แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงใหม่
พ.ศ. ๒๕๕๙

ผ่านความเห็นชอบโดย

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ณ วันที่ ๑๗ พฤษภาคม ๒๕๕๙

คำนำ

ตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานหรือการให้บริการต่างๆ ของหน่วยงานรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ดังนั้น มหาวิทยาลัยราชภัฏเชียงใหม่ จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติจากทุกหน่วยงาน รวมทั้งต้องทำอย่างต่อเนื่อง มีการตรวจสอบและปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว มหาวิทยาลัยราชภัฏเชียงใหม่ จึงหวังเป็นอย่างยิ่งว่า นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏเชียงใหม่ ถือปฏิบัติโดยเคร่งครัดต่อไป

สารบัญ

****

ประกาศมหาวิทยาลัยราชภัฏเชียงใหม่
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏเชียงใหม่ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้อง รวมทั้งการถูกคุกคามจากภัยต่างๆ ที่อาจก่อให้เกิดความเสียหายแก่ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏเชียงใหม่ สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้อง มหาวิทยาลัยราชภัฏเชียงใหม่ จึงได้กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏเชียงใหม่ ถือปฏิบัติโดยเคร่งครัด

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ และอาศัยอำนาจตาม มาตรา ๒๗ และ ๓๑ แห่งพระราชบัญญัติ มหาวิทยาลัยราชภัฏเชียงใหม่ ๒๕๔๗ จึงออกประกาศไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยราชภัฏเชียงใหม่ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดแล้วก่อนหน้านี้ ซึ่งขัดหรือแย้งกับประกาศฉบับนี้ให้ใช้ประกาศฉบับนี้แทน

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏเชียงใหม่มีวัตถุประสงค์ ดังนี้

๔.๑ เพื่อกำหนดมาตรฐาน แนวนโยบาย แนวปฏิบัติ และวิธีการปฏิบัติให้ผู้บริหาร บุคลากร และนักศึกษา ที่ใช้งานระบบสารสนเทศของมหาวิทยาลัย ได้ตระหนักถึงความสำคัญของ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๔.๒ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของมหาวิทยาลัย ให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล และมีความต่อเนื่อง

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๕.๑.๑. การเข้าถึงระบบสารสนเทศ ต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ หรือการมอบอำนาจ

๕.๑.๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตหรือ ผู้ที่ผ่านการฝึกอบรมแล้วเท่านั้น

๕.๑.๓. การเข้าถึงระบบเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๕.๑.๔. การเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๕.๑.๕. การเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control)

๕.๒ ให้จัดทำระบบสำรองข้อมูลสารสนเทศของมหาวิทยาลัย และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถบริการระบบสารสนเทศได้อย่างต่อเนื่องและมีเสถียรภาพ

๕.๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) โดยจัดให้มีผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือมีการตรวจสอบด้านความมั่นคงปลอดภัยจากผู้ตรวจสอบภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) อย่างน้อยดังนี้

๖.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยจัดทำข้อปฏิบัติสำหรับการควบคุมการเข้าถึงสารสนเทศ

๖.๒ มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย โดยกำหนดสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ หลักการ “ตามความจำเป็นที่ต้องรู้”

ข้อ ๗ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) รับผิดชอบในดำเนินการตามนโยบาย กำกับ ดูแล และรับผิดชอบด้านสารสนเทศของมหาวิทยาลัย กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๘ มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

ข้อ ๑๐ ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๑ มกราคม พ.ศ. ๒๕๕๙

(รองศาสตราจารย์ ดร.ประพันธ์ ธรรมไชย)

อธิการบดีมหาวิทยาลัยราชภัฏเชียงใหม่

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของมหาวิทยาลัยราชภัฏเชียงใหม่

ตามประกาศมหาวิทยาลัยราชภัฏเชียงใหม่ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏเชียงใหม่ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏเชียงใหม่ เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏเชียงใหม่ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัยราชภัฏเชียงใหม่นั้น

มหาวิทยาลัยราชภัฏเชียงใหม่ จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

คำนิยาม

“**หน่วยงาน**” หมายถึง คณะ วิทยาลัย สำนัก สถาบัน ศูนย์ กอง ที่อยู่ในสังกัดมหาวิทยาลัยราชภัฏเชียงใหม่

“**ผู้บริหารระดับสูงสุด**” หมายถึง อธิการบดีมหาวิทยาลัยราชภัฏเชียงใหม่

“**ผู้บริหารระดับสูง**” หมายถึง รองอธิการบดี และผู้ช่วยอธิการบดี

“**ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง**” หมายถึง ผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา

“**ผู้บริหาร**” หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ คณบดี ผู้อำนวยการ รองคณบดี รองผู้อำนวยการ หรือเทียบเท่า

“**ผู้ใช้งาน**” หมายถึง ข้าราชการ ลูกจ้าง พนักงานราชการ พนักงานมหาวิทยาลัย และนักศึกษา ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศของหน่วยงาน

“**ผู้ดูแลระบบ**” (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศไม่ว่าส่วนหนึ่งส่วนใด

“เจ้าของระบบ” หมายถึง ผู้ที่ได้รับมอบอำนาจจากมหาวิทยาลัยให้มีสิทธิในการบริหารจัดการระบบสารสนเทศ

“**เจ้าของข้อมูล**” หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูล ของระบบสารสนเทศของหน่วยงานหรือมหาวิทยาลัย โดยเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้น เกิดการสูญหาย

“**สิทธิของผู้ใช้งาน**” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานหรือมหาวิทยาลัย โดยผู้บริหารหน่วยงานหรือผู้บริหารระดับสูงจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์หรือสารสนเทศ

“**สินทรัพย์**” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย และโทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์

“**ระบบเครือข่ายคอมพิวเตอร์**” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงานได้ ได้แก่ ระบบเครือข่ายใช้สาย (Wired Network) และระบบเครือข่ายไร้สาย (Wireless Network)

“**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ**” หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาต การเข้าถึงสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“**ความมั่นคงปลอดภัยด้านสารสนเทศ**” หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

“**เหตุการณ์ด้านความมั่นคงปลอดภัย**” หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด**” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของมหาวิทยาลัยหรือหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยด้านสารสนเทศถูกคุกคาม

หมวดที่ ๑
การควบคุมการเข้าถึงและการใช้งานสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยของระบบสารสนเทศ

๒. เพื่อกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์และการมอบอำนาจของหน่วยงานของมหาวิทยาลัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ ๒ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์เข้าใช้สารสนเทศของหน่วยงานใด จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงานนั้น

ข้อ ๓ ผู้ใช้งานที่ต้องการเข้าใช้งานสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมาย

ข้อ ๔ ผู้ดูแลระบบ ต้องมีการจัดตั้งระบบบันทึกการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบและติดตามการใช้งานสารสนเทศของหน่วยงาน รวมถึงตรวจสอบการละเมิดความปลอดภัยที่มีต่อสารสนเทศ

ข้อ ๕ กำหนดเวลาในการเข้าถึงสารสนเทศ ดังนี้

๕.๑ ระบบงานบริการ e-Service สามารถเข้าถึงได้ตลอดเวลา

๕.๒ ระบบสารสนเทศด้านการบริหารจัดการ ให้กำหนดเวลาในการเข้าถึงสารสนเทศเป็นไปตามที่หน่วยงานกำหนด

ข้อ ๖ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

๖.๑ จัดให้มีการแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๖.๑.๑ ประเภทของข้อมูล แบ่งออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ คำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

- ข้อมูลสารสนเทศด้านการบริการของมหาวิทยาลัย ได้แก่ ข้อมูลการลงทะเบียนเรียน ข้อมูลผลการเรียน ข้อมูลนักศึกษา ข้อมูลบริการชุมชน เป็นต้น

๖.๑.๒ ระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๖.๑.๓ ระดับชั้นความลับของข้อมูล แบ่งออกเป็น

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๖.๑.๔ ระดับชั้นการเข้าถึงข้อมูลในฐานข้อมูล แบ่งออกเป็น ๓ ระดับ คือ

- ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลในฐานข้อมูลได้ตามภารกิจที่มหาวิทยาลัยมอบหมาย

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงข้อมูลในฐานข้อมูลได้เฉพาะข้อมูลส่วนบุคคล และข้อมูลข่าวสารประชาสัมพันธ์ที่ออกสู่สาธารณะ

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย สามารถเข้าถึงข้อมูลในฐานข้อมูลได้ตามหน้าที่ในการดูแลระบบที่มหาวิทยาลัยมอบหมาย

๖.๑.๕ รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่สามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ ได้แก่ TEXT Format, Document Format, PDF Format (Portable Document Format) เป็นต้น

- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่เปิดเห็นเป็นรูปภาพมีรูปแบบที่ใช้ ได้แก่ JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

๖.๑.๖ มีการกำหนดเวลาที่ได้เข้าถึงข้อมูลในฐานข้อมูล

- ข้อมูลที่เปิดเผย ๒๔ ชั่วโมง
- ข้อมูลที่เปิดเผยเฉพาะเวลาทำการ

- ข้อมูลที่เปิดเผยเมื่อมีการมอบหมายตามภารกิจ

๖.๑.๗ มีการกำหนดจำนวนช่องทางที่สามารถเข้าถึงฐานข้อมูล ๒ ช่องทางดังนี้

- ระบบเครือข่ายภายในมหาวิทยาลัย (Intranet)
- ระบบเครือข่ายภายนอกมหาวิทยาลัย (Internet)

๖.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

๖.๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- กลุ่มผู้ใช้อ่านข้อมูลอย่างเดียว
- กลุ่มผู้ใช้สร้างข้อมูลได้
- กลุ่มผู้ใช้ป้อนข้อมูลได้
- กลุ่มผู้ใช้ที่แก้ไขข้อมูลได้
- กลุ่มผู้ใช้ที่ลบข้อมูลออกจากระบบได้
- กลุ่มผู้ใช้ที่ทำการอนุมัติในระบบ
- กลุ่มผู้ใช้ที่ไม่มีสิทธิ์ในการเข้าถึงใด ๆ ในระบบ

๖.๒.๒ กำหนดเกณฑ์ระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตาม **การบริหารจัดการเข้าถึงผู้ใช้งาน (User Access Management)** ที่กำหนดไว้ในส่วนที่ ๒

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงสารสนเทศ ระบบเครือข่าย เฉพาะผู้ที่ได้รับอนุญาต และสามารถตรวจสอบติดตามผู้ใช้งานผ่านระบบพิสูจน์ตัวตน รวมทั้งการกำหนดหลักสูตรในการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตดังนี้

ข้อ ๗ การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๑ กำหนดให้มีหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๗.๒ กำหนดให้มีการจัดอบรมเพื่อให้ความรู้กับผู้ใช้งาน เรื่องความมั่นคงปลอดภัยด้านสารสนเทศเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Information Security Incident) เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานสารสนเทศโดยไม่ระมัดระวัง รวมถึงการกำหนดมาตรการเชิงป้องกันตามความเหมาะสม

ข้อ ๘ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งานของระบบเครือข่าย (User Registration) ดังนี้

๘.๑ นักศึกษาและนักศึกษาใหม่ทุกคน ได้รับบัญชีผู้ใช้โดยอัตโนมัติ ทันทีที่สำนักทะเบียนและประมวลผล ป้อนข้อมูลเข้าสู่ระบบสารสนเทศนักศึกษา

๘.๒ บุคลากรของมหาวิทยาลัย โดยกองบริหารงานบุคคลจะจัดทำบัญชีผู้ใช้ ส่งให้สำนักดิจิทัลเพื่อการศึกษาดำเนินการลงทะเบียนในระบบ

๘.๓ อาจารย์พิเศษและบุคคลภายนอก กรณีคณะ/หน่วยงาน ต้องการบัญชีผู้ใช้เพื่อบริหารจัดการในการให้บริการเป็นรายบุคคลหรือกลุ่มบุคคล ดำเนินการดังนี้

๘.๓.๑ คณะ/หน่วยงาน ของมหาวิทยาลัย จัดทำบัญชีผู้ใช้ ส่งให้สำนักดิจิทัลเพื่อการศึกษา ดำเนินการลงทะเบียนในระบบ หรือดาวน์โหลดแบบฟอร์มได้จาก http://www.digital.cmru.ac.th/ กรอกข้อมูลให้ครบถ้วนส่งสำนักดิจิทัลเพื่อการศึกษา

๘.๓.๒ สำนักดิจิทัลเพื่อการศึกษา จะออกบัญชีผู้ใช้ให้ ตามข้อมูลที่คณะ/หน่วยงานระบุ และแจ้งผู้รับผิดชอบตามอีเมล์ที่ระบุไว้ในแบบฟอร์ม

๘.๓.๓ คณะ/หน่วยงาน จะต้องรับผิดชอบความเสียหายใดๆ ที่จะเกิดจากการใช้งานบัญชีผู้ใช้ที่สำนักดิจิทัลเพื่อการศึกษา ออกให้

๘.๓.๕ หากต้องการยกเลิกบัญชีผู้ใช้ ให้แจ้งสำนักดิจิทัลเพื่อการศึกษา เป็นลายลักษณ์อักษรลงนามโดยผู้บริหารของคณะ/หน่วยงาน ระบุ ชื่อบัญชีผู้ใช้ที่ต้องการยกเลิก

๘.๔ บุคคลอื่นๆที่ มหาวิทยาลัยมอบสิทธิ์ให้ สามารถลงทะเบียนขอใช้งานบัญชีผู้ใช้ โดยติดต่อที่สำนักดิจิทัลเพื่อการศึกษา และมีหนังสือรับรองจากผู้บริหารระดับคณะ/หน่วยงาน และแสดงบัตรประจำตัวประชาชน หรือหนังสือเดินทาง พร้อมสำเนาที่รับรองสำเนาถูกต้อง 1 ฉบับ

ข้อ ๙ กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ์ เพื่อให้การเข้าถึงและใช้งานสารสนเทศแต่ละกลุ่มเป็นไปตามความเหมาะสม รวมถึงสิทธิพิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึงและใช้งานสารสนเทศ ดังนี้

๙.๑ มีกระบวนการในการมอบหมาย หรือกำหนดสิทธิในการใช้งานให้แก่ผู้ใช้งานโดยให้กำหนดกลุ่มผู้ใช้งานออกเป็น ๒ กลุ่ม คือ นักศึกษา และบุคลากรสายสอนและสายสนับสนุนของมหาวิทยาลัย ดังนี้

๙.๑.๑ นักศึกษา

๙.๑.๑.๑ เมื่อนักศึกษา ลาออก หรือพ้นสภาพนักศึกษา ให้แจ้งเพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ออกจากระบบทันที

๙.๑.๑.๒ ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๙.๒.๑ บุคลากรสายสอนและสายสนับสนุน

๙.๒.๑.๑ เมื่อบุคลากรสายสอนและสายสนับสนุน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิ์การใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ออกจากระบบทันที

๙.๒.๑.๒ การแจ้งขอใช้สิทธิ์/เปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น

(๑) ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

(๒) ส่งถึงผู้บริหารของหน่วยงานหลัก

(๓) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

(๔) หน่วยงานหลักสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๙.๒.๑.๓ ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๙.๒.๑.๔ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาโดยต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารระดับสูงสุดหรือผู้ที่ได้รับมอบอำนาจจากผู้บริหารระดับสูงสุด

(๑) ควบคุมการใช้งานอย่างเข้มงวด ต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๙.๒ กรณีผู้ใช้งานที่บุคคลภายนอก ซึ่งไม่มีสิทธิ์ในการเข้าถึงและใช้งานสารสนเทศของมหาวิทยาลัยตามข้อ (๙.๑) อาทิ อาจารย์พิเศษ เป็นต้น หากต้องการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัยจะต้องได้รับการอนุญาตจากผู้บริหารระดับสูงสุด หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

๙.๓ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษแก่ผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารระดับสูงสุด หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) โดยมีการกำหนดระยะเวลาใช้งาน และให้ระงับการใช้งานทันที่เมื่อพ้นระยะเวลาดังกล่าว และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๙.๔ กำหนดให้มีการจัดเก็บข้อมูลในการมอบหมาย หรือกำหนดสิทธิ์

ข้อ ๑๐ ต้องมีการกำหนดสิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน ในการใช้งานสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต (Internet) เป็นต้น

ข้อ ๑๑ ต้องมีการทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

๑๑.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน

๑๑.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

๑๑.๓ ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

๑๑.๔ ขั้นตอนการปฏิบัติ งานสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อพ้นสภาพสิทธิ์การใช้งานต้อง ดำเนินการภายใน ๗ วัน หรือเมื่อเปลี่ยนตำแหน่งงานต้องดำเนินการภายใน ๑๕ วัน

ข้อ ๑๒ การบริหารจัดการรหัสผ่าน (Password Management) มีกระบวนการดังต่อไปนี้

๑๒.๑ การกำหนดรหัสผ่านต้องไม่ตรงกับชื่อผู้ใช้งาน (Username)

๑๒.๒ การส่งมอบรหัสผ่าน (Password) ให้ส่งมอบด้วยวิธีที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่มีการป้องกัน

๑๒.๓ เมื่อมีการส่งรหัสผ่านให้ผู้รับ จะต้องจัดให้มีการตอบรับหรือยืนยันการรับรหัสผ่าน

๑๒.๔ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดไม่เกิน ๓ ครั้ง

๑๒.๕ ห้ามผู้ใช้งานบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่มีการป้องกันการเข้าถึง

๑๒.๖ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานให้มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยต้องมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และต้องกำหนดให้ชื่อผู้ใช้งาน ประเภทนี้ต่างจากชื่อผู้ใช้งานปกติทั่วไป

ข้อ ๑๓ ผู้ดูแลระบบ ต้องบริหารจัดการและควบคุมการเข้าถึงข้อมูลตามประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านทางระบบงาน โดยมีรายละเอียดดังนี้

๑๓.๑ กำหนดระยะเวลาการใช้งานในแต่ละประเภทชั้นความลับและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๑๓.๒ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL,VPN หรือ XML Encryption เป็นต้น

๑๓.๓ กำหนดมาตรการรักษาความปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน ได้แก่ การบำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑๓.๔ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

ข้อ ๑๔ ระบบสารสนเทศในมหาวิทยาลัยที่มีการเชื่อมโยงกัน ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน โดยมีประเด็นที่สำคัญดังนี้

๑๔.๑ กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

๑๔.๒ พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงถ้าไม่จำเป็นสำหรับผู้ใช้งาน

๑๔.๓ พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งานในระบบร่วมกัน

๑๔.๔ ไม่อนุญาตให้มีการใช้การใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๕ การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานต้องปฏิบัติ ดังนี้

๑๕.๑ ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๑๕.๒ กำหนดรหัสผ่านประกอบด้วยตัวอักขระไม่น้อยกว่า ๖ ตัวอักขระ ซึ่งต้องประกอบด้วยตัวเลข (Number Character) ตัวอักษร (Alphabet) และตัวอักขระพิเศษ (Special Character)

๑๕.๓ ไม่กำหนดรหัสผ่านจากข้อมูลส่วนบุคคลที่สามารถคาดเดาได้ ได้แก่ นามสกุล บุคคลในครอบครัว

๑๕.๔ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๑๕.๕ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็น

๑๕.๖ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ทุก ๖ เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้ เปลี่ยนรหัสผ่าน

ข้อ ๑๖ การเข้ารหัสข้อมูล ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๑๗ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

ข้อ ๑๘ การกำหนดวิธีการป้องกันอุปกรณ์ประมวลผลสารสนเทศในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันการเข้าถึงอุปกรณ์ประมวลผลสารสนเทศโดยไม่ได้รับอนุญาต การป้องกันการขโมยอุปกรณ์ฯ ให้กำหนดแนวปฏิบัติเพื่อป้องกัน ดังนี้

๑๘.๑ กำหนดให้มีข้อปฏิบัติในการป้องกันอุปกรณ์คอมพิวเตอร์เพื่อป้องกันการลักขโมย หรือเข้าถึงโดยไม่ได้รับอนุญาต โดยมีการติดตั้งสายล็อกเพื่อการรักษาความปลอดภัยของอุปกรณ์คอมพิวเตอร์ที่ออกแบบเพื่อป้องอุปกรณ์คอมพิวเตอร์ รวมทั้งอาจมีการติดตั้งกล้องวงจรปิดเพื่อตรวจสอบการเข้า-ออกสถานที่ใช้งาน

๑๘.๒ อุปกรณ์และเครื่องคอมพิวเตอร์ขนาดเล็ก ได้แก่ คอมพิวเตอร์โน๊ตบุ๊ค ให้จัดเก็บในตู้ที่สามารถล็อกกุญแจได้

๑๘.๓ ให้ดำเนินการตั้งรหัสผ่าน เพื่อป้องกันการเปิดใช้งานอุปกรณ์ฯ ได้แก่

- การตั้งรหัสผ่าน เพื่อป้องกันการเข้าถึงไบออส (Bios) ของเครื่องคอมพิวเตอร์
- การตั้งรหัสผ่าน เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ
- การติดตั้งโปรแกรมเพื่อป้องกัน โปรแกรมประสงค์ร้าย (Malware) และอัพเดท (Update) ให้ทันสมัยอยู่เสมอ เพื่อป้องกันช่องโหว่ (Vulnerability) ของอุปกรณ์

๑๘.๔ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์ของหน่วยงาน ได้แก่ เข้าถึงระบบปฏิบัติการ การใช้งานระบบคอมพิวเตอร์ ในเครือข่าย และการใช้งานระบบอินเทอร์เน็ต (รวมจาก ๑๖.๑-๑๖.๓ เดิม)

๑๘.๕ เมื่อผู้ใช้งานไม่อยู่ประจำเครื่องคอมพิวเตอร์เป็นเวลา ๑๕ นาทีขึ้นไป ผู้ใช้งานต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนหลังกลับมาใช้งานใหม่

ข้อ ๑๙ ผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัยต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลของมหาวิทยาลัย

ข้อ ๒๐ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง ดูแลของหน่วยงานห้ามไม่ให้ผู้ใช้งานในหน่วยงานทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๑ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของมหาวิทยาลัยหากเกิดการสูญหาย การนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้น

ข้อ ๒๒ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๓ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร มหาวิทยาลัยจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่มหาวิทยาลัยแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๔ ห้ามเปิดหรือใช้งาน โปรแกรมประเภท Peer-to-Peers หรือโปรแกรมที่มีความเสี่ยงเหมือนกัน (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์ ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเสมอเหมือนกันหรือเท่าเทียมกัน โดยแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง ซึ่งการจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แต่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๕ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยโดยเด็ดขาด

ข้อ ๒๖ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๒๗ ห้ามใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๒๘ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นเพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๒๙ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๐ ห้ามผู้ใช้งานเข้าไปในห้องบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Operation Center) หรือสถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๑ ห้ามผู้ใช้งานนำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๒ ห้ามผู้ใช้งานนำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมเข้าระบบเครือข่ายคอมพิวเตอร์เพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๓ ห้ามผู้ใช้งานคัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์ ก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นทุกกรณี

ข้อ ๓๔ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายกระดาษ
Flash Drive	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น Optical	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
Hard Disk	- ใช้การทำลายข้อมูลบน Hard Disk ตามมาตรฐาน DOD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ส่วนที่ ๔ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ โดยกำหนดให้ผู้ใช้งานต้องมีข้อปฏิบัติในการใช้งานดังนี้

ข้อ ๓๕ กำหนดให้มีมาตรการป้องกันทรัพย์สินสารสนเทศของมหาวิทยาลัย โดยมีข้อปฏิบัติในการป้องกันการทรัพย์สินสารสนเทศ ดังนี้

๓๕.๑ ต้องควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญอยู่ในสถานการณ์ที่ไม่ปลอดภัย

๓๕.๒ ต้องกำหนดพื้นที่ใช้งานเพื่อป้องกันผู้ที่ไม่เกี่ยวข้องเข้าไปในพื้นที่

๓๕.๓ ต้องจัดการบริเวณล้อมรอบ

๓๕.๔ ต้องมีการควบคุมการเข้า-ออก พื้นที่

ข้อ ๓๖ กำหนดให้มีมาตรการป้องการการเข้าถึงข้อมูล เอกสาร สื่อบันทึกข้อมูลสารสนเทศโดยกำหนดข้อปฏิบัติในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ดังนี้

๓๖.๑ การหยุดใช้งานชั่วคราว ต้องกำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอและตั้งรหัสผ่านในการพักหน้าจอ เพื่อให้ผู้ใช้งานต้องพิมพ์รหัสผ่านเพื่อเปิดหน้าจอกลับมาใช้งานใหม่

๓๖.๒ ต้องทำการบันทึกออก (Logout) จากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๓๖.๓ สร้างวัฒนธรรมองค์กรให้เกิดความเข้าใจในมาตรการป้องกัน ได้แก่ การเก็บเอกสารสื่อบันทึกข้อมูลจากโต๊ะทำงาน และเก็บให้ปลอดภัย ก่อนพักหรือเลิกงาน

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๓๗ มาตรการควบคุมการเข้า-ออกห้องบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Operation Center)

๓๗.๑ ผู้ติดต่อจากหน่วยงานภายนอก ต้องทำการแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุด “บันทึกการเข้าออกพื้นที่”

๓๗.๒ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ใช้ห้องบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

๓๗.๓ ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาตเข้า-ออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๓๘ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ หรืออุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัดโดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอใช้บริการด้านระบบเครือข่ายคอมพิวเตอร์”

ข้อ ๓๙ การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมอื่นใด ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

ข้อ ๔๐ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการกับอุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์หลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๑ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ เพื่อบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๔๑.๑ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อการเชื่อมต่อของคอมพิวเตอร์และส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์การใช้งานตามภารกิจ ดังนี้

๔๑.๑.๑ อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

๔๑.๑.๒ มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๔๑.๑.๓ ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๔๑.๑.๔ ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

๔๑.๑.๕ ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๔๑.๑.๖ ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อระงับการใช้จากเส้นทางอื่น

๔๑.๑.๗ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔๑.๒ ระบบเครือข่ายคอมพิวเตอร์ ทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายคอมพิวเตอร์อื่น ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๔๑.๓ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานในลักษณะที่ผิดปกติ

๔๑.๔ การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการ ลงบันทึกเข้าใช้งาน (Login) เพื่อแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๔๑.๕ หน่วยงานต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายสามารถมองเห็น IP Address ภายในของหน่วยงานได้

๔๑.๖ หน่วยงานต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งอุปกรณ์ต่าง ๆ และต้องปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๔๑.๗ การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบต้องเก็บบัญชีการขอเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ที่อยู่ในความดูแลรับผิดชอบ อันได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

- ผู้ดูแลระบบต้องจำกัดจำนวนผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ในระบบเครือข่ายที่รับผิดชอบได้

- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากระบบเครือข่ายคอมพิวเตอร์ภายนอก ต้องมีการระบุหมายเลข (MAC Address : Media Access Control Address) อุปกรณ์ที่เข้ามาเชื่อมต่อกับเครือข่ายภายใน

- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางของระบบเครือข่ายคอมพิวเตอร์ได้

- ผู้ขอใช้บริการใหม่ ต้องกรอกแบบฟอร์มชื่อว่า “การขอใช้บริการระบบเครือข่าย”

ข้อ ๔๒ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงการตั้งค่า (Config) ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๔๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการทุกครั้ง

ข้อ ๔๔ กำหนดให้มีการจัดเก็บเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๔๕ กำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ (ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ ๒๕๕๐)

ข้อ ๔๖ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่ายจากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

๔๖.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากหัวหน้าหน่วยงาน

๔๖.๒ กำหนดให้มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศอย่างรัดกุม ดังต่อไปนี้

- การปรับเปลี่ยน หรือการเข้าถึงพอร์ตต้องทำหนังสือขออนุญาตจากผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย

- ต้องบันทึก และควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

- ปิดการใช้งาน หรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้โดยจำกัดระยะเวลาเท่าที่จำเป็นเท่านั้น

๔๖.๓ วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกล (Telnet) ต้องได้รับการอนุญาตจากผู้ดูแลระบบ

๔๖.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานและผู้ดูแลระบบก่อนเสมอ

๔๖.๕ การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลหรือผู้ที่อยู่ภายนอกองค์กร (External Connection) ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อ

ผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๔๗ กำหนดให้มีการแบ่งแยกเครือข่าย ตามกลุ่มดังต่อไปนี้

๔๗.๑ กลุ่มของบริการสารสนเทศ

๔๗.๒ กลุ่มของผู้ใช้งาน

๔๗.๓ กลุ่มของระบบสารสนเทศ

ข้อ ๔๘ กำหนดการป้องกันระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์อย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ ได้แก่ IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๔๙ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายคอมพิวเตอร์ต้องได้รับการอนุมัติจากผู้ดูแลระบบและต้องจำกัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๕๐ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

กำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนในการยืนยันตัวตนที่เหมาะสม มีแนวปฏิบัติ ดังนี้

๕๐.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับการเข้าใช้งานระบบสารสนเทศ

๕๐.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงานหรือด้านเทคนิค

๕๐.๓ สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม ได้แก่ สมาร์ตการ์ด RIFD เครื่องอ่านนิ้วมือ

ข้อ ๕๑ ขั้นตอนและแนวปฏิบัติเพื่อเข้าใช้งานระบบปฏิบัติการ

๕๑.๑ กำหนดให้มีการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัยโดยการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยจะทำการเก็บข้อมูลการจราจรคอมพิวเตอร์ (Log) ในกรณีนี้สำนักงานได้ใช้ระบบ Active Directory เป็นตัวควบคุม

๕๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๕๑.๓ การเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนทุกครั้ง

๕๑.๔ ผู้ใช้งานระบบปฏิบัติการของตนเองต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งานและรหัสผ่านของตนในการเข้าใช้งาน

๕๑.๕ ผู้ใช้งานระบบปฏิบัติการต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕๑.๖ ห้ามให้ผู้ใช้งานระบบปฏิบัติการเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง

๕๑.๗ ซอฟต์แวร์ระบบปฏิบัติการที่ทางมหาวิทยาลัยมีลิขสิทธิ์ใช้ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากตรวจพบถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๕๑.๘ ซอฟท์แวร์ระบบปฏิบัติการที่ทางมหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลงแก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๕๑.๙ ห้ามใช้ซอฟต์แวร์ระบบปฏิบัติการที่เป็นของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า

๕๑.๑๐ ห้ามผู้ใช้ระบบปฏิบัติการนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๕๑.๑๑ ห้ามผู้ใช้ระบบปฏิบัติการของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๕๑.๑๒ การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

๕๑.๑๒.๑ กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

๕๑.๑๒.๒ กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

ข้อ ๕๒ การใช้งานโปรแกรมอรรถประโยชน์ (Utilities Program) บนระบบปฏิบัติการต้องจำกัดและควบคุมการใช้งาน เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์ บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ และให้ดำเนินการ ดังนี้

๕๒.๑ การใช้งานโปรแกรมอรรถประโยชน์บนระบบปฏิบัติการ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๕๒.๒ โปรแกรมอรรถประโยชน์ที่นำมาใช้งานบนระบบปฏิบัติการต้องไม่ละเมิดลิขสิทธิ์

๕๒.๓ ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

๕๒.๔ กำหนดให้มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

๕๒.๕ ต้องยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control)

ข้อ ๕๓ ผู้ดูแลระบบโปรแกรมประยุกต์และสารสนเทศ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน ได้แก่ การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๕๔ ผู้ดูแลระบบโปรแกรมประยุกต์และสารสนเทศ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๕๕ ผู้ดูแลระบบโปรแกรมประยุกต์และสารสนเทศ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน ๑๕ นาที ระบบจะยุติการใช้งานผู้ใช้งานต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๕๖ ผู้ดูแลระบบโปรแกรมประยุกต์และสารสนเทศ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๕๖.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๕๖.๒ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๕๖.๓ การกำหนดรหัสผ่าน ต้องไม่ตรงกับชื่อผู้ใช้งาน

๕๖.๔ ในกรณีมีความจำเป็นต้องให้สิทธิ์กับผู้ใช้งานพิเศษที่มีสิทธิ์สูงสุด ผู้ใช้งานพิเศษนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๕๗ ผู้ดูแลระบบโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๕๗.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๕๗.๒ ต้องกำหนดรายชื่อผู้ใช้งาน และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

๕๗.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๕๗.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๕๗.๕ กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๕๗.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน ได้แก่ บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๕๘ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

๕๘.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายใน ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานปกติของมหาวิทยาลัยเท่านั้น

๕๘.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ข้อ ๕๙ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ได้แก่ ระบบงบประมาณ การเงิน พัสดุและบัญชีกองทุน โดยเกณฑ์พึงรับ-พึงจ่าย ลักษณะ ๓ มิติ ต้องแยกออกจากระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย ให้มีข้อปฏิบัติดังนี้

๕๙.๑ กำหนดมีการควบคุมสภาพแวดล้อมของระบบซึ่งไวต่อการรบกวนโดยเฉพาะ ดังนี้

๕๙.๑.๑ มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่มีหน้าที่ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

๕๙.๑.๒ ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น

๕๙.๑.๓ ทำการป้องกันการมีทรัพยากรไม่เพียงพอ

๕๙.๑.๔ มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

๕๙.๒ กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ โดยมีแนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัวและอุปกรณ์ของทางราชการ ดังนี้

๕๙.๒.๑ ต้องล็อกหรือยึดเครื่องให้อยู่กับที่กรณีที่นำเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๕๙.๒.๒ ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

๕๙.๒.๓ ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา

๕๙.๒.๔ ไม่ใช้อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับบุคคลอื่น

๕๙.๒.๕ ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ

๕๙.๒.๖ ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องเข้ารหัสข้อมูล ทุกครั้ง

๕๙.๒.๗ ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพา เป็นอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายภายในมหาวิทยาลัย

๕๙.๒.๘ ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพา ได้แก่ ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

๕๙.๒.๙ มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์พกพาเกิดการสูญหายหรือถูกขโมย ได้แก่ การเปิดระบบล็อกไบออส เข้ารหัสไฟล์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรมติดตามเครื่อง ฯลฯ

๕๙.๓ กำหนดให้มีการปฏิบัติงานจากภายนอกองค์กร (Teleworking) ดังนี้

๕๙.๓.๑ ผู้ใช้งานงานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๕๙.๓.๒ ต้องรักษาความปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร

๕๙.๓.๓ มีมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

๕๙.๓..๔ ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว

๕๙.๓.๕. ต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศขององค์กรจากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟร์วอลล์อย่างเหมาะสม

๕๙.๓.๖. ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

ข้อ ๖๐ ผู้รับจ้างพัฒนาระบบต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร

ข้อ ๖๑ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้รับจ้างพัฒนาระบบจากภายนอกให้มีสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำเข้าและออกจากระบบสารสนเทศของผู้รับจ้างพัฒนาระบบจากภายนอกทุกครั้ง

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์ลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and Intellectual Property and Preventing Malware)

ข้อ ๖๒ มหาวิทยาลัยราชภัฏเชียงใหม่ ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๖๓ ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งาน ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๖๔ คอมพิวเตอร์ของผู้ใช้งานต้องทำการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่หน่วยงานได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๖๕ ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นหรือหน่วยงานอื่น ต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๖๖ ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบ และปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๖๗ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลารวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๖๘ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๖๙ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสารหรือสิ่งใด ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้างาน

ข้อ ๗๐ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน

ข้อ ๗๑ สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้แต่ต้องไม่ดำเนินการ ดังนี้

๗๑.๑ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

๗๑.๒ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๗๑.๓ พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๗๑.๔ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

๗๑.๕ นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทยกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๗๒ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

๗๒.๑ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๗๒.๒ พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๗๒.๓ พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๗๒.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๗๒.๕ หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๗๓ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ ๗๔ ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ ได้แก่ รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๗๕ ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๗๖ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล โดยให้มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

ข้อ ๗๗ ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูลระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๗๘ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Network Access Control)

ข้อ ๗๙ ผู้ดูแลระบบเครือข่ายไร้สาย ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๘๐ ผู้ดูแลระบบเครือข่ายไร้สาย ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งานและกำหนดให้ซ่อน SSID

ข้อ ๘๑ ผู้ดูแลระบบเครือข่ายไร้สาย ต้องกำหนดค่าโดยต้องทำการกำหนดค่าและติดต่อกับทางหน่วยงานเทคโนโลยีสารสนเทศส่วนกลางเพื่อกำหนดค่าต่าง ๆ ของระบบ Wireless Security ของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

ข้อ ๘๒ ผู้ดูแลระบบเครือข่ายไร้สาย ระดับหน่วยงานที่ต้องการติดตั้งอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) จะต้องได้รับการพิจารณาอนุญาตจากมหาวิทยาลัย

ข้อ ๘๓ ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC address (Media Access Control Address) และชื่อผู้ใช้งาน รหัสผ่าน ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน และรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๘๔ ผู้ดูแลระบบเครือข่ายไร้สาย ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๘๕ ผู้ดูแลระบบเครือข่ายไร้สาย ต้องกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๘๖ ผู้ดูแลระบบเครือข่ายไร้สาย ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สายที่รับผิดชอบ

ข้อ ๘๗ ผู้ดูแลระบบเครือข่ายไร้สาย ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน หากพบกรณีที่ ความผิดปรกติในการใช้งานระบบเครือข่ายไร้สาย ผู้ดูแลระบบรายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ ๘๘ ผู้ดูแลระบบ ต้องควบคุมไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

ข้อ ๘๙ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัย จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ ๙๐ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๙๑ มหาวิทยาลัยต้องมีหน่วยงานบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๙๒ การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๙๓ Firewall จะต้องอนุญาตการเชื่อมต่ออินเทอร์เน็ตตามข้อกำหนดของมหาวิทยาลัยเท่านั้น

ข้อ ๙๔ การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๙๕ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๙๖ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อ ๙๗ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

ข้อ ๙๘ จะต้องมีการสำรองข้อมูลการกำหนดค่าของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๙๙ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๐๐ หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๐๑ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อน

ข้อ ๑๐๒ ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-Mail)

ข้อ ๑๐๓ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ โดยยื่นคำขอกับเจ้าหน้าที่ที่รับผิดชอบหรือดูแลระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๐๔ การใส่รหัสผ่านจดหมายอิเล็กทรอนิกส์ ต้องไม่แสดงรหัสผ่านออกมาขณะทำการใส่รหัส

ข้อ ๑๐๕ เมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน ที่ได้มาจากผู้ดูแลระบบโดยทันที

ข้อ ๑๐๖ ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ ต้องสามารถกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้

ข้อ ๑๐๗ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๐๘ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องทำการเปลี่ยนรหัสผ่าน ของตนเอง ทุก ๓ - ๖ เดือน

ข้อ ๑๐๙ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องไม่ใช้จดหมายอิเล็กทรอนิกส์ ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายนั้น เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

ข้อ ๑๑๐ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องลงบันทึกออก (Logout) จากระบบจดหมายอิเล็กทรอนิกส์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

ข้อ ๑๑๑ การส่งข้อมูลที่เป็นความลับผ่านจดหมายอิเล็กทรอนิกส์ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลจดหมายอิเล็กทรอนิกส์ ที่หน่วยงานกำหนดไว้ และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๑๒ ห้ามส่งจดหมายอิเล็กทรอนิกส์ ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) จดหมายลูกโซ่ (Chain Letter) การละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น และจดหมายอิเล็กทรอนิกส์ ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๑๓ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ ทุกฉบับที่ส่งไป

ข้อ ๑๑๔ ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ ตามความจำเป็นอย่างสม่ำเสมอ และตรวจสอบได้

ข้อ ๑๑๕ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องทำการตรวจสอบเอกสารแนบจากจดหมายกดอิเล็กทรอนิกส์ด้วยโปรแกรมป้องกันไวรัส ก่อนการเปิดทุกครั้ง

ข้อ ๑๑๖ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๑๗ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม อันอาจทำให้เสียชื่อเสียงของหน่วยงาน หรือทำให้เกิดความแตกแยกระหว่างหน่วยงาน

ข้อ ๑๑๘ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องตรวจสอบพื้นที่จัดเก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๑๙ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่องการพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ข้อ ๑๒๐ ผู้ดูแลระบบอินเทอร์เน็ต ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ของมหาวิทยาลัยกับระบบอินเทอร์เน็ตโดยต้องผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น (Proxy, Firewall, IPS-IDS)

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๑๒๑ ห้ามผู้ใช้งานระบบอินเทอร์เน็ตของมหาวิทยาลัยทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นได้รับอนุญาตจากมหาวิทยาลัยเป็นลายลักษณ์อักษร

ข้อ ๑๒๒ คอมพิวเตอร์ส่วนบุคคลที่เชื่อมต่อกับจดหมายอิเล็กทรอนิกส์ ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ โดยการอัพเดท (Update) ระบบปฏิบัติการอย่างสม่ำเสมอ

ข้อ ๑๒๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัสโดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๒๔ ไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัย เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

ข้อ ๑๒๕ การเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๑๒๖ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

ข้อ ๑๒๗ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๒๘ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๑๒๙ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงานการทำลายความสัมพันธ์กับบุคลากรของหน่วยงาน

ข้อ ๑๓๐ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดการเชื่อมต่อหรือออกจากระบบอินเทอร์เน็ตเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ข้อ ๑๓๑ ผู้ใช้งานระบบอินเทอร์เน็ต ต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัย (PC Computer)

ข้อ ๑๓๒ แนวทางปฏิบัติการใช้งานทั่วไป

๑๓๒.๑ เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

๑๓๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรม และนำไปใช้เป็นการส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๓๒.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ ส่วนบุคคลของหน่วยงาน

๑๓๒.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคล เพื่อตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่บำรุงรักษาเครื่องคอมพิวเตอร์ของหน่วยงาน หรือบริษัทผู้จ้างเหมาที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

๑๓๒.๕ ก่อนการใช้งานสื่อบันทึกพกพา ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการเชื่อมต่อกับเครื่องคอมพิวเตอร์

๑๓๒.๖ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๑๓๒.๗ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อไม่ใช้งานเกินกว่า ๑ ชั่วโมง

๑๓๒.๘ ทำการตั้งค่าล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

ข้อ ๑๓๓ การสำรองข้อมูลและการกู้คืนเครื่องคอมพิวเตอร์ส่วนบุคคล

๑๓๓.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD, DVD, External Hard Disk

๑๓๓.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง(Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๓๓.๓ ผู้ใช้งานต้องสำรองข้อมูลปฏิบัติงานไว้ ในระดับที่สามารถนำกลับมาใช้งานได้ตามปกติ ไม่กระทบต่อการดำเนินของหน่วยงานในกรณี Hard Disk เสีย

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Portable Computer)

ข้อ ๑๓๔ แนวทางปฏิบัติการใช้งานทั่วไป

๑๓๔.๑ เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

๑๓๔.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรม และนำไปใช้เป็นการส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๓๔.๓ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๑๓๔.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์แบบพกพาและรักษาสภาพของคอมพิวเตอร์แบบพกพาให้มีสภาพเป็นปกติ

ข้อ ๑๓๕ ความปลอดภัยทางด้านกายภาพ

๑๓๕.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยต้องล๊อคเครื่องคอมพิวเตอร์แบบพกพาขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๓๕.๒ ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อนสูง ความชื้นมาก ฝุ่นละอองสูงและต้องระวังป้องกันการตกจากตำแหน่งที่วาง

ข้อ ๑๓๖ การสำรองข้อมูลและการกู้คืนเครื่องคอมพิวเตอร์แบบพกพา

๑๓๖.๑ ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

๑๓๖.๒ ผู้ใช้งานจะต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลและการสูญเสียของข้อมูล

๑๓๖.๓ แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

๑๓๖.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายหรือลบข้อมูลไม่ให้สามารถนำไปใช้งานได้อีก

๑๓๖.๕ ผู้ใช้งานต้องสำรองข้อมูลปฏิบัติงานไว้ในระดับที่สามารถนำกลับมาใช้งานได้ตามปกติ ไม่กระทบต่อการดำเนินของหน่วยงานในกรณี Hard Disk เสีย

ส่วนที่ ๑๖ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

ข้อ ๑๓๗ให้มีแนวนโยบายการตรวจสอบการบุกรุก (IDS/IPS Policy) เพื่อตรวจสอบความปลอดภัยของเครือข่าย ป้องกันทรัพยากรระบบสารสนเทศ รวมถึงข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคง

ปลอดภัย และทำแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้อง

ข้อ ๑๓๘ กำหนดให้แนวนโยบาย IDS/IPS ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๑๓๙ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๑๔๐ ระบบทั้งหมดใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๑๔๑ โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๑๔๒ ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ ๑๔๓ ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๑๔๔ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศของมหาวิทยาลัย

ข้อ ๑๔๕ เครื่องแม่ข่ายที่มีการติดตั้ง Host-Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวันโดยผู้ดูแลระบบ

ข้อ ๑๔๖ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุกการโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบหรือภายในเวลาอันสั้น

ข้อ ๑๔๗ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๔๘ ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๔๙ มหาวิทยาลัยมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ของหน่วยงานที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๕๐ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของมหาวิทยาลัย การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๗ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๕๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ ๑๕๒ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ ที่เก็บรักษาไว้

ข้อ ๑๕๓ กำหนดให้มีการบันทึกการทำงานผู้ใช้งานและบันทึกรายละเอียดของการเข้า – ออกระบบ เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๕๔ ต้องมีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้น

หมวดที่ ๒
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบข้อมูลและสำรองข้อมูลของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลและสำรองข้อมูล

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

๑.๑ จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

๑.๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องกับฐานข้อมูล

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ์การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบฐานข้อมูลของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๑.๓.๑ ประเภทของข้อมูล แบ่งออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

- ข้อมูลสารสนเทศด้านการบริการของมหาวิทยาลัย ได้แก่ ข้อมูลการลงทะเบียนเรียน ข้อมูลผลการเรียน ข้อมูลนักศึกษา ข้อมูลบริการชุมชน เป็นต้น

๑.๓.๒ ระดับความสำคัญของข้อมูลในฐานข้อมูล แบ่งออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๑.๓.๓ ลำดับชั้นความลับของข้อมูลในฐานข้อมูล แบ่งออกเป็น

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๓.๔ ระดับชั้นการเข้าถึงข้อมูลในฐานข้อมูล แบ่งออกเป็น ๓ ระดับ คือ

- ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลในฐานข้อมูลได้ตามภารกิจที่มหาวิทยาลัยมอบหมาย
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงข้อมูลในฐานข้อมูลได้เฉพาะข้อมูลส่วนบุคคล และข้อมูลข่าวสารประชาสัมพันธ์ที่ออกสู่สาธารณะ
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย สามารถเข้าถึงข้อมูลในฐานข้อมูลได้ตามหน้าที่ในการดูแลระบบที่มหาวิทยาลัยมอบหมาย

๑.๓.๕ มีการกำหนดเวลาที่ได้เข้าถึงข้อมูลในฐานข้อมูล

- ข้อมูลที่เปิดเผย ๒๔ ชั่วโมง
- ข้อมูลที่เปิดเผยเฉพาะเวลาทำการ
- ข้อมูลที่เปิดเผยเมื่อมีการมอบหมายตามภารกิจ

๑.๓.๖ มีการกำหนดจำนวนช่องทางที่สามารถเข้าถึงฐานข้อมูล ๒ ช่องทางดังนี้

- ระบบเครือข่ายภายในมหาวิทยาลัย (Intranet)
- ระบบเครือข่ายภายนอกมหาวิทยาลัย (Internet)

ข้อ ๒ ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓ การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๓

ข้อ ๔ หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

๕.๑ กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๕.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูล ได้แก่ วิธีการส่ง การรับ เป็นต้น

๕.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๕.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

๕.๕ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

๕.๖ กำหนดสิทธิ์การเข้าถึงข้อมูล

๕.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๕.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ ได้แก่ กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖ พิจารณาคัดเลือกระบบข้อมูลหรือฐานข้อมูลที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ ๗ กำหนดหน้าที่ของเจ้าหน้าที่ในการสำรองข้อมูล ดังนี้

๗.๑ มีการตรวจสอบความถูกต้องของข้อมูลก่อนที่จะทำการสำรองข้อมูลก่อนเสมอ

๗.๒ มีการวางวางแผนรูปแบบของการสำรองข้อมูลอย่างชัดเจน ได้แก่ สำรองกี่ครั้งต่อวัน หรือกี่ครั้งต่อสัปดาห์ และระยะเวลาในการสำรองแต่ละครั้ง

๗.๓ มีการเก็บข้อมูลที่สำรองอย่างปลอดภัย เป็นความลับ

๗.๔ ในกรณีข้อมูลหลักเกิดความเสียหาย ข้อมูลที่สำรองไว้ต้องสามารถกู้คืนได้ในเวลาอันรวดเร็ว และเป็นปัจจุบันมากที่สุด

๗.๕ มีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

ข้อ ๘ มีการจัดทำบัญชีระบบฐานข้อมูลที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ กำหนดให้มีการสำรองฐานข้อมูลหรือข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๙.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๙.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

๙.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๙.๔ ตรวจสอบการตั้งค่า คอนฟิกูเรชัน (Configuration) ต่าง ๆ ของระบบการสำรองข้อมูล

๙.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๙.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

๙.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๙.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๙.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๙.๑๐ ระยะความถี่ของการปฏิบัติ การสำรองข้อมูลโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น ดังนี้

- ความถี่ในการสำรองข้อมูลของระบบสารสนเทศ ขึ้นอยู่กับความสำคัญของระบบสารสนเทศ และสภาพการเปลี่ยนแปลงข้อมูล โดยระบบที่มีความสำคัญมาก หรือมีการเปลี่ยนแปลงข้อมูลบ่อยต้องมีความถี่ในการสำรองข้อมูลมากขึ้น
- ทำการทดสอบการกู้คือข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง
- มีการทบทวนและปรับปรุงการบริหารจัดการความเสี่ยงด้านสารสนเทศ แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ และแผนบริหารความต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง

๙.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๑๐ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

๑๐.๑ มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๑๐.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหวการชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๑๐.๓ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๑๐.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๑๐.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๑๐.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ ๑๑ ต้องมีการทดสอบ ทบทวนสภาพพร้อมใช้งานของระบบฐานข้อมูล ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

หมวดที่ ๓
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ ๑ จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ ๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๖.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๖.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๖.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๖.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๖.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๕ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) ได้แก่ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงันหรือหยุดทำงาน และส่งผลให้ ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ดังนี้

๑.๑ จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

๑.๒ จัดทำหนังสือแจ้งเวียนทุกหน่วยงานของมหาวิทยาลัย เรื่องการใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจากซอฟต์แวร์ ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Virus) หนอนอินเตอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

๒.๑ ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

๒.๒ ติดตั้งซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๓.๑. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

๓.๒. ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

๓.๓. ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๔.๑ เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

๔.๒ เก็บอุปกรณ์ Backup ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

๔.๓ ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้าลัดวงจร

๔.๔ เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

๔.๕ กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุม เครือข่ายว่า สามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์ แม่ข่ายและอุปกรณ์เครือข่าย

๔.๖ ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

๔.๗ เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

ประเภทที่ ๕ ภัยจากแผ่นดินไหว จัดเป็นภัยพิบัติสร้างความเสียหายให้แก่ระบบสารสนเทศอีกประเภทหนึ่งที่เกิดขึ้นในสภาวะปัจจุบัน จึงต้องกำหนดแนวปฏิบัติ ดังนี้

๕.๑ เฝ้าระวังภัยจากแผ่นดินไหว โดยติดตามข่าวสารจากกรมอุตุนิยมวิทยาหรือหน่วยงานเฝ้าระวังที่เกี่ยวข้องตลอดเวลา

๕.๒ เก็บอุปกรณ์ Backup ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

๕.๓ ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้าลัดวงจร

๕.๔ เคลื่อนย้ายอุปกรณ์ที่อยู่ในระดับสูงมายังพื้น เพื่อป้องกันการตกกระทบ

๕.๕ ในกรณีอุปกรณ์ใดไม่สามารถเคลื่อนย้ายได้ให้จัดทำระบบป้องกันการสั่นสะเทือน

๕.๖ จัดทำแผนจำลองสถานการณ์แผ่นดินไหว ประจำทุก ๆ ปี

หมวดที่ ๔
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อ ๑ อาคาร สถานที่และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒ ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

๒.๑ไ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

๒.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๒.๔ จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

๒.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

๒.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

๒.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔ การควบคุมการเข้าออก อาคารสถานที่

๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๔.๒ การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ ได้แก่ บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๔.๓ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔.๔ ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๔.๕บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๔.๖ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ ได้แก่ Data Center เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๔.๗ ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๔.๘ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๙ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๔.๑๐ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๔.๑๑ มีการพิสูจน์ตัวตน ได้แก่ การแสกนลายนิ้วมือ การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ ได้แก่ Data Center

๔.๑๒ จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้น อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๖.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๖.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๖.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๖.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๖.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๖.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๖.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๗.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๗.๖ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๘.๑ ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๘.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๘.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๘.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน ได้แก่ การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๙.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment)

๑๐.๑ ให้ลบข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕
การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัย ทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑ ระบบป้องกันผู้บุกรุก

๑.๑ ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมี ดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีแอดเดรสของเครือข่ายที่เป็นผู้โจมตี
- ผู้โจมตีใช้รูปแบบอะไรในการโจมตี

ข้อ ๒ ระบบไฟร์วอลล์

๒.๑ ดำเนินการตรวจสอบระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒.๒ ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- ตรวจสอบ Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ตรวจสอบ ลักษณะของ Packet ที่ถูก Block
- ตรวจสอบ Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๒.๓ กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓ ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์

๓.๑ ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- ตรวจสอบมัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- ตรวจสอบมัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- ตรวจสอบมีการส่งมัลแวร์จากเครือข่ายภายในมหาวิทยาลัยไปยังภายนอกหรือไม่

๓.๒ ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของมหาวิทยาลัย

๓.๓ ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

หมวดที่ ๖
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของมหาวิทยาลัย

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑ จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๓ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๔ ประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการแนะนำเกร็ดความรู้ใหม่ ๆ อยู่เสมอ

ข้อ ๕ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖ สร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ ๗ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน ได้แก่ การจัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์มหาวิทยาลัย

ข้อ ๘ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมาย ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของมหาวิทยาลัย ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตาม ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๗
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ ผู้บริหารระดับสูงสุด ผู้รับผิดชอบ ได้แก่ อธิการบดีมหาวิทยาลัยราชภัฏเชียงใหม่

๑.๑ รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ ในระดับมหาวิทยาลัย

๑.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในระดับมหาวิทยาลัย

ข้อ ๒ ผู้บริหารระดับสูง ผู้รับผิดชอบ ได้แก่ รองอธิการบดีที่ได้รับมอบหมายให้กำกับดูแลด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๒.๑ รับผิดชอบในการกำหนดนโยบาย กำกับดูแลด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย ให้ข้อเสนอแนะ ในระดับมหาวิทยาลัย

๒.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในระดับมหาวิทยาลัย

ข้อ ๓ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา

๑.๑ ดำเนินการตามนโยบาย กำกับ ดูแล และรับผิดชอบด้านสารสนเทศของมหาวิทยาลัย

๑.๒ รับผิดชอบในการวางแผนกลยุทธ์ แผนปฏิบัติการ งบประมาณ ความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนในการนำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในระดับมหาวิทยาลัยไปปฏิบัติ โดยให้รายงานผลการดำเนินงานทั้งหมดต่อ ผู้บริหารระดับสูงสุด

ข้อ ๔ ผู้บริหารระดับหน่วยงาน ผู้รับผิดชอบ ได้แก่ คณบดี ผู้อำนวยการศูนย์ / สำนัก รองคณบดี รองผู้อำนวยการ ผู้อำนวยการกอง หัวหน้าสำนักงาน

๒.๑ รับผิดชอบ ในการปฏิบัติตามนโยบายของมหาวิทยาลัยที่กำหนดขึ้น กำกับดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ปฏิบัติการ ระดับหน่วยงาน

๒.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศระดับหน่วยงาน

ข้อ ๕ ผู้บริหารระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่ หัวหน้างาน

๓.๑ รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๓.๒ รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๖ ระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการของมหาวิทยาลัย ได้แก่ นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่คอมพิวเตอร์

๔.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๔.๓ รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๔.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๔.๖ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

ภาคผนวก

การจัดทำประกาศ
แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑ การจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกาศนี้มี ๒ ส่วน ดังนี้

๑.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๒.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๒.๑.๑ ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการจัดทำนโยบาย

๒.๑.๒ กำหนดให้จัดทำนโยบายเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย

๒.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๒.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๒.๒.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒.๒.๒ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

๒.๒.๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒.๒.๔ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ข้อ ๓ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อยดังนี้

๓.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๓.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๓.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๔ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อยดังนี้

๔.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือ รู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๔.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๔.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม

๔.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๔.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๕ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

๕.๑ การใช้งานรหัสผ่าน กำหนดแนวปฏิบัติสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน

๕.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๕.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๕.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๖ มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๖.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๖.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connection) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๖.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๖.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๖.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๖.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง มีข้อปฏิบัติดังนี้

๖.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๗ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operation System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๗.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๗.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๗.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๗.๔ การใช้งานโปรแกรมอรรถประโยชน์ ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่งคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๗.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

๗.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๘ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

๘.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Function) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๘.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

๘.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๘.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๙ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

๙.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๙.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องโดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๙.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๙.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๙.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๐ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๑๐.๑ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๐.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๑ ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

แนวปฏิบัติ เมื่อเกิดฟิชชิ่ง (Phishing) ที่เว็บเซอร์เวอร์ของหน่วยงาน

วัตถุประสงค์

เพื่อกำหนดมาตรการในการแก้ไขปัญหาการเกิดฟิชชิ่ง (Phishing) ให้สามารถดำเนินการได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหาย และส่งผลกระทบต่อหน่วยงานทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ เมื่อผู้ดูแลระบบเครือข่ายของมหาวิทยาลัยได้รับแจ้งหรือตรวจพบว่าเว็บเซอร์เวอร์ของหน่วยงานใด ๆ เป็นช่องทางให้ผู้ไม่หวังดีทำฟิชชิ่ง (Phishing) ผู้ดูแลระบบของมหาวิทยาลัยจะดำเนินการ ดังนี้

๑.๑ ดำเนินการปิดกั้น (Block IP) ของเว็บเซอร์เวอร์ที่โดนฟิชชิ่งนั้น หรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานดำเนินการโดยเร่งด่วน

๑.๒ แจ้งผู้ดูแลเว็บเซอร์เวอร์ (Web Server) ของหน่วยงานที่ถูกทำฟิชชิ่งทันที เพื่อดำเนินการแก้ไขปัญหา

ข้อ ๒ เมื่อหน่วยงานดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ให้ประสานไปยังผู้ดูแลระบบเครือข่ายของมหาวิทยาลัยหรือผู้ให้บริการเส้นทางเครือข่ายของหน่วยงาน เพื่อปลดล็อก IP Address

ข้อ ๓ ผู้ดูแลเว็บเซอร์เวอร์ของหน่วยงานต้องตรวจสอบเว็บเซอร์เวอร์และเว็บไซต์ภายในหน่วยงานของตนเอง รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (Patch) อย่างสม่ำเสมอเพื่อป้องกันผู้ที่ไม่หวังดี ในการเข้ามาทำ ฟิชชิ่ง

หมายเหตุ : ทางผู้เสียหายส่วนใหญ่ เป็นหน่วยงานที่มีการทำธุรกรรมอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการเงิน ๆ ได้แก่ ธนาคาร เว็บไซต์ที่เกี่ยวกับการซื้อขายออนไลน์ ฯลฯ หากดำเนินการแก้ไขปัญหาดังกล่าวล่าช้าและมีความเสียหาย อาจมีผลทางกฎหมายต่อหน่วยงานของท่าน

แบบขออนุมัติโครงการและแผนปฏิบัติการ
ประเภท โครงการ ( ) ภารกิจประจำ (✓) ภารกิจสนับสนุนยุทธศาสตร์
หน่วยงาน สำนักดิจิทัลเพื่อการศึกษา
ประจำปีงบประมาณ พ.ศ. 2559

1. **โครงการ** อบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ
2. **ผู้รับผิดชอบโครงการ** สำนักดิจิทัลเพื่อการศึกษา
3. **ความสอดคล้องกับ**
   3.1 **ยุทธศาสตร์การจัดสรรงบประมาณรายจ่ายประจำปีของมหาวิทยาลัยราชภัฏเชียงใหม่**
   ยุทธศาสตร์ที่ 3 พัฒนางานวิจัยและการบริการวิชาการเพื่อนำไปใช้ประโยชน์ในการเรียนการสอนและการพัฒนาท้องถิ่น
   เป้าประสงค์ที่ 1 มหาวิทยาลัยมีงานวิจัยและการให้บริการวิชาการที่ใช้ประโยชน์ในการเรียนการสอนได้ การแก้ปัญหาและพัฒนาคุณภาพชีวิตของชุมชนท้องถิ่น
   เป้าประสงค์ที่ 2 สังคมและชุมชนท้องถิ่นมีความเข้มแข็งและมีคุณภาพชีวิตที่ดีจากผลการวิจัยและการให้บริการวิชาการของมหาวิทยาลัย
   3.2 **แผนพัฒนาของหน่วยงาน**
   ยุทธศาสตร์ที่ 2 พัฒนาศักยภาพด้านเทคโนโลยีสารสนเทศและการสื่อสารภายใน และภายนอกมหาวิทยาลัย
   เป้าประสงค์ที่ 1 นักศึกษา บุคลากร และชุมชนมีสมรรถนะและขีดความสามารถในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามความเหมาะสมของแต่ละกลุ่ม
   3.3 **การประกันคุณภาพการศึกษาของ สกอ. องค์ประกอบที่**.....**ตัวบ่งชี้ที่**.....
   การประกันคุณภาพการศึกษาของ สมศ. มาตรฐานที่.....**ตัวบ่งชี้ที่**.....
   3.4 **กรณีเป็นโครงการที่ดำเนินการตามอัตลักษณ์ เอกลักษณ์ของมหาวิทยาลัย**
   ☐ **อัตลักษณ์** “บัณฑิตมีทักษะชีวิต จิตสาธารณะ และสู้งาน”
   ☐ **เอกลักษณ์** “สถาบันอุดมศึกษาเพื่อการพัฒนาท้องถิ่น”
   3.5 **กรณีเป็นโครงการที่ดำเนินการตามคุณลักษณะบัณฑิตที่พึงประสงค์ของมหาวิทยาลัย (5ดี)**
   .....
4. **หลักการและเหตุผล**

การสร้างความรู้ความเข้าใจเกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้กับนักศึกษา อาจารย์และบุคลากร เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์

สำนักดิจิทัลเพื่อการศึกษา ซึ่งรับผิดชอบในการเป็นศูนย์กลางการเรียนรู้ด้านเทคโนโลยีสารสนเทศ จึงสานต่อนโยบายของมหาวิทยาลัยในการสร้างความรู้ความเข้าใจเกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้นักศึกษา อาจารย์ บุคลากร ได้นำเอาความรู้เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไปใช้ในการปฏิบัติงานและใช้ในชีวิตประจำวัน

5. วัตถุประสงค์

5.1 เพื่อดำเนินการจัดฝึกอบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศให้แก่นักศึกษา อาจารย์ และบุคลากร

6. กลุ่มเป้าหมาย

นักศึกษา อาจารย์ และบุคลากร มหาวิทยาลัยราชภัฏเชียงใหม่

7. ตัวชี้วัดความสำเร็จของโครงการ

ตัวชี้วัดความสำเร็จของโครงการ	ค่าเป้าหมาย
เชิงปริมาณ :	
1. จำนวนหลักสูตรอบรม การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ 2. จำนวนรุ่น 3. จำนวนผู้เข้าร่วมอบรม	จำนวน 1 หลักสูตร จำนวน 2 รุ่น จำนวน 50 คน/ หลักสูตร /รุ่น (100 คน)
เชิงคุณภาพ :	
1. ผู้เข้ารับการอบรมได้รับความพึงพอใจ 2. ผู้เข้ารับการอบรมได้ความรู้ความเข้าใจและสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ	ร้อยละ 80 ร้อยละ 80
เชิงเวลา :	
โครงการ/กิจกรรมแล้วเสร็จตามระยะเวลาที่กำหนด	สิงหาคม 2559
เชิงต้นทุน :	
- ค่าใช้จ่ายของโครงการเป็นไปตามที่ได้รับอนุมัติ	จำนวน 5,000 บาท

8. สถานที่ดำเนินงาน

สำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่

9. กิจกรรมและแผนการดำเนินกิจกรรม

กิจกรรม	กลุ่มเป้าหมายและจำนวน	แผนการดำเนินงาน
1.วางแผนการดำเนินงาน (Plan) 1) ประชุมปรึกษาหารือ 2) แต่งตั้งคณะกรรมการ	คณะกรรมการ 1 ชุด	ต.ค. 2558
2.ดำเนินการ (Do) 1) อบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ	นักศึกษา อาจารย์ และบุคลากร จำนวน 100 คน	พ.ย.2558 – ก.ค.2559
3. สรุปและประเมินผล (Check) 1) สรุปและประเมินผลการดำเนินงาน	รายงาน 1 เล่ม	ส.ค. 2559
4. นำผลการประเมินไปปรับปรุง (Act) 1) นำผลการดำเนินงานไปปรับปรุง	1 ครั้ง	ส.ค. 2559

10. งบประมาณรวมของโครงการ 5,000 บาท

10.1 งบประมาณแผ่นดิน ..... บาท

10.2 งบประมาณเงินรายได้ ..... บาท

11. กิจกรรมและรายละเอียดงบประมาณ

แหล่งงบประมาณ	ประเภทงบรายจ่าย	จำนวนเงิน	รายละเอียดค่าใช้จ่าย
	งบดำเนินงาน	5,000	<u>กิจกรรมที่ 1</u> อบรม 1 หลักสูตร จำนวน 2 รุ่น เป็นเงิน 5,000 บาท ดังนี้ 1) ค่าเอกสารพร้อมเข้าเล่ม 1 หลักสูตร จำนวน 2 รุ่น (100 x 50 บาท) เป็นเงิน 5,000 บาท

12. ผลการดำเนินงานที่คาดว่าจะได้รับ

12.1 ผลผลิต (Output)

1) นักศึกษา อาจารย์ และบุคลากร ได้เข้าร่วมอบรมการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

12.2 ผลลัพธ์ (Outcome)

1) นักศึกษา อาจารย์ และบุคลากร ได้รับความรู้ความเข้าใจและความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

12.3 ผลกระทบ (Impact)

1) นักศึกษา อาจารย์ และบุคลากร มีความรู้และตระหนักถึงการใช้งานระบบสารสนเทศอย่างระมัดระวัง
2) อาจารย์ และบุคลากร สามารถนำความรู้ เกี่ยวกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไปใช้ในการปฏิบัติงานและนำไปใช้ในชีวิตประจำวันได้

13. วิธีการติดตามและประเมินผล

13.1 ตามตัวชี้วัดความสำเร็จโครงการ

13.2 รูปเล่มรายงานสรุปโครงการ

แผนเตรียมความพร้อมกรณีฉุกเฉิน

ด้านเทคโนโลยีสารสนเทศ

สำนักดิจิทัลเพื่อการศึกษา มหาวิทยาลัยราชภัฏเชียงใหม่

****

1. หลักการและเหตุ

ในปัจจุบันรัฐบาลได้ประกาศใช้ พ.ร.บ.ความมั่นคงภายในราชอาณาจักร พ.ศ.๒๕๕๑ และให้หน่วยงานราชการจัดเตรียมความพร้อมรองรับสถานการณ์ในกรณีเกิดเหตุฉุกเฉินไม่สามารถปฏิบัติงานได้

การเตรียมความพร้อมเพื่อรองรับสถานการณ์ฉุกเฉิน เช่น ระบบไฟฟ้า สามารถเกิดเหตุขัดข้องหรือเกิดสถานการณ์ที่ไม่คาดฝันขึ้น เช่น อัคคีภัยและแผ่นดินไหว ได้เสมอ ซึ่งเมื่อเกิดเหตุขึ้นจะส่งผลกระทบต่อระบบสารสนเทศหลักของมหาวิทยาลัยราชภัฏเชียงใหม่ สำนักดิจิทัลเพื่อการศึกษา ซึ่งมีหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่างๆ และเป็นแหล่งเก็บฐานข้อมูลสำคัญของมหาวิทยาลัยราชภัฏเชียงใหม่ จึงมีความจำเป็นอย่างยิ่งที่ต้องมีการวางแผนการเตรียมพร้อมกรณีฉุกเฉิน เพื่อให้การทำงานไม่เกิดข้อขัดข้อง ซึ่งจะส่งผลกระทบต่อการทำงานของบุคลากรของหน่วยงานในภาพรวมได้

สำนักดิจิทัลเพื่อการศึกษา ได้จัดทำแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ได้แก่ แผนกรณีเกิดกระแสไฟฟ้าขัดข้อง แผนกรณีเกิดอัคคีภัย และแผนกรณีแผ่นดินไหว โดยมีวัตถุประสงค์ เพื่อลดอัตราความเสี่ยงและลดผลกระทบในการพัฒนาด้านการบริหารจัดการให้มีประสิทธิภาพและได้มาตรฐาน

2. วัตถุประสงค์

2.1 เพื่อป้องกันการสูญเสียข้อมูลสำคัญและทรัพย์สินของเจ้าหน้าที่รวมทั้งลดผลกระทบจากการเกิดสถานการณ์ฉุกเฉิน จากกรณี ไฟฟ้าดับ อัคคีภัย และแผ่นดินไหว

2.2 เพื่อพัฒนาระบบบริหารจัดการด้านระบบไฟฟ้าของหน่วยงาน ลดอัตราความเสี่ยงต่อการเกิดเหตุ

2.3 เพื่อให้เจ้าหน้าที่เกิดความตระหนักและมีความพร้อมสามารถระงับเหตุรวมทั้งช่วยเหลือตนเองได้อย่างปลอดภัยเมื่อเกิดเหตุ

<u>แผนเตรียมความพร้อมกรณีกระแสไฟฟ้าดับ</u>

ผู้รับผิดชอบ : 1. นายมารุต เปี่ยมเกตุ ตำแหน่ง รองผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา
เบอร์โทรภายใน 5939 มือถือ 081-2939749
2. ผู้ดูแลระบบ (Admin) ประจำหน่วยงานภายในมหาวิทยาลัย มหาวิทยาลัยราชภัฏเชียงใหม่

1. กรณีไฟฟ้าดับ เวลาไม่เกิน 30 นาที

ผู้ดูแลระบบ (Admin) สำนักดิจิทัลเพื่อการศึกษามีหน้าที่ ดังนี้

1. หัวหน้า/รองหัวหน้า หรือผู้รับแจ้งปัญหาของสำนักดิจิตอลเพื่อการศึกษาประสานงานกับงานอาคารฝ่ายระบบไฟฟ้า เพื่อขอทราบสาเหตุของปัญหาและระยะเวลาในการแก้ไข หากสามารถแก้ไขได้ภายใน 30 นาที ให้ตรวจสอบการทำงานของ UPS ที่ห้อง server
2. หากสามารถใช้ไฟสำรองจากแผนกฉุกเฉินได้ ให้เตรียมสะพานไฟจากห้อง Serverและเปลี่ยนจุดจ่ายไฟฟ้าจากตำแหน่งปกติ เป็นตำแหน่งจ่ายไฟสำรองจากจากแผนกฉุกเฉิน
3. ประกาศแจ้งทางช่องทางระบบโทรศัพท์ภายใน/Social Network/แจ้งด้วยวาจา ให้หน่วยงานต่างๆทราบเพื่อปิดคอมพิวเตอร์และเครื่องสำรองไฟชั่วคราว
4. สำรวจ/รับแจ้งปัญหา การทำงานของเครื่องสำรองไฟฟ้า(UPS) เครื่องคอมพิวเตอร์ของหน่วยงานต่างๆขณะไฟฟ้าดับว่าสามารถไฟได้หรือไม่
5. เมื่อระบบไฟฟ้าสามารถทำงานได้ปกติ ให้ตรวจสอบความเรียบร้อยของ Server และอุปกรณ์เครือข่าย Switch HUB, Access Point
6. ประกาศแจ้งให้หน่วยงานต่างๆ เปิดคอมพิวเตอร์ใช้งานระบบ ได้ตามปกติ

ผู้ดูแลระบบ (Admin) ประจำหน่วยงานภายในมหาวิทยาลัย มีหน้าที่ ดังนี้

1. เมื่อได้รับแจ้งจากสำนักดิจิตอลเพื่อการศึกษาให้ปิดเครื่องปรับอากาศ /ปิดคอมพิวเตอร์ชั่วคราว
2. ประชาสัมพันธ์ให้ผู้มาใช้บริการที่รอรับบริการทราบ ให้บริการตามปกติ และเขียนข้อมูลลงในแบบฟอร์มแบบใช้มือทำเพื่อลงบันทึกลงระบบย้อนหลัง
3. กรณีเครื่องสำรองไฟฟ้า (UPS) มีปัญหาไม่สำรองไฟ ให้แจ้งสำนักดิจิตอลเพื่อการศึกษา
4. เมื่อได้รับแจ้งว่าระบบคอมพิวเตอร์สามารถใช้งานได้ตามปกติ ให้นำข้อมูลบันทึกลงในระบบตามปกติ

2. กรณีไฟฟ้าดับ เวลาเกิน 30 นาที

ผู้ดูแลระบบ (Admin) สำนักดิจิทัลเพื่อการศึกษามีหน้าที่ ดังนี้

1. หัวหน้า/รองหัวหน้า หรือผู้รับแจ้งปัญหาของสำนักดิจิตอลเพื่อการศึกษาประสานงานกับงานอาคารฝ่ายระบบไฟฟ้า เพื่อขอทราบสาเหตุของปัญหาและระยะเวลาในการแก้ไข หากสามารถไม่แก้ไขได้ภายใน 30 นาที ให้แจ้งผู้บริการระดับรองผู้อำนวยการ/ผู้อำนวยการทราบ

2. ผู้อำนวยการ/รองผู้อำนวยการ/หัวหน้าส่วน ประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ ให้หน่วยงานต่างๆทราบ
3. ประกาศแจ้งทางช่องทางระบบโทรศัพท์ภายใน/Social Network/แจ้งด้วยวาจา ให้หน่วยงานต่างๆทราบเพื่อปิดคอมพิวเตอร์และเครื่องสำรองไฟชั่วคราว
4. สำรวจ/รับแจ้งปัญหา การทำงานของเครื่องสำรองไฟฟ้า(UPS) เครื่องคอมพิวเตอร์ของหน่วยงานต่างๆขณะไฟฟ้าดับว่าสามารถไฟได้หรือไม่
5. เมื่อระบบไฟฟ้าสามารถทำงานได้ปกติ ให้ตรวจสอบความเรียบร้อยของ Server และอุปกรณ์เครือข่าย Switch HUB, Access Point
6. ประกาศแจ้งให้หน่วยงานต่างๆ เปิดคอมพิวเตอร์ใช้งานระบบ ได้ตามปกติ
7. ผู้อำนวยการ/รองผู้อำนวยการ/หัวหน้าส่วน ประกาศแจ้งยกเลิกแผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ให้หน่วยงานต่างๆทราบ เมื่อระบบสามารถใช้งานได้ตามปกติ
8. ติดตามตรวจสอบการลงบันทึกข้อมูลของหน่วยงานต่างๆ
9. สรุปรายงานนำเสนอผู้บริหารระดับสูงทราบ

ผู้ดูแลระบบ (Admin) ประจำหน่วยงานภายในมหาวิทยาลัย มีหน้าที่ ดังนี้

1. เมื่อได้รับแจ้งจากสำนักดิจิตอลเพื่อการศึกษาให้ปิดเครื่องปรับอากาศ /ปิดคอมพิวเตอร์ชั่วคราว
2. ประชาสัมพันธ์ให้ผู้มาใช้บริการที่รอรับบริการทราบ ให้บริการตามปกติ และเขียนข้อมูลลงในแบบฟอร์มแบบใช้มือทำเพื่อลงบันทึกลงระบบย้อนหลัง
3. กรณีเครื่องสำรองไฟฟ้า (UPS) มีปัญหาไม่สำรองไฟ ให้แจ้งสำนักดิจิตอลเพื่อการศึกษา
4. เมื่อได้รับแจ้งว่าระบบคอมพิวเตอร์สามารถใช้งานได้ตามปกติ ให้นำข้อมูลบันทึกลงในระบบตามปกติ

แผนเตรียมความพร้อมกรณีอัคคีภัย

ผู้รับผิดชอบ : นายมารุต เปี่ยมเกตุ ตำแหน่ง รองผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา
เบอร์โทรภายใน 5939 มือถือ 081-2939749

แผนเตรียมความพร้อมต่อสภาวะวิกฤตในกรณีเกิดอัคคีภัยเพื่อให้มหาวิทยาลัยราชภัฏเชียงใหม่มีระบบป้องกันและระงับอัคคีภัย เพื่อป้องกันและระงับอัคคีภัยตามสถานการณ์ได้อย่างรวดเร็ว ทันการณ์และมีประสิทธิภาพ รวมทั้งเพื่อสร้างความมั่นใจในความปลอดภัยต่อชีวิตและทรัพย์สินของบุคลากรทุกคน ได้กำหนดวิธีการบริหารจัดการเพื่อเตรียมความพร้อมต่อสภาวะวิกฤตในกรณีเกิดอัคคีภัย ดังนี้

1. การปฏิบัติก่อนเกิดเหตุอัคคีภัย

1.1 สำรวจ ตรวจตรา อาคารสถานที่อุปกรณ์เครื่องใช้ไฟฟ้า อุปกรณ์เกี่ยวกับการป้องกันและระงับ อัคคีภัย หากพบบริเวณใดเป็นจุดเสี่ยงต่อการเกิดอัคคีภัยให้รีบซ่อมแซม แก้ไข หรือเพิ่มความระมัดระวังเป็นพิเศษ

1.2 ให้มีการซ่อมบำรุงและตรวจตราปั๊มน้ำ สายท่อน้ำ และถังดับเพลิงให้ใช้งานได้อย่างมีประสิทธิภาพ โดยถังดับเพลิงจะต้องมีสารเคมีที่ใช้ในการดับเพลิง ตามปริมาณที่กำหนด และเปลี่ยนน้ำยาตามวาระและอายุของ น้ำยานั้น และต้องติดตั้งในพื้นที่ ที่เห็นชัดเจน สามารถนำมาใช้งานได้สะดวกทันต่อเหตุการณ์

1.3 กำหนดให้มีป้ายบอกทาง “บันไดหนีไฟ” หรือ “ทางหนีไฟ” เห็นได้อย่างชัดเจน มีป้ายข้อความ เตือน “ห้ามใช้ลิฟท์ขณะเกิดเพลิงไหม้”

1.4 กำชับให้บุคลากรติดบัตรประชาชนแสดงตน เข้า-ออก ขณะปฏิบัติ หน้าที่ภายในหน่วยงาน ตลอดจนผู้มาติดต่อราชการ โดยขอบัตรประจำตัวไว้และให้ติดบัตรผู้มาติดต่อราชการ แทน เพื่อเป็นมาตรการรักษาความปลอดภัย

1.5 จัดทำผังการติดต่อสื่อสาร หมายเลขโทรศัพท์ของฝ่ายบริหารหน่วยงาน ผู้ดูแลอาคาร หรือห้องเวร รักษาการณ์สถานีตำรวจในพื้นที่และสถานีดับเพลิง โดยทำป้ายติดให้เห็นชัดเจนทุกชั้นพร้อมทั้งกำหนดพื้นที่เป็น จุดนัดพบหรือจุดรวมพล

1.6 บุคลากรภายในหน่วยงาน มีส่วนร่วมในการจัดระเบียบ ความเรียบร้อย สถานที่ทำงาน สิ่งที่น่าจะเกิด อัคคีภัยได้ง่าย จัดเก็บให้ถูกตองตามลักษณะการเก็บรักษาโดยไม่สะสมสิ่งของ ที่อาจเป็นเชื้อเพลิงไว้ปริมาณมาก เช่น กระดาษใช้แล้ว หนังสือพิมพ์เก่า เป็นต้น

1.7 การปฏิบัติตามกฎระเบียบ ข้อบังคับที่เกี่ยวกับการป้องกันอัคคีภัย เช่น สถานที่ใดมีข้อความห้ามสูบ บุหรี่ก็ต้องปฏิบัติตาม

1.8 อบรมความรู้ให้กับบุคลากร ระงับอัคคีภัยเบื้องต้น ฝึกการใช้อุปกรณ์เครื่องมือ เครื่องใช้ในการ ดับเพลิง ตลอดจนฝึกซ้อมการปฏิบัติเมื่อเกิดอัคคีภัย ว่าจะปฏิบัติอย่างไร การแจ้งเหตุทำอย่างไร

2. การปฏิบัติเมื่อเกิดเหตุอัคคีภัย

2.1. ผู้พบเห็นเพลิงไหม้ตัดสินใจว่าดับเพลิงได้ด้วยตนเองหรือไม่ โดยพิจาณาจากสถานการณ์ดังนี้

2.1.1 ถ้าดับได้ให้ดำเนินการดับไฟนั้นทันที (ควรฝึกการใช้เครื่องดับเพลิงให้เป็นทุกคน) และ รายงานให้ผู้บังคับบัญชาทราบตามลำดับ

2.1.2 ถ้าดับไม่ได้ให้แจ้งเพื่อนร่วมงาน/หัวหน้า ช่วยกันดับไฟ กรณีดับได้แล้วให้รายงาน ผู้บังคับบัญชาตามลำดับชั้น หากยังไม่หยุดสามารถยุติการเกิดอัคคีภัยได้ให้เข้าสู่แผนปฏิบัติการเหตุอัคคีภัยขั้น ลุกลาม

3. การเข้าสู่แผนปฏิบัติการบริหารความพร้อมต่อสภาวะวิกฤตในกรณีเกิดอัคคีภัยขั้นลุกลาม

3.1 ตัดกระแสไฟฟ้าบริเวณที่เกิดเหตุ

3.2 เปิดสัญญาณแจ้งเหตุเพลิงไหม้แจ้งเตือนภัย

3.3 แจ้งเจ้าหน้าที่รักษาความปลอดภัย เวรยาม ช่วยทำการดับเพลิงเป็นการเฉพาะหน้า

3.4 แจ้งหน่วยดับเพลิง โดยบอกชื่อผู้แจ้ง สถานที่เกิดเหตุลักษณะของไฟที่กำลังลุกไหม้ หมายเลข โทรศัพท์ของผู้แจ้ง

3.5 ควบคุมอย่าให้บุคลากรกลับเข้าในอาคารเพื่อไปเก็บสิ่งของส่วนตัวอีก

3.6 ผู้นำทางหนีไฟ จะเป็นผู้นำทางอพยพหนีไฟไปตามทางออกที่จัดไว้ไปยังบริเวณที่เตรียมการองรับการอพยพที่กำหนดไว้ซึ่งเป็นจุดนัดพบหรือจุดรวมพล ห้ามหนีขึ้นข้างบน และไม่ควรผ่าน ด้านที่เกิดเหตุเพลิงไหม้ หากมีกลุ่มให้คลานต่ำ

3.7 หน่วยปฐมพยาบาลทำการปฐมพยาบาลเบื้องต้น ในกรณีมีผู้เป็นลม บาดเจ็บหรือหมดสติและรีบ นำส่งโรงพยาบาลโดยเร็วทันที

4. การปฏิบัติภายหลังเพลิงสงบ

4.1 ส่วนบริหารการพัสดุสำรวจความเสียหายร่วมกับหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานตำรวจแห่งชาติ สำนักป้องกันและบรรเทาสาธารณภัย สำนักงานเขต ในกรณีอาคารที่ถูกเพลิงไหม้ไม่สามารถซ่อมแซมได้ ให้จัดการรื้อถอนออกเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นอีก และแจ้งต่อทีมงานคณะบริหารความต่อเนื่อง

4.2 ประชาสัมพันธ์ฟื้นฟูสภาพจิตใจของเจ้าหน้าที่ภายในหน่วยงานให้กลับคืนสู่สภาพปกติโดยเร็ว

4.3 ปรับปรุง ซ่อมแซม สิ่งที่เสียหายให้กลับคืนสภาพปกติหรือจัดหาใหม่ทดแทน ทีมงานคณะบริหารความต่อเนื่อง ดำเนินการ

1) รายงานผลสำรวจความเสียหายให้หัวหน้าคณะบริหารความต่อเนื่องทราบ

2) จัดหาสถานที่ในการปฏิบัติงานและให้บริการผู้มารับบริการ/ผู้มาติดต่อประสานงานหน่วยงานที่ให้บริการ/ดำเนินงานผ่านระบบ สำนักดิจิตอลเพื่อการศึกษา ให้ดำเนินการตามแผนบริหารความต่อเนื่อง ณ สถานที่กำหนดไว้

แผนเตรียมความพร้อมกรณีแผ่นดินไหว

ผู้รับผิดชอบ : นายมารุต เปี่ยมเกตุ ตำแหน่ง รองผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษา
เบอร์โทรภายใน 5939 มือถือ 081-2939749

แผนเตรียมความพร้อมต่อสภาวะวิกฤตในกรณีเกิดแผ่นดินไหว เพื่อให้มหาวิทยาลัยราชภัฏเชียงใหม่มีระบบป้องกันและบรรเทาเหตุแผ่นดินไหวตามสถานการณ์ได้อย่างรวดเร็ว ทันการณ์ และมีประสิทธิภาพ รวมทั้งเพื่อสร้างความมั่นใจในความปลอดภัยต่อชีวิตและทรัพย์สินของบุคลากรทุกคน ซึ่งได้กำหนดแผนการบริหารจัดการ ดังนี้

1. การปฏิบัติก่อนเกิดเหตุแผ่นดินไหว

1. ทีมงานบริหารความต่อเนื่อง ดำเนินการเผยแพร่แผนบริหารความพร้อมต่อสภาวะวิกฤต การให้ความรู้แก่ผู้ที่เกี่ยวข้องและบุคลากรในสังกัด เกี่ยวกับมาตรการรับมือการเกิดแผ่นดินไหว ขั้นตอน/แนวทางปฏิบัติในการเตรียมตัวรับมือเหตุแผ่นดินไหว และแนวทางการป้องกันเอาตัวรอดเฉพาะหน้าขณะเกิดเหตุดังกล่าวรวมทั้งกำหนดแผนฟื้นฟูและบรรเทาความเดือดร้อนบริเวณอาคารและพื้นที่ เพื่อให้สามารถปฏิบัติงานได้ตามปกติ
2. ตรวจสอบสภาพความปลอดภัยของอาคาร และเครื่องใช้ภายในอาคาร ทำการยึดติดอุปกรณ์ที่อาจก่อให้เกิดอันตราย เช่น ตู้และชั้นหนังสือยึดติดกับผนังหรือเสา ไม่วางของหนักบนที่สูง เป็นต้น
3. สำรวจ รวบรวมพื้นที่เสี่ยง รวมทั้งพื้นที่ปลอดภัยเพื่อรองรับการอพยพ และเตรียมอุปกรณ์จำเป็น เช่น ไฟสำรอง วิทยุสื่อสาร อาหาร น้ำดื่ม เครื่องมือช่าง อุปกรณ์ดับเพลิง ชุดปฐมพยาบาลและยา เพื่อเตรียมรับแผ่นดินไหวและอาคารถล่มที่อาจเกิดขึ้น

2. การปฏิบัติเมื่อเกิดแผ่นดินไหว

2.1 กรณีเหตุการณ์ไม่รุนแรง (สามารถปฏิบัติงานในอาคารเทคโนโลยีสารสนเทศได้)

2.1.1 เจ้าหน้าที่ส่วนบริหารงานพัสดุดำเนินการตรวจสอบ/ประเมินสถานการณ์

2.1.2 คณะ/สำนัก/ศูนย์/กอง ดำเนินการตรวจสอบผู้บาดเจ็บและให้การปฐมพยาบาลเบื้องต้นก่อนนำส่งโรงพยาบาล

2.1.3 ทีมงานบริหารความต่อเนื่องด้านการประชาสัมพันธ์ (งานประชาสัมพันธ์) ดำเนินการติดตามข้อมูลข่าวสารอย่างต่อเนื่องและประชาสัมพันธ์ข้อมูลข่าวสารให้บุคลากรทราบเพื่อเตรียมความพร้อมในกรณีที่อาจเกิดเหตุการณ์พลิกผันที่ส่อเค้าถึงความรุนแรงที่มากขึ้น

2.2 กรณีเหตุการณ์รุนแรง (ไม่สามารถปฏิบัติงานในอาคารเทคโนโลยีสารสนเทศได้)

2.2.1 ทีมงานบริหารความต่อเนื่องมหาวิทยาลัยราชภัฏเชียงใหม่และเจ้าหน้าที่ส่วนบริหารการพัสดุดำเนินการตรวจสอบ/ประเมินสถานการณ์

2.2.2 ทีมงานผู้ประสานความต่อเนื่อง ประสานให้ผู้ประสานคณะบริหารความต่อเนื่องของทุกคณะ/สำนัก/ศูนย์/กอง ดำเนินการตรวจสอบสถานการณ์และให้ความช่วยเหลือ

2.2.3 ทีมงานบริหารความต่อเนื่องด้านการประชาสัมพันธ์ติดตามข้อมูลข่าวสารอย่างต่อเนื่องพร้อมทั้งดำเนินการประชาสัมพันธ์ข้อมูลข่าวสารให้บุคลากรทราบและแจ้งส่วนราชการต่างๆ รวมถึงผู้รับบริการทราบถึงช่องทางการติดต่อกับมหาวิทยาลัยราชภัฏเชียงใหม่ ณ สถานที่ปฏิบัติงานสำรอง

2.2.4 หัวหน้าทีมและทีมงานบริหารความต่อเนื่องด้านระบบเทคโนโลยีสารสนเทศและอุปกรณ์คอมพิวเตอร์ ประชุมหน่วยงานที่เกี่ยวข้องเพื่อย้ายสถานที่ปฏิบัติงานไปยังสถานที่ปฏิบัติงานสำรอง ดำเนินการปิดระบบ ทำการย้ายระบบงานต่างๆ ไปปฏิบัติงาน ณ สถานที่ปฏิบัติงานสำรองที่กำหนดตามแผนรับสถานการณ์ฉุกเฉินที่กำหนดไว้

2.2.5 ส่วนบริหารการพัสดุ เตรียมที่พัก ชุดปฐมพยาบาลเบื้องต้น และอาหารสำหรับเจ้าหน้าที่ผู้อยู่เวรยาม เพื่อเฝ้าระวังและเตรียมขนย้ายตลอด 24 ชั่วโมง และเตรียมให้ความช่วยเหลืออำนวยความสะดวกในด้านการเดินทางไปปฏิบัติราชการของเจ้าหน้าที่ในกรณีต้องไปปฏิบัติงาน ฯ ณ สถานที่ปฏิบัติงานสำรอง

2.2.6 เมื่อบุคลากรในสังกัดมหาวิทยาลัยราชภัฏเชียงใหม่ทราบถึงเหตุการณ์ ให้ดำเนินการเก็บรักษาทรัพย์สินในที่ปลอดภัยและเตรียมพร้อมในการอพยพ

3. การอพยพ

3.1 เมื่อได้รับแจ้งให้อพยพ ให้หยุดทำงานทันที

3.2 ตั้งสติอย่าตื่นตระหนก และเก็บรวบรวมเอกสาร หรือทรัพย์สินที่สำคัญให้เรียบร้อย หากอยู่ในอาคารให้ยืนหรือหมอบอยู่ในส่วนของอาคารที่โครงสร้างแข็งแรงสามารถรับน้ำหนักได้มาก หรืออยู่ใต้โต๊ะที่แข็งแรงเพื่อป้องกันอันตรายจากสิ่งปรักหักพังที่ร่วงหล่นลงมา อยู่ให้ห่างจากประตู หน้าต่าง สายไฟ อุปกรณ์ไฟฟ้าและสิ่งห้อยแขวน

3.3 สำรวจ ปิดและดึงปลั๊กเครื่องใช้ไฟฟ้าทุกชนิดออก

3.4 อาคารสูงจะล้มหรือพงทลายช้ากว่าอาคารเตี้ย (เนื่องจากมีคาบของการสั่นหรือแกว่งนานกว่า) ให้หมอบหลบใต้โต๊ะจนกว่าการสั่นสะเทือนจะหยุดลง สำหรับอาคารสูง 2 ชั้น อาจล้มพังได้ในเวลา 2 นาที

3.5 ถ้าอยู่นอกอาคาร ให้อยู่ในที่โล่ง ห่างจากตึก อาคารสูง เสาไฟ สายไฟ หรือส่งที่อาจล้มใส่ได้

3.6 ให้รีบออกจากอาคาร ไปยังพื้นที่นัดพบ เมื่อแผ่นดินไหวสงบลง

4. การสำรวจความเสียหายหลังเกิดเหตุเกิดแผ่นดินไหว

4.1 ทีมงานบริหารความต่อเนื่องดำเนินการสำรวจ/ประเมินความเสียหาย/ตรวจสอบทรัพย์สินของทางราชการที่เสียหาย

4.2 หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศและอุปกรณ์คอมพิวเตอร์ ตรวจสอบความเสียหายของระบบ server รวมทั้งอุปกรณ์คอมพิวเตอร์

4.3 ทีมงานคณะบริหารความต่อเนื่อง เมื่อได้สำรวจความเสียหายแล้ว ให้ดำเนินการดังนี้

4.3.1 รายงานผลสำรวจความเสียหายให้หัวหน้าคณะบริหารความต่อเนื่องทราบ

4.3.2 จัดหาสถานที่ในการปฏิบัติงานและให้บริการผู้มารับบริการ/ผู้มาติดต่อประสานงาน

แผนการสำรองข้อมูล

ผู้รับผิดชอบ : 1. นายวิวัฒน์ชัยขำประไพ ตำแหน่ง นักวิชาการคอมพิวเตอร์ เบอร์โทรศัพท์ 084-1732278
2. นายวิทูร อุ่นแสน ตำแหน่ง นักวิชาการคอมพิวเตอร์ เบอร์โทรศัพท์ 086-8527303
3. นายอานนท์ มะโนเมือง ตำแหน่ง นักวิชาการคอมพิวเตอร์ เบอร์โทรศัพท์ 084-1701762

ผู้รับผิดชอบในการดำเนินการ จะต้องดำเนินการปฏิบัติและเข้าตรวจสอบระบบงานของระบบเครือข่าย พร้อมทั้งรายงานความเสียหายเพื่อแจ้งผู้อำนวยการสำนักดิจิทัลเพื่อการศึกษาทราบ

กรณีฐานข้อมูล

1. ให้มีการสำรองข้อมูลฐานข้อมูลทุก 1 เดือนเป็นอย่างน้อย

กรณีโจมตีระบบเครือข่าย

1. มีการติดตั้ง firewall เพื่อป้องกันไม่ให้ผู้ไม่ได้รับอนุญาตจากระบบเครือข่ายสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา
2. มีเจ้าหน้าที่ดูแลระบบเครือข่ายตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุการป้องกันต่อไป

กรณีการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

1. ควบคุมสถานการณ์
   - ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา
   - ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย
   - เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก
2. วิเคราะห์การถูกโจมตี
   - ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการและไฟล์อื่นๆ
   - วิเคราะห์ล็อกไฟล์ ตรวจสอบโปรแกรมหรือข้อมูลที่ผู้บุกรุกทิ้งไว้
   - ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System
   - ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ
3. กู้คืนระบบคอมพิวเตอร์
   - กู้คืนข้อมูลหรือสารสนเทศที่เสียหายหรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่
   - งดใช้เซอร์วิสที่ไม่จำเป็น
   - ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล Update Patch
   - อุดช่องโหว่ในระบบเครือข่าย
   - เปลี่ยนแปลงรหัสผ่านใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว