

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา
พ.ศ.๒๕๖๘

จัดทำโดย
สำนักคอมพิวเตอร์
มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

บทนำ

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ผ่านเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาเป็นไป มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งกำหนดให้หน่วยงานของรัฐจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง โดยมีวัตถุประสงค์ เพื่อ

๑. คงไว้ซึ่งการให้บริการเครือข่ายคอมพิวเตอร์มหาวิทยาลัยได้อย่างมีประสิทธิภาพและเสถียรภาพ

๒. ปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้

๓. ปกป้องและรักษาซึ่งเอกภาพของข้อมูลและทรัพยากรสารสนเทศของมหาวิทยาลัย

๔. ให้ผู้มีส่วนเกี่ยวข้องเข้าใจหลักปฏิบัติการใช้เครือข่ายตามหลักจริยธรรมและหลักกฎหมายมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาจึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ดังนี้

(๑) แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

(๒) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

(๓) แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(๔) แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

(๕) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(๖) แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยห้องปฏิบัติการคอมพิวเตอร์

(๗) การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

(๘) แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

(๙) แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

(๑๐) แผนการสำรองข้อมูลและกู้คืนข้อมูล(Backup and Recover)

(๑๑) แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

(๑๒) ข้อกำหนดการใช้งานระบบระบบเครือข่ายและคอมพิวเตอร์

(๑๓) ข้อกำหนดการใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์

(๑๔) ข้อปฏิบัติในการใช้จดหมาย อิเล็กทรอนิกส์

(๑๕) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑๖) นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

สารบัญ

หน้า

๑. แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย.....	1
๒. แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ.....	4
๓. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย.....	6
๔. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์.....	8
๕. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control).....	10
๖. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยห้องปฏิบัติการคอมพิวเตอร์.....	12
๗. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ.....	16
๘. แนวปฏิบัติควบคุมการใช้กล้องวงจรปิด(CCTV)	18
๙. แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ.....	21
๑๐. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure).....	23
๑๑. แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน.....	29
๑๒. ข้อกำหนดการใช้งานระบบระบบเครือข่ายและคอมพิวเตอร์	30
๑๓. ข้อกำหนดการใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์.....	32
๑๔. ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)	34
๑๕. นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	38
๑๖. นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ	39

๑. แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยเป็นสิ่งสำคัญ เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อมหาวิทยาลัยนั้น

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย ดังนี้

แนวปฏิบัติของทิศทางการบริหารจัดการความมั่นคงปลอดภัย (Management Directions for Information Security) เพื่อใช้เป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยซึ่งจัดทำเป็นลายลักษณ์อักษรโดยผู้มีอำนาจเป็นผู้ลงนามอนุมัติและเผยแพร่ให้บุคลากรที่เกี่ยวข้องกับงานของมหาวิทยาลัยทุกคนได้รับทราบ

๑. แนวปฏิบัติสำหรับความมั่นคงปลอดภัย (Information Security) เพื่อให้เกิดความเชื่อมั่น และมีความปลอดภัยในการใช้งานระบบสารสนเทศของมหาวิทยาลัย ทำให้การดำเนินงานของมหาวิทยาลัยมีประสิทธิภาพและประสิทธิผล

๑.๑ เพื่อสร้างความตื่นตัวให้บุคลากรของมหาวิทยาลัย ผู้ดูแลระบบและหน่วยงานภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัยตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศ

๑.๒ เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่น ๆ ในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัยที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

๒. การสอบทานแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ (Review of the Policies for information Security) เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิ์ผล กำหนดให้มีการตรวจสอบและประเมินแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเกิดการเปลี่ยนแปลงที่มีนัยสำคัญ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ

๓. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติดังนี้

๓.๑ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน หรือเมื่อระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๒ เลือกรหัสผ่านที่ปลอดภัยและรักษารหัสนั้นให้เป็นความลับอยู่ตลอดเวลา

๓.๓ ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ให้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ

๓.๔ ไม่ลักลอบใช้รหัสผ่าน หรือแกระหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้ใช้

๓.๕ รายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

๔. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล ผู้ใช้งานต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ดูแล เพื่อป้องกันข้อมูลสำคัญสูญหาย

๔.๑ ผู้ดูแลระบบมีอำนาจที่จะยุติหรือเพิกถอนสิทธิการใช้คอมพิวเตอร์และเครือข่ายโดยทันที หากตรวจพบผู้ใช้ที่ฝ่าฝืนระเบียบหรือกระทำการใดที่อาจสร้างความเสียหายให้กับระบบ

๔.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องกำหนดรหัสในการเข้าใช้งาน

๔.๓ การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานจะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานนั้น

๕. ต้องไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

๕.๑ ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๕.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งาน และรหัสผ่านของผู้ดูแลระบบ

๕.๓ ผู้ใช้งานต้องล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๕.๔ การป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและสินทรัพย์ด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา smart mobile device เมื่อปฏิบัติงานอยู่นอกสถานที่ ได้แก่

๕.๔.๑ ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

๕.๔.๒ ต้องเข้ารหัสข้อมูลที่สำคัญไว้

๕.๕ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ได้แก่

๕.๕.๑ การสำรองข้อมูลที่เป็นข้อมูลลับต้องเข้ารหัสด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ ๑๒๘ bits (๑๒๘-bits Encryption) เป็นอย่างน้อยเพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง

๕.๕.๒ การอนุญาตให้เข้าถึงข้อมูลลับผ่านเครือข่ายต้องเข้ารหัสด้วยรหัสผ่าน กำหนดวันหมดอายุของการเข้าถึง และระบุให้เข้าถึงได้เฉพาะผู้มีสิทธิ

๕.๕.๓ ไม่อนุญาตให้ส่งผ่านข้อมูลลับผ่านเครือข่าย หากต้องส่งผ่านเครือข่ายต้องขออนุญาตจากผู้บังคับบัญชาทุกครั้ง และในกรณีที่แนบไฟล์แนบต้องเข้ารหัสด้วยรหัสผ่านทุกครั้ง

๕.๕.๔ การสำเนาข้อมูลชั้นความลับต้องจดบันทึกจำนวนชุดที่สำเนา รายละเอียดผู้ดำเนินการทุกครั้ง

๖. การทำลายสื่อบันทึกข้อมูลหรือข้อมูลลับให้เป็นไปตามแนวปฏิบัติในการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๒. แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

การควบคุมการเข้าถึงระบบ (Access Control) จัดทำขึ้นเพื่อเป็นแนวปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศภายในมหาวิทยาลัยได้อย่างเหมาะสม มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา จึงกำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ ดังนี้

๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน จำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้สารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

๒.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- เพิ่มข้อมูล
- แก้ไขข้อมูล
- ลบข้อมูล
- อนุมัติ/อนุญาต
- ไม่มีสิทธิ

๒.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๓.๑ จัดแบ่งประเภทข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์
คำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

- อนุมัติ

- ข้อมูลสารสนเทศด้านการศึกษาและวิจัยที่ให้บริการ เช่น ข้อมูลการลงทะเบียนเรียนของนักศึกษา ข้อมูลนักศึกษา ข้อมูลบุคลากร เป็นต้น

๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

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

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๓.๔ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๓.๕ การกำหนดเวลาที่ได้เข้าถึง

๓.๖ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๔. มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๔.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๔.๒ มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๓. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยากำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

๑.๑ ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซน

ภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

๑.๒ ผู้ให้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการสำนักคอมพิวเตอร์ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๑.๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการสำนักคอมพิวเตอร์ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบ และผู้ใช้บริการอื่นๆ

๑.๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๑.๕ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๑.๕.๑ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๑.๕.๒ ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

๑.๕.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๑.๕.๔ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๑.๕.๕ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๑.๕.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๑.๕.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑.๕.๘ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๑.๕.๙ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๑.๖ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๑.๖.๑ ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๑.๖.๒ ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๑.๖.๓ ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๑.๖.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑.๗ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๑.๗.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักคอมพิวเตอร์

๑.๗.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๑.๗.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากกระยะไกลต้องได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักคอมพิวเตอร์

๑.๗.๔ การเข้าสู่ระบบจากกระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๑.๗.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

๔. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์(Firewall) ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยามีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

- ๑.๑ สำนักคอมพิวเตอร์ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
- ๑.๒ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์
- ๑.๓ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User password)
- ๑.๔ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
- ๑.๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
- ๑.๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน
- ๑.๗ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อ นอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์ก่อน
- ๑.๘ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์สารสนเทศ โดยต้องระบุข้อมูลดังนี้
 - ๑.๘.๑ หมายเลข Port ที่ต้องการขอให้เปิด
 - ๑.๘.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
 - ๑.๘.๓ วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ
 - ๑.๘.๔ วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้
- ๑.๙ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า
- ๑.๑๐ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

- ๑.๑๑ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยามีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข
- ๑.๑๒ ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาหรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางศูนย์สารสนเทศจะยกเลิกการให้บริการทันที
- ๑.๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากสำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

๕. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑) ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาจะต้องทำการลงทะเบียนกับ ผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์หรือผู้ที่ได้รับมอบหมายอย่างเป็นทางการเป็นลายลักษณ์อักษร

๒) ผู้ดูแลระบบ ต้องดำเนินการดังนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึง อย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้ สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจาก ภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

(๔) ควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรตรวจสอบว่าสัญญาณรั่วไหลออกไป ภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจ ช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

(๕) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มา จากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๖) ควรเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแล ระบบควรเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ไม่สามารถเดาหรือ เจาะรหัสได้โดยง่าย

(๗) ต้องกำหนดค่าใช้ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

(๘) ควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะ

อุปกรณ์ที่มี MAC Address และ ชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

(๙) ควรจะมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

(๑๐) ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

(๑๑) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อยกยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการสำนักคอมพิวเตอร์ทราบโดยทันที

๖. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยห้องปฏิบัติการคอมพิวเตอร์

แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยห้องปฏิบัติการคอมพิวเตอร์ เพื่อการใช้ห้องปฏิบัติการในการเรียนการสอนได้อย่างมีประสิทธิภาพส่งผลให้เกิดความปลอดภัยภายในห้องปฏิบัติการ

การให้บริการห้องปฏิบัติการคอมพิวเตอร์

ให้บริการแก่นักศึกษา อาจารย์ บุคลากร หน่วยงานภายในของมหาวิทยาลัยฯ เพื่อใช้ในการเรียนการสอน และการจัดโครงการอบรมต่างๆ ทั้งของสำนักคอมพิวเตอร์ และรองรับการอบรมของสาขาวิชาต่างๆ ที่เข้ามาขอใช้บริการใช้ห้องปฏิบัติการคอมพิวเตอร์ ตั้งอยู่ ณ อาคาร ๑๐ มีทั้งหมด ๓ ชั้น เปิดให้บริการ วันจันทร์ – ศุกร์ เวลา ๘.๓๐ - ๑๖.๓๐ และวันอาทิตย์ เวลา ๘.๓๐ - ๑๖.๓๐ สามารถแบ่งห้องปฏิบัติการคอมพิวเตอร์ได้ จำนวน ๗ ห้องดังนี้

- ชั้น ๕ อาคาร ๑๐ ห้อง ๑๐๕๑ จำนวน ๔๘ เครื่อง และเครื่องผู้สอน ๑ เครื่อง
- ชั้น ๕ อาคาร ๑๐ ห้อง ๑๐๕๓ จำนวน ๔๘ เครื่อง และเครื่องผู้สอน ๑ เครื่อง
- ชั้น ๕ อาคาร ๑๐ ห้อง ๑๐๕๕ จำนวน ๘๐ เครื่อง และเครื่องผู้สอน ๑ เครื่อง
- ชั้น ๖ อาคาร ๑๐ ห้อง ๑๐๖๑ จำนวน ๕๔ เครื่อง และเครื่องผู้สอน ๑ เครื่อง
- ชั้น ๖ อาคาร ๑๐ ห้อง ๑๐๖๓ จำนวน ๕๔ เครื่อง และเครื่องผู้สอน ๑ เครื่อง
- ชั้น ๖ อาคาร ๑๐ ห้อง ๑๐๖๔ จำนวน ๕๔ เครื่อง และเครื่องผู้สอน ๑ เครื่อง
- ชั้น ๖ อาคาร ๑๐ ห้อง ๑๐๖๖ จำนวน ๕๐ เครื่อง และเครื่องผู้สอน ๑ เครื่อง
- ชั้น ๙ อาคาร ๑๐ ห้อง ๑๐๙๒ จำนวน ๕๖ เครื่อง และเครื่องผู้สอน ๑ เครื่อง

อุปกรณ์ประจำห้อง

- ระบบเสียง (เครื่องขยายเสียง ,ไมค์โครโฟน,ลำโพง)
- ระบบภาพ (โปรเจคเตอร์พร้อมรีโมทควบคุม, ฉากรับภาพ, ตัวแปลงสัญญาณภาพ)
- กระดานไวท์บอร์ด
- เครื่องคอมพิวเตอร์ใช้ในการเรียน และเครื่องคอมพิวเตอร์ใช้ในการสอน
- เครื่องปรับอากาศ
- ถังดับเพลิง

ข้อปฏิบัติการในการใช้ห้องปฏิบัติการคอมพิวเตอร์ ในอาคาร ๑๐

1. แต่งกายชุดนักศึกษาตามระเบียบมหาวิทยาลัยฯ หรือชุดสุภาพที่เหมาะสมกับกิจกรรมการเรียนการสอนหรือกิจกรรมโครงการอบรมต่าง ๆ ที่เกี่ยวข้อง
2. ห้ามส่งเสียงดัง เปิดเพลง ตูหนัง การกระทำรบกวนผู้อื่น
3. ช่วยรักษาความสะอาด ไม่นำอาหาร เครื่องดื่ม ขนมขบเคี้ยวทุกชนิดเข้ามาในห้องปฏิบัติการ
4. ห้ามใช้คอมพิวเตอร์เพื่อวัตถุประสงค์อื่นนอกเหนือจากการเรียนการสอน
5. ในช่วงเวลาที่มีการเรียนการสอน ห้ามนักศึกษาที่ไม่เกี่ยวข้องเข้ามาในห้องปฏิบัติการคอมพิวเตอร์
6. ห้ามนำซอฟต์แวร์ (Software) ใด ๆ มาติดตั้งลงในเครื่องคอมพิวเตอร์ของห้องปฏิบัติการ หากมีความจำเป็นให้แจ้งเจ้าหน้าที่ห้องปฏิบัติการ และหากเป็นโปรแกรมที่ไม่มีลิขสิทธิ์ อาจารย์ผู้สอนต้องรับผิดชอบเกี่ยวกับความเสียหายที่อาจเกิดขึ้น
7. ห้ามเคลื่อนย้ายอุปกรณ์ (Hardware) ห้ามถอดปลั๊กไฟ เครื่องคอมพิวเตอร์หรือนำอุปกรณ์อื่นใดมาต่อพ่วงกับเครื่องคอมพิวเตอร์ เว้นแต่ จะได้รับอนุญาตจากเจ้าหน้าที่ประจำห้องปฏิบัติการคอมพิวเตอร์
8. เมื่อเลิกใช้งานห้องปฏิบัติการ ควรปิดเครื่องคอมพิวเตอร์ ปิดเครื่องปรับอากาศ และเก็บโต๊ะเก้าอี้ให้เรียบร้อย และปิดไฟส่องสว่างทุกครั้ง
9. หากมีปัญหาเกี่ยวกับการใช้งานให้ติดต่อเจ้าหน้าที่ประจำห้องปฏิบัติการคอมพิวเตอร์

ข้อปฏิบัติการในการเกิดอุบัติเหตุและวิธีแก้ไขเบื้องต้น

1. ไฟไหม้/ไฟฟ้าลัดวงจร ไม่นำอุปกรณ์มาต่อพ่วงให้เกิดไฟลัดวงจรหรือนำเครื่องดื่มเข้ามาในห้องปฏิบัติการเพราะอาจทำให้เกิดไฟฟ้าลัดวงจรได้

ข้อปฏิบัติเมื่อเกิดอุบัติเหตุไฟไหม้ /ไฟฟ้าลัดวงจร สิ่งแรกที่เราควรทำคือต้องรีบตัดไฟในห้องปฏิบัติการ และต้องรีบแจ้งให้ผู้ที่เกี่ยวข้องรีบดำเนินการแก้ไข หากไฟลุกลามจะต้องใช้เครื่องดับเพลิงซึ่งจะติดไว้บริเวณในห้องปฏิบัติการทุกห้อง

2. ไฟฟ้าดูด เนื่องจากการปฏิบัติการห้องปฏิบัติการคอมพิวเตอร์ ในบางห้องปฏิบัติการจะต้องมีการทดสอบในการประกอบ ตรวจสอบเครื่องมือ และการทดสอบของเครื่องหลังจากประกอบเสร็จแล้ว ต้องมีการทดสอบโดยการเสียบอุปกรณ์เข้ากับเมนบอร์ด และทดสอบการใช้งานของเครื่อง

ข้อปฏิบัติแก้ไขเมื่อเกิดอุบัติเหตุไฟดูด

รีบตัดกระแสไฟฟ้าทันที โดยการถอดเต้าเสียบหรือยกสะพานไฟหรือใช้ฉนวนฉกหรือฉุดให้ผู้ที่ได้รับอันตรายออกจากแหล่งกระแสไฟฟ้า หรือเชี่ยสายไฟให้หลุดออกไปจากตัวผู้บาดเจ็บ ห้ามใช้มือเปล่าแตะต้องตัวผู้ที่กำลังได้รับอันตรายจากกระแสไฟฟ้า เมื่อนำผู้ที่ถูก

กระแสไฟฟ้าดูดออกจากแหล่งกระแสไฟฟ้าแล้วต้องทำการปฐมพยาบาลเบื้องต้น โดยการผายปอดหรือเป่าปากให้ปอดทำงานชั่วคราวแล้วรีบนำส่งแพทย์ทันที

ข้อปฏิบัติ การปฐมพยาบาลและรักษาเบื้องต้น

- ทำการดึงผู้ป่วยออกจากกระแสไฟฟ้า หรือ ตัดกระแสไฟฟ้าโดยการปิดสวิตช์ แต่ถ้าไม่สามารถกระทำได้โดยวิธีนี้ ต้องดึงผู้ป่วยออกจากกระแสไฟฟ้า โดยยืนบนกระดานที่ไม่เปียกน้ำ หรือยืนบนวัสดุที่เป็นฉนวนที่ไม่นำไฟฟ้า เช่น แผ่นยาง
- เมื่อดึงผู้ป่วยออกจากกระแสไฟฟ้าแล้ว ลงมือกระตุ้นหัวใจและผายปอดให้ทันที ควรช่วยเหลือจนกระทั่งผู้ป่วยหายใจได้ และควรรีบนำส่งโรงพยาบาลทันที ถ้าหากผู้ป่วยมีอาการหนักมาก

3. อุบัติเหตุจากโต๊ะและเก้าอี้ เนื่องจากการปฏิบัติงานในห้องปฏิบัติการคอมพิวเตอร์ มีโต๊ะเก้าอี้สำหรับนักศึกษาและผู้ใช้งานห้องปฏิบัติการ แต่เนื่องจากเก้าอี้มีล้อเลื่อน และการใช้งานผิดประเภทอาจจะทำให้เกิดอันตรายได้

ข้อปฏิบัติ เมื่อเกิดอุบัติเหตุจากโต๊ะเก้าอี้

รีบทำการตรวจสอบอาการผู้ได้รับอุบัติเหตุ โดยการตรวจเช็ค บาดแผลและอวัยวะตามร่างกายว่าประสบปัญหาบาดเจ็บหรือมีการหัก เคล็ด ชัด ยอด ตรงไหนแล้วรีบดำเนินการปฐมพยาบาลเบื้องต้น และรีบพาผู้ประสบอุบัติเหตุส่งโรงพยาบาลทันทีหากผู้ได้รับอุบัติเหตุมีอาการบาดเจ็บสาหัส

4. อุบัติเหตุจากการลื่น ไถล และสะดุดรางเก็บสายไฟ เนื่องจากการปฏิบัติงานในห้องปฏิบัติการคอมพิวเตอร์มีพื้นต่างระดับกันบริเวณหน้าห้องที่เป็นกระดานไวท์บอร์ด และมีรางเก็บไฟสำหรับระหว่างแถวที่โต๊ะคอมพิวเตอร์ ถ้านักศึกษาหรือผู้ใช้งานห้องปฏิบัติการคอมพิวเตอร์ขาดความระมัดระวังในการใช้งานในห้องปฏิบัติการคอมพิวเตอร์อาจทำให้เกิดอุบัติเหตุได้

ข้อปฏิบัติ เมื่อเกิด อุบัติเหตุจากการลื่น ไถล และสะดุดรางเก็บสายไฟ

รีบตรวจสอบผู้ได้รับอุบัติเหตุ โดยการตรวจเช็ค บาดแผลและอวัยวะตามร่างกายว่าประสบปัญหาบาดเจ็บหรือมีการหัก เคล็ด ชัด ยอด ให้รีบดำเนินการปฐมพยาบาลเบื้องต้น และรีบพาผู้ประสบอุบัติเหตุส่งโรงพยาบาลทันทีหากผู้ได้รับอุบัติเหตุมีอาการบาดเจ็บสาหัส

ข้อปฏิบัติในการดำเนินการในเหตุฉุกเฉิน

เมื่อเกิดเหตุการณ์ ผู้ควบคุมห้องปฏิบัติการหรือผู้ที่ได้รับมอบหมายต้องไปถึงที่เกิดเหตุทันทีเพื่อควบคุมสถานการณ์และดำเนินการดังต่อไปนี้

- ควบคุมบริเวณที่เกิดเหตุ
- ปฐมพยาบาลเบื้องต้น และเรียกทีมหน่วย ชมรมสุริยะอาสาพยาบาล

เพื่อช่วยเหลือ

- ควบคุมอุบัติเหตุที่อาจเกิดขึ้นอีกครั้ง

- หาสาเหตุและเก็บรวบรวมข้อมูลที่เกี่ยวข้อง
- เก็บรักษาหลักฐานที่ทำให้เกิดอุบัติเหตุ เมื่อจะมีการเปลี่ยนแปลงหรือเคลื่อนย้าย
- รายงานอุบัติเหตุอุบัติภัยที่เกิดขึ้นให้ผู้บังคับบัญชาทราบ
- มีการสอบสวนเหตุการณ์ที่เกิดขึ้นเพื่อหาสาเหตุ และมาตรการป้องกันการเกิดซ้ำ

ข้อปฏิบัติในกรณีฉุกเฉิน ทั้งกรณีเพลิงไหม้ห้องปฏิบัติการคอมพิวเตอร์ เกิดเหตุการณ์ระเบิดหรืออุบัติเหตุต่าง ๆ ในห้องปฏิบัติการ

1. ให้ความช่วยเหลือผู้อยู่ในเหตุการณ์ และนำออกนอกบริเวณนั้น
2. มีการเตือนบุคคลต่าง ๆ ถึงอันตรายเพื่อความปลอดภัย
3. ให้การปฐมพยาบาลทันที ตามความเหมาะสม
4. ดับเพลิงขนาดย่อมด้วยถังดับเพลิงที่เตรียมไว้ในพื้นที่นั้น ๆ หากเพลิงรุนแรงหรือเกินบริเวณกว้าง
ให้ติดต่อหน่วยดับเพลิงทันที
5. ปิดเครื่องมือต่าง ๆ แล้วสับสวิทช์ไฟฟ้าหรือเบรกเกอร์ทันที
6. ห้ามเคลื่อนย้ายคนเจ็บหากการเคลื่อนย้ายทำให้เกิดอันตรายมากขึ้น
7. หากเสื้อผ้าติดไฟ ให้กลิ้งไปมาบนพื้นเพื่อให้ไฟดับหรือใช้ สปริงเกอร์ดับไฟ

ข้อปฏิบัติเมื่อเกิดเหตุเพลิงไหม้

1. ช่วยเหลือผู้ที่ตกอยู่ในอันตรายก่อน โดยตัวเองต้องไม่ตกอยู่ในอันตรายเสียเอง
2. กดปุ่มสัญญาณเตือนภัยที่อยู่บริเวณใกล้เคียง และแจ้งเหตุให้ผู้อยู่ใกล้เคียงทราบ
3. แจ้งเหตุเพลิงไหม้กับหน่วยงานที่รับผิดชอบ เพื่อขอความช่วยเหลือ
4. แยกส่วนที่เกิดเพลิงไหม้ออกจากส่วนอื่น ๆ เช่น โดยการปิดประตู หน้าต่าง
5. ทำการหยุดกระบวนการที่อาจก่อให้เกิดอันตราย หรือปิดเครื่องมือที่กำลังทำงานอยู่ หากสามารถดำเนินการได้อย่างปลอดภัย
6. ในกรณีเหตุเพลิงไหม้บริเวณกว้างให้อพยพหลบภัยอยู่นอกอาคาร

๗. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เป็นไปอย่างมั่นคงปลอดภัย มีแนวทางปฏิบัติดังนี้

แนวทางปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

๑) ผู้อำนวยการสำนักคอมพิวเตอร์กำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและ การสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและ กำหนดมาตรการรองรับหรือแก้ไขที่ เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสารได้

๒) การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ภายนอก

(๑) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและ การสื่อสารของมหาวิทยาลัย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติ จากผู้อำนวยการสำนักคอมพิวเตอร์

(๒) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความ จำเป็นที่ต้องเข้าใช้ งานระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้ เหตุผลในการขอใช้ ระยะเวลาในการใช้ การตรวจสอบความปลอดภัยของอุปกรณ์ ที่เชื่อมต่อเครือข่าย และการตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๓) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

(๑) หน่วยงานภายนอกที่ทำงานให้กับมหาวิทยาลัยทุกหน่วยงานไม่ว่าจะทำงานอยู่ ภายใน มหาวิทยาลัยหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของ มหาวิทยาลัย โดยสัญญา ต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยี สารสนเทศ

(๒) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงาน ภายนอก ต้อง กำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอก ลงนามในสัญญาไม่เปิดเผยข้อมูล

(๓) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มี ความสำคัญของ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ผู้ดูแลระบบต้องควบคุมการ

ปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๔) มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่ามหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(๕) กำหนดให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และ เอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๘. แนวปฏิบัติควบคุมการใช้กล้องวงจรปิด(CCTV) และคุ้มครองข้อมูลส่วนบุคคลในการใช้กล้องวงจรปิด

แนวปฏิบัติการใช้งานกล้องวงจรปิด CCTV ของสำนักคอมพิวเตอร์ เพื่อให้เกิดความมั่นคงปลอดภัย กล้องวงจรปิดที่สำนักคอมพิวเตอร์ดูแลจะมีเครื่องบันทึกภาพ ๕๕ เครื่อง ห้องควบคุมกล้องวงจรปิด อยู่ ณ อาคาร ๑๐ ชั้น ๕ ห้อง ๑๐๕๔ ใช้ตรวจสอบจำนวนกล้องที่ติดตั้ง เพื่อสำหรับการเฝ้าระวังสังเกตการณ์ในพื้นที่ภายในห้องปฏิบัติการคอมพิวเตอร์ และรอบบริเวณสำนักคอมพิวเตอร์

แนวปฏิบัติการใช้กล้องวงจรปิดภายในอาคาร ๑๐

- ๑) เพื่อการปกป้องอาคาร สิ่งอำนวยความสะดวกและทรัพย์สินของมหาวิทยาลัยจากความเสียหาย การขัดขวาง การทำลายซึ่งทรัพย์สินหรืออาชญากรรมอื่น
- ๒) เพื่อสนับสนุนหน่วยงานที่เกี่ยวข้องในการบังคับใช้กฎหมายเพื่อการยับยั้ง ป้องกัน สืบค้น และดำเนินคดีทางกฎหมาย
- ๓) เพื่อการให้ความช่วยเหลือในกระบวนการระงับข้อพิพาทซึ่งเกิดขึ้นในระหว่างที่มีกระบวนการทางวินัยหรือกระบวนการร้องทุกข์
- ๔) เพื่อการให้ความช่วยเหลือในกระบวนการสอบสวน หรือ กระบวนการเกี่ยวกับการส่งเรื่องร้องเรียน
- ๕) เพื่อการให้ความช่วยเหลือในกระบวนการริเริ่มหรือป้องกันการฟ้องร้องทางแพ่ง ซึ่งรวมไปถึงแต่ไม่จำกัดเพียงการดำเนินการทางกฎหมายที่เกี่ยวข้องกับการจ้างงาน

มหาวิทยาลัยทำการติดตั้งกล้องวงจรปิดในตำแหน่งที่มองเห็นได้ โดยจะจัดวางป้ายเตือนว่ามีการใช้งานกล้องวงจรปิด ณ ทางเข้าและทางออก รวมถึงพื้นที่ที่มหาวิทยาลัยเห็นสมควรว่าเป็นจุดที่ต้องมีการเฝ้าระวัง เพื่อเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเมื่อท่านเข้ามายังพื้นที่ โดยมีการจัดเก็บดังรายการต่อไปนี้

- ๑) ภาพนิ่ง
- ๒) ภาพเคลื่อนไหว
- ๓) ภาพทรัพย์สินของท่าน เช่น พาหนะ กระเป๋า หมวก เครื่องแต่งกาย เป็นต้น

ทั้งนี้ หน่วยงานจะไม่ทำการติดตั้งกล้องวงจรปิดในพื้นที่ที่อาจล่วงละเมิดสิทธิขั้นพื้นฐานของท่านจนเกินสมควร ได้แก่ ห้องน้ำ ห้องอาบน้ำ หรือสถานที่เพื่อใช้ในการพักผ่อนของผู้ปฏิบัติงาน เว้นแต่จะได้รับความยินยอมจากท่าน

ข้อปฏิบัติ การเปิดเผยข้อมูลส่วนบุคคล

การเก็บรักษาข้อมูลในกล่องวงจรปิดที่เกี่ยวกับนักศึกษา อาจารย์ ไว้เป็นความลับ และจะไม่ทำการเปิดเผย เว้นแต่ กรณีที่มหาวิทยาลัยมีความจำเป็นเพื่อให้สามารถบรรลุวัตถุประสงค์ในการเฝ้าระวังสังเกตการณ์ อาจเปิดเผยข้อมูลในกล่องวงจรปิดแก่ประเภทของบุคคล อาจารย์ หรือ นักศึกษา ดังต่อไปนี้

- ๑) หน่วยงานที่เข้ามาใช้บริการห้องปฏิบัติการ เพื่อช่วยเหลือ สนับสนุนในการบังคับใช้กฎหมาย หรือเพื่อการดำเนินการสืบสวน สอบสวน หรือการดำเนินคดีความต่าง ๆ
- ๒) ผู้ให้บริการซึ่งเป็นบุคคลภายนอก บุคคลภายใน อาจารย์ และนักศึกษา เพื่อความจำเป็นในการสร้างความมั่นใจในเรื่องการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย สุขภาพ รวมทั้งทรัพย์สินของท่านหรือบุคคลอื่น

ข้อปฏิบัติ สิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ของท่าน

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีวัตถุประสงค์เพื่อให้ข้อมูลส่วนบุคคลของท่านอยู่ในความควบคุมของท่านได้มากขึ้น โดยท่านสามารถใช้สิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เมื่อพบปัญหาสิทธิในส่วนที่เกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลมีผลใช้บังคับ ซึ่งมีรายละเอียดดังต่อไปนี้

- ๑) สิทธิในการเข้าถึง รับสำเนา และขอให้เปิดเผยที่มาของข้อมูลส่วนบุคคลของท่านที่มหาวิทยาลัยเก็บรวบรวมอยู่ เว้นแต่กรณีที่มหาวิทยาลัยมีสิทธิปฏิเสธคำขอของท่านตามกฎหมายหรือคำสั่งศาล หรือกรณีที่คำขอของท่านจะมีผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น
- ๒) สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลของท่านที่ไม่ถูกต้องหรือไม่ครบถ้วน เพื่อให้มีความถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
- ๓) สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคลของท่านในกรณีหนึ่งกรณีใด ดังต่อไปนี้
 - ๓.๑ เมื่ออยู่ในช่วงเวลาที่ยังไม่พ้นโทษหรือการตรวจสอบตามคำร้องขอของท่านให้แก้ไขข้อมูลส่วนบุคคลของท่านให้ถูกต้อง สมบูรณ์และเป็นปัจจุบัน
 - ๓.๒ ข้อมูลส่วนบุคคลของท่านถูกเก็บรวบรวม ใช้หรือเปิดเผยโดยมิชอบด้วยกฎหมาย
 - ๓.๓ เมื่อข้อมูลส่วนบุคคลของท่านหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์มหาวิทยาลัย

ได้แจ้งไว้ในการเก็บรวบรวม แต่ท่านประสงค์ให้มหาวิทยาลัยเก็บรักษาข้อมูลนั้นต่อไป เพื่อประกอบการใช้สิทธิตามกฎหมายของท่าน

- ๔) เมื่ออยู่ในช่วงเวลาที่มหาวิทยาลัยกำลังพิสูจน์ให้ท่านเห็นถึงเหตุอันชอบด้วยกฎหมายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน หรือตรวจสอบความจำเป็นในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่านเพื่อประโยชน์สาธารณะ อันเนื่องมาจากการที่ท่านได้ใช้สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน
- ๕) สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน เว้นแต่กรณีที่มหาวิทยาลัยเหตุในการปฏิเสธคำขอของท่านโดยชอบด้วยกฎหมาย (เช่น มหาวิทยาลัยสามารถแสดงให้เห็นว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่านมีเหตุอันชอบด้วยกฎหมายยิ่งกว่า หรือเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องทางกฎหมาย หรือเพื่อประโยชน์สาธารณะตามภารกิจของมหาวิทยาลัย)

ข้อปฏิบัติ ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

เพื่อบรรลุวัตถุประสงค์ของการเฝ้าระวังสังเกตโดยการใช้อุปกรณ์กล้องวงจรปิด มหาวิทยาลัยจะเก็บรักษาข้อมูลส่วนบุคคลในกล้องวงจรปิดที่เกี่ยวข้อง เป็นระยะเวลา ๑๒ วันย้อนหลัง เนื่องจากความสามารถในการเก็บข้อมูลขึ้นอยู่กับ ฮาร์ดดิสก์ เครื่องบันทึกภาพ เมื่อพ้นระยะเวลาดังกล่าว เครื่องบันทึกภาพจะทำการบันทึกภาพทับข้อมูลเดิม จะไม่สามารถดูย้อนหลังได้อีกต่อไป

ข้อปฏิบัติ การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

มาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของท่านอย่างเหมาะสม ทั้งในเชิงเทคนิค เพื่อป้องกันมิให้ข้อมูลสูญหายเมื่อถึงเวลาใช้งานตามระยะเวลา หรือมีการเข้าถึง ลบ ทำลาย ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

๙. แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องตอบสนองต่อเหตุการณ์อย่างทันทีทันใด ดังนั้นจึงต้องมีแนวปฏิบัติเมื่อเกิดเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๑. ระบบไฟร์วอลล์

๑.๑ ดำเนินการตรวจสอบกฎ(Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละครั้ง

๑.๒ ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก(Log File) และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๑.๒.๑ กลุ่มข้อมูล (Packet) ที่ไฟร์วอลล์ได้ปิดกั้น

๑.๒.๒ ลักษณะของกลุ่มข้อมูล (Packet) ที่ถูกปิดกั้น

๑.๒.๓ หมายเลขไอพี ของเครือข่ายใดที่ถูกปิดกั้น เป็นจำนวนมาก

๑.๓ หากตรวจสอบพบการโจมตี และไม่สามารถแก้ไขปัญหาได้ให้รายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศต่อผู้บังคับบัญชาเพื่อตัดสินใจดำเนินการแก้ไขปัญหาต่อไป

๑.๔ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลกระทบต่อเครือข่าย โดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๒. เครื่องคอมพิวเตอร์แม่ข่าย

๒.๑ ต้องตรวจสอบความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายก่อนเปิดให้บริการ โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

๒.๑.๑ ติดตั้งไฟร์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ปิดเฉพาะ port ที่ใช้งาน

๒.๑.๒ ปิด Service ที่ไม่ได้ใช้งาน

๒.๑.๓ ติดตั้ง NTP เพื่อเทียบเวลาให้ถูกต้อง

๒.๑.๔ จำกัดการเข้าถึงจาก root หรือ Administrator โดยตรง

๒.๒ หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และกำหนดผู้ดูแลรับผิดชอบหลัก และผู้รับผิดชอบสำรอง

๒.๓ หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบความมั่นคงปลอดภัย ต้องจดบันทึกตรวจสอบแก้ไข และรายงาน เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยต่อผู้บังคับบัญชา

๒.๔ ต้องตรวจสอบ แก้ไข และรายงานช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายต่อผู้บังคับบัญชา

๒.๕ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ต้องดำเนินการแจ้งไปยังผู้รับผิดชอบหน่วยงาน หรือผู้มีอำนาจที่ได้รับมอบหมาย ระวังการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

๓. ภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต ประกอบด้วย ไวรัส หนอน อินเทอร์เน็ต โทรจันรวมถึงสเปย์แวร์

๓.๑ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาต้องดำเนินการจัดหาซอฟต์แวร์เพื่อป้องกัน

๓.๒ หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต ต้องดำเนินการติดตั้งโปรแกรมป้องกันภัยคุกคามทางอินเทอร์เน็ต และต้องตั้งให้ Update อย่างน้อยสัปดาห์ละครั้ง

๓.๓ ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของของอุปกรณ์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

๓.๓.๑ การคุกคามทางอินเทอร์เน็ตใดที่มีเป็นจำนวนมาก

๓.๓.๒ ถูกส่งมาจากที่ใด และถูกส่งไปยังที่ใด

๓.๔ ต้องศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่มีภัยคุกคามทางอินเทอร์เน็ต โดยเฉพาะที่ตรวจพบว่ามีกระจายภายในเครือข่ายมหาวิทยาลัย

๓.๕ กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลกระทบต่อเครือข่ายโดยรวม ให้ระวังการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

ระดับความรุนแรงของเหตุการณ์

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
๐	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินการกิจ
๑	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่นับสำคัญต่อการดำเนินงานขององค์กร
๒	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่ไม่นับสำคัญเล็กน้อย
๓	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินการกิจ
๔	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
๕	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

๑๐. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

เพื่อให้ระบบอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากข้อมูลไม่สามารถให้บริการได้ จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุด การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณต้องทำอย่างรวดเร็วเพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด โดยวางแผนการดำเนินการให้ระบบคอมพิวเตอร์ และแฟ้มข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน

- ๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
- ๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
- ๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง
- ๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
- ๕) นำ BACKUP /CD-ROM/HARDDISK ที่ได้สำรองข้อมูลไว้นากลับมา Restore ใช้
- ๖) ทिमกู้ระบบ (ผู้ดูแลระบบ นักวิชาการคอมพิวเตอร์) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง
- ๗) ทำการตรวจสอบระบบปฏิบัติการระบบฐานข้อมูลตรวจสอบความถูกต้องของข้อมูลและระบบ
- ๘) อื่น ๆ ที่เกี่ยวข้อง

๑. การจัดองค์กรปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน

กำหนดอำนาจหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง ในการวางระบบรักษาความปลอดภัย (Security) และระบบการบริหารความเสี่ยงของระบบสารสนเทศ เพื่อเตรียมพร้อมในการแก้ไขสถานการณ์ฉุกเฉินได้อย่าง รวดเร็ว ต่อเนื่อง และมีประสิทธิภาพ ดังนี้

๑.๑ การจัดหน่วยปฏิบัติการเมื่อเกิดสถานการณ์ฉุกเฉิน หรือสายการบังคับบัญชา (Lines of Authority)

๑) ผู้บริหารทางด้านสารสนเทศ (Chief Information Officer : CIO) หรือผู้ที่ได้รับมอบหมายให้ดูแลด้านระบบสารสนเทศของมหาวิทยาลัย

(๑) กำหนดนโยบายให้สำนักคอมพิวเตอร์

(๒) ให้คำปรึกษาแก่ผู้อำนวยการสำนักคอมพิวเตอร์ในฐานะผู้มีอำนาจหน้าที่ในการควบคุมการดำเนินงานด้านสารสนเทศและดูแลสำนักคอมพิวเตอร์

๒) ผู้อำนวยการสำนักคอมพิวเตอร์

(๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ

(๒) มีอำนาจสั่งการให้ทุกหน่วยปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศ

(๓) มีอำนาจสั่งทำลายกุญแจอาคารเก็บวัตถุดิบอันตรายเพื่อการระงับเหตุฉุกเฉิน

(๔) ประชุมหารือกับคณะกรรมการนโยบายและพัฒนาระบบสารสนเทศและคณะกรรมการอื่นที่เกี่ยวข้อง

(๕) ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

(๖) รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหาร (CIO) หรือผู้บริหารระดับสูงที่ดูแลด้านระบบสารสนเทศ

๓) ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบ

(๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการสำนักคอมพิวเตอร์

(๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น

(๓) สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

(๔) ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมายหรือขณะที่ท่าน ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

(๕) ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง

(๖) รายงานให้ผู้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

(๗) กำหนดอัตรากำลังพลวัสดุอุปกรณ์และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

(๘) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๔) ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administor and Staffs)

(๑) กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

(๒) พิจารณาแจ้งสถานีดับเพลิงหรือหน่วยงานภายนอกอื่น ๆ มาช่วย

(๓) ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

(๔) ป้องกันชีวิตทรัพย์สินและสิ่งแวดลอมให้ได้รับความเสียหายน้อยที่สุด

(๕) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ผู้อำนวยการสำนักคอมพิวเตอร์ทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ Firewall
- ทำการตรวจสอบ Virus, Worm, Spyware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๕) ผู้ประสานงานและดูแลสภาพความพร้อมของระบบเครือข่าย

(๑) ดำเนินการให้ผู้ที่เกี่ยวข้อง ปฏิบัติตามแผนฯ

(๒) ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วย

ดับเพลิง

(๓) ตรวจสอบความเสียหายของทรัพย์สิน ทั้งระบบคอมพิวเตอร์และระบบเครือข่าย

(๔) เตรียมเครื่องมืออุปกรณ์ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้อง เพื่อดำเนินการกู้ระบบโดยเร็ว

(๕) ทำการสำรองข้อมูลในส่วนของคุณข้อมูล และสำรองข้อมูลทั้งระบบ สัปดาห์ละ ๑ วัน

(๖) ทำการเก็บสิ่งสำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัยโดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบโปรแกรม และเพิ่มข้อมูล Copy Backup รายชื่อโปรแกรมเอกสารที่เกี่ยวข้อง ระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์ สำเนาคู่มือต่างๆ

(๗) นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๖) หัวหน้าหน่วยงานที่เกิดเหตุ (On-Site Manager)

(๑) แจ้งเหตุฉุกเฉินและเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

(๒) ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ผู้อำนวยการสำนักคอมพิวเตอร์ เพื่อประสานงานใน การรักษาความปลอดภัยระบบสารสนเทศ

(๓) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสอบสภาพและสอบถามบัญชีทรัพย์สินที่จัดทำขึ้นมาและทำรายงานเสนอผู้บังคับบัญชาตามลำดับชั้น

การประเมินสถานการณ์ความเสี่ยง

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ ในระบบสารสนเทศมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาพบว่า ความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ซึ่งเป็นองค์ประกอบหลักในระบบ เทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาสามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

๑) ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

ได้แก่ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้เกิดการชะงัก หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้นเพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้นทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(๒) นำเสนอนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อพิจารณาในการประชุมคณะกรรมการนโยบายและพัฒนาระบบสารสนเทศ

(๓) จัดทำนโยบายว่าด้วยการใช้งานคอมพิวเตอร์ทั่วไปและการเข้าถึงระบบเครือข่ายอินเทอร์เน็ต เผยแพร่ผ่านเว็บไซต์สำนักคอมพิวเตอร์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

๒) ภัยที่เกิดจาก Software

เป็นภัยที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) ซึ่ง Software ประเภทนี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหาย ให้แก่ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาใช้งานไม่ได้

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่ายทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่อง คอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

(๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่เป็นซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

(๓) แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านทางระบบอินเทอร์เน็ตที่ <http://cc.bsru.ac.th> อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจาก Software ดังกล่าวให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๓) ภัยจากไฟไหม้หรือระบบไฟฟ้า

จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบสารสนเทศ ซึ่งสำนักคอมพิวเตอร์ ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้อง

(๑) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง (Gennalator) เพื่อเป็นแหล่งจ่ายไฟฟ้าสำรองในกรณีไฟฟ้าขัดข้อง

(๒) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง โดยมีการสำรวจตรวจสอบระยะเวลาการสำรองไฟ กรณีที่เกิด กระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและ สำรองข้อมูลได้อย่างปลอดภัย

(๓) ติดตั้งอุปกรณ์ตรวจจับควันกรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายใน ห้องควบคุมระบบเครือข่ายอุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและ รีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงทีซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๔) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟ ไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบสารสนเทศของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาให้มีการ จัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ ดังนี้

- ๑) แผ่น Boot Disk (กรณีไม่สามารถเริ่มระบบปฏิบัติการของเครื่องแม่ข่ายได้)
- ๒) แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- ๓) ข้อมูลสำรองและระบบงานที่สำคัญ (External Backup)
- ๔) แผ่นโปรแกรมอื่นๆที่จำเป็น
- ๕) แผ่น Driver อุปกรณ์ต่าง ๆ
- ๖) ระบบสำรองไฟฉุกเฉิน
- ๗) Hard Disk สำรอง
- ๘) สำเนารายละเอียดการบันทึกค่าต่าง ๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

๑๑. แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

เพื่อป้องกันไม่ให้ผู้ที่ไม่มียุติการใช้งานสามารถเข้าถึงระบบสารสนเทศได้ และควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต จึงได้มีการกำหนดขั้นตอนแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน ต่อไปนี้

๑. มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ครอบคลุมในเรื่องดังนี้

๑.๑ จัดทำแบบฟอร์มขอใช้ระบบสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๑.๒ มีการระบุชื่อ นามสกุล ของผู้ใช้งาน

๑.๓ มีการระบุรหัสบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตของผู้ใช้งาน

๑.๔ มีการระบุ ตำแหน่ง หน่วยงานที่สังกัด และหมายเลขโทรศัพท์ติดต่อ

๑.๕ มีการลงนามของผู้บังคับบัญชาของผู้ใช้งาน

๑.๖ มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๑.๗ จัดทำเอกสารแสดงถึงสิทธิ และหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

๑.๘ มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๑.๙ มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๒. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

๓. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๔. ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๕. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

๖. การทบทวนสิทธิการเข้าใช้งาน ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้ระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสถานภาพ เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๗. ต้องกำหนดหลักสูตร และฝึกอบรมเกี่ยวกับการสร้างความรู้ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ และความตระหนักเรื่องความมั่นคงปลอดภัย และกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๑๒. ข้อกำหนดการใช้งานระบบระบบเครือข่ายและคอมพิวเตอร์

เพื่อให้การใช้งานระบบเครือข่ายและคอมพิวเตอร์ของมหาวิทยาลัยเป็นไปอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด มหาวิทยาลัยจึงได้ข้อกำหนดการใช้งานระบบเครือข่ายและคอมพิวเตอร์

๑. ข้อกำหนดนี้จัดทำขึ้นสำหรับนักศึกษาหรือบุคลากรอื่นที่มหาวิทยาลัยอนุญาตให้เข้าใช้งานระบบเครือข่ายและคอมพิวเตอร์ และระบบข้อมูลของมหาวิทยาลัยรวมถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตโดยผ่านทางเครือข่ายของมหาวิทยาลัยโดยให้ถือปฏิบัติอย่างเคร่งครัด
๒. มหาวิทยาลัยดำเนินการภายใต้กฎหมายไทยดังนั้นการใช้งานระบบเครือข่ายและคอมพิวเตอร์รวมทั้งการเชื่อมต่อทางอินเทอร์เน็ตจึงให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง
๓. ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อเป็นทรัพย์สินของมหาวิทยาลัยจัดหาไว้เพื่อบริการที่เกี่ยวข้องกับกิจการของมหาวิทยาลัยเท่านั้น
๔. มหาวิทยาลัยสงวนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่าการละเมิดข้อกำหนดการใช้งานระบบเครือข่ายและคอมพิวเตอร์ และการเชื่อมต่ออินเทอร์เน็ต

ข้อปฏิบัติการใช้งานระบบเครือข่ายและคอมพิวเตอร์

๑. ข้อปฏิบัติการใช้งานระบบเครือข่ายและคอมพิวเตอร์
 - ๑.๑ การใช้งานระบบเครือข่ายจะต้องใช้งานผ่านเครื่องคอมพิวเตอร์ของมหาวิทยาลัยเท่านั้น
 - ๑.๒ การใช้งานระบบเครือข่ายจากเครื่องคอมพิวเตอร์ที่ไม่ใช่เครื่องคอมพิวเตอร์ของมหาวิทยาลัย จะต้องได้รับอนุญาตจากผู้ดูแลระบบก่อน และหากพบว่าการใช้งานโดยไม่ได้รับอนุญาต ผู้ดูแลระบบสามารถตัดการใช้งานออกจากระบบเครือข่ายได้ทันที
๒. ข้อปฏิบัติการใช้งานระบบข้อมูล
 - ๒.๑ การพัฒนาระบบข้อมูลหรือการแก้ไข จะต้องมีการทดสอบร่วมกันระหว่างผู้ใช้งานและผู้ดูแลระบบข้อมูลก่อนการใช้งานจริง
 - ๒.๒ การใช้งานระบบข้อมูล ให้เป็นไปตามการกำหนดสิทธิที่ส่วนจัดการระบบข้อมูลได้ตกลงไว้กับผู้ใช้งาน ตามตารางกำหนดสิทธิที่จัดทำไว้โดยผู้ช่วยกรรมการผู้จัดการใหญ่บริหารองค์กรขึ้นไปให้ความเห็นชอบ

ข้อปฏิบัติสำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศ

๑. ข้อปฏิบัติของผู้ดูแลระบบเครือข่ายและคอมพิวเตอร์

๑.๑ ควบคุม ดูแลบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ต่อเนื่อง กรณีพบความผิดปกติเกิดขึ้นในระบบ ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจระงับการใช้เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเพื่อป้องกันความเสียหายได้

๑.๒ ไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่ได้รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และต้องไม่เปิดเผยข้อมูลที่ได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

๑.๓ จัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยถือปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑.๔ ควบคุมดูแลซอฟต์แวร์ และโปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนของพนักงาน ให้ถูกต้องตามลิขสิทธิ์ของซอฟต์แวร์หรือโปรแกรมที่ติดตั้งอยู่

๑.๕ จัดทำคู่มือการใช้งานระบบเครือข่ายและคอมพิวเตอร์ เพื่อเป็นแนวทางและวิธีปฏิบัติแก่ผู้ใช้งานระบบ

๑.๖ ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายตามที่ผู้บังคับบัญชามอบหมาย

๒. ข้อปฏิบัติสำหรับผู้ดูแลระบบข้อมูล

๒.๑ พัฒนา ปรับปรุง และบำรุงรักษาระบบข้อมูล รวมทั้งต้องระบุข้อกำหนดความปลอดภัย

๒.๒ กำหนดสิทธิการใช้งานของระบบ ก่อนการใช้งาน

๒.๓ ควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงในระบบข้อมูลหรือในเครื่องคอมพิวเตอร์ของพนักงานโดยไม่ให้กระทบต่อระบบหลักหรือก่อให้เกิดความเสียหายต่อระบบรวม

๒.๔ ระงับการใช้งานระบบงานของพนักงาน เมื่อมีการตรวจสอบพบว่าใช้งานไม่ถูกต้องหรือละเมิดข้อตกลงการใช้งาน หรือไม่ถูกต้องตามกฎหมาย

๒.๕ จัดทำคู่มือการใช้งานระบบข้อมูล เพื่อเป็นแนวทางและวิธีปฏิบัติให้แก่ผู้ใช้งานระบบ

๒.๖ ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับระบบข้อมูลตามที่ผู้บังคับบัญชามอบหมาย

๑๓. ข้อกำหนดการใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์

๑. ผู้ดูแลระบบต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เพื่อให้สามารถ ควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

๒. ผู้ให้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบ เครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักคอมพิวเตอร์ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๓. การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงาน รับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักคอมพิวเตอร์ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อ การกระทำของระบบและผู้ให้บริการอื่นๆ

๔. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์ จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบ เครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๕. การควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๕.๑ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ให้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๕.๒ ต้องกำหนดให้มีวิธีจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

๕.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๕.๔ ระบบเครือข่ายต้องมีระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๕.๕ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ของผู้ใช้บริการ

๕.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมี การป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๕.๘ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขต ของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบัน อยู่เสมอ

๕.๙ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแล ระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น ๕.๑๐ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบใน การดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๖. การกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทาง คอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๖.๑ ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความ ครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้อง กำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงาน มอบหมาย

๖.๒ ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออก ระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อ ประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การให้บริการ สิ้นสุดลง

๖.๓ ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๖.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึก เหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๗. การกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อ ดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๗.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่อง คอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจาก ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักคอมพิวเตอร์

๗.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๗.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากกระยะไกลต้องได้รับการ อนุญาต จากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักคอมพิวเตอร์

๗.๔ การเข้าสู่ระบบจากกระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็น ใน การดำเนินงานกับหน่วยงานอย่างเพียงพอ

๗.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

๑๔. ข้อปฏิบัติในการใช้จดหมาย อิเล็กทรอนิกส์ (e-mail)

ข้อปฏิบัติในการใช้จดหมาย อิเล็กทรอนิกส์ (e-mail) มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ตามรายละเอียด ดังต่อไปนี้

จดหมายอิเล็กทรอนิกส์ (E-mail)

เป็นบริการที่มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาจัดให้มีเพื่อสนับสนุนการศึกษา การวิจัย การบริการวิชาการ และการบำรุงศิลปวัฒนธรรม ตลอดจน การบริหารจัดการตามภารกิจของหน่วยงาน ผู้ใช้จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาภายใต้ชื่อโดเมน (Domain) ที่จดทะเบียนโดยมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มีหน้าที่ พึงปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ โดยไม่ขัดกับนโยบายการใช้คอมพิวเตอร์ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ไว้ดังต่อไปนี้

๑. ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

๑.๑ ผู้ใช้มีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบผู้ใช้ ต้องรักษารหัสผ่านเป็นความลับเฉพาะตัว และไม่อนุญาตให้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนาม ของตนเองในทุกกรณีผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมาย อิเล็กทรอนิกส์และการอนุญาตให้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ ในนามของตนเอง

๑.๒ ผู้ใช้พึงทราบว่าผู้ดูแลระบบไม่มีสิทธิ์ที่จะถามหรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

๑.๓ ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

๑.๔ การใช้จดหมายอิเล็กทรอนิกส์ ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

- (๑) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น
- (๒) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่จดหมายลูกโซ่
- (๓) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลชั้นความลับของมหาวิทยาลัย
- (๔) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลการประชุมของที่ประชุมผู้บริหารมหาวิทยาลัย หรือในการประชุมอื่นๆ โดยที่มิได้มีหน้าที่ หรือมิได้รับมอบหมายจากประธานในที่ประชุม
- (๕) การปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นส่งมาจากบุคคลอื่น
- (๖) การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

- (๗) การปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง
- (๘) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่กล่าวร้ายต่อบุคคล หรือกลุ่มบุคคล
- (๙) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่ดูหมิ่นเหยียดหยามหรือแบ่งแยกทาง ศาสนา เชื้อชาติ หรือเพศ
- (๑๐) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่มีลักษณะหยาบคาย หรือลามกอนาจาร
- (๑๑) การส่งจดหมายอิเล็กทรอนิกส์ เพื่อเผยแพร่โปรแกรมหรืองานหรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองาน ในลักษณะที่ละเมิดลิขสิทธิ์
- (๑๒) การส่งจดหมายอิเล็กทรอนิกส์ กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคมการเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร
- (๑๓) การส่งจดหมายอิเล็กทรอนิกส์ โฆษณาสินค้า ผลิตภัณฑ์ หรือส่งข้อความลักษณะของสแปมเมล (Spam Mail) ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร
- (๑๔) การส่งจดหมายอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบให้ระบบจดหมายอิเล็กทรอนิกส์หรือเครือข่าย ลดทอนประสิทธิภาพลง
- (๑๕) การส่งจดหมายอิเล็กทรอนิกส์กระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

๒. การจัดการรายชื่อบัญชีผู้ใช้จดหมาย อิเล็กทรอนิกส์ (Mailing List)

สำนักคอมพิวเตอร์จัดให้มีระบบรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ เพื่อสร้างช่องทางการส่ง จดหมายอิเล็กทรอนิกส์แบบกลุ่ม รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ที่บรรจุรายชื่อบัญชีผู้ใช้ที่ขึ้นทะเบียนในเครือข่ายของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาเป็นข้อมูลปกปิดที่ไม่เผยแพร่ให้ผู้ใช้หรือหน่วยงานใด ๆ การใช้รายชื่อบัญชีผู้ใช้จดหมาย อิเล็กทรอนิกส์ดังกล่าวมีข้อกำหนดเฉพาะดังนี้

๒.๑ หน่วยงานที่ได้รับมอบหมายจากอธิการบดีใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่ข่าวสารและประชาสัมพันธ์ภารกิจของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

๒.๒ สำนักคอมพิวเตอร์ใช้เพื่อแจ้งเตือนหรือแจ้งข่าวที่เกี่ยวข้องกับความมั่นคงปลอดภัยหรือการรักษาประสิทธิภาพของระบบคอมพิวเตอร์ และเครือข่าย

๒.๓ สำนักคอมพิวเตอร์จัดให้มีระบบรายชื่อบัญชีผู้ใช้ จดหมายอิเล็กทรอนิกส์กลุ่มย่อยตามคำร้องขอของหน่วยงานซึ่งต้องให้ผู้ใช้สมัครใจเข้าเป็นสมาชิกกลุ่มเพื่อรับข่าวสารเอง และผู้ใช้สามารถถอนการเป็นสมาชิกเพื่องดรับข่าวสารนั้นได้ตลอดเวลา ทั้งนี้ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาไม่อนุญาตให้มีการสร้างบริการรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์อื่นใดเอง เพื่อป้องกันการใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ที่บรรจุรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ โดย

ผู้ที่ไม่สมัครใจยอมรับ ทั้งนี้ สำนักคอมพิวเตอร์ สงวนสิทธิ์ในการอนุมัติการขอจดทะเบียนชื่อกลุ่ม ตลอดจนการตั้งชื่อกลุ่ม ตามความเหมาะสม

๓. โควตาบัญชีจดหมายอิเล็กทรอนิกส์

บัญชีจดหมายอิเล็กทรอนิกส์ ของผู้ใช้แต่ละรายจะมีโควตากำหนดการใช้งานดังนี้

๓.๑ ขนาดข้อมูลรวมที่เก็บในเซิร์ฟเวอร์ (Server)

๓.๒ ขนาดของไฟล์แนบต่อการส่งจดหมายอิเล็กทรอนิกส์ หนึ่งฉบับ

๓.๓ จำนวนบัญชีผู้รับต่อการส่งจดหมายอิเล็กทรอนิกส์ หนึ่งฉบับ

๓.๔ อัตราส่งจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนด

๓.๕ จำนวนจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนดโควตาเหล่านี้อาจแตกต่างกันตามประเภทและภารกิจของผู้ใช้ การกำหนดโควตาให้อยู่ในดุลยพินิจของสำนักคอมพิวเตอร์ โดยสามารถเพิ่มหรือลดค่าแต่ละบัญชีจดหมายอิเล็กทรอนิกส์ตามความเหมาะสม เพื่อให้การใช้งานและการบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ

๔. การตรวจระบบ

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยามีนโยบายปกป้องข้อมูลส่วนบุคคลและให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนภารกิจของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา โดยไม่ตรวจดูจดหมายอิเล็กทรอนิกส์ที่รับส่งตามปกติ แต่มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มีภาระผูกพันตามกฎหมายที่ต้องติดตั้งระบบบันทึกข้อมูล จราจรและการเฝ้าระวังเพื่อคงไว้ซึ่งบริการที่มั่นคงปลอดภัยและมีประสิทธิภาพ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาสงวน สิทธิ์ในการใช้ระบบเฝ้าระวังเพื่อตรวจเนื้อหาจดหมายอิเล็กทรอนิกส์ที่เป็นภัยต่อระบบคอมพิวเตอร์ และกลั่นกรอง หรือระงับการเผยแพร่โดยอัตโนมัติ ตลอดจนสงวนสิทธิ์การเข้าถึงจดหมายอิเล็กทรอนิกส์ เพื่อสืบสวนสอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้จดหมายอิเล็กทรอนิกส์ใดๆ หรือการร้อง ขอร้องจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๕. การระงับบัญชีจดหมาย อิเล็กทรอนิกส์

บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ให้แก่ผู้ใช้ ซึ่งผู้ใช้ไม่สามารถโอนสิทธิ์ให้แก่ผู้อื่นได้ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาคงไว้ ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิ์การใช้โดยไม่ ต้องแจ้ง ให้ผู้ใช้ทราบล่วงหน้า หาก ได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบาย หรืออาจก่อให้เกิดปัญหาความมั่นคง ปลอดภัยหรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การ ระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์ มีแนวปฏิบัติดังนี้

๕.๑ เมื่อผู้ใช้พ้นสภาพการอยู่ในสังกัดของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา สำนักคอมพิวเตอร์สามารถระงับบัญชีผู้ใช้ ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย หากแต่ผู้ใช้อาจยังสามารถมีใช้ชื่อบัญชีจดหมายอิเล็กทรอนิกส์สำหรับใช้ติดต่อได้ผ่านระบบจดหมายอิเล็กทรอนิกส์อีกระบบหนึ่ง ที่สำนักคอมพิวเตอร์จัดบริการไว้ให้ (e-mail for Life)

๕.๒ ผู้ใช้สามารถร้องขอการขยายสิทธิการใช้บัญชีผู้ใช้เพื่อคงสิทธิการใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้เมื่อต้องพ้นสภาพการอยู่ในสังกัดของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัดพร้อมแนบเหตุผลความจำเป็นส่งถึงสำนักคอมพิวเตอร์ การอนุญาตและระยะเวลาการขยายสิทธิให้เป็นอำนาจของผู้อำนวยการสำนักคอมพิวเตอร์หรือ ผู้ที่อธิการบดีมอบหมาย

๕.๓ บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งานโดยคำร้องขอจากหัวหน้าภาควิชา หรือคณบดี หรือผู้บริหารที่เทียบเท่ากับหัวหน้าภาควิชาหรือคณบดี หากพบว่าการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้

๕.๔ บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งาน โดยทันทีโดยผู้ดูแลระบบ หากตรวจพบว่าการใช้งานที่ส่งผลกระทบให้ประสิทธิภาพระบบเครือข่ายด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้อ้างหรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้ สำนักคอมพิวเตอร์มีสิทธิระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์ นั้นๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

๑๕. นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ เพื่อป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ จึงกำหนดนโยบายไว้ดังนี้

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดย

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) เพื่อให้หน่วยงาน ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อย ปีละ ๑ ครั้ง

๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่เป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) ควรกำหนดให้มีการเผื่อระวางการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนี้จากการเข้าถึงโดยไม่ได้รับอนุญาต

๑๖. นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา มีการกำหนดนโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศเพื่อให้ระบบสารสนเทศของหน่วยงาน ให้บริการได้อย่างต่อเนื่อง และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ดังนี้

๑. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบ สารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรอง ข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการ สำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรอง ข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อ ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวข้องกักระบบสารสนเทศ ข้อมูลคอนฟิกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับ หน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูล อย่างสม่ำเสมอ

- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อม กรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทาง ต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

- (๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- (๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อ ลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
- (๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
- (๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบ สำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อม กรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อ สภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๙ ตุลาคม พ.ศ.๒๕๖๘

A handwritten signature in blue ink, consisting of two distinct, stylized characters.

(ผู้ช่วยศาสตราจารย์ ดร.ประไพ ศรีตามมา)
ผู้อำนวยการสำนักคอมพิวเตอร์