นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ พ.ศ. ๒๕๖๕

จัดทำโดย : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรให้มีประกาศมหาวิทยาลัยมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

อาศัยอำนาจตามความในมาตรา ๒๔ และมาตรา ๒๗ แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. ๒๕๔๘ ประกอบกับมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙ และมติคณะกรรมการผู้รับผิดชอบแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์พ.ศ. ๒๕๖๕ ในการประชุมครั้งที่ ๑/๒๕๖๕ เมื่อวันที่ ๒๔ มีนาคม ๒๕๖๕ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ พ.ศ. ๒๕๖๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

“อธิการบดี” หมายความว่า อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

ข้อ ๔ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ มี ๒ ส่วน ดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๕ การจัดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มี ๒ ส่วน ดังนี้

(๑) ส่วนที่ว่าด้วยการจัดทำนโยบาย

๑. ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๒. นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย

๓. กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๔. มีการทบทวนและปรับปรุงนโยบาย ปีละ ๑ ครั้ง

(๒) ส่วนที่ว่าด้วยรายละเอียดของนโยบายให้เป็นไปตามเอกสารแนบท้ายประกาศนี้ รวมทั้งมีรายละเอียด ดังนี้

๑. การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๒. มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรอง ระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๓. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ ปีละ ๑ ครั้ง

๔. การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์ มีนโยบายในการสร้างความเข้าใจด้วยการจัดทำคู่มือจัดฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๖ ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) มีดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๗ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ที่ซึ่งไม่ได้รับอนุญาต มีดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือ รู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องการกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนา ข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศมีเนื้อหา ดังนี้

(๑) การใช้งานรหัสผ่าน กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะ เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต มีดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึง ระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงานต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายและควรใช้อุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ต ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุม การจัดเส้นทางบนเครือข่าย ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต มีดังนี้

(๑) กำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการที่จะต้องควบคุม โดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบบและยืนยันตัวตนของผู้ใช้งาน ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วเมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น

(๕) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่น และสารสนเทศ โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้า ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเอง โดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจาก ภายนอกหน่วยงาน (Mobile Computing WLAN Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อป้องกันสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงานโดยใช้ VPN (Visual Private Network) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานภายนอก

ข้อ ๑๒ การจัดทำระบบสำรองสำหรับระบบสารสนเทศ มีแนวทาง ดังนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณี ที่ ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถดำเนินการได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการงานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ ปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรองปีละ ๑ ครั้ง

ข้อ ๑๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศปีละ ๑ ครั้ง ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยหน่วยตรวจสอบภายใน เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๔ กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้รองอธิการบดีที่มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง และความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๑๕ ให้อธิการบดีเป็นผู้รักษาการตามประกาศนี้ ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้อธิการบดีเป็นผู้วินิจฉัยชี้ขาดและให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๐ เมษายน พ.ศ.๒๕๖๕

(รองศาสตราจารย์ ดร.อุดมวิทย์ ไชยสกุลเกียรติ)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

ส่วนที่ ๑
เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ว่าด้วยคำนิยาม

๑. มหาวิทยาลัย	หมายความว่า	มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
๒. สำนักวิทยบริการฯ	หมายความว่า	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
๓. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	หมายความว่า	หน่วยงานที่ให้บริการด้านห้องสมุด ให้บริการทรัพยากรสารสนเทศ ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา บำรุงรักษาระบบคอมพิวเตอร์ ระบบชุดคำสั่ง ชุดคำสั่งโปรแกรมและเครือข่ายภายในมหาวิทยาลัย
๔. ผู้บริหาร	หมายความว่า	อธิการบดี หรือผู้ที่อธิการบดีมอบหมายให้ดูแล รับผิดชอบงานด้านเทคโนโลยีสารสนเทศด้านต่างๆ ของมหาวิทยาลัย
๕. ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายความว่า	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ
๖. ผู้ใช้งาน	หมายความว่า	ข้าราชการ พนักงาน ลูกจ้างประจำ/ชั่วคราว ลูกจ้างตามสัญญาจ้างในมหาวิทยาลัย บุคลากรและนักศึกษามหาวิทยาลัย หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบเครือข่ายของมหาวิทยาลัย

๗. ผู้ดูแลระบบ (System Administrator)	หมายความว่า	ผู้ที่ได้รับมอบหมายจากผู้บริหาร ให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
๘. สิทธิของผู้ใช้งาน	หมายความว่า	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย
๙. สินทรัพย์	หมายความว่า	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีมีตัวตน อันมีมูลค่าหรือคุณค่าสำหรับมหาวิทยาลัย ได้แก่ข้อมูลระบบข้อมูลและสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร เช่น อุปกรณ์ระบบเครือข่ายที่มีลิขสิทธิ์ เป็นต้น
๑๐. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	หมายความว่า	การอนุญาต การการกำหนดสิทธิหรือมอบ อำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบ สารสนเทศ โดยที่เจ้าของข้อมูลอนุญาตให้ใช้งานระบบสารสนเทศนั้นได้
๑๑. เจ้าของข้อมูล	หมายความว่า	ผู้ใช้ได้รับมอบอำนาจจากผู้บริหารให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
๑๒. หน่วยงานภายนอก	หมายความว่า	องค์กรหรือหน่วยงานภายนอกที่มหาวิทยาลัยอนุญาตให้มีสิทธิในการเข้าถึง และใช้งานข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
๑๓. ข้อมูลคอมพิวเตอร์	หมายความว่า	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจ

		ประมวลผลได้และให้ความหมายรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
๑๔. สารสนเทศ	หมายความว่า	ข้อเท็จจริงที่ได้จากข้อมูล นำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผน การตัดสินใจ และอื่นๆ
๑๕. ระบบคอมพิวเตอร์	หมายความว่า	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานได้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
๑๖. ระบบเทคโนโลยีสารสนเทศ	หมายความว่า	ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมประยุกต์ข้อมูลสารสนเทศ ฯลฯ
๑๗. ระบบเครือข่าย	หมายความว่า	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของมหาวิทยาลัยได้ เช่น ระบบแลน(LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)

๑๘. ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet)	หมายความว่า	เครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
๑๙. ระบบอินเทอร์เน็ต (Internet)	หมายความว่า	ระบบเครือข่ายอินเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
๒๐. จดหมายอิเล็กทรอนิกส์ (E-mail)	หมายความว่า	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงกับข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพเคลื่อนไหว ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ ผ่านโพรโทคอลต่างๆ เช่น SMTP, POP3, IMAP, ฯลฯ
๒๑. สื่อบันทึกพกพา (Portable Media)	หมายความว่า	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึก หรือจัดเก็บข้อมูล เช่น CD, DVD, Flash, Drive, External, Hard Disk, ฯลฯ
๒๒. ชื่อผู้ใช้ (Username)	หมายความว่า	ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้น เพื่อใช้ในการเข้าใช้ในระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้
๒๓. รหัสผ่าน (Password)	หมายความว่า	ชุดของตัวอักษรหรืออักขระ หรือตัวเลขที่ถูกกำหนดขึ้น เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้
๒๔. การเข้ารหัสลับ (Encryption)	หมายความว่า	การนำข้อมูลมาเข้ารหัสลับ เพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมี

		โปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
๒๕. อุปกรณ์จัดเส้นทาง (Router)	หมายความว่า	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทาง เพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
๒๖. การพิสูจน์ยืนยันตัวตน (Authentication)	หมายความว่า	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไป และจะเป็นการพิสูจน์โดยใช้ชื่อและรหัสผ่าน
๒๗. SSID (Service Set Identifier)	หมายความว่า	ชื่อระบุเครือข่ายไร้สาย
๒๘. WPA (Wi-Fi Protected Access)	หมายความว่า	ระบบการเข้ารหัส เพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายพัฒนาขึ้นมาใหม่ มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP
๒๙. MAC Address (Media Access Control Address)	หมายความว่า	หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ติดต่อกับเครือข่ายหมายเลขนี้ จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกันตัวเลขจะอยู่ในรูปของเลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
๓๐. VPN (Virtual Private Network)	หมายความว่า	เครือข่ายคอมพิวเตอร์เสมือน โดยในการรับส่งข้อมูลจริงจะทำได้โดยการเข้ารหัสเฉพาะแล้วรับ-ส่ง ผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๑. แผนผังระบบเครือข่าย (Network Diagram)	หมายความว่า	แผนผัง ซึ่งแสดงถึงการเชื่อมต่อของระบบของมหาวิทยาลัย
๓๒. มาตรฐาน (Standard)	หมายความว่า	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย
๓๓. วิธีการปฏิบัติ (Procedure)	หมายความว่า	รายละเอียดที่บอกขั้นตอนเป็นข้อๆที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
๓๔. แนวทางปฏิบัติ	หมายความว่า	แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
๓๕. ชุดคำสั่งไม่พึงประสงค์	หมายความว่า	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
๓๖. สถานการณ์ความเสี่ยง	หมายความว่า	ความเสี่ยงที่อาจเป็นอันตราย(Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยสามารถแยกเป็นภัยต่างๆ ได้ ๔ ประเภทได้แก่ - ภัยที่เกิดจากเจ้าหน้าที่ หรือบุคคลของหน่วยงาน (Human Error) - ภัยที่เกิดจากซอฟต์แวร์ (Software) - ภัยจากไฟไหม้หรือระบบไฟฟ้า - ภัยจากน้ำท่วม (อุทกภัย)

๓๗. สถานการณ์และความไม่แน่นอนและภัยพิบัติ	หมายความว่า	สถานการณ์หรือเหตุการณ์ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผยหรือเปลี่ยนแปลงทำลาย ปฏิเสธการทำงานหรือการกระทำอื่นๆ
๓๘. เหตุการณ์ด้านความปลอดภัย	หมายความว่า	กรณีที่ระบบเกิดเหตุการณ์ สภาพของการบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดจากการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่รู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๓๙. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	หมายความว่า	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ พ.ศ. ๒๕๖๕

จัดทำโดย : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

คำนำ

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นสิ่งสำคัญที่ต้องปฏิบัติอย่างต่อเนื่อง และจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากทุกฝ่าย นอกจากนั้นยังต้องมีการตรวจสอบอย่างสม่ำเสมอ เพื่อปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้มีการถูกคุกคามจากภัยต่างๆ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ พ.ศ. ๒๕๖๕ ขึ้น เพื่อเผยแพร่ให้ข้าราชการ เจ้าหน้าที่บุคลากรทุกระดับ และนักศึกษาในมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ได้รับทราบและขอความร่วมมือให้ปฏิบัติอย่างเคร่งครัดต่อไป

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
มีนาคม ๒๕๖๕

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

๑. หลักการและเหตุผล

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัย และเชื่อถือได้ ดังนั้น มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ได้จัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากร เจ้าหน้าที่ และผู้ดูแลระบบนำไปปฏิบัติ

๒. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ และขั้นตอนปฏิบัติให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ ให้มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ทำให้การดำเนินงานเป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ อ้างอิงตามมาตรฐาน ISO/IEC27001 และมีการปรับปรุงอย่างต่อเนื่อง

๒.๓ เพื่อเผยแพร่นโยบายและแนวปฏิบัตินี้ให้กับข้าราชการ พนักงานราชการ พนักงานมหาวิทยาลัย เจ้าหน้าที่ บุคลากรทุกระดับ และนักศึกษาในมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ได้รับทราบ และถือปฏิบัติตามอย่างเคร่งครัด ผ่านช่องทางเว็บไซต์มหาวิทยาลัยฯ

๒.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร ข้าราชการ พนักงานราชการ พนักงานมหาวิทยาลัย บุคลากร เจ้าหน้าที่ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานร่วมกับมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ในการดำเนินงานและถือปฏิบัติตามอย่างเคร่งครัด

๒.๕ เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๒.๖ เพื่อส่งเสริมให้ข้าราชการ เจ้าหน้าที่ บุคลากร และนักศึกษาของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ มีความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓. องค์ประกอบของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑ คำนิยาม

ส่วนที่ ๒ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๑) นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

กำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๒) นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

กำหนดให้ระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ให้บริการได้อย่างต่อเนื่อง เป็นมาตรฐาน โดยแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับมหาวิทยาลัยเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

(๓) นโยบายแผนเตรียมความพร้อมกรณีฉุกเฉิน

กำหนดแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เพื่อรองรับสถานการณ์ดังกล่าวที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๔) นโยบายการตรวจสอบแลประเมินความเสี่ยงด้านสารสนเทศ

กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

(๕) นโยบายการสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

กำหนดให้มีการสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับ ผู้ใช้งานทั้งภายในและภายนอกมหาวิทยาลัย

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวปฏิบัติควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑) การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ

๗) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control

๘) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๙) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑๐) การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย (Network System Control Room)

๑๑) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑๒) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๓) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

๑๔) การใช้งานระบบอินเทอร์เน็ต (Use of the Internet)

๑๕) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๖) การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

แนวปฏิบัติระบบสารสนเทศและระบบสำรองของสารสนเทศ

๑) การสำรองข้อมูลและระบบคอมพิวเตอร์

๒) การกู้คืนระบบ

๓) การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายมหาวิทยาลัย

๔) การบริหารจัดการการเข้าถึงระบบเครือข่าย

๕) การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๖) การบริหารจัดการการบันทึกและตรวจสอบ

๗) การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศ

๘) การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๙) การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control)

๑๐) ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวปฏิบัติแผนเตรียมความพร้อมกรณีฉุกเฉิน

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

แนวปฏิบัติการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

องค์ประกอบของแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ รายละเอียด ของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการ รักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย เพื่อให้มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ มีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ของมหาวิทยาลัย ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์นี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ซึ่งข้าราชการ พนักงานราชการ บุคลากร พนักงานมหาวิทยาลัย และนักศึกษาของมหาวิทยาลัยมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

ส่วนที่ ๒
แนวปฏิบัติควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. แนวทางปฏิบัติการควบคุมการเข้าถึงการใช้งานสารสนเทศ (Access Control)

มาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

๑.๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

(๑) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับพิจารณาจากหัวหน้าหน่วยงาน/ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ หรือผู้ดูแลระบบที่ได้รับมอบหมาย โดยผ่านการลงทะเบียนในระบบบัญชีสมาชิกอินเทอร์เน็ต และบุคคลภายนอกให้ลงทะเบียนผ่านระบบบัญชีสมาชิกชั่วคราว

(๒) การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๓) ผู้ดูแลระบบสารสนเทศ ได้จัดให้มีการบันทึกและติดตามการใช้งานระบบสารสนเทศของมหาวิทยาลัยและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

(๔) ผู้ดูและระบบสารสนเทศ ได้จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ

(๑) ผู้ดูแลระบบ มีหน้าที่ตรวจสอบการอนุมัติและกำหนดสิทธิในการเข้าระบบสารสนเทศ โดยที่ผู้ขอใช้งานต้องทำการอนุญาตเข้าระบบที่ต้องการอย่างเป็นลายลักษณ์อักษรตามแบบฟอร์มการขอสิทธิในการเข้าระบบสารสนเทศซึ่งต้องได้รับการลงนามอนุมัติจากเจ้าของข้อมูลและระบบ

(๒) เจ้าของข้อมูลและระบบ มีหน้าที่อนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นตามหน้าที่ในการปฏิบัติงานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

(๓) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศเท่านั้น

(๔) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

(๕) ผู้ดูแลระบบจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของมหาวิทยาลัย และตรวจตราการละเมิดนโยบายความปลอดภัยด้านสารสนเทศที่มีต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศที่สำคัญ

(๕) ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุยาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

การอนุญาต การกำหนดสิทธิ หรือ การมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- สิทธิอ่านอย่างเดียว
- สิทธิสร้างข้อมูล
- สิทธิป้อนข้อมูล
- สิทธิการแก้ไข
- สิทธิในการอนุมัติและไม่อนุมัติ
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัยจะต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๑.๓ ขั้นตอนการปฏิบัติเพื่อการจัดเก็บข้อมูล

การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์

โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศตามพันธกิจ เช่น ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด ได้แก่ ข้อมูลผลการเรียนนักศึกษา ข้อมูลส่วนบุคคล ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านการวิจัย
- ข้อมูลที่มีระดับความสำคัญมาก ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

หากนอกเหนือจากที่กำหนด การจัดระดับความสำคัญของข้อมูล ให้พิจารณาในระบบ

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล แบ่งเป็น ๔ ระดับ

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

(๔) จัดแบ่งลำดับชั้นประเภทผู้ใช้งาน

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๕) ผู้ดูและระบบ ต้องจัดให้ติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

(๖) ผู้ดูแลระบบ ต้องจัดให้บันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

(๗) ผู้ดูแลระบบ ต้องจัดให้บันทึกการผ่านเข้า – ออก สถานที่ตั้งของระบบสารสนเทศ เพื่อเป็นหลักฐานในการตรวจสอบ

(๘) การกำหนดเวลาที่ได้เข้าถึงระบบสารสนเทศ ดังนี้

- ระบบงานบริการ e-Service (Font Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอดเวลา
- ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด โดยสามารถเข้าถึงระบบได้ตามช่วงเวลาดังต่อไปนี้
    ๑. ในเวลาราชการ (๐๘.๓๐ น. – ๑๖.๓๐ น.)
    ๒. นอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ น. – ๑๖.๓๐ น.)
    ๓. ช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)
    ๔. ช่วงเวลาพิเศษเป็นครั้งคราว โดยระบุเป็นช่วงเวลา ระยะเวลาการเข้าถึง

(๙) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

- ผู้ใช้งานเข้าใช้บริการผ่านระบบเครือข่ายภายในมหาวิทยาลัย ได้ตลอด ๒๔ ชั่วโมง
- ผู้ใช้งานเข้าใช้บริการผ่านเครือข่ายนอกมหาวิทยาลัย (VPN) ได้ตลอด ๒๔ ชั่วโมง
- การประชุมทางไกล สามารถเข้าถึงได้เฉพาะเวลาราชการเท่านั้น และต้องมีการกำหนดช่วงเวลา
- การติดต่อประสานงานผ่านโทรศัพท์ ติดต่อภายในเวลาราชการเท่านั้น

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ

เพื่อควบคุมการเข้าถึงสารสนเทศ (Mission Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) ควบคุมการเข้าถึงสารสนเทศได้ โดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) ปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรฐานการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายใน โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ และให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

ได้กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๒.๑ การสร้างความตระหนัก เรื่อง ความมั่นคงปลอดภัยของสารสนเทศ

(๑) กำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนัก เรื่อง ความมั่นคงปลอดภัยสารสนเทศ

(๒) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๒ ต้องกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่องต่างๆ ต่อไปนี้

(๑) จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) ต้องระบุชื่อบัญชีผู้ใช้งาน (Username) แยกเป็นรายบุคคลไม่ซ้ำซ้อนกัน

๒.๑ การระบุชื่อบัญชีผู้ใช้ สำหรับนักศึกษาจะใช้เป็น รหัสนักศึกษา

๒.๒ การระบุชื่อบัญชีผู้ใช้ สำหรับบุคลากรจะใช้เป็น ชื่อ.นามสกุล (๓ ตำแหน่งแรก) กรณีที่ซ้ำซ้อนกัน จะเพิ่มตำแหน่งของนามสกุล

(๓) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้เท่าที่จำเป็น

(๔) ต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๕) ต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

(๖) กำหนดให้มีการจัดทำและแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสาร ดังกล่าว หลังจากที่ได้ทำความเข้าใจแล้ว

(๗) ต้องทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๙) มีหลักเกณฑ์ในการยกเลิก เพิกถอน การอนุญาต ให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการดำเนินการ เช่น ลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง ฯลฯ

(๑๐) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบ ต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๒.๓ บริหารจัดการสิทธิของผู้ใช้งาน (User Management)

โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) กำหนดแสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบ ต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ ตามหน้าที่รับผิดชอบ และตามความจำเป็นในการใช้งาน

(๔) ผู้ดูแลระบบ ต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๕) ผู้ดูแล ต้องจัดเก็บเอกสารการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(๖) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ผู้ใช้งานต้องได้รับความเห็นชอบจากผู้อำนวยการสำนักวิทยบริการฯ และผู้บังคับบัญชาของเจ้าของระบบ โดยมีการควบคุมการใช้งาน ดังนี้

(๖.๑) ต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการสำนักวิทยบริการฯ

(๖.๒) ควบคุมการใช้งานอย่างเข้มงวด กำหนดให้มีการใช้งานที่จำเป็นเท่านั้น

(๖.๓) กำหนดระยะเวลาในการใช้งาน และระงับการใช้งานทันทีเมื่อครบกำหนด

(๖.๔) มีการเปลี่ยนรหัสผ่านทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือกำหนดระยะเวลาในการใช้งาน ไม่เกิน ๓ เดือน หลังจากนั้นต้องมีการเปลี่ยนรหัสผ่านทุกครั้ง

๒.๔ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้งเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) กำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

(๓) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน และอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติเพื่อยืนยันรหัสผ่านใหม่

(๔) ส่งมอบรหัสผ่านชั่วคราว ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรทำการล็อกอินเข้าใช้งานระบบงานครั้งแรกและทำการเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

(๕) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๖) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๗) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นขอบ และอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยมีการกำหนดระยะเวลาใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับว่าเข้าได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๘) ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน เช่น ให้แสดงเป็นเครื่องหมายดอกจัน (*) บนหน้าจอ เป็นต้น

๒.๕ การทบทวนสิทธิการเข้าถึงผู้ใช้งาน (Review of User Access Rights)

ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง ฯลฯ ดังนี้

(๑) ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ๑ ครั้ง/ปี เป็นอย่างน้อย

(๒) ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

(๓) ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

(๔) ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

๒.๖ การเพิกถอนสิทธิการเข้าถึงของผู้ใช้งาน

(๑) ผู้ดูแลระบบดำเนินการเพิกถอนสิทธิผู้ใช้งานที่พ้นสภาพการเป็นนักศึกษาและบุคลากร ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ยกเว้นกรณีเกษียณอายุราชการ

(๒) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย และเพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต มีข้อปฏิบัติ ดังนี้

(๑) ผู้ใช้งานเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

(๒) ผู้ใช้งานตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๓) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ผู้ใช้งานไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจารึกคำศัพท์ที่ปรากฏในพจนานุกรม

(๕) ผู้ใช้งานหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓, abcd หรือกลุ่มของตัวอักขระทีเหมือนกัน เช่น ๑๑๑, ๐๐๐ เป็นต้น

(๖) ผู้ใช้งานไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๑๐) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์

(๑๑) ผู้ใช้งานเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

(๑๒) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการ

เรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๓) ผู้ใช้งานตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำที่กำหนดไว้

(๑๔) ผู้ใช้งานตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

(๑๕) ผู้ใช้งานเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

(๑๖) ผู้ใช้งานเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(๑๗) ผู้ดูแลระบบเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกๆ ๓ เดือน สำหรับผู้ดูแล และ ๖ เดือนสำหรับผู้ใช้งานทั่วไป

๓.๒ การป้องกันอุปกรณ์ ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

ให้กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของมหาวิทยาลัย ในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) กำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) ป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อเสร็จสิ้นงาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา

(๕) ผู้ใช้งาน ควรล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน

(๖) ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(๗) ตั้งล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๓.๓ การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)

เพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) เจ้าหน้าที่ต้องควบคุมเอกสารข้อมูลหรือสื่อต่างๆที่มีข้อมูลสำคัญจัดเก็บหรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

(๒) การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล ผู้ใช้งานต้องมีวิถีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ใช้ดูแลเพื่อป้องกันข้อมูลสำคัญสูญหาย

(๓) เครื่องคอมพิวเตอร์ส่วนบุคคลต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งาน ป้องกันตู้หรือ

(๔) การป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลสินทรัพย์ด้านสารสนเทศ ที่อยู่ในเครื่องประเภทพกพา เมื่อปฏิบัติงานอยู่นอกสถานที่

(๕) การทำลายสื่อบันทึกข้อมูลหรือข้อมูลลับให้เป็นไปตามมาตรฐานการทำลายสื่อบันทึกข้อมูลของกระทรวงกลาโหมสหรัฐอเมริกา

๓.๔ การเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ

โดยผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

(๑) การเข้ารหัสข้อมูลที่เป็นความลับในระดับ ลับที่สุด ลับมาก และลับ ด้วยมาตรการเข้ารหัสที่มีความปลอดภัยและเป็นที่ยอมรับตามมาตรฐานสากล อย่างน้อยต้องเข้ารหัสโดยการเข้ารหัส Secured Socket Layer (SSL)

(๒) หัวหน้าหน่วยงานเจ้าของข้อมูลและระบบงานที่ต้องรักษาข้อมูลที่เป็นความลับต้องแต่งตั้งผู้ที่ทำหน้าที่ดูแลและเก็บรักษากุญแจที่ใช้เข้ารหัสข้อมูลที่เป็นความลับให้มีความปลอดภัย

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

๔.๑ การใช้บริการเครือข่าย

ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) กำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) ผู้ดูแลระบบต้องให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) ผู้ดูแลระบบต้องระบุเครือข่ายและบริการที่อนุญาตให้หน่วยงานสามารถเข้าถึงได้

(๓) ผู้ดูแลระบบต้องจัดทำมาตรการควบคุมการเข้าถึงและใช้งานบริการระบบเครือข่าย

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ฯลฯ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ ๑ ครั้ง

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานภายนอกมหาวิทยาลัย (User Authentication for External Connection)

ต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัยเข้าใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

(๒) ตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน การใช้สมาร์ทการ์ด หรือการใช้ User Token ที่ใช้เทคโนโลยี KPI ฯลฯ

(๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของมหาวิทยาลัย ๑ วิธี

(๔) การเข้าสู่ระบบสารสนเทศของมหาวิทยาลัยจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network)

ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๑) ผู้ดูแลระบบต้องจัดทำบันทึกรายละเอียดการขอเชื่อมต่อระบบเครือข่ายได้แก่ รายชื่อหน่วยงาน สถานที่ตั้ง หมายเลขเครือข่ายทั้งระดับ IP Address และ Mac Address

(๒) ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุแกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน Mac Address ของอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายเพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๑) ผู้ดูแลระบบต้องตรวจสอบและดำเนินการเปิด-ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยปิดพอร์ตที่เสี่ยงต่อการเกิดความเสียหายต่อระบบเครือข่าย และปิดพอร์ตที่ไม่มีความจำเป็นในการใช้งาน

(๒) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้ในระยะเวลาที่จำกัดเท่าที่จำเป็น และการขอใช้งานต้องได้รับการอนุญาตจากหัวหน้าหน่วยงานดูแลระบบเป็นลายลักษณ์อักษร

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Network)

ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๑) แบ่งแยกระบบเครือข่ายเป็นวิทยาเขต คณะและหน่วยงาน

(๒) แบ่งแยกระบบเครือข่ายออกเป็นระบบเครือข่ายตามการให้บริการสารสนเทส

(๓) แบ่งแยกระบบเครือข่ายออกเป็นระบบเครือข่ายของระบบสารสนเทศ

(๔) แบ่งแยกระบบเครือข่ายออกเป็นระบบเครือข่ายภายในและระบบเครือข่ายภายนอก

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) ตรวจสอบการเชื่อมต่อระบบเครือข่ายโดยใช้เครื่องมือ (Monitoring tools) เป็นประจำ

(๒) มีระบบการตรวจจับผู้บุกรุกในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๓) ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

๔.๗ การควบคุมการจัดเส้นทางเครือข่าย (Network Routing Control)

ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยการใช้งานเลขเครือข่าย (IP Address Plan)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน วิธีการเข้ารหัส ฯลฯ

(๕) วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

(๔) ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัยอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ อย่างเป็นทางการ

(๕) ควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสูรระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(๖) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ โดยมีแนวปฏิบัติ ดังนี้

๕.๑ ผู้ดูแลระบบ (System Administrator)

ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของมหาวิทยาลัย และกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๕.๒ กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่จะเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ต้องกำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงานหรือด้านเทคนิค

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น สมาร์ทการ์ด RFID หรือ เครื่องอ่านลายพิมพ์นิ้วมือ ฯลฯ

๕.๔ การบริหารจัดการรหัสผ่าน (Password Management System)

กำหนดระบบบริการจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ หรือกำหนดการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้ไม่ปลอดภัย ให้ดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องการใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๖ การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out) มีแนวปฏิบัติ ดังนี้

(๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบ เมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๕.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Imitation of Connection Time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากขึ้น สำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง ฯลฯ กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของมหาวิทยาลัยตามปกติเท่านั้น

(๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือ ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน ฯลฯ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access control)

ต้องมีคุณสมบัติ ดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) และการพัฒนาซอฟแวร์โดยหน่วยงานภายนอก (Outsourced software development)

ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๖.๑.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

(๑) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมกำหนดสิทธิตามอำนาจหน้าที่ที่ได้รับ จะต้องมีการทบทวนสิทธิการใช้งาน

(๒) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา ๑๕ นาที ต้องทำการยุติการใช้งานทันที

(๓) ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๖.๑.๒ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์โดยระบุไว้ในสัญญาจ้าง

(๔) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่างๆ

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย

ต้องดำเนินการ ดังนี้

(๑) ต้องแยกระบบซึ่งไวต่อการรบกวน ดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย

(๒) ทำการติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์แม่ข่ายเครื่องหนึ่งต่างหาก

(๓) ทำการป้องกันการมีทรัพยากรไม่เพียงพอ

(๔) มีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกันระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่นๆที่มีความสำคัญน้อยกว่า

(๕) ทำการตั้งค่าไฟร์วอลล์ควบคุมการเข้าใช้งานจากเครือข่ายภายในและภายนอกมหาวิทยาลัย

(๖) มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

(๗) ควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Mobile and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

ต้องปฏิบัติ ดังนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๖.๔ การปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking)

ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของมหาวิทยาลัยจากภายนอกมหาวิทยาลัย

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) โดยเข้าสู่ระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ต้องได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ ก่อนทุกครั้ง

(๒) มีการควบคุมพอร์ต (Port) ที่ใช้เข้าระบบอย่างรัดกุม

(๓) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องมีความจำเป็นเท่านั้น

(๔) การเปิดพอร์ต ต้องไม่เปิดพอร์ตที่ไม่จำเป็น และไม่เปิดพอร์ตทิ้งไว้ และต้องตัดการเชื่อมต่อทุกครั้งที่ไม่ได้ใช้งานแล้ว

(๕) มีการสำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกล

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access control)

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(๑) ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษร

(๒) ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๓) ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๔) ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่คบคุมได้

(๕) ผู้ดูแลระบบ ควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

(๖) ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๗) ผู้ดูแลระบบ ควรเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๘) ผู้ดูแลระบบ ต้องกำหนดค่าใช้ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

(๙) ผู้ดูแลระบบ ควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

(๑๐) ผู้ดูแลระบบ ควรจะมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๑๑) ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

(๑๒) ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศทราบโดยทันที

๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๘.๑ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) ให้สำนักฯเป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ทราบทั่วกัน โดยภายในมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ มีการจำแนกและกำหนดพื้นที่ของเครื่องแม่ข่าย อุปกรณ์เครื่องแม่ข่าย ระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม และให้กำหนดพื้นที่รักษาความมั่นคงปลอดภัย ของระบบสารสนเทศและเครือข่ายมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ มีจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคง ปลอดภัย จากผู้ที่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้น โดยการกำหนดพื้นที่ ดังกล่าว อาจแบ่งออกได้เป็น

- พื้นที่ทำงาน
- พื้นที่ติดตั้งและเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย
- พื้นที่ใช้งานระบบเครือข่ายไร้สาย

(๒) ให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

- จัดทำ“ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

- จัดให้มีเจ้าหน้าที่ทำหน้าที่ ตรวจสอบประวัติการเข้า-ออกที่เป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ ปีละ ๑ ครั้ง เป็นอย่างน้อย
- บุคคลภายนอกเข้ามาติดต่อต้องลงชื่อขออนุญาตการเข้า-ออก ในแบบฟอร์มการเข้า-ออก ให้ถูกต้องและจะต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา
- ประกาศห้ามผู้ไม่มีส่วนเกี่ยวข้องเข้าพื้นที่ เว้นแต่ได้รับอนุญาตให้รับทราบทั่วกัน
- หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในมหาวิทยาลัย จะต้องได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
- มีระบบสนับสนุนการทำงานของระบบสารสนเทศของมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดับเพลิง ระบบปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้มั่นใจได้ว่า ระบบทำงานตามปกติและลดความเสี่ยงจาการล้มเหลวในการทำงานของระบบ
- ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๘.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของมหาวิทยาลัยในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้

(๒) ให้มีการป้องกันสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์ เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงบุคคลภายนอก

(๗) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจสอบหาการติดตั้งอุปกรณ์ดักจับสัญญาณ โดยผู้ไม่ประสงค์ดี

๘.๓ การบำรุงรักษาอุปกรณ์

(๑) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๘) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๙) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ใช้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในมหาวิทยาลัย

(๑๐) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจาก

ภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๘.๔ การนำทรัพย์สินของมหาวิทยาลัยออกนอกมหาวิทยาลัย

(๑) ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกมหาวิทยาลัย

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกมหาวิทยาลัย

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกมหาวิทยาลัย

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๖) บันทึกข้อมูลการนำอุปกรณ์ของมหาวิทยาลัยออกไปใช้งานนอกมหาวิทยาลัย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๘.๕ การจัดการอุปกรณ์ที่ใช้งานอยู่นอกมหาวิทยาลัย

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยออกไปใช้งาน เช่น การขนส่ง และการเกิดอุบัติเหตุกับอุปกรณ์ ฯลฯ

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๘.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น ฯลฯ

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑ การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัยเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้นที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนการดำเนินงาน

(๔) ไม่ควรติดตั้งรหัสต้นฉบับ (Source Code) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่

ข่ายที่ให้บริการนั้นๆ

(๕) กำหนดให้มีการจัดเก็บรหัสต้นฉบับและคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ ฯลฯ

(๗) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(๘) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมและขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

(๙) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๙.๒ การทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่มหาวิทยาลัยต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ควรจัดให้มีการควบคุมการพัฒนาซอฟต์แวร์ที่จัดจ้างจากบุคคลหรือหน่วยงานภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ ในการพัฒนาซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้รับจ้างในบริการจากภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี (Malware) ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ขอระบบเหล่านั้น ควรมีการบันทึก ดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน
- สถานที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์

- ข้อมูลสำหรับติดต่อ

(๒) กำหนดให้มีการจัดการช่องโหว่ของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศให้ผู้ดูและระบบดำเนินการ ดังนี้

- เฝ้าระวังติดตาม ประเมินความเสี่ยงเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- กำหนดตำแหน่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของมหาวิทยาลัย
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับการแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๙.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging)

บันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนคอนฟิกกูเรชัน (Configuration) ของระบบ

(๘) ข้อมูลแสดงการใช้งานแอพพลิเคชัน

(๙) ข้อมูลแสดงการเข้าถึงและการกระทำกับไฟล์ เช่น เปิด ปิด เขียน หรืออ่านไฟล์ ฯลฯ

(๑๐) ข้อมูลที่อยู่ไอพีที่เข้าถึง

(๑๑) ข้อมูลโพรโทคอลเครือข่ายที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๐. การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย (Network System Control Room)

เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูล และระบบข้อมูลของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเขาออกห้องควบคุมระบบเครือข่าย

๑๐.๑ ผู้ที่เกี่ยวข้อง บทบาทและหน้าที่รับผิดชอบ

(๑) หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต

- อนุมัติสิทธิเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
- อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

(๒) ผู้ดูแลห้องควบคุมระบบเครือข่าย

- ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์ปฏิบัติการให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

๑๐.๒ กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

ผู้ดูแลห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่ มีแนวทางปฏิบัติ ดังนี้

(๑) ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคลากรภายในที่ปฏิบัติหน้าที่ทีเกี่ยวข้องและมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

(๒) สิทธิในการเข้าออกห้องต่างๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

(๓) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

(๔) การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๑๐.๓ แนวปฏิบัติการจัดทำเอกสารระบุสิทธิในการเข้าถึงพื้นที่

การจัดทำเอกสารระบุสิทธิของผู้ใช้และ “หน่วยงานภายนอก” ในการเข้าถึงพื้นที่ มีดังนี้

(๑) กำหนดสิทธิผู้ใช้ที่มีสิทธิผ่านเข้าออกและช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ที่ออกโดยหน่วยงานราชการ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

(๓) บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๔) เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้อง และต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

(๕) บุคคลภายนอกหรือผู้ติดต่อต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่ออุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

(๖) ผู้ใช้จะได้รับสิทธิให้เข้าออกพื้นที่ทำงานได้เฉพาะบริเวณที่ที่ถูกกำหนด เพื่อใช้ในการทำงานเท่านั้น

(๗) หากมีบุคคลอื่นที่ไม่ใช่ผู้ขอใช้พื้นที่ โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผล และความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่หน่วยงานราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการเข้าออกไว้เป็นหลักฐานทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๑๑. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา

๑๑.๑ การใช้งานทั่วไป

(๑) ผู้ใช้งานต้องยอมรับกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

(๒) เครื่องคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เป็นสมบัติของทางราชการ ผู้ใช้งานควรใช้เพื่อประโยชน์ทางราชการเท่านั้น

(๓) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์เพิ่มเติมและก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบเพียงฝ่ายเดียว

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของสำนักฯหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และ/หรือสื่อบันที่ที่อาจก่อให้เกิดความเสียหายได้

(๗) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์พกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ ฯลฯ

(๘) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่อากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๙) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๑๐) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(๑๑) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ ชา กาแฟ และเครื่องดื่มต่างๆ ฯลฯ

(๑๒) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องคอมพิวเตอร์

แบบพกพาขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย ฯลฯ

(๑๓) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

(๑๔) ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

(๑๕) ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต เช่น การบุกรุก (Hack) เข้าสู่ บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว

(๑๖) ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คำแนะนำที่มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์กำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม

(๑๗) หากผู้ใช้งานกระทำการล่วงละเมิด หรือพยายามจะล่วงละเมิด สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ในฐานะผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย ขอสงวนสิทธิที่จะยกเลิกการใช้งาน หรือระงับการเชื่อมต่อ และ/หรือ การใช้งานใดๆ ตามความเหมาะสม

(๑๘) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๑๙) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

(๒๐) ในการเข้าใช้ระบบปฏิบัติการใส่ User และ Password ทุกครั้ง

(๒๑) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

(๒๒) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

(๒๓) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา หรือสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๒๔) ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(๒๕) ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟต์แวร์ที่มหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น

(๒๖) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า

(๒๗) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพ ที่ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๒๘) ห้ามผู้ใช้งานใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๑๑.๒ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD และ External Hard Disk ฯลฯ

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Hard Disk ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

๑๒. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

(๑) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีการปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๒) เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ ปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๓) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

(๔) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN, XML encryption ฯลฯ

๑๓. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (User of Electronic Mail)

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

(๑) ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

(๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวจนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๓) รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น (*) ในการพิมพ์แต่ละตัวอักษร

(๔) ผู้ดูแลระบบ ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ได้ไม่เกิน ๓ ครั้ง

(๕) ผู้ดูแลระบบ ควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์มีการล็อคเอ้าท์ออกจากหน้าจอจัดการใช้งานของผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

(๖) ผู้ใช้งาน ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

(๗) ผู้ใช้งาน ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

(๘) ผู้ใช้งาน ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ หรือละเมิดสิทธิบุคคลอื่น สร้างความรำคาญต่อผู้อื่น หรือกระทำการผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้บุคคลอื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๙) ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail Address) ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(๑๐) ผู้ใช้งาน ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เพื่อการทำงานของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เท่านั้น

(๑๑) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการล็อกเอาท์จากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(๑๒) ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

(๑๓) ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๑๔) ผู้ใช้งาน ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ทำให้เกิดความแตกแยกระหว่างมหาวิทยาลัยผ่านทางจดหมายอิเล็กทรอนิกส์

(๑๕) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวจดหมายอิเล็กทรอนิกส์

(๑๖) ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(๑๗) ผู้ใช้งาน ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

(๑๘) ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๑๔. การใช้งานระบบอินเทอร์เน็ต (Use of the Internet)

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งาน อินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

(๑) ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

(๒) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

(๓) ในการับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการทดสอบไวรัส (Virus Canning) ป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

(๔) ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

(๕) ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๖) ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๗) ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

(๘) ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ ดังกล่าว ผ่านอินเทอร์เน็ต

(๙) ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

(๑๐) ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

(๑๑) ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรม ใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

(๑๒) ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

(๑๓) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์กันการเข้าใช้งานโดยบุคคลอื่น

๑๕. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

(๑) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยกำหนดไว้เท่านั้น

(๒) ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับมหาวิทยาลัย ผู้ใช้งานต้องแจ้งสำนักวิทยบริการและเทคโนโลยีสารสนเทศ โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๖. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

(๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

(๒) ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (IT Auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

(๓) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ ฯลฯ เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้ ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๓
แนวปฏิบัติระบบสารสนเทศและระบบสำรองของสารสนเทศ

แนวทางปฏิบัติ

๑. สำรองข้อมูลและระบบคอมพิวเตอร์

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทางปฏิบัติ ดังนี้

(๑) จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของมหาวิทยาลัย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ ๑ ครั้ง

(๒) กำหนดให้สำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- มีขั้นตอนการปฏิบัติการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
- ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้ในการจัดเก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่างๆ (Incremental Backup)
- การจัดทำบันทึกการสำรองข้อมูล ได้แก่ วัน/เวลา เริ่มต้นและสิ้นสุดชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก สำเร็จ/ไม่สำเร็จ
- ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุ ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหา และสรุปผลการแก้ไขปัญหาและรายงานต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
- ตรวจสอบข้อมูลทั้งหมดในระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน (Configuration) ข้อมูลในฐานข้อมูล ฯลฯ
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บสำรองกับมหาวิทยาลัยควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลจัดเก็บไว้นอกสถานที่นั้น ในกรณีทีเกิดภัยพิบัติกับมหาวิทยาลัย เช่น ไฟไหม้ น้ำท่วม ฯลฯ

- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
- ให้ผู้ดูแลระบบคอมพิวเตอร์ มอบหมายหน้าที่การสำรองข้อมูลให้กับเจ้าหน้าที่คนอื่น เพื่อช่วยสำรองข้อมูล ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้
- การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย
- นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

(๓) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๔) ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการ ตามความถี่ ทุกรายการที่ปรากฏในตารางจะใช้วิธีแบบ Full Backup ดังนี้

ลำดับ	รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑	Mail Server	- ค่า Configure - ค่าข้อมูลในเมล์บ็อกซ์	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๒	Web Server	- ค่า Configure - ข้อมูลเผยแพร่บนเว็บไซต์	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๓	Database Server	- ค่า Configure - ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๔	Firewall Server	- ค่า Configure - ข้อมูล Rule ของ Firewall	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน
๕	Server ระบบต่างๆ	- ค่า Configure - ข้อมูลบน Server อื่นๆ	- ก่อนและหลังการเปลี่ยนแปลง - ๑ ครั้งต่อเดือน

(๕) ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพ ตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๒. แนวปฏิบัติการกู้คืนระบบ

(๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึก และรายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

(๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

(๓) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

(๔) ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

๓. การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายมหาวิทยาลัย (Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ได้อย่างถูกต้อง

๓.๑ กระบวนการหลักในการควบคุมการเข้าถึงระบบ

(๑) สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

(๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและ การสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๓) ผู้ดูและระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

(๔) ผู้ดูแล ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

(๕) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓.๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(๑) ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

(๒) เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่

ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(๓) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงาน ตามความจำเป็น

๓.๓ การบริหารจัดการการเข้าถึงของผู้ใช้

(๑) การลงทะเบียนบุคลากรใหม่ของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนบุคลากรใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป ต้องทำภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน

(๒) กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application Program) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูและระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๓) ผู้ใช้งาน ต้องลงนามรับทราบสิทธิและหน้าที่ เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๓.๔ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

(๑) ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ใน “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

(๒) การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ใน “การบริหารจัดการการเข้าถึงของผู้ใช้งาน”

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึงผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ในการประกอบการพิจารณา

- ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ
- ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้ งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๔. การบริหารจัดการการเข้าถึงระบบเครือข่าย

(๑) ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีการใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

(๒) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๓) ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

(๔) ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

(๕) ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การแก้ไขหรือการเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๖) ระบบเครือข่ายทั้งหมดของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกมหาวิทยาลัย ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

(๗) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๘) การเข้าสู่ระบบงานเครือข่ายภายในมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการล็อกอินและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

(๙) IP Address ภายในของระบบงานเครือข่ายภายในของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

(๑๐) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑๑) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑๒) การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เท่านั้น

(๑๓) ผู้ใช้งาน ที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด เพื่อให้การเชื่อต่ออุปกรณ์ต่างๆ เป็นไปตามมาตรฐาน และไม่เกิดผลกระทบกับระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๑๔) การขออนุญาตนำเครื่องคอมพิวเตอร์เชื่อมต่อระบบเครือข่ายและขอหมายเลขไอพี (IP Address) และเชื่อมโดเมน (Domain name) ของหน่วยงานใดๆ หน่วยงานนั้นจะต้องทำหนังสือขออนุญาตส่งผ่านหน่วยงานต้นสังกัดมายังสำนักวิทยบริการและเทคโนโลยีสารสนเทศเพื่อพิจารณาดำเนินการ

(๑๕) ห้ามบุคคลใดกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

(๑๖) ในกรณีที่ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลักของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ อาจจะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

(๑๗) ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายไร้ สายด้วย

๕. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

(๑) กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรม ระบบ (System Software) อย่างชัดเจน

(๒) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

(๓) เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet FTP หรือ Ping เป็นต้น ทั่งนี้หากมีบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการเพิ่มเติมด้วย

(๔) ติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

(๕) มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

(๖) การติดตั้งและเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยเจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๖. การบริหารจัดการการบันทึกและตรวจสอบ

(๑) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๓ เดือน

(๒) มีการตรวจสอบการบันทึกการปฏิบัติงานของผู้ใช้อย่างสม่ำเสมอ

(๓) มีวิธีป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๗. การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศ

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในมหาวิทยาลัย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

(๑) การเข้าสู่ระบบระยะไกล สู่ระบบเครือข่ายของมหาวิทยาลัย ต้องควบคุมบุคคลที่จะเข้าสู่ระบบของมหาวิทยาลัยจากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการสำนักวิทยบริการเทคโนโลยีสารสนเทศก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

(๓) การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัยอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

(๔) มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๕) การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อ เมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๘. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของมหาวิทยาลัย ดังนี้

(๑) แสดงชื่อ (Username)

(๒) ใส่รหัสผ่าน (Password)

๙. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control)

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูลความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้องและการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

๙.๑ แนวทางปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

(๙.๑.๑) ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ กำหนดให้มีการประเมินความความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผล โดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

(๙.๑.๒) การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๑) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่ออนุมัติจากผู้อำนวยการสำนักวิทยฯ

๒) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผล ความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่ง ต้องมีรายละเอียดอย่างน้อย ดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๙.๑.๓) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๑) หน่วยงานภายนอกที่ทำงานให้กับมหาวิทยาลัยทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในมหาวิทยาลัยหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของมหาวิทยาลัย โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๒) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่ มี การเข้าถึงข้อมูล โดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๓) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๔) มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ มีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่ามหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๕) กำหนดให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๑๐. ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ภายใต้ข้อบังคับของมาตรา ๒ ๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ กำหนดประเภทของผู้ให้บริการ ไว้ดังนี้

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือ เพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ได้แก่ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสาย และไร้สาย ผู้ประกอบการ ซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือ ร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด และผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการบริษัท หรือ สถาบันการศึกษา

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (Host Service Provider) ได้ แก่ ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting) การให้บริการเช่า Web Server ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) ผู้ให้บริการการเข้าถึง

จดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) และผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)

ง. ผู้ให้บริการร้านอินเทอร์เน็ต

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Application Service Provider) ได้แก่

- ผู้ให้บริการเว็บบอร์ด (Web Board) หรือผู้ให้บริการบล็อก (Blog)
- ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชาระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider)
- ผู้ให้บริการเว็บเซอร์วิส (Web Services)
- ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e- Transactions)

“ผู้ให้บริการ” มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น ด้วยวิธีการที่มั่นคง ปลอดภัย ดังต่อไปนี้

๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบบตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

๒) ระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่ เก็บรักษาไว้เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กรกำหนดให้สามารถเข้าถึงข้อมูล ดังกล่าว ได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของ องค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตาม พระราชบัญญัตินี้

๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือ บริการ Free Internet หรือ บริการ ๑๒๒๒ หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ให้บริการในนาม ตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุ ให้ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการ เช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิด ให้ตรงกับเวลาอ้างอิงสากล โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ เป็นผู้ให้บริการบุคคลทั่วไป ข้อ ข, ค (“ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์”, “ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ”) และเป็นผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ โดยเริ่มเก็บข้อมูลเมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ในราชกิจจานุเบกขา (๒๑ สิงหาคม ๒๕๕๐) มีรายการดังต่อไปนี้

ประเภท	รายการ
๑) ผู้ให้บริการทั่วไป ข้อ ข, ค	
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	๑) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึง ระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิใน การเข้าถึงเครือข่าย (Access Logs Specific to Authentication and Authorization Servers เช่น TACACS (Terminal Access Controller Access-Control System) or RADIUS (Remote Authentication Dial-In User Service) or DIAMETER (Used to Control Access to IP Routers or Network Access Servers) ๒) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของ เครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server) ๓) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID) ๔) ข้อมูลหมายเลขอินเทอร์เน็ตที่ถูกกำหนดให้ โดยระบบผู้ให้บริการ (Assigned IP Address) ๕) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้า (Calling Line Identification)
ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail Server)	๑) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่อง ให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol : SMTP Log) ซึ่ง ได้แก่ - ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID) - ข้อมูลที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender e-mail Address) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver e-mail Address) - ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมาย อิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมาย อิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น

ประเภท	รายการ
	๒) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะ เข้ามาใช้บริการ ๓) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้า มาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to server) ๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่อ อยู่ในขณะนั้น (IP Address of Sending Computer) ๕) ชื่อผู้ใช้งาน (User ID) (ถ้ามี) ๖) ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ (POP๓ (Post Office Protocol Version ๓) Log or IMAP๔ (Internet Message Access Protocol Version ๔))
ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่อง	๑) ข้อมูล Log ที่บันทึก เมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล ๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Data and Time of Connection of Client to Server) ๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address) ๔) ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี) ๕) ข้อมูลตำแหน่ง (Path) และชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป ()Path and Filename of Data Object Uploaded of Downloaded)

ประเภท	รายการ
ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ ให้บริการเว็บและเครื่องให้บริการ ๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ ๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น ๔) ข้อมูลคำสั่งการใช้งานระบบ ๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดู ข้อมูล (URL: Uniform Resource Identifier) เช่น ตำแหน่งเว็บเพ็จ
จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP (Usenet) [Network News Transfer Protocol] Log) ๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้า มาใช้บริการ และเครื่องให้บริการ (Date and Time of Connection of Client to Server) ๓) ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID) ๔) ข้อมูลชื่อเครื่องให้บริการ (Host Name) ข้อมูล Log เช่นข้อมูลเกี่ยวกับวัน เวลา การ ติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server) และข้อมูลชื่อ เครื่องบนเครือข่าย และหมายเลขเครื่องของผู้ ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ใน ขณะนั้น (Hostname and IP Address) เป็นต้น
ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต	เช่น Internet Relay Chat (IRC) หรือ Instant Messaging (IM) เป็นต้น

ประเภท	รายการ
๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล	
ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการ (Content Service Provider)	๑) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่ สามารถระบุเก็บรักษาข้อมูลคอมพิวเตอร์ตัวผู้ใช้บริการได้ หรือเลข ประจำตัว (Use ID) ของผู้ขายสิ้นค้า หรือ บริการ หรือเลขประจาตัว ผู้ใช้บริการ (Use ID) และที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ ๒) บันทึกข้อมูลการเข้าใช้บริการ ๓) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล

ส่วนที่ ๔
แผนเตรียมความพร้อมกรณีฉุกเฉิน

ข้อมูล สารสนเทศ ถือเป็น ทรัพย์สินทางการบริหารที่มีความสำคัญต่อองค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิด ความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพกลุ่มสารนิเทศ ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยเสี่ยงต่างๆ ทั้งจากภายนอกและภายในมากระทบทำให้ระบบฐานข้อมูล และสารสนเทศรวมทั้งระบบอุปกรณ์เสียหายได้โดยเฉพาะอย่างยิ่ง ฐานข้อมูลและสารสนเทศที่ใช้ในการบริหารจัดการ กลุ่มสารนิเทศจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผล กระทบต่อฐานข้อมูลและสารสนเทศขององค์กร

วัตถุประสงค์

๑) เพื่อสร้างความเข้า ใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศขององค์กร
๒) เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ
๓) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูล และสารสนเทศ เพื่อให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
๔) เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมี ประสิทธิภาพ สามารถแก้ไขสถานการณ์ที่อาจเกิดขึ้นได้อย่างทันท่วงที
๕) เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติ แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ (Contingency Plan)

<u>ภัยพิบัติจากภายนอก</u>

(ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้ง ของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แมลงกัดแทะ ฯลฯ

<u>การป้องกันอัคคีภัย</u>

<u>การดำเนินการ</u>

๑. กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ

๒. อบรมขั้นต้นสำหรับพนักงานทุกคนในแผนป้องกันและระงับอัคคีภัย และมีการซ้อม ดับเพลิงการหนีไฟ

๓. ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย

๔. จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์แม่ข่ายเพื่อประสิทธิภาพในการเคลื่อน ย้ายเมื่อเกิดเหตุฉุกเฉิน

การป้องกันอุทกภัย และการป้องกันความชื้นและอุณหภูมิมิที่ไม่เหมาะสม

เนื่องจากที่ทำการอยู่บนอาคารสูงปัญหาจากอุทกภัยจึงไม่มี แต่เนื่องจากเครื่องปรับอากาศมีความชื้นสูงจึงมีความเสี่ยงต่อการอายุการใช้งานของอุปกรณ์คอมพิวเตอร์แม่ข่าย

การดำเนินการ

๑. การเปิดเครื่องปรับอากาศ ตลอด 24 ชั่วโมง

๒. ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

(ข) การโจรกรรมอุปกรณ์ระบบเครือข่ายหรือคอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บ และรวบรวมข้อมูล

การดำเนินการ

๑. ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่'ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของกลุ่มสารนิเทศเป็นผู้รับผิดชอบนำพาเข้าไป

๒. จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึง อุปกรณ์คอมพิวเตอร์แม่ข่าย โดยมีระบบยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๓. ติดตั้งกล้อง วงจรปิด และส่งสัญญาณภาพมาไว้ที่จอ ภาพส่วนกลาง

(ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้องสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีเส้นทางออกสู่อินเตอร์เน็ตผ่านสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)

การดำเนินการ

๑. การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ทุกวัน

(ง) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

การดำเนินการ

๑. แยกไฟระบบคอมพิวเตอร์แม่ข่าย ออกจากสายเมนหลัก

๒. ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหาย ที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้า ได้ประมาณ 20-30 นาที

๓. เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุง รักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอตรวจสอบระบบสำรองไฟฟ้า(UPS)ทุกวันศุกร์

๔. เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ

(จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึง หรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

การดำเนินการ

๑. สแกนหาชุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยการใช้ซอฟท์แวร์เพื่อเป็นเครื่อง มือในการค้นหาช่องโหว

๒. ติดตั้ง Firewall เพื่อฟ้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓. ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กร และกลั่นกรองข้อมูลที่มาทาง Website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบ สารสนเทศและเครือข่ายคอมพิวเตอร์

๔. จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณ ข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบ สารสนเทศ มีความถี่ใน การเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕. ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสมาเสมอ และปิดพอร์ตที่ไม่ใช้บริการทั้งหมด

๖. กำหนดรหัสผ่านไม่น้อยกว่า 8 ตัวอักษร ไม่ใช่คำที่ก่อให้เกิดการคาดเดาได้ง่าย ไม่ใช่รหัสผ่านเดียวกันทุกระบบ และมีการเปลี่ยนรหัสผ่านทุก 3 เดือน

๗. ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ D-DOS

(ฉ) ไวรัสคอมพิวเตอร์

<u>การดำเนินการ</u>

๑. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัส
- อัพเดตข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือชื่อบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๒. ระวังภัยจากการเปิดไฟล์จากชื่อบันทึกข้อมูลต่างๆ เช่น แผ่นดิสก์ แผ่นซีดี เป็นต้น
- สแกนหาไวรัสจากชื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จักหรือน่าสงสัย เช่น .pif เป็นต้น
- ไม่ใช้ชื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๓. ใช้ความระมัดระวังในการเปิด E-mail
- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๔. ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet
- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น ICQ MSN เป็นต้น
- ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสมาเสมอ
- หลีกเลี่ยง การแชร์ไฟล์โดยไม่จำเป็น

<u>ภัยพิบัติจากภายใน</u>

(ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

<u>การดำเนินการ</u>

๑. ทำการสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้ในจานแม่เหล็ก 1 ชุดในเวลาเที่ยงคืนของทุกวันศุกร์

๒. การสำรองข้อมูลห้วยระบบ Manual โดยกำหนดให้เข้าหน้าที่ทำการสำรองข้อมูล ตามระยะเวลาที่กำหนดเป็นประจำเดือน โดยจะทำการสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในแผ่นซีดีรอมทุกวันศุกร์แรกของทุกเดือน

๓. ทำการทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ให้ทำการสำรองไว้ในแผ่นซีดีรอม

๔. ทำการทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ให้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่อง แม่ข่ายหลักเสียหาย

๕. ข้อมูลที่ห้อง ทำการ Recovery ทันที ได้แก่ โปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์องค์กร (Web Application Programming) และข้อมูลระบบงานสารบรรณอิเล็กทรอนิกส์

๖. จัดเข้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลจานแม่เหล็กของเครื่องแม่ข่าย เพื่อลดความเสียหายของข้อมูล

(ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

<u>การดำเนินการ</u>

๑. ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้

๒. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

๓. ไตร่ตรองให้รอบคอบก่อนที่จะขอข้อมูลของผู้อื่นโดยผ่านอุปกรณ์ Thumb Drive

๔. หลีกเลี่ยง การใช้แชร์ไฟล์โดยไม่จำเป็น

(ค) เจ้าหน้าที่หรือ บุคลากรของหน่วยงานขาดความรู้ความในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

<u>การดำเนินการ</u>

๑. ให้ความรู้แก่บุคลากรและหน่วยงาน

๒. ใส่กุญแจตู้ชุมสาย (Hub)และตู้สวิทช์ (Switches) เพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่หรือบุคคลการที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

๑. การสำรองข้อมล (Backup)

(๑) การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้ในจานแม่เหล็ก ๑ ชุดในเวลาเที่ยง คืนของทุกวันศุกร์

(๒) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรองข้อมูลตามระยะเวลาที่กำหนดเป็นประจำทุกเดือน โดยจะทำการสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในแผ่นซีดีรอม

๒. การกู้ข้อมูล (Recovery)

(๑) มีหนังสือแจ้งเตือนการกระทำอันควรจะกระทำให้ระบบเครือข่ายภายในล่มไปยังสำนัก / หน่วยงานภายในองค์กรเพื่อกำกับการดำเนินการดังกล่าว

- ทำการทดสอบ Recovery ข้อมูลโครงสร้างและโปรแกรมปฏิบัติการฐานข้อมูลที่ได้ทำการสำรองไว้ในแผ่นซีดีรอมทุกวันศุกร์ของสัปดาห์
- ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

(๒) ข้อมูลที่ต้องทำการ Recovery ทันทีได้แก่ โปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์องค์กร (Web Application Programming) และข้อมูลระบบงานสารบรรณอิเล็กทรอนิกส์

๓. การป้องกันไวรัส

(๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

(๒) มีการตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือชื่อบันทึกข้อมูล นอกจากนี้ ควรมีการตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

(๓) ใช้ความระมัดระวังในการเปิด e-mail ที่ไม่ทราบแหล่งที่มา

(๔) ระมัดระวังในการดาวน์โหลดไฟล์ต่างๆ จากอินเตอร์เน็ต

(๕) หลีกเลี่ยงการใช้แชร์ไฟล์โดยไม่จำเป็น

๔. ระบบไฟฟ้า

(๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล

(๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่อง สำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่กำลังใช้งานอยู่

๕. อุปกรณ์อื่นๆที่เกี่ยวข้อง

(๑) อุปกรณ์บันทึกข้อมูล และอุปกรณ์ควบคุมการเข้า ออกห้องคอมพิวเตอร์แม่ข่าย และห้องสำรองข้อมูล

(๒) เครื่อง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่าย คอมพิวเตอร์ขององค์กรได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

(๓) อุปกรณ์ดับเพลิงด้วยสารเคมี สำหรับอุปกรณ์ IT ติดตั้งอยู่ที่ห้อง Datacenter ชั้น 2 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สำหรับกรณีเกิดไฟไหมในอาคาร

(๔) คอมพิวเตอร์ที่ใช้บันทึกข้อมูลผู้ใช้งานอินเตอร์เน็ต

(๕) โปรแกรมตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กรเพื่อสังเกตปริมาณข้อมูล ความถี่ และการเรียกใช้บน เครือข่าย เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

(๖) มีอุปกรณ์คอมพิวเตอร์ที่แสดงความเคลื่อนไหวของระบบงานต่างๆ หากเกิดปัญหาจะสามารถแก้ไขได้ทันที

มาตรการความปลอดภัยด้วยรหัสผ่าน

การสร้างความปลอดภัยให้กับระบบสารสนเทศมีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศไม่สามารถเข้าถึงแก้ไขเปลี่ยนแปลงข้อมูล หรือไม่สามารถใช้งานระบบสารสนเทศในส่วน ที่มิได้อำนาจหน้าที่เกี่ยว ข้อง โดย

๑. กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบโดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยว ข้อง ผู้ที่รับ ผิดชอบสามารถเข้า ในระบบได้ตามความรับผิดชอบ โดยมีลำดับชั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละดับ ดังนี้

(๑) ผู้ดูแลระบบเครือข่ายหรือผู้ดูแลเครื่องแม่ข่ายจะต้องเป็นผู้ควบคุมรหัสผู้ใช้งานทั้งหมดโดยกำหนดรหัส ผู้ใช้งานให้แก่บุคคลที่รับผิดชอบโดยตรงในแต่ละงานให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบเครือข่าย

(๒) การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ FTP Server จะต้องระบุถึง IP Address ของผู้ใช้งานและแฟ้มข้อมูลที่ต้องการเข้าถึง

(๓) การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ Database Server จะต้องกำหนดแยกเป็นรายฐานข้อมูลที่ต้องการใช้งานและเข้าถึง

๒. กำหนดระยะเวลาการใช้งานระบบสารสนเทศของผู้ใช้ระบบ โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้เมื่อพ้นระยะเวลาที่กำหนดไว้

๓. การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๘ ตัวอักษร และควรใช้ตัวเลข อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือนโดยการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้ายซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไห้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่น รู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหมโดยทันทีเพื่อป้องกันความปลอดภัย ของการใช้ระบบสารสนเทศ

ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๑. กรณีเครื่องลูกข่าย

(๑) ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศรับทราบหรือกรณีมีเหตุอันทำให้ศูนย์เทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

(๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องนั้นโดยเร็ว

(๓) ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ดึงสายแลนออกจากชุดชุมสายในชั้นนั้นออกให้หมด

(๔) ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ แจ้งเหตุขัดข้องนั้นให้หัวหน้าหรือผู้อำนวยการรับทราบโดยเร็วที่สุด

๒. กรณีเครื่อง แม่ขายและอุปกรณ์เครือข่าย

(๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็วแล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

(๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่อง สำรองไฟฟ้า

(๓) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

(๔) รีบขนย้ายเครื่อง ไปไว้ในที่ปลอดภัย

(๕) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

(๖) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รบหาอุปกรณ์สำรอง หรือแว้งให้บริษัท ที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

(๗) ผู้ดูแลระบบ ต้องริบแจ้งให้หัวหน้าหรือผู้อำนวยการรับทราบโดยเร็ว

๓. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

(๑) เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้น ๆดึง สาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

(๒) ทำการสแกนและฆ่า ไวรัสหรือ กักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัสที่มีอยู่ในเครื่อง

(๓) แจ้งเจ้าหน้าที่กลุ่มสารนิเทศ เพื่อตรวจสอบละเอียด

๔ หลักปฏิบัติของบุคลากรในการ!เองกันอัคคีภัย

เพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติของบุคลากรในกลุ่มสารนิเทศ ดังนี้

(๑) ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

(๒) ควรศึกษาเรื่อง ตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

(๓) ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบดูทางออกฉุกเฉินไม่ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัยให้นับจำนวนประดูห้องโดยเริ่มจากห้องทำงานตนเอง ไปอังทางออกฉุกเฉินทั้งสองทางเพื่อให้ไปถึงทางหนีฉุกเฉินไต้ถึงแม้ว่าจะดับ หรือปกคลุมไปด้วยควัน

(๔) เมื่อเกิดเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้จากนั้นหนีจากอาคารแล้วโทรศัพท์แว้งหน่วยดับเพลิงโทร ๑๙๙ ทันทีหรือแจ้ง ๑๖๖๙

(๕) เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ให้รบหาทางหนีออกจากอาคารทันที

(๖) ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันที รบแจ้งฝ่ายอาคาร และสถานที่เพื่อโทรศัพท์แจ้งหน่วยดับเพลิงต่อไป

(๗) ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงานก่อนจะหนีออกมาให้วางมือบนประตูหากประตูมีความเย็นอยู่ค่อยๆปิดประตูแล้วหนีไปยังทางหนีไฟฉุกเฉินที่อยู่ใกล้ที่สุด

(๘) ถ้าเพลิงไหม้อยู่บริเวณใกล้ๆ ประตูจะมีความร้อนห้ามเปิดประตูเด็ดขาดให้รีบโทรศัพท์เรียกหน่วยดับเพลิง และแจ้งให้ทราบว่าท่าน อยู่ที่ใดของอาคารซึ่งถูกเพลิงไหม้ หาผ้าเช็ดตัวเปียกๆ ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

(๙) เมื่อต้องเผชิญกับควันไฟที่ปกคลุมให้ใช้วิธีคลานหนีไปทางฉุกเฉินเพราะอากาศ บริสุทธิ์จะอยู่ด้านล่าง (เหนือพื้นห้อง) นำกุญแจห้องทำงานไปด้วยหากหมดหนทางหนีจะได้สามารถกลับ เข้าห้องไต้

(๑๐) ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

๕. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ จะมีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับสูงมากดังนั้นสิ่ง ที่มักจะเกิด ขึ้นและยากที่จะหลีกเลี่ยงได้ก็คือผลกระทบต่างๆ ที่เกิดขึ้นจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลที่สำคัญรวมถึงการสูญเสียเวลา จากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ซึ่งประกอบด้วย

(๑) ไฟฟ้า ตก (Sag หรือ Brown out)

ไฟฟ้าตก คือ สภาวะที่แรงดันไฟฟ้าลดต่ำลงจากปกติในช่วงเวลาสั้นๆ ซึ่งเป็นปัญหาทางไฟฟ้าที่พบบ่อยที่สุด

สาเหตุ เกิดจากการเปิดสวิตซ์อุปกรณ์บางชนิดที่ต้องการใช้กระแสไฟฟ้ามาก เช่นเครื่องปรับอากาศ ลิฟต์ และเครื่องมือเครื่องจักร เป็นต้น อุปกรณ์เหล่านี้ต้องการ

กระแสไฟฟ้ามากในการติดเครื่อง เมื่อเทียบกับการทำงานในภาวะปกติ ส่งผลให้แรงดันไฟฟ้า ในสายส่งการไฟฟ้าฯ ลดต่ำลง

(๒) ไฟฟ้าดับ (Black out)

ไฟฟ้าดับ คือ สภาวะที่กระแสไฟฟ้า หยุดไหล

สาเหตุ เกิดจากความต้องการกระแสไฟฟ้าจากสายส่งการไฟฟ้าฯ ที่มากเกินไปเกิดไฟฟ้าลัดวงจรในสายส่ง พายุฟ้าคะนอง แผ่นดินไหว และปัญหาที่เกิดกับสายส่งไฟฟ้าฯ เช่น เสาไฟฟ้าล้มหรือหม้อแปลงระเบิด ฯลฯ ซึ่งส่งผลให้ไม่สามารถจ่ายไฟจากการไฟฟ้าได้ผลกระทบ การทำงานของ RAM หยุดชะงักทันที ทำให้ข้อมูลปัจจุบันสูญหายได้ รวมถึงการบันทึกข้อมูลของตารางการจัดการแท้เม (FAT) สูญหายได้มีผลให้ข้อมูลที่เก็บไว้ทั้งหมดสูญหายได้

(๓) ไฟฟ้ากระชาก (Spike)

ไฟฟ้ากระชากคือ สภาวะที่แรงดันไฟฟ้าเพิ่มสูงขึ้นอย่างกะทันหันโดยสามารถเข้าไป ยังอุปกรณ์ไฟฟ้าได้ทั้งจากสายส่งการไฟฟ้าฯ เครือข่ายคือสาร และสายโทรศัพท์

สาเหตุ เกิดจากฟ้าผ่าในบริเวณใกล้เคียง หรืออาจเกิดจากสายส่งการไฟฟ้าฯ ที่หยุดการ ทำงานไปและกลับมาทำงานใหม่อย่างกะทันหัน

ผลกระทบ สร้างความเสียหายหรือทำลายชิ้นส่วนอุปกรณ์อิเล็กทรอนิกส์ของอุปกรณ์ ไฟฟ้าได้รวมถึงข้อมูลเกิดการสูญหาย

(๔) ไฟฟ้าเกิน (Surge)

ไฟฟ้าเกิน คือ สภาวะที่มีแรงดันไฟฟ้าไหลมามากเกินในช่วงเวลาสั้นๆ (1/120 วินาที)

สาเหตุ เกิดจากการใช้อุปกรณ์ไฟฟ้าที่มีมอเตอร์กินไฟมาก เช่น เครื่องปรับอากาศ หรืออุปกรณ์ไฟฟ้าอื่นๆ ที่ลักษณะใกล้เคียงกัน ฯลฯ เนื่องจากอุปกรณ์เหล่านี้เมื่อหยุดทำงานแรงดันไฟฟ้าส่วนหนึ่งที่เหลืออยู่ในมอเตอร์จะไหลกลับเข้าไปในสายส่งการไฟฟ้าฯ ทำให้เกิดแรงดันไฟฟ้าสูงเกิน

ผลกระทบ ทำให้ชิ้นส่วนอุปกรณ์ภายในเสื่อมสภาพเร็วกว่าปกติหรือเสียหายได้ รวมถึง หน่วยความจำของคอมพิวเตอร์สูญ หายและคลาดเคลื่อน Power Supply เสียหาย และการทำงานของ ระบบคือสารผิดพลาด

(๕) สัญญาณรบกวน (Noise)

สัญญาณรบกวน คือ สัญญาณรบกวนที่เกิดจากสนามแม่เหล็กไฟฟ้า (EMI) และสัญญาณคลื่นความถี่วิทยุ (RFI) ซึ่ง 2 สัญญาณเหล่านี้จะไปรบกวนสัญญาณคลื่นไซน์ (Sine Wave) ของสายส่งการไฟฟ้าฯ

สาเหตุ เกิดขึ้นได้จากปรากฏการณ์ทางธรรมชาติ (เช่น ฟ้าผ่า) การเปิด-ปิดสวิตช์อุปกรณ์ ไฟฟ้า เครื่อง ส่งวิทยุ เป็นต้น โดยสัญญาณรบกวนอาจเกิดขึ้นเป็นระยะๆ หรืออาจเกิดอย่าง สม่ำเสมอได้

ผลกระทบ ทำให้การประมวลผลของโปรแกรมและแฟ้มข้อมูลผิดพลาด และเกิด ข้อบกพร่องศูนย์เทคโนโลยีสารสนเทศและการคือสารได้มี

การป้องกันปัญหาจากกระแสไฟฟ้าดังกล่าวโดยการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptable Power Supply : UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล

แผนทำระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม

การกู้คืน ระบบเครื่อง แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติ ระบบเครื่องแม่ข่ายและอุปกรณ์เครือข่าย จะต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ไต้ตลอดเวลา ๒๔ ชั่วโมงหากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุด หรือเท่าที่จะทำไต้ แผนการนี้เป็นวิธีการที่ทำ ให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการ ดังนี้

(๑) จัดหาอุปกรณ์ชิ้นส่วน ใหม่เพื่อทดแทน

(๒) เปลี่ยนอุปกรณ์ชิ้น ส่วนที่เสียหาย

(๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

(๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

(๕) นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง

(๖) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

ส่วนที่ ๕

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

(๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

(๒) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

(๑) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๒) สำนักงานตรวจสอบภายใน

(๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การประเมินผลกระทบ

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ให้หน่วยงานหรือองค์กรยึดถือหลักการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้เป็นแนวทางในการประเมินระดับผลกระทบโดยกำหนดการประเมินระดับผลกระทบของธุรกรรมทาง อิเล็กทรอนิกส์ จะต้องประเมินผลกระทบในด้านต่อไป

(๑) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน

(๒) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกาย หรืออนามัย

(๓) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียทีอาจได้รับความเสียหายอื่นใดนอกจากข้อ (๒)

(๔) ผลกระทบด้านความมั่นคงของรัฐ

๑.๑ การประเมินผลกระทบด้านมูลค่าความเสียหายทางการเงิน

ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีมูลค่าความเสียหายทางการเงินไม่เกินหนึ่งล้านบาทให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งล้านบาทแต่ไม่เกินหนึ่งร้อยล้านบาท ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งร้อยล้านบาทขึ้นไปให้จัดเป็นผลกระทบระดับสูงในการประเมินมูลค่าความเสียหายทางการเงินตามวรรคหนึ่งให้คำนวณจากความเสียหายที่จะเกิดขึ้นในหนึ่งวันและคำนวณความเสียหายโดยตรงเท่านั้น

๑.๒ การประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตราย ต่อชีวิต ร่างกาย หรืออนามัย

ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีที่ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรือ อนามัย ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรือ อนามัย ตั้งแต่หนึ่งคน แต่ไม่เกินหนึ่งพันคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรือ อนามัย เกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน ให้จัดเป็นผลกระทบ ระดับสูงในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตราย ต่อชีวิต ร่างกายหรืออนามัยตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับ ผลกระทบใน ๑ วัน

๑.๓ การประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความ เสียหายอื่น

ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบไม่เกินหนึ่งหมื่นคนให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่า หนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับกลาง

(๓) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับสูง ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบ ในหนึ่งวัน และคำนวณความ เสียหายโดยตรงเท่านั้น

๑.๔ การประเมินผลกระทบด้านความมั่นคงของรัฐ

ให้จัดเป็นสองระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(๑) ในกรณีไม่มีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับต่ำ

(๒) ในกรณีมีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับสูง หากปรากฏว่ามีผลประเมินที่เป็นผลกระทบในระดับสูงด้านหนึ่งด้านใดให้ธุรกรรมทางอิเล็กทรอนิกส์นั้นต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด และหากมีผลกระทบในระดับกลางอย่างน้อยสอง

ด้านขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับกลางขึ้นไปในกรณีที่ไม่เป็นไปตามวรรคหนึ่ง ให้ธุรกรรมทางอิเล็กทรอนิกส์ใช้วิธีการแบบปลอดภัย ในระดับไม่ต่ำกว่าระดับพื้นฐาน

๒. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) ปีละ ๑ ครั้ง

๒) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยสำนักงานตรวจสอบภายใน เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัย สารสนเทศ

(๒) มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๑) มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ ๑ ครั้ง

๒) มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ ปีละ ๑ ครั้ง

๓) ตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๔) มีมาตรการในการตรวจประเมินระบบสารสนเทศ ดังนี้

- ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว
- ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
- ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบ ระบบบริหารจัดการความมั่นคงปลอดภัย
- ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบนทึก ข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
- ในกรณีที่มีเครื่องมือสำหรับการตรวจสอบประเมินระบบสารสนเทศควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

(๓) รายงานผลการประเมินความเสี่ยงด้านสารสนเทศปีละ 1 ครั้ง ต่อคณะกรรมการนโยบายและพัฒนาสารสนเทศ และแจ้งคณะกรรมการบริหารความเสี่ยงมหาวิทยาลัยเพื่อดำเนินการต่อไป

(๔) แสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนของการรายงานผลการติดตามตรวจสอบและประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๖

แนวปฏิบัติ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

(๑) เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของมหาวิทยาลัย

(๒) เพื่อเป็นการป้องกันการกระทำที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

(๓) เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

(๑) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

(๑) จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของมหาวิทยาลัยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

(๒) จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย

(๓) จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของ มหาวิทยาลัย

(๔) จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน

(๕) ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวัง ในรูปแบบที่สามารถเข้าใจและนาไปปฏิบัติได้ง่ายโดยมีการปรับปรุงความรู้อยู่เสมอ

(๖) การมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความ ต้องการผู้ใช้งาน

ส่วนที่ ๗

การกำหนดผู้รับผิดชอบ

เพื่อกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

๑. ระดับนโยบาย

ให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน ที่ทำหน้าที่ (Chief information officer : CIO) และผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ ติดตามและกำกับดูแลควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติการ และให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง เสียหาย หรืออันตรายที่เกิดขึ้น

๒. แนวทางปฏิบัติ ของผู้รับผิดชอบ

๒.๑ ระดับนโยบาย ผู้รับผิดชอบ

๒.๑.๑. ผู้บริหารระดับสูงสุดของหน่วยงาน (CEO)

มีหน้าที่

- รับผิดชอบในการกำหนดนโยบาย ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ ผู้บริหารเทคโนโลยีสารสนเทศ (CIO)
- รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหนึ่งผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

มีหน้าที่

- ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติการ
- ทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันทุก ๔ ปี

๒.๒ ระดับบริหาร ผู้รับผิดชอบ

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

รองผู้อำนวยการสำนักวิทยบริการ/หัวหน้าฝ่าย ที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หรือเทียบเท่าหัวหน้างาน

มีหน้าที่

๒.๒.๑ รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒.๒.๒ รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๒.๓ ระดับปฏิบัติการ ผู้รับผิดชอบ

ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากระดับบริหาร ได้แก่ นักวิชาการคอมพิวเตอร์
มีหน้าที่

๒.๓.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๓.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูล และสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๓.๓ รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องแม่ข่ายคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่าย

๒.๓.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๓.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลเว็บไซต์หน่วยงาน จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๓.๖ ควบคุมการเข้า-ออกห้อง Server ตามการกำหนดสิทธิ์การเข้าถึง Server

๒.๓.๗ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ปกติตลอด ๒๔ ชั่วโมง

๒.๓.๘ กำกับ ดูแลการติดตั้ง รื้อถอน ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN ,Internet ,Intranet ที่ให้บริการในมหาวิทยาลัย

๒.๓.๙ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๒.๓.๑๐ รายงานผลการปฏิบัติงานสถานการณ์ที่เกิดขึ้นกับระบบเครือข่าย ระบบฐานข้อมูล และระบบสารสนเทศ ให้แก่ ผู้บริหารระดับสูง ให้ทราบอย่างสม่ำเสมอ

๒.๓.๑๑ กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิ์การเข้าถึงระบบ

๒.๓.๑๒ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่บน Server ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์ ให้สามารถใช้งานได้ตามปกติ