



ประกาศมหาวิทยาลัยราชภัฏยะลา

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏยะลา

พ.ศ. ๒๕๕๘

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏยะลา เป็นมาตรการ สำหรับใช้ในการควบคุมการดำเนินงาน การให้บริการ และการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการสื่อสารของมหาวิทยาลัยให้มีความมั่นคงปลอดภัย ครอบคลุมการรักษาความลับ การรักษาความถูกต้อง และการรักษาสภาพความพร้อมในการใช้งานของระบบสารสนเทศ ตามข้อกำหนดภายใต้ประกาศคณะกรรมการ อุตสาหกรรมทางอิเล็กทรอนิกส์และมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของด้านสารสนเทศของมหาวิทยาลัย ราชภัฏยะลาเป็นไปตามมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๓๑(๑) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ.๒๕๔๗ มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ และหนังสือสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๐๒๐๙/ว๒๙๒๗ ลงวันที่ ๑๓ ตุลาคม ๒๕๕๔ เรื่อง ขอความร่วมมือดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล และประกาศคณะกรรมการอุตสาหกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕ จึงออก ประกาศมหาวิทยาลัยราชภัฏยะลา เรื่อง นโยบายการรักษาความปลอดภัยด้านสารสนเทศ ความดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยราชภัฏยะลา เรื่อง นโยบายการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏยะลา พ.ศ. ๒๕๕๘”

ข้อ ๒ ประกาศนี้ให้บังคับใช้ในวันถัดไปหลังจากวันประกาศ เป็นต้นไป

ข้อ ๓ กำหนดคำนิยามดังต่อไปนี้

“มหาวิทยาลัย” หมายถึง มหาวิทยาลัยราชภัฏยะลา

“หน่วยงาน” หมายถึง คณะ สำนัก สถาบัน ศูนย์ กอง และหน่วยงานในกำกับที่เป็นหน่วยงาน ภายในมหาวิทยาลัยราชภัฏยะลา

“ผู้ใช้งาน” หมายถึง อาจารย์ บุคลากร นักศึกษา หรือผู้ที่มหาวิทยาลัยอนุญาตให้ใช้สิทธิของมหาวิทยาลัย

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบ สารสนเทศของมหาวิทยาลัย หรือสิทธิ์เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัย

“สินทรัพย์” หมายถึง เครื่องคอมพิวเตอร์ เครื่องแม่ข่าย เครือข่ายย่อย และระบบสารสนเทศ ต่าง ๆ ที่มหาวิทยาลัย พัฒนาขึ้น หรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

/“เครื่องคอมพิวเตอร์” ...

“เครื่องคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีกำหนดคำสั่ง ชุดคำสั่งซึ่งมีหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ห้องศูนย์กลางข้อมูล” หมายถึง สถานที่ติดตั้งอุปกรณ์คอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในมหาวิทยาลัย

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง ความสามารถในการเข้าถึงระบบสารสนเทศที่ได้รับการอนุญาต จากการกำหนดสิทธิหรือได้รับมอบอำนาจในการเข้าถึงระบบ ในการสร้าง อ่าน สำเนา และแก้ไขสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการทางกายภาพ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง ความมั่นคงและความปลอดภัยในบริบทของการรักษาความลับ ข้อมูลการใช้งาน ของระบบสารสนเทศมหาวิทยาลัย โดยมีเป้าหมายเพื่อปกป้องสิทธิของมหาวิทยาลัยจากเหตุการณ์ หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ซึ่งอาจทำให้เกิดความเสียหายต่อสิทธิของมหาวิทยาลัย

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุงการเกิดเหตุการณ์ สภาพใช้งาน การให้บริการเครือข่ายสารสนเทศมหาวิทยาลัยที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

“เครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏยะลา” หรือเรียกอีกนามหนึ่ง “เครือข่าย YRUNet” หมายถึง ระบบเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย โดยมีวัตถุประสงค์การใช้งานเพื่อการบริหารงาน การปฏิบัติงาน การบริการวิชาการการศึกษาและงานวิจัยที่เป็นพันธกิจของมหาวิทยาลัย

“ผู้ดูแลเครือข่ายสารสนเทศ” หมายถึง บุคลากรที่ได้รับมอบหมายจากมหาวิทยาลัยเพื่อปฏิบัติงานด้านการดูแลบริหารจัดการระบบเครือข่ายสารสนเทศของมหาวิทยาลัยให้พร้อมสำหรับการใช้งาน

“ผู้ปฏิบัติงานระบบสารสนเทศ” หมายถึง บุคลากรที่ได้รับมอบหมายจากมหาวิทยาลัยหรือหน่วยงานภายในมหาวิทยาลัย เพื่อทำการป้อนข้อมูลและแก้ไขข้อมูลของระบบสารสนเทศของมหาวิทยาลัย

“เครือข่ายย่อย” หมายถึง อุปกรณ์ต่อพ่วงต่างๆ รวมถึงอุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่างๆ ภายในเครือข่ายสารสนเทศของมหาวิทยาลัยตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ

“ผู้ดูแลระบบเครือข่ายย่อย” หมายถึง บุคลากรที่ได้รับมอบหมายจากหัวหน้าหน่วยงานเพื่อปฏิบัติงานด้านระบบเครือข่ายของหน่วยงาน

“ผู้ใช้บริการเครือข่าย” หมายถึง บุคคล หน่วยงาน ที่เชื่อมต่อและรับบริการจากเครือข่ายสารสนเทศของมหาวิทยาลัย

“ผู้บริหารระดับสูงสุด” หมายถึง อธิการบดีมหาวิทยาลัยราชภัฏยะลา

/“ผู้บริหารเทคโนโลยีสารสนเทศ...

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” หมายถึง ผู้ที่ได้รับการแต่งตั้งจากมหาวิทยาลัยให้รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง คณะกรรมการที่ได้รับการแต่งตั้งจากมหาวิทยาลัย เพื่อมีหน้าที่ในการกำหนดตรวจสอบ ทบทวน ปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“ผู้ตรวจสอบภายใน” หมายถึง บุคลากรภายในมหาวิทยาลัยที่ได้รับการแต่งตั้งจากมหาวิทยาลัยเพื่อมีหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“ผู้ตรวจสอบจากภายนอก” หมายถึง บุคลากรภายนอกมหาวิทยาลัยที่มีความรู้ ความสามารถทางด้านเทคโนโลยีสารสนเทศที่ได้รับเชิญเป็นผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“บทลงโทษ” หมายถึง บทลงโทษที่มหาวิทยาลัยเป็นผู้กำหนดหรือบทลงโทษตามกฎหมาย

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

#### ๔.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร บุคลากรทางด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการจัดทำ ข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

(๒) นโยบายได้จัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

#### ๔.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การให้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

/ข้อ ๕ มีข้อกำหนด...

ข้อ ๕ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

๕.๑ ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๕.๒ กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๕.๓ กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ บริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความรู้ความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๖.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๖.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๗ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

๗.๑ การใช้งานรหัสผ่าน (Password Usage) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๗.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓ การควบคุมสินทรัพย์และการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๗.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘ ควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๘.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๘.๒ การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวตนบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๘.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๘.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๘.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๘.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๘.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูล หรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙ ควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๙.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยการเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๙.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง



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

๙.๔ การใช้งานโปรแกรมมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทมอรรถประโยชน์ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๙.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐ ควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชัน และสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศ และฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๐.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน

๑๐.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่

๑๐.๔ การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๑ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทาง ต่อไปนี้

๑๑.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑๑.๒ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๑.๓ มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งมีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๑.๔ ต้องมีการทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๒ ครั้ง

๑๑.๕ ปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

๑๒.๑ ให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

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

ข้อ ๑๓ กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเอียด หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ดังนี้

๑๓.๑ ระดับนโยบาย

(๑) ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบในการกำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย โดยมีหน้าที่กำกับ ดูแล รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นอันเนื่องมาจากความบกพร่องละเอียด หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้การสนับสนุนและส่งเสริมการดำเนินงานด้านสารสนเทศอย่างมีประสิทธิภาพ

(๒) ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีหน้าที่ติดตาม กำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงานผู้รับผิดชอบระดับปฏิบัติงาน กำกับดูแลให้มีการปฏิบัติ และดำเนินการตามประกาศ ฉบับนี้

๑๓.๒ ระดับปฏิบัติงาน ได้แก่

(๑) ผู้ดูแลรับผิดชอบเครือข่ายของมหาวิทยาลัย ในตำแหน่งนักวิชาการคอมพิวเตอร์ รับผิดชอบงานพัฒนาระบบเครือข่ายและระบบสารสนเทศ กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตาม การปฏิบัติงานตามแผน การบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการรวมทั้งรับผิดชอบ ดังนี้

/(๒) ควบคุมการเข้า – ออก...

(๒) ควบคุมการเข้า – ออกห้องศูนย์กลางข้อมูล (Data Center) ตามการกำหนดสิทธิการเข้าถึงห้องศูนย์กลางข้อมูล (Data Center)

(๓) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ และอุปกรณ์เครือข่าย (Network) ของระบบเทคโนโลยีสารสนเทศทั้งหมดที่ให้บริการในมหาวิทยาลัยราชภัฏยะลาให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

(๔) กำกับดูแล การติดตั้ง รื้อถอน ตรวจสอบการเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN Internet Intranet ที่ให้บริการในมหาวิทยาลัย

(๕) กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของห้องคอมพิวเตอร์แม่ข่าย (Server) ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

(๖) แก้ไขปัญหาที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

(๗) รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบทุกเดือน

(๘) กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

(๙) กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๑๐) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของระบบฐานข้อมูลทั้งหมดที่ให้บริการให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

(๑๑) กำกับดูแล ตรวจสอบในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของระบบ

(๑๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๑๓) รายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยง ให้ผู้บังคับบัญชาทราบ

(๑๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(๑๕) บริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Management) ระบบสารสนเทศแต่ละระบบของมหาวิทยาลัย เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต



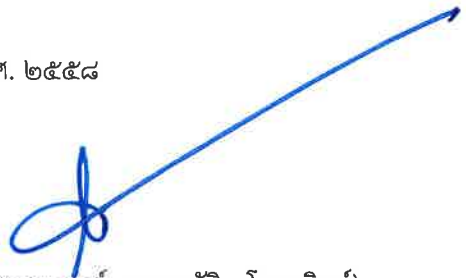
๑๕.๓ ผู้ดูแลระบบจากบริษัทที่จัดจ้างให้ดูแลระบบสารสนเทศของมหาวิทยาลัย  
รับผิดชอบ ดังนี้

(๑) แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบสารสนเทศและฐานข้อมูลที่เกิดจากการถูกภัยคุกคามจากผู้ไม่ประสงค์ดี

(๒) รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบสารสนเทศและฐานข้อมูลถูกทำลายจากผู้ไม่ประสงค์ดีต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

(๓) บำรุงรักษาระบบสารสนเทศและฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัย ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

ประกาศ ณ วันที่ ๑๗ พฤศจิกายน พ.ศ. ๒๕๕๘



(ผู้ช่วยศาสตราจารย์ ดร.สมบัติ โยธาทิพย์)

อธิการบดีมหาวิทยาลัยราชภัฏยะลา