหรือวัสดุติดไฟได้ง่าย การนำไฟมาใช้หรือก่อให้เกิดไฟในพื้นที่ใด ๆ ต้องห่างจากบริเวณที่มีสารไวไฟหรือวัสดุติดไฟได้ง่ายอย่างน้อยในรัศมี ๑๐ เมตร กรณีที่ไม่อาจทำได้ต้องทำการป้องกันสารไวไฟหรือวัสดุติดไฟได้ง่ายอย่างปลอดภัย ภายใต้การควบคุมของเจ้าหน้าที่ความปลอดภัย/ฝ่ายช่างอาคาร

(๕) การป้องกันการรั่วไหลของเชื้อเพลิงและสารไวไฟต่าง ๆ เจ้าหน้าที่ที่พบเห็นภาชนะที่ใสสารไวไฟหรือเชื้อเพลิงต่าง ๆ อยู่ในสภาพที่ชำรุด หรืออาจเกิดการรั่วไหล ให้รีบรายงานผู้มีหน้าที่รับผิดชอบ และกรณีที่พบว่าการรั่วไหลนั้นอาจก่อให้เกิดอันตรายร้ายแรงหากไม่แก้ไข ให้รีบทำการแก้ไขและ/หรือรายงานผู้มีหน้าที่รับผิดชอบแก้ไขทันที

(๖) การกำจัดขยะหรือเศษวัสดุที่ติดไฟได้ง่าย เจ้าหน้าที่จะต้องเก็บรวบรวมขยะหรือเศษวัสดุที่ติดไฟได้ง่ายไวในภาชนะที่ไม่ติดไฟได้ง่ายและให้นำออกจากบริเวณที่ทำงานไปเก็บไวในสถานที่ปลอดภัย อย่างน้อยวันละ ๑ ครั้ง

(๗) การป้องกันอัคคีภัยจากยานพาหนะ พนักงานที่ใช้ยานพาหนะขนถ่ายสิ่งของในบริเวณที่มีสารไวไฟ หรือถังแก๊ส จะต้องระมัดระวังการชน การกระแทก หรือการก่อให้เกิดอัคคีภัย

(๘) การป้องกันอันตรายจากไฟฟ้า สายไฟ หลอดไฟ สวิทช์มอเตอร์ไฟฟ้าพัดลม เครื่องมือเครื่องจักรที่ใช้ไฟฟ้าที่มีหรือใช้อยู่ในบริเวณสารไวไฟหรือวัสดุติดไฟได้ง่ายจะต้องตรวจตราเป็นประจำในเรื่องสภาพที่ชำรุดการต่อสายไฟ ปลั๊กไฟ การต่อสายดินหรือกรณีอื่นใดที่อาจเป็นสาเหตุของอัคคีภัย

๒.๑.๓ ฝ่ายอาคารสถานที่

(๑) กำหนดเขตพื้นที่เสี่ยงต่อการเกิดอัคคีภัย

(๒) ตรวจสอบสถานที่ล่อแหลมต่อการเกิดอัคคีภัยเป็นประจำ

(๓) กำหนดรายละเอียดของแผนป้องกันและระงับอัคคีภัย ตลอดจนจัดให้มีการอบรมและฝึกปฏิบัติเป็นระยะ ๆ

(๔) จัดหา ซ่อมบำรุง และตรวจสอบเครื่องดับเพลิงและอุปกรณ์ดับเพลิงให้อยู่ในสภาพที่พร้อมต่อการใช้งานได้ตลอดเวลา

(๕) ควบคุมการทำงานของผู้รับเหมาหรือบุคคลภายนอกในเรื่องที่เกี่ยวกับอัคคีภัย

๒.๒ การฝึกอบรม

จัดทำเพื่อเป็นแนวทางป้องกันอัคคีภัยในอาคารกรมส่งเสริมคุณภาพสิ่งแวดล้อมและอาคารศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อม โดยกำหนดให้มีการอบรมพนักงานหรือเจ้าหน้าที่ผู้ปฏิบัติงานทุกคนทุกระดับในเรื่องการดับเพลิงและการหนีไฟ

๒.๒.๑ วัตถุประสงค์

เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเกี่ยวกับวิธีการดับเพลิงขั้นต้นและสามารถใช้ถังดับเพลิง รวมทั้งสายดับเพลิงและหัวฉีดดับเพลิงได้อย่างถูกต้องเหมาะสม

๒.๒.๒ หัวข้อการฝึกอบรม

(๑) ทฤษฎีในการเกิดเพลิงไหม้

(๒) การแบ่งประเภทของเพลิง

(๓) จิตวิทยาเมื่อเกิดอัคคีภัย

(๔) การป้องกันแหล่งกำเนิดเพลิง

(๕) การใช้เครื่องมือดับเพลิง และวิธีดับเพลิงประเภทต่าง ๆ

(๖) การอพยพเมื่อเกิดเหตุเพลิงไหม้

(๗) การค้นหาและช่วยเหลือผู้ประสบภัย

๒.๓ การรณรงค์ป้องกันอัคคีภัย

เป็นแผนที่จัดทำขึ้นเพื่อป้องกันการเกิดอัคคีภัยในอาคารและเป็นการสร้างความสนใจรวมทั้งส่งเสริมในเรื่องของการป้องกันอัคคีภัยให้เกิดขึ้นกับผู้ปฏิบัติงานทุกคนทุกระดับในอาคาร การจัดทำแผนการรณรงค์ป้องกันอัคคีภัย ดังนี้

๒.๓.๑ กำหนดบุคคลผู้รับผิดชอบในการจัดการรณรงค์

๒.๓.๒ กำหนดเรื่อง หรือหัวขอที่จะทำการรณรงค์ได้แก่

(๑) องค์ประกอบของการเกิดเพลิงไหม้

(๒) การจัดเก็บวัสดุไวไฟ

(๓) การลดการสูบบุหรี่

(๔) ผลที่เกิดขึ้นจากอัคคีภัย

(๕) การทำความสะอาด

๒.๓.๓ เลือกวิธีการหรือรูปแบบการรณรงค์ที่เหมาะสม เช่น

(๑) การประกวด

(๒) การจัดทำโปสเตอร์และป้ายต่าง ๆ

(๓) การจัดนิทรรศการ

(๔) การใช้สื่อต่าง ๆ

๒.๓.๔ กำหนดระยะเวลาที่ใช้ในการรณรงค์

๒.๓.๕ กำหนดบุคคลหรือกลุ่มเป้าหมายที่ใช้ในการรณรงค์

๒.๓.๖ ประเมินผลจากการรณรงค์ทุกครั้ง

๒.๔ การตรวจตรา

เพื่อป้องกันอัคคีภัย โดยกำหนดให้ตรวจเกี่ยวกับวัตถุที่เป็นเชื้อเพลิงของเสียที่ติดไฟง่าย แหล่งความร้อน อุปกรณ์ดับเพลิง การจัดทำแผน มีดังนี้

๒.๔.๑ กำหนดบุคคลและพื้นที่ที่รับผิดชอบในการตรวจตราอย่างชัดเจนโดยกำหนดบุคคลที่จะทำหน้าที่แทนได้ด้วย

๒.๔.๒ กำหนดเรื่องที่ต้องการในแต่ละพื้นที่เป็นการเฉพาะโดยจัดทำเป็นแบบรายงานผลการตรวจที่สะดวกต่อการรายงาน

๒.๔.๓ กำหนดระยะเวลาที่ตรวจและส่งแบบรายงาน

๒.๔.๔ กำหนดบุคคลตรวจสอบแบบรายงานแล้วสรุปข้อบกพร่องให้ผู้บริหารในแต่ละฝ่ายปรับปรุงแก้ไข เช่น หัวหน้าฝ่าย ฯลฯ แล้วสรุปรายงานผู้อำนวยการฝ่ายฯ ทุกเดือน

๒.๔.๕ ควรให้มีการตรวจตราทุกวัน

๒.๕ อพยพหนีไฟ

กำหนดขึ้นเพื่อความปลอดภัยของชีวิตและทรัพย์สินของพนักงานและอาคารในขณะเกิดเหตุเพลิงไหม้ จึงได้กำหนดการดำเนินการของแผนอพยพ ดังนี้

๒.๕.๑ กำหนดผู้รับผิดชอบแต่ละหน่วยงานโดยขึ้นตรงต่อผู้อำนวยการอพยพหนีไฟหรืออำนวยการดับเพลิง (รายละเอียดการกำหนดผู้รับผิดชอบ ดังภาคผนวก ๑)

๒.๕.๒ ตรวจนับจำนวนพนักงานว่าได้อพยพหนีไฟ ออกมาภายนอกบริเวณที่ปลอดภัยครบทุกคนหรือไม่

๒.๕.๓ มีผู้นำทางพนักงานอพยพหนีไฟตามทางออกที่จัดไว้

๒.๕.๔ กำหนดจุดรวมพล จะเป็นสถานที่ที่ปลอดภัยซึ่งพนักงานที่จะสามารถมารายงานตัวและทำการตรวจนับจำนวนได้ หากพบว่าพนักงานอพยพหนีไฟออกมาไม่ครบตามจำนวนจริง ซึ่งหมายถึงมีพนักงานติดอยู่ในพื้นที่ที่เกิดอัคคีภัย

๒.๕.๕ ทำการค้นหาและทำการช่วยชีวิตพนักงานที่ยังติดค้างอยู่ในอาคารหรือในพื้นที่ที่ได้เกิดอัคคีภัย รวมถึงกรณีของพนักงานที่ออกมาอยู่ที่จุดรวมพลแล้วมีอาการเป็นลม ช็อคหมดสติหรือบาดเจ็บเป็นต้น หน่วยช่วยชีวิตและยานพาหนะจะทำการปฐมพยาบาลเบื้องต้นและติดต่อหน่วยยานพาหนะให้ในกรณีที่พยาบาลหรือแพทย์พิจารณาแล้วต้องนำส่งโรงพยาบาล

๒.๖ การยกเลิกภาวะฉุกเฉิน

หลังจากควบคุมสถานการณ์ทั้งหมดได้แล้ว ให้ผู้ควบคุมเหตุฉุกเฉิน/ผู้ประสานงานเหตุฉุกเฉิน ร่วมกันพิจารณา เพื่อยกเลิกภาวะฉุกเฉินแล้วเสนอให้ผู้อำนวยการเหตุฉุกเฉิน พิจารณาสั่งการยกเลิกภาวะฉุกเฉิน ทั้งนี้ ทุกฝ่ายต้องมั่นใจว่าจะไม่เกิดอันตรายใด ๆ ขึ้นอีกในพื้นที่เกิดเหตุหรือพื้นที่ข้างเคียง แต่ถ้าพิจารณาเห็นว่า ควรมีทีมฉุกเฉินบางทีม เตรียมพร้อมรับสถานการณ์ที่อาจเกิดขึ้นอีกให้ปิดล้อมกันผู้ไม่เกี่ยวข้องออกจากจุดเกิดเหตุแล้วให้ทีมฉุกเฉินเท่าที่จำเป็นเตรียมพร้อมรองรับเหตุฉุกเฉินจนกว่าจะเห็นว่าปลอดภัย

๒.๗ การบรรเทาทุกข์

หลังจากระงับเหตุหรือควบคุมสถานการณ์ และยกเลิกภาวะฉุกเฉินแล้ว ให้ดำเนินการบรรเทาทุกข์ จากความเสียหายที่เกิดขึ้น ดังนี้

๒.๗.๑ ประสานงานกับหน่วยงานของรัฐ

๒.๗.๒ การสำรวจความเสียหาย

๒.๗.๓ การรายงานตัวของเจ้าหน้าที่ทุกฝ่ายและกำหนดจุดนัดพบเพื่อรอรับคำสั่ง

๒.๗.๔ การช่วยชีวิตและการค้นหาผู้เสียชีวิต

๒.๗.๕ การเคลื่อนย้ายผู้ประสบภัย ทรัพย์สินและผู้เสียชีวิต

๒.๗.๖ การประเมินความเสียหายผลการปฏิบัติงานและรายงานสถานการณ์เพลิงไหม้

๒.๗.๗ การช่วยเหลือสงเคราะห์ผู้ประสบภัย

๒.๗.๘ การปรับปรุงแก้ไขเฉพาะหน้าเพื่อให้ภารกิจสามารถดำเนินการได้โดยเร็วที่สุด

๒.๘ การปรับปรุงและฟื้นฟู

แผนปฏิรูปฟื้นฟู ได้แก่ การนำรายงานผลการประเมินจากทุกด้านจากสถานการณ์จริงมาปรับปรุง โดยเฉพาะแผนการป้องกันอัคคีภัย (ก่อนเกิดเหตุ) และแผนระงับเมื่อเกิดเพลิงไหม้ แผนบรรเทาทุกข์ (ทันทีที่เพลิงสงบ) รวมทั้งการปรับปรุงแก้ไขตัวบุคลากรต่าง ๆ ที่บกพร่อง นอกจากนี้ ยังมีโครงการเพื่อรับรองแผนปฏิรูปฟื้นฟู ได้แก่

๒.๘.๑ โครงการประชาสัมพันธ์ชี้แจง สาเหตุการเกิดอัคคีภัยและแนวทางป้องกันในรูปแบบต่าง ๆ

๒.๘.๒ โครงการสงเคราะห์ผู้ป่วย/บาดเจ็บเรื้อรัง ทุพลภาพ จากเหตุอัคคีภัย

๒.๘.๓ โครงการปรับปรุงซ่อมแซมและสรรหาสิ่งที่สูญเสียให้กลับคืนสภาพปกติ

๓. แผนรองรับภัยพิบัติระบบเทคโนโลยีสารสนเทศ

การดำเนินงานของกระบวนการต่าง ๆ ของมหาวิทยาลัยราชภัฏเพชรบูรณ์ มีการใช้ระบบเทคโนโลยีสารสนเทศ เป็นสื่อกลางในการให้บริการ เก็บข้อมูลและโปรแกรม เพื่อการดำเนินงาน ทางมหาวิทยาลัยจึงได้ประเมินสถานการณ์ความเสี่ยงในด้านความเสียหายต่อระบบคอมพิวเตอร์ ฐานข้อมูลและเครือข่าย เพื่อจัดทำแผนรองรับภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT) ในภาพรวมของมหาวิทยาลัยในรูปแบบต่าง ๆ

๓.๑ ก่อนเกิดเหตุ

การเตรียมการเบื้องต้น โดยมีขั้นตอนดังนี้

๓.๒.๑ กำหนดผู้ที่มีหน้าที่รับผิดชอบและผู้ที่เกี่ยวข้อง

ผู้รับผิดชอบ	บทบาทหน้าที่
ผู้อานวยการสำนัก/ศูนย์	กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา และกำกับดูแล ควบคุม ตรวจสอบการปฏิบัติงานของเจ้าหน้าที่ผู้ที่ดูแลระบบเครือข่าย
ผู้ดูแลระบบเครือข่าย	กำกับดูแล การบำรุงรักษา การตรวจสอบแก้ไขข้อบกพร่องของระบบ ดูแลบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย สำรองข้อมูล

ผู้รับผิดชอบ	บทบาทหน้าที่
	ตรวจสอบการทำงาน/การให้บริการของระบบอย่างสม่ำเสมอ และดำเนินการตามแผนเมื่อเกิดเหตุภัยพิบัติ

๓.๑.๒ จัดทำแผนผังการติดต่อฉุกเฉิน (Emergency Call Tree)

๓.๑.๓ ทำการสำรองข้อมูล ทั้งที่อยู่ในรูปแบบเอกสารและอิเล็กทรอนิกส์ รวมถึงการสำรองระบบเว็บไซต์ และเตรียมสถานที่จัดเก็บที่ปลอดภัย

๓.๑.๔ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ซึ่งอาจทำความเสียหายแก่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ได้แก่ ติดตั้ง UPS ดูแลให้ใช้งานได้ตลอดเวลา

๓.๑.๕ จัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็น เช่น แผ่น Boot disk แผ่นติดตั้งระบบ แผ่น Driver อุปกรณ์ต่าง ๆ แผ่นสำรองข้อมูล ฯลฯ

๓.๑.๖ ทดสอบ/ทบทวน และปรับปรุงแผนรองรับ รวมทั้งจัดฝึกอบรมและให้ความรู้แก่บุคลากรให้สามารถปฏิบัติตามขั้นตอนตามที่ระบุในแผนได้ถูกต้อง

๓.๒ ขณะเกิดเหตุ

การแก้ไขปัญหาภัยพิบัติต่อระบบเครือข่าย จากด้านต่าง ๆ คือ

๓.๒.๑ ภัยพิบัติด้านกายภาพและสิ่งแวดล้อม อาจเกิดจากเหตุแผ่นดินไหว แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้ากระเพื่อม ไฟไหม้ พายุ หรือสัตว์กัดแทะ มีข้อปฏิบัติ ดังนี้

(๑) ปิดเครื่องคอมพิวเตอร์ คอมพิวเตอร์แม่ข่าย

(๒) นำอุปกรณ์จัดเก็บข้อมูลสำรองติดตัวไปด้วยขณะหนีภัย

(๓) กรณีสัตว์กัดแทะให้หุ้มสายป้องกัน หยอดเจลฆ่าแมลง

(๔) ปฏิบัติตนตามขั้นตอนหนีภัยในแต่ละกรณี

๓.๒.๒ ภัยพิบัติด้านระบบ (Systems Threats) อาจเกิดจากการทำลายระบบและข้อมูลโดยเจตนา การโจมตีเพื่อห้ามการบริการ การก่อกวนระบบด้วยโปรแกรม มีข้อปฏิบัติ ดังนี้

(๑) ปิดการเข้าถึงระบบ/คอมพิวเตอร์/เว็บไซต์

(๒) ตรวจสอบความเสียหายที่เกิดขึ้น

(๓) ตรวจสอบแหล่งที่มา

(๔) ใช้โปรแกรมต่อต้านไวรัส ฯลฯ

(๕) ดำเนินการแก้ไขความเสียหาย เช่น การติดตั้งระบบปฏิบัติการใหม่ ปรับปรุงระบบความมั่นคงปลอดภัย ลบแฟ้มข้อมูลที่ติดไวรัส

๓.๒.๓ ภัยพิบัติด้านบริหารจัดการ (Administrative Threats) อาจเกิดจากการแทรกแซงเว็บไซต์ การก่อวินาศกรรม ความผิดพลาดของซอฟแวร์ หรือฮาร์ดแวร์ มีข้อปฏิบัติ ดังนี้

(๑) ปิดกั้นการเข้าถึงเครื่องที่ให้บริการ

(๒) ตรวจสอบความเปลี่ยนแปลงของข้อมูล

(๓) สำรองข้อมูลล่าสุด เพื่อเตรียมความพร้อมในสถานการณ์การกู้คืน

(๔) ตรวจสอบปัญหา ปิดช่องโหว่

๓.๓ หลังเกิดเหตุ

๓.๓.๑ ทำการกู้คืนระบบ เครื่องแม่ข่ายให้บริการเว็บกลับสู่สภาวะปกติ

๓.๓.๒ นำ CD-ROM, Hard disk, Tape ที่สำรองข้อมูลไว้มา Restore กู้ระบบคืนโดยเร็ว
๓.๓.๓ ตรวจสอบระบบ ความถูกต้องของข้อมูลให้การทำงานกลับสู่สภาพเดิม

การติดตาม/รายงานผล

มหาวิทยาลัยราชภัฏเพชรบูรณ์ กำหนดการติดตามและรายงานผล ในการเตรียมความพร้อมรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน และการติดตาม/รายงานผลกรณีเกิดภัยพิบัติและสถานการณ์ฉุกเฉินและการดูแลแก้ไขให้กลับสู่สภาพเดิม ดังต่อไปนี้

๑. การซักซ้อมและทดสอบแผน อย่างน้อยปีละ ๑ ครั้ง

๒. รายงานสถานการณ์ และผลการปฏิบัติงาน โดยเจ้าหน้าที่ผู้รับผิดชอบให้ผู้กำกับดูแลทราบรวมทั้งรายงานปัญหาและผลการแก้ไขให้ทราบ