ประกาศราชวิทยาลัยจุฬาภรณ์
เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

.....

มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศราชวิทยาลัยจุฬาภรณ์ กำหนดขึ้นภายใต้กรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อเป็นแนวทางปฏิบัติสำหรับผู้ปฏิบัติงานในราชวิทยาลัยจุฬาภรณ์และผู้ที่เกี่ยวข้อง เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการอิเล็กทรอนิกส์มีความปลอดภัยด้านสารสนเทศ เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕ และให้สอดคล้องกับมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓

อาศัยอำนาจตามความในมาตรา ๒๒ แห่งพระราชบัญญัติราชวิทยาลัยจุฬาภรณ์ พ.ศ. ๒๕๕๙ และที่แก้ไขเพิ่มเติม ประกอบมติที่ประชุมคณะกรรมการนโยบายและบริหารจัดการด้านเทคโนโลยีสารสนเทศ ครั้งที่ ๓/๒๕๖๓ เมื่อวันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๓ จึงขอออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศราชวิทยาลัยจุฬาภรณ์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ ประกาศนี้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“ราชวิทยาลัย” หมายความว่า ราชวิทยาลัยจุฬาภรณ์

“เลขาธิการ” หมายความว่า เลขาธิการราชวิทยาลัยจุฬาภรณ์

“คณะผู้บริหาร” หมายความว่า ผู้บริหารระดับ ๑ – ๔ ตามข้อบังคับราชวิทยาลัยจุฬาภรณ์ ว่าด้วยการบริหารงานบุคคลผู้ปฏิบัติงานในราชวิทยาลัย พ.ศ. ๒๕๖๒

“คณะกรรมการ” หมายความว่า คณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศ

“ผู้ปฏิบัติงานในราชวิทยาลัย” หมายความว่า พนักงานราชวิทยาลัยและลูกจ้างของราชวิทยาลัย

“ผู้ดูแลระบบ” หมายความว่า เจ้าหน้าที่หรือหน่วยงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“ผู้ใช้งาน” หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานระบบสารสนเทศของราชวิทยาลัย โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดไว้

“การรักษาความมั่นคงปลอดภัย” หมายความว่า การทำให้ระบบสารสนเทศมีความมั่นคงและปลอดภัย พ้นจากภัยคุกคาม ธำรงไว้ซึ่ง ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

“ข้อมูล (Data)” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“สารสนเทศ (Information)” หมายความว่า ข้อมูลที่ได้ผ่านการประมวลผลหรือวิเคราะห์สรุปผลด้วยวิธีการต่าง ๆ แล้วเก็บรวบรวมไว้ เพื่อนำมาใช้ประโยชน์ตามต้องการ

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลระหว่างระบบสารสนเทศต่าง ๆ ของราชวิทยาลัย ได้แก่

(๑) ระบบเครือข่ายอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่มี ขอบเขตในราชวิทยาลัยเชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ เข้าด้วยกันโดยมีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายใน เครือข่ายนี้บริหารจัดการโดยราชวิทยาลัยประกอบไปด้วยเครือข่าย แบบใช้สาย (LAN) และเครือข่ายแบบไร้สาย (Wireless LAN)

(๒) ระบบเครือข่ายอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ ภายนอกที่เชื่อมต่อกับเครือข่ายอินเตอร์เน็ตทั่วโลกซึ่งมีการเชื่อมต่อระบบเครือข่ายอินทราเน็ตหรือมีการเข้าใช้ งานโดยหน่วยงานหรือผู้ปฏิบัติงานในราชวิทยาลัย

“ทรัพย์สินสารสนเทศ” หมายความว่า สารสนเทศที่มีคุณค่าสำหรับราชวิทยาลัย อันได้แก่

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์และระบบงานสารสนเทศเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา อุปกรณ์คอมพิวเตอร์ สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ และอุปกรณ์ประมวลผลอื่นใด

(๒) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

ข้อ ๔ ให้เลขาธิการเป็นผู้รักษาการตามประกาศนี้ ในกรณีที่มีปัญหาหรือข้อสงสัยเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้เลขาธิการเป็นผู้มีอำนาจวินิจฉัยและให้ถือเป็นที่สุด

หมวดที่ ๑
บททั่วไป

ข้อ ๕ มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดขึ้นเพื่อวัตถุประสงค์ ดังนี้

(๑) เพื่อให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของราชวิทยาลัยซึ่งสอดคล้องกับแนวทางที่ยอมรับในระดับสากล

(๒) เพื่อให้เกิดความเชื่อมั่นในการใช้งานระบบงานสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์ของราชวิทยาลัย

(๓) เพื่อให้หน่วยงานรวมถึงผู้ปฏิบัติงานในราชวิทยาลัยและบุคคลภายนอกที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศได้ตระหนักถึงมาตรการและแนวทางที่จะต้องปฏิบัติ เมื่อใช้งานระบบสารสนเทศของราชวิทยาลัย

ข้อ ๖ มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศราชวิทยาลัย ประกอบด้วย

(๑) นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของราชวิทยาลัย (Information security policies)

(๒) โครงสร้างการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of information security)

(๓) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human resource security)

(๔) การบริหารจัดการทรัพย์สินสารสนเทศ (IT asset management)

(๕) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (Access control)

(๖) การเข้ารหัสข้อมูล (Cryptography)

(๗) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and environmental security)

(๘) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

(๙) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Communication security)

(๑๐) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

(๑๑) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

(๑๒) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)

(๑๓) การบริหารความต่อเนื่องในการดำเนินงาน (Business continuity management)

(๑๔) การติดตาม ตรวจสอบ และประเมินผลการดำเนินงานตามนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ (Compliance)

ข้อ ๗ ให้ทำการเผยแพร่มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทางอินทราเน็ต อีเมล และเว็บไซต์ราชวิทยาลัย โดยให้ฝ่ายเทคโนโลยีสารสนเทศดำเนินการทบทวนมาตราฐานฉบับนี้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญของมาตราฐานสากล ISO/IEC ๒๗๐๐๑ หรือตามกฎหมายที่เกี่ยวข้อง

หมวดที่ ๒

ส่วนที่ ๑

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

(Information security policies)

ข้อ ๘ กำหนดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เพื่อให้การดำเนินการด้านสารสนเทศเป็นไปอย่างปลอดภัยและตรวจสอบได้ โดยไม่ขัดต่อกฎหมายระเบียบ ข้อบังคับที่เกี่ยวข้อง สอดคล้องตามยุทธศาสตร์ของราชวิทยาลัย

ข้อ ๙ การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ให้ดำเนินการดังต่อไปนี้

(๑) กำหนดให้มีการประเมินและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน

(๒) ให้กำหนดหน่วยงานและบุคคลในการดำเนินการปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศโดยต้องผ่านการอนุมัติและได้รับความเห็นชอบจากเลขาธิการ

(๓) กำหนดให้คณะกรรมการนโยบายและบริหารจัดการด้านเทคโนโลยีสารสนเทศเป็นผู้ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศและเสนอกรรมการสภาราชวิทยาลัยเพื่อพิจารณา

(๔) จัดทำนโยบายเป็นลายลักษณ์อักษร และประกาศให้ผู้ปฏิบัติงานในราชวิทยาลัยและบุคคลภายนอกที่เกี่ยวข้องทราบทางอินทราเน็ต อีเมลหรือเว็บไซต์ของหน่วยงาน

ส่วนที่ ๒

โครงสร้างการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ

(Organization of information security)

ข้อ ๑๐ ให้กำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศภายในราชวิทยาลัยเพื่อดำเนินการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ ๑๑ โครงสร้างการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ

(๑) ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศ”

(๒) คณะกรรมการมีหน้าที่ พิจารณา ทบทวน แนวทางในการบริหารจัดการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน

(๓) เลขาธิการและคณะผู้บริหารทุกคนมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของราชวิทยาลัย ให้การสนับสนุน กำหนดทิศทางและมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

(๔) กำหนดโครงสร้างทีมผู้ปฏิบัติงานความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีขอบเขตและหน้าที่ความรับผิดชอบต่าง ๆ อย่างชัดเจน

(๕) มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศเมื่อดำเนินการร่วมกับบุคคลหรือหน่วยงานภายนอกราชวิทยาลัย

(๖) กำหนดให้มีขั้นตอนการติดต่อกับผู้เชี่ยวชาญหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

ส่วนที่ ๓
การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
(Human resource security)

ข้อ ๑๒ การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร เพื่อให้ผู้ปฏิบัติงานในราชวิทยาลัยสามารถปฏิบัติงานได้ตรงตามความต้องการ พร้อมทั้งเข้าใจในหน้าที่และความรับผิดชอบ และมีการตระหนักรู้ถึงความเสี่ยงต่าง ๆ ของการใช้งานระบบสารสนเทศ เพื่อปฏิบัติหน้าที่ตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศราชวิทยาลัย

ข้อ ๑๓ การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร ให้ดำเนินการดังต่อไปนี้

(๑) กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของผู้ปฏิบัติงานในราชวิทยาลัย หรือบุคคลภายนอกที่ว่าจ้าง โดยให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ประกาศใช้

(๒) เลขาธิการและคณะผู้บริหารต้องกำหนดให้ผู้ปฏิบัติงานในราชวิทยาลัย หน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง ปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศที่ประกาศใช้

(๓) กำหนดให้มีขั้นตอนการลงโทษผู้ปฏิบัติงานในราชวิทยาลัย ที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของราชวิทยาลัย

(๔) กำหนดขั้นตอนปฏิบัติในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน

(๕) ผู้ปฏิบัติงานในราชวิทยาลัย หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศที่ได้รับจากราชวิทยาลัย เมื่อสิ้นสุดสถานะการเป็นผู้ปฏิบัติงานในราชวิทยาลัย หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับราชวิทยาลัย

(๖) กำหนดให้ยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศของราชวิทยาลัยของผู้ปฏิบัติงานในราชวิทยาลัย หรือบุคคลภายนอก เมื่อสิ้นสุดสถานะการเป็นผู้ปฏิบัติงานในราชวิทยาลัย หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการเข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น

(๗) กำหนดให้จัดการอบรมผู้ปฏิบัติงานในราชวิทยาลัยเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านสารสนเทศ

ส่วนที่ ๔
การบริหารจัดการทรัพย์สินสารสนเทศ
(IT Asset Management)

ข้อ ๑๔ ให้มีการบริหารจัดการทรัพย์สินสารสนเทศ ข้อมูลที่เก็บอยู่ในระบบสารสนเทศของราชวิทยาลัย รวมไปถึงการระบุทรัพย์สินสารสนเทศและการกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินสารสนเทศของราชวิทยาลัย

ข้อ ๑๕ การบริหารจัดการทรัพย์สินสารสนเทศ ให้ดำเนินการดังต่อไปนี้

(๑) กำหนดให้มีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อประโยชน์การใช้งานในภายหลัง

(๒) ให้กำหนดผู้มีหน้าที่ดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศไว้อย่างชัดเจน

(๓) ให้กำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศ โดยจัดทำเป็นลายลักษณ์อักษร ให้ผู้ปฏิบัติงานในราชวิทยาลัยรับทราบและปฏิบัติตาม

(๔) ให้มีการจำแนกประเภทของข้อมูลสารสนเทศ โดยจำแนกตามมูลค่าของข้อมูล ข้อกำหนดทางกฎหมาย ระดับชั้นความลับและความสำคัญต่อหน่วยงาน

(๕) มีการกำหนดและประกาศใช้ขั้นตอนที่เหมาะสมในการจำแนกประเภท และจัดการข้อมูลสารสนเทศ

ส่วนที่ ๕
การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (Access Control)

ข้อ ๑๖ การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ ต้องมีการกำหนดสิทธิ์การเข้าถึงของระบบสารสนเทศของราชวิทยาลัย รวมถึงอุปกรณ์ประมวลผลสารสนเทศแก่ผู้ที่มีความจำเป็นและได้รับอนุญาต

ข้อ ๑๗ การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ ให้ดำเนินการดังต่อไปนี้

(๑) จัดให้มีข้อกำหนดการควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้ข้อกำหนดดังกล่าว สอดคล้องกับความต้องการด้านการดำเนินงานหรือการให้บริการ และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ เพื่อควบคุมการให้สิทธิ์และการยกเลิกสิทธิ์ในการเข้าใช้งานระบบสารสนเทศใด ๆ ของราชวิทยาลัย

(๓) การกำหนดสิทธิ์ในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุม

(๔) ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศ ที่อยู่ภายใต้ความดูแลรับผิดชอบ

(๕) จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับข้อกำหนดการควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอปพลิเคชันเพื่อการดำเนินงาน

(๖) ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีขั้นตอนการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้

(๗) ให้ยุติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติ หากไม่มีการใช้งานเกินระยะเวลา ๕ นาที

(๘) จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอปพลิเคชันของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับข้อกำหนดการเข้าถึงที่ได้ระบุไว้

(๙) กำหนดแนวทางการจัดการด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ เช่น คอมพิวเตอร์แบบพกพา (Laptop Computer) หรือสมาร์ทโฟน (Smartphone) เป็นต้น

(๑๐) ให้ผู้ใช้งานปฏิบัติตามขั้นตอนเพื่อการใช้รหัสผ่านอย่างมั่นคงปลอดภัยตามข้อกำหนด

(๑๑) ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น

(๑๒) ให้มีการกำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล

(๑๓) มีการควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและการเชื่อมต่อผ่านคอมพิวเตอร์ สำหรับระบบสารสนเทศที่สามารถเข้าถึงจากระยะไกลได้ เช่น Remote diagnostic หรือConfiguration facility ของอุปกรณ์เครือข่ายคอมพิวเตอร์

(๑๔) มีการจัดกลุ่มตามประเภทของข้อมูลสารสนเทศที่ให้บริการ ระบบสารสนเทศ กลุ่มผู้ใช้งานโดยมีการแบ่งแยกบนเครือข่ายคอมพิวเตอร์อย่างเป็นสัดส่วน

(๑๕) มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของราชวิทยาลัย

(๑๖) กำหนดให้มีขั้นตอนการ Log-on เพื่อควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์

(๑๗) ให้จัดทำหรือจัดให้มีระบบการบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการใช้งานรหัสผ่านที่มีความมั่นคงปลอดภัย

ส่วนที่ ๖
การเข้ารหัสข้อมูล (Cryptography)

ข้อ ๑๘ กำหนดให้มีมาตรการเข้ารหัสข้อมูลโดยให้ใช้การเข้ารหัสข้อมูลอย่างเหมาะสม เพื่อป้องกันความลับ การปลอมแปลง หรือความถูกต้องของข้อมูลระบบสารสนเทศของราชวิทยาลัย

ข้อ ๑๙ การเข้ารหัสข้อมูล ให้ดำเนินการดังนี้

(๑) กำหนดมาตรการเข้ารหัสข้อมูล เป็นไปตามระดับชั้นความลับและความสำคัญของข้อมูลสารสนเทศ

(๒) ให้กำหนดความยาวของคีย์ (Key length) อัลกอริทึม (Algorithm) และใช้วิธีควบคุมการเข้ารหัสข้อมูลตามมาตรฐานที่ยอมรับในระดับสากล หรือเป็นที่ยอมรับในอุตสาหกรรมเทคโนโลยีสารสนเทศ โดยฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนด

(๓) ให้จัดทำการบริหารจัดการกุญแจสำหรับการเข้ารหัส (Key management) อย่างเหมาะสม โดยต้องประกอบไปด้วยฟังก์ชั่นต่าง ๆ ดังนี้

(๓.๑) การสร้างกุญแจเข้ารหัส (Key generation)

(๓.๒) การเปลี่ยนกุญแจเข้ารหัส (Key change)

(๓.๓) การนำกุญแจเข้ารหัสใหม่มาใช้ (Key Renewal)

ส่วนที่ ๗
การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
(Physical and environmental security)

ข้อ ๒๐ การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม เพื่อป้องกันการเข้าถึงทางกายภาพของศูนย์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อป้องกันการสูญหาย การเสียหาย หรือป้องกันอันตรายต่อทรัพย์สินและป้องกันการหยุดชะงักต่อการดำเนินงานของราชวิทยาลัย

ข้อ ๒๑ การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ให้ดำเนินการดังต่อไปนี้

(๑) ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ

(๒) มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอก รวมไปถึงภัยที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

(๓) จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ

(๔) มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities)

(๕) มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๖) มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันพื้นที่หรือสถานที่ปฏิบัติงาน หรืออุปกรณ์สารสนเทศต่าง ๆ

(๗) ไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของหน่วยงานหากมิได้รับอนุญาต

ส่วนที่ ๘
ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

ข้อ ๒๒ ให้กำหนดมาตรการความมั่นคงปลอดภัยสำหรับการดำเนินงานเพื่อให้การปฏิบัติงาน การดำเนินงานกับระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศของราชวิทยาลัยเป็นไปอย่างถูกต้อง และมั่นคงปลอดภัย

ข้อ ๒๓ มาตรการความมั่นคงปลอดภัยสำหรับการดำเนินงาน มีดังต่อไปนี้

(๑) ให้มีการจัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับสารสนเทศที่สำคัญของหน่วยงาน เพื่อป้องกันการปฏิบัติงานด้านสารสนเทศผิดพลาด

(๒) ให้มีการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

(๓) ให้มีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงระบบสารสนเทศ

(๔) ให้มีการตรวจสอบ และติดตามทรัพยากรของระบบสารสนเทศ

(๕) ให้แยกระบบที่ใช้สำหรับการพัฒนาการทดสอบและระบบการใช้งานจริงออกจากกัน

(๖) ให้กำหนดมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware)

(๗) ให้ติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและโปรแกรมที่เกี่ยวข้องก่อนเชื่อมต่ออินเทอร์เน็ต

(๘) ให้เครื่องคอมพิวเตอร์แม่ข่ายให้บริการต้องดำเนินการสำรองข้อมูล ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

(๙) ให้จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล

(๑๐) ให้ควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง

(๑๑) ให้จัดเก็บข้อมูลบันทึกกิจกรรมของผู้ใช้งาน เพื่อใช้ติดตามกรณีเกิดเหตุความมั่นคงปลอดภัย

(๑๒) ให้เข้าถึงข้อมูลบันทึกกิจกรรมของผู้ใช้งาน ได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๑๓) ให้เครื่องแม่ข่ายทุกเครื่องต้องตั้งเวลาให้ตรงกัน

(๑๔) ให้ติดตั้งเฉพาะซอฟต์แวร์ที่ได้รับการอนุมัติจากราชวิทยาลัยเท่านั้น

(๑๕) ให้ทำการอัพเดตซอฟต์แวร์และอุดช่องโหว่ของซอฟต์แวร์อย่างสม่ำเสมอ

(๑๖) ให้ติดตามข้อมูลทางด้านเทคนิคของช่องโหว่อย่างสม่ำเสมอ

ส่วนที่ ๙
การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (Communication security)

ข้อ ๒๔ กำหนดให้มีการบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศเพื่อให้อุปกรณ์สารสนเทศในเครือข่ายมีความพร้อม และปลอดภัยจากความเสี่ยงจากการถูกโจมตีหรือเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๒๕ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบ มีดังต่อไปนี้

(๑) มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้ผู้ปฏิบัติงานในราชวิทยาลัยสามารถนำไปปฏิบัติได้

(๒) มีการกำกับดูแลบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

(๓) มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการ แก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

(๔) จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุงหรือที่มีเวอร์ชั่นใหม่ และให้มีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ

(๕) มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์

(๖) มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามข้อกำหนดการสำรองข้อมูลที่หน่วยงานประกาศใช้

(๗) มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอปพลิเคชันที่ติดตั้งบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศ ที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว

(๘) มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการ ในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ ไม่ว่าเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยังผู้ให้บริการภายนอก

(๙) กำหนดให้มีขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

(๑๐) จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

(๑๑) กำหนดให้มีขั้นตอนปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือ แลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ

(๑๒) จัดให้มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต

(๑๓) มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

(๑๔) ข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลง โดยมิได้รับอนุญาต และรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

(๑๕) มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งาน (User) และผู้ดูแลระบบ (System administrator) เพื่อประโยชน์ในการสืบสวน สอบสวน เกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยต่าง ๆ และมีการวิเคราะห์ Audit log ดังกล่าวอย่างสม่ำเสมอ

(๑๖) มีการป้องกันการเข้าถึงหรือเปลี่ยนแปลงข้อมูล Audit log โดยมิได้รับอนุญาต

(๑๗) มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบเครือข่ายคอมพิวเตอร์ (Network Monitoring)

(๑๘) มีการจัดการควบคุมการเปลี่ยนแปลงของระบบเครือข่ายคอมพิวเตอร์

(๑๙) มีการติดตามผลการใช้งานทรัพยากรระบบเครือข่ายคอมพิวเตอร์ และวางแผนด้านทรัพยากรระบบเครือข่ายคอมพิวเตอร์ให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม

(๒๐) มีขั้นตอนการปฏิบัติงานในการจัดการและจัดเก็บข้อมูลสารสนเทศเพื่อมิให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ผิดประเภท

(๒๑) ระบบเวลาของระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ต้องมีการตั้งค่าเวลาที่สอดคล้องกัน (Time synchronization) จากแหล่งเวลาที่เชื่อถือได้

ส่วนที่ ๑๐
การจัดหา การพัฒนา และการบำรุงรักษาระบบ
(System acquisition, development and maintenance)

ข้อ ๒๖ กำหนดให้มีมาตรการในการจัดหา การพัฒนาและการบำรุงรักษาระบบเพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบ ตลอดวงจรของการพัฒนาและบำรุงรักษาระบบสารสนเทศของราชวิทยาลัย

ข้อ ๒๗ การจัดหา การพัฒนาและการบำรุงรักษาระบบ ให้ดำเนินการดังต่อไปนี้

(๑) ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย

(๒) ให้มีการดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างพัฒนาซอฟต์แวร์

(๓) ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอปพลิเคชันก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม

(๔) ให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอปพลิเคชัน เพื่อให้มั่นใจได้ว่า ข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม

(๕) จัดให้มีแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของราชวิทยาลัย

(๖) ให้เลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล

(๗) ให้มีการจำกัดการเข้าถึงรหัสต้นทาง (Source code) ของโปรแกรม

(๘) ให้มีการกำหนดค่าขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติงานระบบสารสนเทศใหม่ที่จะเกิดขึ้นการสร้าง การติดตั้ง หรือการใช้งานระบบสารสนเทศใหม่ ในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่อย่างปลอดภัย

(๙) หากมีการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการคอมพิวเตอร์ ให้มีการตรวจสอบทบทวนการทำงานของโปรแกรมที่มีความสำคัญ และทดสอบการใช้งานเพื่อให้มั่นใจว่าผลของการเปลี่ยนแปลงดังกล่าวจะไม่ส่งผลกระทบใดๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของราชวิทยาลัย

ส่วนที่ ๑๑
ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

ข้อ ๒๘ กำหนดให้มีการควบคุมการปฏิบัติงานของผู้ให้บริการภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยกำหนดแนวทางการคัดเลือก การควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก เพื่อลดความเสี่ยงในการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น

ข้อ ๒๙ การควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก ให้ดำเนินการดังนี้

(๑) ให้มีการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของราชวิทยาลัยเมื่อมีความจำเป็น ที่ต้องให้ผู้ให้บริการภายนอกเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศของราชวิทยาลัย

(๒) ให้การติดตาม ทบทวน และตรวจประเมินการบริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ (Monitoring and review of supplier services)

(๓) หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญจะต้องจัดทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

ส่วนที่ ๑๒
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
(Information security incident management)

ข้อ ๓๐ กำหนดให้มีมาตรการในการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีวิธีการที่เหมาะสม และมีประสิทธิภาพ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ และจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

ข้อ ๓๑ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการดังนี้

(๑) กำหนดขั้นตอนและวิธีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดผ่านช่องทางการบริหารจัดการที่เหมาะสม มีความรวดเร็ว และมีประสิทธิภาพ

(๒) กำหนดขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนการปฏิบัติงาน เพื่อตอบสนองต่อ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล

ส่วนที่ ๑๓
การบริหารความต่อเนื่องในการดำเนินงาน
(Business continuity management)

ข้อ ๓๒ กำหนดให้มีการบริหารความต่อเนื่องในการดำเนินงาน เพื่อป้องกันการหยุดชะงักในการดำเนินงานที่เป็นผลมาจากวิกฤตหรือภัยพิบัติ และการบริหารจัดการด้านการบริการหรือการดำเนินงานของราชวิทยาลัยเพื่อให้มีความต่อเนื่อง

ข้อ ๓๓ การบริหารความต่อเนื่องในการดำเนินงาน ให้ดำเนินการดังต่อไปนี้

(๑) ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ หลังเกิดเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ ภายในระยะเวลาที่กำหนดไว้

(๒) ให้มีแผนบริหารด้านความมั่นคงปลอดภัยด้านสารสนเทศ ที่ได้รับการอนุมัติจากคณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดให้เป็นส่วนหนึ่งของแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน

(๓) กำหนดให้มีกรอบงานหลักสำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน เพื่อให้การพัฒนาแผนต่าง ๆ เป็นไปในทิศทางเดียวกัน รวมทั้งสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ตลอดจนมีการจัดลำดับความสำคัญก่อนหลังในการทดสอบและการดูแล

(๔) ให้มีการทดสอบและปรับปรุงแผนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าแผนดังกล่าวเป็นปัจจุบันและมีประสิทธิผลอยู่เสมอ

ส่วนที่ ๑๔
การติดตาม ตรวจสอบ และประเมินผลการดำเนินงาน
ตามนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ (Compliance)

ข้อ ๓๔ ให้มีการติดตาม ตรวจสอบ และประเมินผลการดำเนินงานตามนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และที่เป็นความต้องการด้านความมั่นคงปลอดภัย

ข้อ ๓๕ การติดตาม ตรวจสอบ และประเมินผลการดำเนินงานตามนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ ให้ดำเนินการดังต่อไปนี้

(๑) ให้มีการวางแผนการตรวจสอบในการดำเนินงานของระบบสารสนเทศ ให้มีความสอดคล้องตามกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ห้ามใช้งานระบบสารสนเทศผิดวัตถุประสงค์ ตามข้อกำหนดหรือสัญญาการให้บริการ

(๓) ผู้ใช้งานต้องดูแลให้งานระบบสารสนเทศอยู่ในขอบเขตความรับผิดชอบให้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดต่าง ๆ ของราชวิทยาลัย

(๔) จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและข้อกำหนดต่าง ๆ ของราชวิทยาลัย

หมวดที่ ๓
การขอยกเว้น

ข้อ ๓๖ หากมีความจำเป็นที่หรือข้อจำกัดด้านเทคโนโลยีที่มีอยู่ทำให้ไม่สามารถปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ได้ ให้คณะกรรมการพิจารณาและนำเสนอขออนุมัติการไม่ปฏิบัติตามมาตรฐานในส่วนดังกล่าวต่อเลขาธิการ ทั้งนี้ผู้ร้องขอการยกเว้น จะต้องดำเนินการเพื่อนำเสนอต่อคณะกรรมการ ดังนี้

(๑) วิเคราะห์ความเสี่ยงหรือผลกระทบ ที่อาจเกิดขึ้นต่อการไม่ปฏิบัติตาม รวมทั้งจัดทำเอกสารที่ระบุหลักการและเหตุผลหรือเอกสารหลักฐานที่สนับสนุน การตัดสินใจไม่ปฏิบัติตามมาตรฐานฉบับนี้

(๒) พิจารณานำเสนอการควบคุมทดแทน (Compensated Control) เพื่อลดความเสี่ยงที่อาจเกิดขึ้น

ประกาศ ณ วันที่ ๒๒ เดือน ธันวาคม พ.ศ. ๒๕๖๓

(ศาสตราจารย์ นายแพทย์นิธิ มหานนท์)
เลขาธิการราชวิทยาลัยจุฬาภรณ์