ประกาศราชวิทยาลัยจุฬาภรณ์
เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓

.....

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศราชวิทยาลัยจุฬาภรณ์ กำหนดขึ้นมาภายใต้กรอบนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้ผู้ปฏิบัติงานในราชวิทยาลัยจุฬาภรณ์ และผู้ที่เกี่ยวข้อง นำไปใช้เป็นแนวทางการปฏิบัติสำหรับผู้ใช้งานและผู้ให้บริการ เพื่อให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

อาศัยอำนาจตามความในมาตรา ๒๒ (๒) แห่งพระราชบัญญัติราชวิทยาลัยจุฬาภรณ์ พ.ศ ๒๕๕๙ และที่แก้ไขเพิ่มเติม ประกอบมติที่ประชุมคณะกรรมการนโยบายและบริหารจัดการด้านเทคโนโลยีสารสนเทศ ครั้งที่ ๓/๒๕๖๓ เมื่อวันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๓ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศราชวิทยาลัยจุฬาภรณ์ เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓ ”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับนับแต่วันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“เลขาธิการ” หมายความว่า เลขาธิการราชวิทยาลัยจุฬาภรณ์

“คณะผู้บริหาร” หมายความว่า ผู้บริหารระดับ ๑ – ๔ ตามข้อบังคับราชวิทยาลัยจุฬาภรณ์ ว่าด้วยการบริหารงานบุคคลผู้ปฏิบัติงานในราชวิทยาลัย

“ผู้ปฏิบัติงานในราชวิทยาลัย” หมายความว่า พนักงานและลูกจ้างของราชวิทยาลัยจุฬาภรณ์

“ผู้ดูแลระบบ” หมายความว่า เจ้าหน้าที่หรือหน่วยงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

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

“ผู้ให้บริการ”หมายความว่า หน่วยงานที่ให้บริการระบบสารสนเทศ ซึ่งหมายรวมถึงฝ่ายเทคโนโลยีสารสนเทศราชวิทยาลัยจุฬาภรณ์ หน่วยงานภายในที่ให้บริการระบบสารสนเทศ

“ผู้ให้บริการภายนอก”หมายความว่า หน่วยงานภายนอกที่ให้บริการระบบสารสนเทศ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า ผู้มีอำนาจหน้าที่ตัดสินใจ ในการรวบรวม จัดเก็บและใช้ รวมถึงเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า ผู้ที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ ผู้ซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“การรักษาความมั่นคงปลอดภัย” หมายความว่า การทำให้ระบบสารสนเทศมีความมั่นคงและปลอดภัย พ้นจากภัยคุกคาม ธำรงไว้ซึ่งลักษณะสำคัญ ๓ ประการ คือ ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

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

ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“สารสนเทศ” (Information)” หมายความว่า ข้อมูลที่ได้ผ่านการประมวลผลหรือวิเคราะห์สรุปผลด้วยวิธีการต่าง ๆ แล้วเก็บรวบรวมไว้ เพื่อนำมาใช้ประโยชน์ตามต้องการ

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลระหว่างระบบสารสนเทศต่าง ๆ ของราชวิทยาลัยจุฬาภรณ์ ได้ เช่น

(๑) ระบบเครือข่ายอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่มีขอบเขตในราชวิทยาลัยจุฬาภรณ์เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ เข้าด้วยกันเครือนี้ข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายใน เครือข่ายนี้บริหารจัดการโดยราชวิทยาลัยจุฬาภรณ์ ระบบนี้ประกอบไปด้วยเครือข่ายแบบใช้สาย (LAN) และเครือข่ายแบบไร้สาย (Wireless LAN)

(๒) ระบบเครือข่ายอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ภายนอกที่เชื่อมต่อกับเครือข่ายอินเตอร์เน็ตทั่วโลกซึ่งมีการเชื่อมต่อระบบเครือข่ายอินทราเน็ตหรือมีการเข้าใช้งานโดยหน่วยงานหรือผู้ปฏิบัติงานในราชวิทยาลัย

“ทรัพย์สินสารสนเทศ” หมายความว่า สารสนเทศที่มีคุณค่าสำหรับราชวิทยาลัยจุฬาภรณ์ อันได้แก่

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์และระบบงานสารสนเทศ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา อุปกรณ์คอมพิวเตอร์ สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ และอุปกรณ์ประมวลผลอื่นใด

(๒) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

“บัญชีผู้ใช้งาน (user account)” หมายความว่า ชุดอักษรหรือตัวเลขที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของ เพื่อใช้ในการอ้างถึงเพื่อเข้าสู่ระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์ บัญชีผู้ใช้งานจะถูกสร้างโดยผู้ดูแลระบบที่ได้รับมอบหมาย บัญชีผู้ใช้งานประกอบไปด้วยสองส่วนได้แก่ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

"เครื่องคอมพิวเตอร์” หมายความว่า เครื่องคอมพิวเตอร์ตั้งโต๊ะ (Desktop) ที่จัดหาและติดตั้งโดยผู้ให้บริการ ระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

“เครื่องคอมพิวเตอร์พกพา” หมายความว่า เครื่องคอมพิวเตอร์ที่สามารถพกพาได้ เช่น โน้ตบุ๊กคอมพิวเตอร์ (Notebook computer) แล็ปท็อป (Laptop) แท็บเล็ต (Tablet) ที่จัดหาและติดตั้งโดยผู้ให้บริการของราชวิทยาลัยจุฬาภรณ์

“เครื่องพิมพ์” หมายความว่า อุปกรณ์เครื่องพิมพ์ที่รับสัญญาณตรงจากเครื่องคอมพิวเตอร์เพื่อพิมพ์งานออกมาเป็นข้อความ ภาพ ลงบนกระดาษหรือวัตถุอื่นในประเภทเดียวกัน

“เครื่องโทรศัพท์” หมายความว่า เครื่องโทรศัพท์ ที่จัดหาและติดตั้งโดย ผู้ให้บริการของราชวิทยาลัยจุฬาภรณ์

“โทรศัพท์เคลื่อนที่” หมายความว่า เครื่องโทรศัพท์เคลื่อนที่ ที่จัดหาและติดตั้งโดยผู้ให้บริการของราชวิทยาลัยจุฬาภรณ์

“เครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอก (BYOD)” หมายความว่าเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ที่ไม่ได้จัดหาโดยผู้ให้บริการของราชวิทยาลัยจุฬาภรณ์ ซึ่งผู้ปฏิบัติงานในราชวิทยาลัย หรือบุคลากรภายนอกมีความจำเป็นต้องใช้ในการปฏิบัติงาน

“การเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก” หมายความว่า การเข้าใช้ทรัพยากรสารสนเทศที่ อยู่ในระบบเครือข่ายภายในราชวิทยาลัยจุฬาภรณ์ จากเครือข่ายภายนอกราชวิทยาลัยจุฬาภรณ์

“ระบบสารสนเทศทางการแพทย์” หมายความว่า ระบบสารสนเทศที่ใช้ในการสนับสนุนการบริการทางการแพทย์และพยาบาลที่ดำเนินการโดยโรงพยาบาลจุฬาภรณ์ ทั้งนี้รวมถึงระบบอุปกรณ์เครื่องมือการ

วินิจฉัย วิเคราะห์และรักษา (Biomedical devices)

“ระบบสารสนเทศการศึกษา” หมายความว่า ระบบทะเบียนนักศึกษา ระบบบริหารจัดการการศึกษา ระบบประกันคุณภาพการศึกษา ระบบห้องสมุด ระบบฐานข้อมูลเพื่องานวิจัย

“ระบบสารสนเทศเพื่อการวิจัยและพัฒนา” หมายความว่า ระบบคอมพิวเตอร์สมรรถนะสูง ระบบโครงสร้างพื้นฐานสำหรับงานปัญญาประดิษฐ์เพื่อการวิจัยและพัฒนา

“การโจมตีทางไซเบอร์” หมายความว่า การกระทำที่พยายามสร้างความเสียหายหรือทำลายระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ซึ่งการโจมตีนี้อาจจะส่งผลต่อการเปิดเผยข้อมูลสำคัญ หรือถูกนำมาใช้งานโดยผู้ที่ไม่ได้รับอนุญาต

“E-Mail” หมายความว่า จดหมายอิเล็กทรอนิกส์ หรือ ไปรษณีย์อิเล็กทรอนิกส์

“Social Media” หมายความว่า สังคมออนไลน์ที่มีผู้ใช้เป็นผู้สื่อสาร หรือเขียนเล่า เนื้อหาเรื่องราว ประสบการณ์ บทความ รูปภาพ และวิดีโอ ที่ผู้ใช้เขียนขึ้นเอง ทำขึ้นเอง

“Instant Messaging” หมายความว่า โปรแกรมประยุกต์ส่งข้อความโต้ตอบแบบทันที

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ได้แก่ ข้อมูลผู้ป่วย ข้อมูลญาติผู้ป่วย ข้อมูลเจ้าหน้าที่ ข้อมูลนักศึกษาและผู้สมัครศึกษา แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์” หมายความว่า สถานที่เก็บเครื่องแม่ข่ายและระบบการเชื่อมต่อ Internet ศูนย์คอมพิวเตอร์หลักกำหนดให้มีอย่างน้อยสองที่ และต้องเชื่อมต่อถึงกันผ่านระบบการสื่อสารแบบปลอดภัย

“เครื่องมือทางการแพทย์” หมายความว่า อุปกรณ์ที่ใช้ในการตรวจหรือรักษาผู้มารับบริการทางการแพทย์ที่โรงพยาบาลจุฬาภรณ์ โดยอุปกรณ์นี้ต้องเชื่อมต่อกับระบบเครือข่ายการให้บริการทางการแพทย์ของโรงพยาบาลจุฬาภรณ์

ข้อ ๔ ให้เลขาธิการเป็นผู้รักษาการตามประกาศนี้ ในกรณีที่มีปัญหาหรือข้อสงสัยเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้เลขาธิการเป็นผู้มีอำนาจวินิจฉัยและให้ถือเป็นที่สุด

หมวด ๑
ความทั่วไป

ข้อ ๕ วัตถุประสงค์ของประกาศแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีดังนี้

(๑) เพื่อให้ผู้ปฏิบัติงานในราชวิทยาลัยทุกระดับ ปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อใช้บริการ หรือให้บริการงานระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

(๒) เพื่อให้เกิดความเชื่อมั่นในการใช้งานระบบงานสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์ของราชวิทยาลัยจุฬาภรณ์

(๓) เพื่อให้หน่วยงานต่างๆ ผู้ปฏิบัติงานในราชวิทยาลัย และเจ้าหน้าที่ที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศได้ตระหนักถึงมาตรการและแนวทางที่จะต้องปฏิบัติ เมื่อใช้งานระบบสารสนเทศของ ราชวิทยาลัยจุฬาภรณ์

ข้อ ๖ ให้เผยแพร่แนวปฏิบัติฉบับนี้ผ่านช่องทางต่างๆ ได้แก่ อินทราเน็ต อีเมล และเวปไซต์ราชวิทยาลัยจุฬาภรณ์ โดยฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการทบทวนแนวปฏิบัติการฉบับนี้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงให้เหมาะสมกับการปฏิบัติงานให้เกิดความมั่นคงปลอดภัย

ข้อ ๗ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีดังต่อไปนี้

(๑) แนวปฏิบัติการใช้บัญชีผู้ใช้งานระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

(๒) แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา เครื่องพิมพ์ เครื่องโทรศัพท์ และโทรศัพท์เคลื่อนที่ของราชวิทยาลัยจุฬาภรณ์

(๓) แนวปฏิบัติการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกเข้ามาใช้ในพื้นที่ราชวิทยาลัยจุฬาภรณ์

(๔) แนวปฏิบัติในการเข้าใช้ระบบเครือข่ายภายในราชวิทยาลัยจุฬาภรณ์

(๕) แนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก

(๖) แนวปฏิบัติการใช้งานระบบสารสนเทศทางการแพทย์

(๗) แนวปฏิบัติการใช้งานระบบสารสนเทศการศึกษา

(๘) แนวปฏิบัติการใช้งานระบบสารสนเทศเพื่อการวิจัยและพัฒนา

(๙) แนวปฏิบัติการใช้งาน E-Mail, Social Media และ Instant Messaging

(๑๐) แนวปฏิบัติตาม กฎหมายคุ้มครองข้อมูลส่วนบุคคล ของระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

(๑๑) แนวปฏิบัติในการควบคุมทรัพย์สินสารสนเทศ

(๑๒) แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์

(๑๓) แนวปฏิบัติการรักษาความมั่นคงปลอดภัยศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์

(๑๔) แนวปฏิบัติการป้องกันการโจมตีทางไซเบอร์

(๑๕) แนวปฏิบัติการจัดทำการสำรองข้อมูลระบบสารสนเทศ

(๑๖) แนวปฏิบัติการเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

(๑๗) แนวปฏิบัติการจัดหา การพัฒนา และการบำรุงรักษาระบบ

(๑๘) แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเครื่องมือทางการแพทย์

(๑๙) แนวปฏิบัติการรักษาความมั่นคงปลอดภัยอุปกรณ์ Internet of Things (IoT), กล้องวงจรปิด และระบบควบคุมอัตโนมัติ

(๒๐) แนวปฏิบัติการกำกับดูแลและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ

หมวด ๒
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ส่วนที่ ๑
แนวปฏิบัติการใช้บัญชีผู้ใช้งานระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

ข้อ ๘ บัญชีผู้ใช้งานของราชวิทยาลัยจุฬาภรณ์ แบ่งออกเป็น ๓ ประเภท คือ

(๑) บัญชีผู้ใช้งานสำหรับผู้ปฏิบัติงานในราชวิทยาลัย

(๒) บัญชีผู้ใช้งานสำหรับนักศึกษาของราชวิทยาลัยจุฬาภรณ์

(๓) บัญชีผู้ใช้งานชั่วคราว สำหรับบุคคลภายนอกที่มีความจำเป็นต้องเข้าถึงระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

ข้อ ๙ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งานระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์ทุกคน และผู้ให้บริการ

ข้อ ๑๐ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) บัญชีผู้ใช้งานสำหรับผู้ปฏิบัติงานในราชวิทยาลัยและบัญชีนักศึกษาราชวิทยาลัยจุฬาภรณ์จะถูกสร้างเมื่อมีการแจ้งและอนุมัติจากหน่วยงานที่ได้รับมอบหมายเท่านั้น

(๒) บัญชีผู้ใช้งานชั่วคราว สำหรับบุคคลภายนอกจะถูกสร้างก็ต่อเมื่อได้รับการอนุมัติจากผู้บริหารสูงสุดของหน่วยงานนั้น และจะต้องกำหนดวันสิ้นสุดการใช้งาน

(๓) บัญชีผู้ใช้งานจะต้องอนุมัติให้ผู้ใช้งานเข้าถึงระบบสารสนเทศเท่าที่จำเป็นเท่านั้น (Least Privilege) เพื่อให้สามารถบรรลุภารกิจของหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

(๔) มีหน้าที่ต้องเก็บรักษารหัสผ่านให้เป็นความลับและไม่เปิดเผยกับบุคคลอื่น

(๕) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทันที กรณีดังต่อไปนี้

๕.๑ ลืมรหัสผ่าน

๕.๒ เมื่อใช้รหัสผ่านเริ่มต้น (default password)

๕.๓ เมื่อเข้าใช้งานครั้งแรก หลังจากได้รับรหัสผ่านชั่วคราว (Temporary password)

๕.๔ เมื่อสงสัยว่ามีบุคคลอื่นทราบรหัสผ่าน

(๖) ผู้ใช้งานห้ามให้ข้อมูลบัญชีผู้ใช้งานของตนแก่บุคคลอื่น หรือให้บุคคลอื่นใช้งานแทนตนเอง

(๗) ผู้ใช้งานจะต้องใช้บัญชีผู้ใช้งานของตนเองเท่านั้น ในการเข้าถึงระบบสารสนเทศ

(๘) ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการกระทำใด ๆ ที่ผ่านบัญชีผู้ใช้งานของตนทั้งหมดไม่สามารถปฏิเสธความรับผิดชอบต่อการใช้งานได้

(๙) ผู้ใช้งานห้ามเข้าถึง หรือใช้งานระบบระบบสารสนเทศที่ไม่ได้รับอนุญาต

(๑๐) ผู้บริหารของหน่วยงานมีหน้าที่รับผิดชอบ แจ้งต่อผู้ให้บริการหรือผู้ดูแลระบบให้ดำเนินการยกเลิกบัญชีของบุคลากรและเจ้าหน้าที่ในหน่วยงาน เมื่อไม่มีความจำเป็นต้องใช้งาน

ข้อ ๑๑ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) ผู้ให้บริการหรือผู้ดูแลระบบที่ได้รับมอบหมาย มีหน้าที่สร้างบัญชีผู้ใช้งาน และกำหนดสิทธิหรือเปลี่ยนแปลงสิทธิตามที่ได้รับอนุมัติเท่านั้น

(๒) มีหน้าที่ระงับบัญชีผู้ใช้งานทันที หากพบว่ามีการเข้าใช้งานที่ผิดปกติหรือส่งผลกระทบต่อระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์

(๓) มีหน้าที่ยกเลิกบัญชีผู้ใช้งาน เมื่อได้รับแจ้งในกรณี ดังต่อไปนี้

๓.๑ พ้นสภาพการเป็นผู้ปฏิบัติงานในราชวิทยาลัย

๓.๒ พ้นสภาพการเป็นนักศึกษา

๓.๓ เปลี่ยนแปลงความรับผิดชอบของหน้าที่ และไม่มีความจำเป็นต้องเข้าถึง

ส่วนที่ ๒
แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา เครื่องพิมพ์เครื่องโทรศัพท์ และโทรศัพท์เคลื่อนที่ของราชวิทยาลัยจุฬาภรณ์

ข้อ ๑๒ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการและส่วนงานที่เกี่ยวข้อง

ข้อ ๑๓ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา เครื่องพิมพ์ เครื่องโทรศัพท์และโทรศัพท์เคลื่อนที่ มีหน้าที่ดูแลรักษาอุปกรณ์ที่ได้รับ หากมีการสูญหาย เสียหาย ชำรุด ผู้ใช้งานจะต้องรายงานต่อผู้ให้บริการทันที

(๒) ผู้ใช้งานไม่ได้รับอนุญาตในการเคลื่อนที่เครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องโทรศัพท์ เครื่องพิมพ์ และทรัพย์สินสารสนเทศโดยพลการ หากประสงค์จะดำเนินการดังกล่าวผู้ใช้งานต้องแจ้งผู้ให้บริการทราบและเป็นผู้ดำเนินการ

(๓) ผู้ใช้งานมีหน้าที่แจ้งส่งคืนเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา เครื่องโทรศัพท์ และโทรศัพท์เคลื่อนที่ รวมถึงทรัพย์สินสารสนเทศที่อยู่ในความครอบครองต่อผู้ให้บริการ ก่อนวันพ้นสภาพการเป็นผู้ปฏิบัติงานในราชวิทยาลัย

(๔) ผู้ใช้งานมีหน้าที่ Lock screen เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพาทันที เมื่อไม่มีการใช้งาน

(๕) ผู้ใช้งานไม่ได้รับอนุญาตให้ต่อเชื่อมอุปกรณ์บันทึกข้อมูล (Removable media) ทุกชนิดหากมีความจำเป็นต้องใช้งานต้องได้รับการเห็นชอบจากผู้บริหารสูงสุดของหน่วยงาน และได้รับการอนุมัติจากผู้บริหารของฝ่ายเทคโนโลยีสารสนเทศ ของราชวิทยาลัยจุฬาภรณ์

(๖) ผู้ใช้งานไม่ได้รับอนุญาตให้เปิดใช้การแชร์ข้อมูล (File sharing) ระหว่างเครื่องคอมพิวเตอร์

(๗) ผู้ใช้งานห้ามใช้เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา เข้าถึงเว็บไซต์ละเมิดลิขสิทธิ์ ละเมิดทรัพย์สินทางปัญญา ข้อมูลอนาจาร หรือเล่นเกมส์

(๘) เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา จะต้องติดตั้งซอฟต์แวร์ลิขสิทธิ์ตามมาตรฐานที่กำหนดเท่านั้นหากผู้ใช้งานมีความจำเป็นต้องใช้ซอฟต์แวร์อื่นๆเพิ่มเติมนั้น จะต้องปฏิบัติดังต่อไปนี้

๘.๑ เป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง

๘.๒ ให้ผู้ให้บริการตรวจเช็คความเสี่ยงด้านความปลอดภัยของซอฟต์แวร์นั้น

๘.๓ ได้รับความเห็นชอบจากผู้บริหารสูงสุดในหน่วยงานของผู้ใช้งาน

ข้อ ๑๔ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่ในการติดตั้ง กำหนดค่าตามมาตรฐาน(Standard configuration) ที่กำหนดโดยฝ่ายเทคโนโลยีสารสนเทศของราชวิทยาลัยจุฬาภรณ์

(๒) มีหน้าที่จะต้องติดตั้งโปรแกรมป้องกันไวรัส และต้องอัพเดตฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ

(๓) กรณีตรวจพบการใช้งานที่ผิดปกติ เช่น เครื่องติดไวรัส มัลแวร์ สแปมเมล์ หรือตรวจพบการติดตั้งโปรแกรมที่นอกเหนือจากการที่ติดตั้งจากผู้ให้บริการ ผู้ให้บริการขอสงวนสิทธิ์ในการเข้าตรวจเช็ค หรือระงับการใช้งานจนกว่าจะแก้ไขเป็นที่เรียบร้อย

ส่วนที่ ๓
แนวปฏิบัติการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกเข้ามาใช้ในพื้นที่ราชวิทยาลัยจุฬาภรณ์

ข้อ ๑๕ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๑๖ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานที่มีความจำเป็นต้องนำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกมาใช้งาน หรือเชื่อมต่อระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์ ต้องได้รับการเห็นชอบจากผู้บริหารสูงสุดของหน่วยงานและได้รับการอนุมัติจากผู้บริหารสูงสุดด้านเทคโนโลยีสารสนเทศของราชวิทยาลัยจุฬาภรณ์

(๒) เครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอก ที่ได้รับการอนุมัติการใช้งานจากผู้บริหารสูงสุดของหน่วยงานแล้ว ผู้ใช้งานจะต้องแจ้งลงทะเบียนหมายเลขเครือข่ายประจำเครื่อง (Mac Address) ที่ผู้ให้บริการ ก่อนเชื่อมต่อระบบเครือข่าย

(๓) เครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกที่จะนำมาใช้งาน หรือเชื่อมต่อระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์ จะต้องติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องเท่านั้น

(๔) เครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกที่จะนำมาใช้งาน หรือเชื่อมต่อระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์ จะต้องติดตั้งซอฟต์แวร์ในการป้องกัน เช่น ต้องติดตั้ง Antivirus, ติดตั้ง Endpoint security

ข้อ ๑๗ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่จัดทำทะเบียนหมายเลขเครือข่ายประจำเครื่อง (Mac Address) ของเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกเข้ามาใช้งาน

(๒) มีหน้าที่ดำเนินการหยุดการเข้าถึงระบบเครือข่ายและระบบสารสนเทศทันที หากพบว่ามีการติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ และแจ้งผู้รับผิดชอบให้ดำเนินการแก้ไขให้แล้วเสร็จ

(๓) มีหน้าที่ตรวจเช็ค หรือระงับการใช้ทันที ในกรณีตรวจพบการใช้งานที่ผิดปกติ เช่น เครื่องติดไวรัส การเข้าถึงโปรแกรมหรือระบบที่ไม่ได้รับอนุญาต

ส่วนที่ ๔
แนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์

ข้อ ๑๘ ระบบเครือข่ายภายในราชวิทยาลัยจุฬาภรณ์ ประกอบไปด้วย

(๑) ระบบเครือข่ายอินทราเน็ต (Intranet)

(๒) ระบบเครือข่ายอินเตอร์เน็ต (Internet)

ข้อ ๑๙ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๒๐ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานเพื่อเข้าถึงระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์ จะต้องใช้บัญชีผู้ใช้งานของตนเองที่ได้รับอนุญาตเท่านั้น

(๒) ผู้ใช้งานจะต้องเข้าถึงระบบเครือข่ายภายในราชวิทยาลัยจุฬาภรณ์ เท่าที่ได้รับอนุญาต

เท่านั้น

(๓) ผู้ใช้งานห้ามใช้งานระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์ เข้าถึงเว็บไซต์ละเมิดลิขสิทธิ์ ละเมิดทรัพย์สินทางปัญญา ข้อมูลอนาจาร ดาวน์โหลดโปรแกรมผิดลิขสิทธิ์ เล่นเกมส์ หรือใช้งาน BitTorrent

(๔) ผู้ใช้งานห้ามติดตั้งหรือใช้งานโปรแกรมประเภท Remote Access เช่น Team viewer ไว้บนเครื่องคอมพิวเตอร์ทั้งของราชวิทยาลัยจุฬาภรณ์และเครื่องคอมพิวเตอร์ส่วนตัว ในการเข้าใช้งานระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์

(๕) ผู้ใช้งานที่ต้องการใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ต้องได้รับการอนุมัติการใช้งานจากผู้บริหารสูงสุดของหน่วยงานเท่านั้น

(๖) ผู้ใช้งานมีหน้าที่จะต้องแจ้งลงทะเบียนหมายเลขเครือข่ายประจำเครื่อง (Mac Address) ต่อผู้ ให้บริการ

ข้อ ๒๑ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่เฝ้าระวังการใช้งานระบบเครือข่าย (Network monitoring)

(๒) จัดทำทะเบียนและหมายเลขเครือข่ายประจำเครื่อง (Mac Address)

(๓) มีหน้าที่ตรวจเช็ค หรือระงับการใช้ทันที ในกรณีตรวจพบการใช้งานที่ผิดปกติ

(๔) มีหน้าที่เก็บข้อมูลการจราจรคอมพิวเตอร์ไว้อย่างน้อย ๙๐ วัน

ส่วนที่ ๕
แนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก

ข้อ ๒๒ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๒๓ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานที่จะใช้งานระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก จะต้องได้รับการเห็นชอบจากผู้บริหารสูงสุดของหน่วยงาน และต้องได้รับอนุมัติจากผู้บริหารสูงสุดด้านเทคโนโลยีสารสนเทศ

(๒) ผู้ใช้งานจะต้องใช้โปรแกรม VPN Client ตามที่ผู้ให้บริการกำหนดเท่านั้น เพื่อเข้าถึงระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก (VPN network)

(๓) ผู้ใช้งานห้ามใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก (VPN network) เข้าถึงเว็บไซต์ละเมิดลิขสิทธิ์ ละเมิดทรัพย์สินทางปัญญา ข้อมูลอนาจาร ดาวน์โหลดโปรแกรมผิดลิขสิทธิ์เล่นเกมส์ หรือใช้งาน BitTorrent

ข้อ ๒๔ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่ต้องจัดทำทะเบียนบัญชีผู้ใช้งานที่มีสิทธิ์เข้าถึงระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก (VPN network)

(๒) มีหน้าที่เก็บข้อมูลการจราจรคอมพิวเตอร์ไว้อย่างน้อย ๙๐ วัน

ส่วนที่ ๖
แนวปฏิบัติการใช้งานระบบสารสนเทศทางการแพทย์

ข้อ ๒๕ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ เจ้าหน้าที่โรงพยาบาลจุฬาภรณ์ และส่วนงานที่เกี่ยวข้อง

ข้อ ๒๖ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานที่สามารถเข้าใช้งานระบบบริหารจัดการข้อมูลโรงพยาบาลต้องเป็นผู้ปฏิบัติงานในราชวิทยาลัยที่ได้รับมอบหมายที่มีบัญชีผู้ใช้งาน และต้องได้รับเสนอจากฝ่ายการแพทย์ หรือฝ่ายการพยาบาล ซึ่งได้รับการอนุมัติจากผู้อำนวยการโรงพยาบาลจุฬาภรณ์ แล้วเท่านั้น ผู้ใช้งานนอกเหนือจากสองฝ่ายนี้ หากประสงค์จะเข้าใช้งานต้องได้รับการอนุญาตจากผู้บังคับบัญชาเท่านั้น

(๒) ผู้ใช้งานไม่ได้รับอนุญาตให้นำข้อมูลภายในระบบสารสนเทศทางการแพทย์ เช่น ข้อมูลผู้ป่วย ข้อมูลการตรวจรักษา ข้อมูลแพทย์ ข้อมูลยา ข้อมูลการเงิน ออกจากระบบด้วยวิธีใดๆ ก็ตาม

(๓) การส่งข้อมูลภายในระบบสารสนเทศทางการแพทย์ ไปยังหน่วยงานภายนอกจะทำได้ก็ต่อเมื่อมีการทำข้อตกลงการแลกเปลี่ยนข้อมูลแล้ว และได้รับการอนุมัติจากผู้อำนวยการโรงพยาบาลจุฬาภรณ์แล้วเท่านั้น

(๔) เครื่องคอมพิวเตอร์ที่ได้รับอนุญาตเข้าใช้งานระบบสารสนเทศทางการแพทย์ได้ จะต้องแจ้งการลงทะเบียนหมายเลขเครือข่ายประจำเครื่อง (Mac Address) ต่อผู้ให้บริการแล้วเท่านั้น

(๕) กรณีผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงจากระยะไกล (VPN Network) จะต้องปฏิบัติตามแนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก พร้อมทั้งกำหนดระยะเวลาสิ้นสุดที่ชัดเจน

ข้อ ๒๗ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่แจ้งการใช้งานที่ผิดปกติ ต่อผู้บังคับบัญชาของบัญชีผู้ใช้งานนั้น

(๒) มีหน้าที่ปฏิบัติตามแนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์

ส่วนที่ ๗
แนวปฏิบัติการใช้งานระบบสารสนเทศการศึกษา

ข้อ ๒๘ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๒๙ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานที่สามารถเข้าใช้งานระบบสารสนเทศการศึกษาต้องเป็นผู้ปฏิบัติงานในราชวิทยาลัยจุฬาภรณ์ที่เกี่ยวข้องกับการบริหารและการบริการด้านการศึกษา นักศึกษา ที่มีบัญชีผู้ใช้งาน ในกรณีที่เป็นนักศึกษาต้องทำการขึ้นทะเบียนเป็นนักศึกษาของราชวิทยาลัยจุฬาภรณ์ แล้วเท่านั้น

(๒) การใช้งานเครือข่าย นักศึกษาที่ประสงค์จะใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์พกพา อุปกรณ์โทรศัพท์เคลื่อนที่ส่วนตัว ในการเข้าใช้งานระบบสารสนเทศการศึกษา ต้องใช้ระบบที่กำหนดให้เท่านั้น เช่น ระบบงานทะเบียนนักศึกษา ระบบห้องสมุด ระบบฐานข้อมูลเพื่องานวิจัย และระบบ Internet

ข้อ ๓๐ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่แจ้งการใช้งานที่ผิดปกติ ต่อผู้บังคับบัญชาหรือฝ่ายการศึกษาของบัญชีผู้ใช้งานนั้น

(๒) มีหน้าที่ปฏิบัติตามแนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์

ส่วนที่ ๘
แนวปฏิบัติการใช้งานระบบสารสนเทศเพื่อการวิจัยและพัฒนา

ข้อ ๓๑ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๓๒ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานที่เข้าใช้งานระบบสารสนเทศเพื่อการวิจัยและพัฒนา ต้องเป็นผู้ปฏิบัติงานในราชวิทยาลัย หรือนักศึกษาของราชวิทยาลัยจุฬาภรณ์ มีบัญชีผู้ใช้งานระบบสารสนเทศแล้วเท่านั้น ผู้ใช้งานนอกเหนือจากนี้หากประสงค์จะเข้าใช้งาน ต้องได้รับการอนุญาตจากผู้บังคับบัญชาเท่านั้น

(๒) อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา ที่เข้าใช้ระบบสารสนเทศเพื่อการวิจัยและพัฒนา และต้องแจ้งการลงทะเบียนหมายเลขเครือข่ายประจำเครื่อง (Mac Address) ต่อผู้ให้บริการแล้วเท่านั้น

(๓) การใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ส่วนตัว ที่ไม่ได้จัดหาโดยผู้ให้บริการต้องปฏิบัติตามแนวปฏิบัติการนำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์จากภายนอกเข้ามาใช้ในพื้นที่ราชวิทยาลัยจุฬาภรณ์

(๔) การใช้งานเครือข่าย ผู้ใช้งานระบบสารสนเทศเพื่อการวิจัยและพัฒนา จะใช้งานผ่านเครือข่ายภายในสำหรับงานบริการงานวิจัยเท่านั้น

(๕) ข้อมูลที่ใช้ในการวิจัย ผู้ใช้งานไม่ได้รับอนุญาตให้นำข้อมูลงานวิจัย หรือข้อมูลที่ใช้ในงานวิจัยภายในระบบสารสนเทศเพื่อการวิจัยและพัฒนาออกจากระบบไม่ว่าด้วยวิธีการใดๆ ก็ตามกรณีมีความจำเป็นต้องนำข้อมูลออก ต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานนั้น และได้รับการอนุมัติจากเลขาธิการราชวิทยาลัยจุฬาภรณ์ ก่อนทุกครั้ง

(๖) ผู้ใช้งานที่ต้องการเข้าถึงจากระยะไกลเพื่อการใช้ระบบสารสนเทศเพื่อการวิจัยและพัฒนา จะต้องปฏิบัติตาม แนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์จากภายนอก

ข้อ ๓๓ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่แจ้งการใช้งานที่ผิดปกติ ต่อผู้บังคับบัญชาของบัญชีผู้ใช้งานนั้น

(๒) มีหน้าที่ปฏิบัติตามแนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์

ส่วนที่ ๙

แนวปฏิบัติการใช้งาน E-Mail, Social Media และ Instant Messaging

ข้อ ๓๔ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๓๕ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) ผู้ใช้งานที่ได้รับ E-Mail ของราชวิทยาลัยจุฬาภรณ์ (@cra.ac.th และ @pccms.ac.th) จะต้องใช้เพื่อภารกิจที่เกี่ยวข้องกับงานของราชวิทยาลัยจุฬาภรณ์เท่านั้น

(๒) ผู้ใช้งานห้ามใช้ E-Mail ส่วนตัว ในการส่งข้อมูลที่เกี่ยวข้องกับงานของราชวิทยาลัยจุฬาภรณ์

(๓) ผู้ใช้งานสื่อสังคมออนไลน์ (Social Media) ให้ถือปฏิบัติตามแนวทางตามประกาศคณะกรรมการสุขภาพแห่งชาติ เรื่อง แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานด้านสุขภาพ พ.ศ. ๒๕๕๙

(๔) ห้ามผู้ใช้งานใช้สื่อสังคมออนไลน์ (Social Media) ในการหมิ่นเบื้องสูง หมิ่นประมาท ประกอบกิจกรรมการเมือง กล่าวว่าให้ร้าย โพสขายสินค้า ดูภาพอนาจาร

(๕) ผู้ใช้งาน Instant Messaging ของราชวิทยาลัยจุฬาภรณ์ ให้ใช้เพื่อภารกิจที่เกี่ยวข้องกับงานของราชวิทยาลัยจุฬาภรณ์เท่านั้น

(๖) ห้ามใช้งาน Instant Messaging ของราชวิทยาลัยจุฬาภรณ์ ในการหมิ่นเบื้องสูงหมิ่นประมาท ประกอบกิจกรรมการเมือง กล่าวว่าให้ร้ายผู้อื่น

ข้อ ๓๖ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่ตรวจเช็ค หรือระงับการใช้ทันที ในกรณีตรวจพบการใช้งานที่ผิดปกติ

(๒) มีหน้าที่แจ้งการใช้งานที่ผิดปกติ ต่อผู้บังคับบัญชาของบัญชีผู้ใช้งานนั้น

(๓) มีหน้าที่เก็บข้อมูลการจราจรคอมพิวเตอร์ไว้อย่างน้อย ๙๐ วัน

ส่วนที่ ๑๐

แนวปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของระบบสารสนเทศ ของราชวิทยาลัยจุฬาภรณ์

ข้อ ๓๗ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๓๘ แนวปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคล

(๑) ให้ยึดถือปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนข้อบังคับ ระเบียบ และประกาศของราชวิทยาลัยจุฬาภรณ์ที่เกียวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นบัญญัติให้กระทำได้

(๓) การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

(๔) ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้จะกระทำมิได้

(๕) ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ให้แก่ผู้ปฏิบัติงานหรือบุคคลที่เกี่ยวข้องทราบรวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กลุ่มบุคคลดังกล่าวปฏิบัติตามอย่างเคร่งครัด

(๖) ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลซึ่งควรครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ มาตรการป้องกันด้านเทคนิคและมาตรา

การป้องกันทางกายภาพ ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคลโดยอย่างน้อยต้องประกอบด้วยการดำเนินการ ดังต่อไปนี้

๖.๑ การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๖.๒ การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

๖.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๖.๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

๖.๕ การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ ๓๙ ผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล และจะต้องดำเนินการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนข้อบังคับ ระเบียบ ประกาศที่ราชวิทยาลัยจุฬาภรณ์กำหนด

ข้อ ๔๐ ผู้ใช้งานที่มีหน้าที่เกี่ยวกับการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล จะต้องดำเนินการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนข้อบังคับ ระเบียบ ประกาศที่ราชวิทยาลัยจุฬาภรณ์กำหนด และปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด

ข้อ ๔๑ ผู้ให้บริการมีหน้าที่ ออกแบบ พัฒนา ระบบสารสนเทศให้สอดคล้องกับมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดและให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนข้อบังคับ ระเบียบ ประกาศของราชวิทยาลัยจุฬาภรณ์ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑๑
แนวปฏิบัติในการควบคุมทรัพย์สินสารสนเทศ

ข้อ ๔๒ แนวปฏิบัตินี้มีวัตถุประสงค์เพื่อเป็นการกำหนดแนวทางปฏิบัติในการกำกับดูแล และการปกป้องทรัพย์สินสารสนเทศราชวิทยาลัยจุฬาภรณ์

ข้อ ๔๓ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๔๔ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) มีหน้าที่ดูแลรักษา และปกป้องสินทรัพย์สารสนเทศที่ได้รับมอบจากผู้ให้บริการ เพื่อใช้ในการปฏิบัติภารกิจของราชวิทยาลัยจุฬาภรณ์

(๒) มีหน้าที่ส่งคืนทรัพย์สินสารสนเทศต่อผู้ให้บริการ ก่อนวันพ้นสภาพการเป็นผู้ปฏิบัติงานในราชวิทยาลัย

ข้อ ๔๕ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่จัดทำทะเบียนทรัพย์สินของราชวิทยาลัยจุฬาภรณ์

(๒) มีหน้าที่ควบคุม แก้ไข เปลี่ยนแปลงบัญชีทรัพย์สินสารสนเทศให้เป็นปัจจุบัน

(๓) มีหน้าที่ยุติการเชื่อมต่อและนำอุปกรณ์ดังกล่าวมาตรวจเช็ค หากตรวจพบว่าหน่วยงานใดนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์ โดยไม่ได้ลงทะเบียนทรัพย์สิน

(๔) เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องนำส่งสื่อบันทึกข้อมูลให้กับเจ้าหน้าที่ของผู้ให้บริการเป็นผู้ทำลายข้อมูลกำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์ บนสื่อบันทึกข้อมูล ดังนี้

๔.๑ ฮาร์ดดิสก์ที่ยกเลิกการใช้งาน ใช้วิธีการทำลายข้อมูลตามข้อกำหนด U.S. National Industrial Security Program Operating Manual (DoD ๕๒๒๐.๒๒-M)

๔.๒ แผ่น CD/DVD ใช้การหั่น ตัด เผา ให้สิ้นสภาพการใช้งาน

๔.๓ เทป ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย

ส่วนที่ ๑๒

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์

ข้อ ๔๖ แนวปฏิบัตินี้มีวัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์ให้มีความปลอดภัยพ้นจากภัยคุกคามให้ครบองค์ประกอบความมั่นคงปลอดภัยทั้ง ๓ ประการ คือ คงความลับ คงความถูกต้องครบถ้วน และคงความพร้อมใช้งาน

ข้อ ๔๗ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๔๘ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) มีหน้าที่แจ้งผู้ให้บริการทราบทันที หากพบเห็นเหตุการณ์ใดก็ตามที่อาจจะส่งผลกระทบต่อเครือข่ายของราชวิทยาลัยจุฬาภรณ์

(๒) ผู้ใช้งานไม่ได้รับอนุญาตให้ติดตั้งอุปกรณ์เน็ตเวิร์ค เช่น Router, Switch, Wi-Fi device, Modem ภายในราชวิทยาลัยจุฬาภรณ์ โดยพลการ

(๓) ผู้ใช้งานไม่ได้รับอนุญาตให้ติดตั้งเซิฟเวอร์ เช่น Active Directory, NTP Server, DHCP Server, DNS Server, Database Server ภายในระบบคอมพิวเตอร์หรือระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์ โดยพลการ

(๔) ผู้ใช้งานไม่ได้รับอนุญาตให้นำอุปกรณ์ใดก็ตาม เชื่อมต่อเครือข่ายราชวิทยาลัยจุฬาภรณ์ โดยพลการ

(๕) หน่วยงานของราชวิทยาลัยจุฬาภรณ์ที่ต้องการใช้ชื่อโดเมน ภายใต้ชื่อโดเมนของ ราชวิทยาลัยจุฬาภรณ์ (Subdomain) ต้องได้รับอนุมัติโดยผู้บริหารสูงสุด และต้องผ่านการพิจารณาจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

(๖) โครงการใดๆ ที่ได้รับอนุมัติจากราชวิทยาลัยจุฬาภรณ์ให้สามารถขอจดชื่อโดเมนใหม่ (New domain) ประจำโครงการได้ ต้องได้รับอนุมัติโดยผู้บริหารสูงสุด และต้องผ่านการพิจารณาจากผู้บริหารสูงสุดของฝ่ายเทคโนโลยีสารสนเทศ

ข้อ ๔๙ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่ออกแบบและแบ่งแยกระบบเครือข่ายออกเป็นเครือข่ายย่อย (network segmentation) และระบบเครือข่ายใดที่ไม่จำเป็นต้องเชื่อมต่อถึงกัน ให้ทำการแยกการเชื่อมต่อถึงกันโดยเด็ดขาด

(๒) มีหน้าที่จัดทำและปรับปรุง Network diagram และห้ามเผยแพร่ต่อบุคคลอื่น ก่อนได้รับอนุญาตจากผู้บริหารสูงสุดของผู้ให้บริการ

(๓) มีหน้าที่วางแผนการตรวจจับการรั่วไหลของข้อมูลออกภายนอกของราชวิทยาลัยจุฬาภรณ์

(๔) มีหน้าที่วางแผนการติดตั้งระบบบันทึกข้อมูลจราจรคอมพิวเตอร์ไว้ที่จุดเชื่อมต่อกับ Internet gateway ของราชวิทยาลัยจุฬาภรณ์

(๕) มีหน้าที่ตรวจเช็คเวอร์ชั่นของอุปกรณ์เครือข่ายว่าเป็นปัจจุบันหรือไม่

(๖) มีหน้าที่วางแผนการดำเนินการปรับปรุง firmware อุปกรณ์เครือข่ายให้เป็นปัจจุบันและสามารถใช้งานร่วมกับระบบเดิมได้ (Compatible) โดยต้องทำการทดสอบให้มั่นใจก่อนอัปเดตเสมอ

(๗) มีหน้าที่ วางแผนการต่อสัญญาบำรุงรักษาอุปกรณ์ระบบเครือข่ายอย่างเป็นประจำทุกปี

(๘) มีหน้าที่จัดสรร IP Address ให้เพียงพอต่อการใช้งานทั้งสำหรับเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ภายในเครือข่ายราชวิทยาลัยจุฬาภรณ์

(๙) ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ให้บริการจดทะเบียนชื่อโดเมนต่าง ๆ ภายใต้ชื่อโดเมนของราชวิทยาลัยจุฬาภรณ์

ส่วนที่ ๑๓

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์

ข้อ ๕๐ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๕๑ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) การเข้า-ออก ศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์ จะต้องเป็นผู้ปฏิบัติงานในราชวิทยาลัยหรือบุคลากรที่ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศอนุมัติ หรือได้รับมอบหมายเท่านั้น

(๒) ผู้ใช้งานมีหน้าที่ต้องเซ็นชื่อบันทึกข้อมูลการ เข้า-ออก ศูนย์คอมพิวเตอร์หลักของ ราชวิทยาลัยจุฬาภรณ์

(๓) ไม่อนุญาตให้บุคคลภายนอกเข้า-ออก ศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์ โดยไม่ได้รับอนุญาต

(๔) ไม่อนุญาตให้รับประทานอาหารในศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์ หรือห้องคอมพิวเตอร์

ข้อ ๕๒ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่วางแผนการต่อสัญญาบำรุงรักษาอุปกรณ์ที่ติดตั้งในศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์

(๒) มีหน้าที่ควบคุม และอนุมัติอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่นำไปติดตั้งที่ศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์

(๓) มีหน้าที่กำกับดูแล ให้บันทึกข้อมูลการเข้า-ออก ศูนย์คอมพิวเตอร์หลักของราชวิทยาลัยจุฬาภรณ์ ไม่น้อยกว่า ๙๐ วัน

ส่วนที่ ๑๔
แนวปฏิบัติการป้องกันการโจมตีทางไซเบอร์

ข้อ ๕๓ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๕๔ ผู้ใช้งานมีหน้าที่แจ้งผู้ให้บริการทราบทันที หากพบภัยคุกคามทางไซเบอร์หรือการพยายามโจมตีทาง ไซเบอร์ ที่อาจส่งผลกระทบต่อราชวิทยาลัยจุฬาภรณ์ เช่น เครื่องติดไวรัส พบอีเมลฟิชชิง (Phishing)

ข้อ ๕๕ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่เฝ้าระวังการโจมตีทางไซเบอร์ทั้งจากเครือข่ายภายนอกและเครือข่ายภายใน ราชวิทยาลัยจุฬาภรณ์

(๒) มีหน้าที่วางแผนป้องกันการโจมตีทางไซเบอร์ เช่น โจมตีจากไวรัส การโจมตีด้วย DDOS

(๓) มีหน้าที่จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (Point of Contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบเพื่อดำเนินการต่อไป (Escalation Process)

(๔) มีหน้าที่จัดทำรายงานสรุปการโจมตี (Security Incident Report) และบทเรียนจากการโจมตีทางไซเบอร์ (Lesson Learned)

(๕) กรณีเมื่ออยู่ในสถานะถูกโจมตีจากภายนอก ให้ปิดช่องทางระบบเครือข่ายที่ถูกการโจมตีและเปิดใช้เส้นทางสำรองทดแทนแจ้งผู้ให้บริการเครือข่ายอินเทอร์เน็ตที่ใช้บริการอยู่

(๖) เมื่อถูกโจมตีจากภายใน ให้ปิดกั้นเครื่องที่โจมตีออกจากระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์ เจ้าหน้าที่ผู้ให้บริการเข้าตรวจเช็คเครื่องต้นทาง เพื่อดำเนินการแก้ไข ผู้รับผิดชอบหลักของหน่วยงานที่ให้บริการเครื่องแม่ข่ายจะเป็นผู้รับผิดชอบ หากแก้ไขไม่ได้ให้ติดตั้งระบบปฏิบัติการใหม่และนำข้อมูลสำรองมาใช้งานทันที

(๗) หากถูกโจมตีจนไม่สามารถดำเนินการต่อได้ ให้พิจารณาปฏิบัติตามแนวปฏิบัติการเตรียมความพร้อมกรณีฉุกเฉินในกรณีไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

ส่วนที่ ๑๕
แนวปฏิบัติการจัดทำการสำรองข้อมูลระบบสารสนเทศ

ข้อ ๕๖ แนวปฏิบัตินี้มีวัตถุประสงค์เพื่อการบริหารจัดการระบบสำรองข้อมูล สำหรับงานสารสนเทศอย่างถูกต้องเหมาะสม และพร้อมใช้ให้สอดคล้องกับความต้องการในการให้บริการของราชวิทยาลัยจุฬาภรณ์

ข้อ ๕๗ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๕๘ ผู้ใช้งานมีหน้าที่ยืนยันความถูกต้อง ครบถ้วนของข้อมูลการทดสอบการเรียกคืนข้อมูล (Restore) กรณีที่ผู้ให้บริการร้องขอ

ข้อ ๕๙ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่วางแผนและดำเนินการสำรองข้อมูลให้สอดคล้องกับความต้องการในการให้บริการ

(๒) มีหน้าที่วางแผนการ จัดให้มีระบบสำรองข้อมูลจากระบบงานสารสนเทศ ให้สามารถเรียกคืน (Restore) ได้สอดคล้องกับความต้องการในการให้บริการ ตามที่ได้ตกลงไว้กับผู้ใช้บริการ

(๓) มีหน้าที่วางแผนการทดสอบการเรียกคืนข้อมูล (Restore) อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๖
แนวปฏิบัติการเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

ข้อ ๖๐ แนวปฏิบัตินี้มีวัตถุประสงค์เพื่อการบริหารจัดการความต่อเนื่องในการดำเนินงาน เมื่ออยู่ภายใต้กรณีฉุกเฉินหรือในกรณีไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ และมีการบริหารจัดการอย่างเหมาะสมเพื่อให้สามารถดำเนินการ เป็นไปอย่างต่อเนื่อง

ข้อ ๖๑ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ คณะกรรมการบริหารความต่อเนื่องการดำเนินงานระบบสารสนเทศ ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๖๒ ผู้ใช้งานที่ได้รับมอบหมาย มีหน้าที่ร่วมทดสอบการใช้ระบบในกรณีฉุกเฉิน ตามแผนการทดสอบของคณะกรรมการบริหารความต่อเนื่องการดำเนินงานระบบสารสนเทศ

ข้อ ๖๓ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) ให้จัดตั้งคณะกรรมการบริหารความต่อเนื่องการดำเนินงานระบบสารสนเทศ มีหน้าที่ประเมินผลกระทบในกรณีฉุกเฉิน และให้ข้อมูลสถานการณ์แก่ผู้บริหารระดับสูง

(๒) คณะกรรมการบริหารความต่อเนื่องการดำเนินงานระบบสารสนเทศ ต้องจัดทำแผนการให้บริการระบบสารสนเทศในกรณีฉุกเฉินที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดการให้มีการทดสอบแผนในกรณี ดังกล่าว

(๓) กรณีที่เกิดความเสียหายของระบบสารสนเทศของราชวิทยาลัยจุฬาภรณ์ให้คณะกรรมการบริหารความต่อเนื่องการดำเนินงานระบบสารสนเทศ พิจารณาการประกาศใช้และดำเนินการตามแผนการให้บริการระบบสารสนเทศในกรณีฉุกเฉิน

(๔) มีหน้าที่จัดทำแผนการดำเนินงาน การให้บริการระบบสารสนเทศ เพื่อให้ผู้ใช้งานที่จำเป็นสามารถปฏิบัติงานได้จากระยะไกล ในกรณีระบบที่ศูนย์คอมพิวเตอร์หลักใช้การไม่ได้

(๕) มีหน้าที่วางแผนการทำ High availability สำหรับอุปกรณ์โครงสร้างพื้นฐานทางสารสนเทศ ตัวอย่างเช่น Firewall, Core switch, IPS, DHCP server, Time server

(๖) คณะกรรมการบริหารความต่อเนื่องการดำเนินงานระบบสารสนเทศ ต้องวางแผนทดสอบตามแผนการให้บริการระบบสารสนเทศในกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๗
แนวปฏิบัติการจัดหา การพัฒนา และการบำรุงรักษาระบบ

ข้อ ๖๔ แนวปฏิบัตินี้มีวัตถุประสงค์เพื่อสร้างให้ความมั่นคงปลอดภัยของสารสนเทศเป็นองค์ประกอบสำคัญของวงจรการพัฒนาระบบงานต่างๆ ทั้งภายในราชวิทยาลัยจุฬาภรณ์และระบบบริการทางการแพทย์

ข้อ ๖๕ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๖๖ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) มีหน้าที่ต้องให้ข้อมูลความต้องการทางธุรกิจ (Business requirements) ต่อผู้ให้บริการเพื่อวางแผนการจัดหา หรือพัฒนาระบบสารสนเทศ

(๒) ผู้ใช้บริการที่ได้รับมอบหมายมีหน้าที่ร่วมทดสอบระบบก่อนใช้งานจริง (User acceptance test) ตามที่ผู้ให้บริการร้องขอ เพื่อให้มั่นใจว่าระบบที่จัดหาหรือพัฒนาตรงกับความต้องการทางธุรกิจ (Business requirements)

ข้อ ๖๗ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่วิเคราะห์ วางแผน ออกแบบ การดูแลควบคุม ติดตามกระบวนการในการจัดหา การพัฒนา และการบำรุงรักษาระบบงานสารสนเทศ (Software Development Lifecycle)

(๒) มีหน้าที่วางแผนการแก้ไข ทดสอบแก้ไข การเข้าถึงซอร์สโค้ด (Source code) และรวมถึงการ Deployment เข้าสู่ระบบ

(๓) มีหน้าที่ดำเนินการจัดให้มีการขึ้นทะเบียนผู้ให้บริการภายนอก

(๔) มีหน้าที่ต่อสัญญาการบำรุงรักษาระบบงานสารสนเทศ (Maintenance agreement) ก่อนที่จะหมดสัญญา

(๕) มีหน้าที่วางแผนการพัฒนา และแยกระบบเครือข่ายและอุปกรณ์สารสนเทศสำหรับระบบงานพัฒนา (Development environment) ระบบงานทดสอบ (Testing environment) และระบบงานใช้งานจริง (Production environment) ออกจากกัน

ส่วนที่ ๑๘
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเครื่องมือทางการแพทย์

ข้อ ๖๘ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๖๙ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) การนำเครื่องมือทางการแพทย์ที่มาติดตั้งที่โรงพยาบาลจุฬาภรณ์ ต้องแจ้งขึ้นทะเบียนทรัพย์สินก่อนนำมาติดตั้ง

(๒) การนำเครื่องมือแพทย์มาติดตั้ง และเชื่อมต่อระบบเครือข่ายการให้บริการทางการแพทย์ จะต้องให้ข้อมูลต่อผู้ให้บริการ เกี่ยวกับเครื่องมือทางการแพทย์และรายละเอียดของผู้ติดต่อประสานงาน

ข้อ ๗๐ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่วางแผน ออกแบบ ติดตั้งระบบเครือข่ายของเครื่องมือทางการแพทย์ ให้แยกออกจากระบบเครือข่ายหลักของราชวิทยาลัยจุฬาภรณ์ (Network separation)

(๒) มีหน้าที่ต้องออกแบบให้มีระบบสำรองข้อมูล การกู้คืนข้อมูลได้

(๓) มีหน้าที่ต้องติดตั้งระบบป้องกันไวรัส และต้อง Update ให้เป็นปัจจุบัน

(๔) กรณีมีความจำเป็นต้องเข้าถึงจากระยะไกลของผู้ให้บริการเครื่องมือแพทย์ต้องผ่านเครือข่าย VPN Network ให้ปฏิบัติตามแนวปฏิบัติในการเข้าใช้ระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์ จากภายนอก

ส่วนที่ ๑๙
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยอุปกรณ์ Internet of Things (IoT), กล้องวงจรปิด และระบบควบคุมอัตโนมัติ

ข้อ ๗๑ แนวปฏิบัตินี้มีวัตถุประสงค์เพื่อการควบคุมและรักษาความมั่นคงปลอดภัยของอุปกรณ์ Internet of Things (IoT), กล้องวงจรปิด และระบบควบคุมอัตโนมัติ ที่ใช้งานหรือเชื่อมต่อกับระบบเครือข่ายของราชวิทยาลัยจุฬาภรณ์

ข้อ ๗๒ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๗๓ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) การนำอุปกรณ์ IoT, กล้องวงจรปิด และระบบควบคุมอัตโนมัติ มาเชื่อมต่อกับระบบเครือข่ายภายในของราชวิทยาลัยจุฬาภรณ์ ผู้ใช้งานมีหน้าที่แจ้งให้ผู้ให้บริการพิจารณาและอนุมัติก่อนดำเนินงานเสมอ

(๒) การติดตั้งอุปกรณ์ IoT, กล้องวงจรปิด และระบบควบคุมอัจฉริยะที่นำมาติดตั้งในราชวิทยาลัยจุฬาภรณ์ จะต้องแจ้งขึ้นทะเบียนทรัพย์สินทางสารสนเทศ

(๓) ข้อมูลใดๆ จากอุปกรณ์ IoT, กล้องวงจรปิด และระบบควบคุมอัตโนมัติ ถือว่าเป็นข้อมูลของราชวิทยาลัยจุฬาภรณ์ ห้ามนำออกจากระบบเครือข่ายราชวิทยาลัยจุฬาภรณ์ โดยไม่ได้รับอนุญาต

ข้อ ๗๔ ผู้ให้บริการมีหน้าที่วางแผน ออกแบบ ติดตั้งระบบสารสนเทศของอุปกรณ์ IoT, กล้องวงจรปิด และระบบควบคุมอัตโนมัติ ให้แยกระบบออกจากเครือข่ายหลักของราชวิทยาลัยจุฬาภรณ์ (Network separation)

ส่วนที่ ๒๐

แนวปฏิบัติการกำกับดูแลและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ

ข้อ ๗๕ แนวปฏิบัตินี้มีวัตถุประสงค์เพื่อการประเมินความเสี่ยง ให้หน่วยงานผู้ประเมินกำกับสอบทานความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นในการดำเนินงาน ป้องกันการละเมิดเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัย เงื่อนไขในสัญญา และข้อกำหนดความมั่งคงปลอดภัย

ข้อ ๗๖ ผู้มีหน้าที่ต้องปฏิบัติตามแนวปฏิบัตินี้ ได้แก่ ผู้ใช้งาน ผู้ให้บริการ และส่วนงานที่เกี่ยวข้อง

ข้อ ๗๗ แนวปฏิบัติสำหรับผู้ใช้งาน

(๑) มีหน้าที่ต้องระวังการใช้งานระบบสารสนเทศที่ผิดวัตถุประสงค์ หรือละเมิดข้อกำหนดการใช้งานระบบสารสนเทศ

(๒) มีหน้าที่วางแผนบริหารความเสี่ยงการปฏิบัติงานปกติประจำวัน (Business as usual หรือ BAU) กรณีพบเหตุการณ์ความผิดปกติ ความเสี่ยง หรือช่องโหว่ของระบบสารสนเทศจะต้องรายงาน (Incident report) อย่างเป็นลายลักษณ์อักษรต่อผู้มีหน้าที่รับผิดชอบ หรือผู้ให้บริการทันที

(๓) มีหน้าที่ประเมินความเสี่ยงในกระบวนการทำงาน (Working operation process) รวมถึงขั้นตอนปฏิบัติงานระบบสารสนเทศที่ใช้บริการ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗๘ แนวปฏิบัติสำหรับผู้ให้บริการ

(๑) มีหน้าที่กำกับดูแลและประเมินผลกระทบ รวมถึงแก้ไขความผิดปกติ ความเสี่ยง หรือช่องโหว่ของระบบสารสนเทศที่ได้รับแจ้งรายงาน (Incident report) ทันที

(๒) มีหน้าที่ประเมินความเสี่ยงระบบสารสนเทศที่ให้บริการ อย่างน้อยปีละ ๑ ครั้ง

(๓) มีหน้าที่ส่งรายงานผลการประเมินความเสี่ยงระบบสารสนเทศให้กับหน่วยงานที่มีหน้าที่กำกับดูแลและควบคุม (Compliance) และบริหารความเสี่ยง (Risk Management) ที่ได้รับมอบหมาย

ประกาศ ณ วันที่ ๒๒ เดือน ธันวาคม พ.ศ. ๒๕๖๓

นิธิ มหานนท์

(ศาสตราจารย์ นายแพทย์นิธิ มหานนท์)
เลขาธิการราชวิทยาลัยจุฬาภรณ์