นโยบายและแนวปฏิบัติ ความมั่นคงปลอดภัยทางไซเบอร์

มหาวิทยาลัยมหาสารคาม

Cybersecurity Policy

คำนำ

นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม จัดทำขึ้นโดยอ้างอิงจากระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Management Systems: ISMS) ตามมาตรฐาน ISO/IEC 27001:2013 และกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล NIST Cybersecurity Framework เพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยมหาสารคาม โดยทำการเผยแพร่นโยบายและแนวปฏิบัติฯ ให้แก่คณะ/หน่วยงานได้รับทราบ เพื่อนำไปปรับใช้เพื่อให้เกิดความมั่นคงปลอดภัยทางไซเบอร์และสามารถแก้ไขปัญหาจากที่เกิดขึ้นได้ มีการจัดการองค์กร โครงสร้าง อำนาจ หน้าที่ ขีดความสามารถในการป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์ มีการกำหนดระบบบริหารจัดการภายในมหาวิทยาลัยในแต่ละระดับให้ชัดเจน มีการเสริมสร้างและการรายงานในสถานการณ์ฉุกเฉิน มีการควบคุมกำกับ ติดตามและประเมินผล อย่างต่อเนื่อง

คณะกรรมการดำเนินงานจัดทำแผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม พ.ศ.2566-2569 ได้มีมติเห็นชอบในนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม และจะนำไปใช้ในการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคามต่อไป

ผู้อำนวยการสำนักคอมพิวเตอร์

มหาวิทยาลัยมหาสารคาม

สารบัญ

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้ในมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

คำศัพท์	ความหมาย
การกู้คืน (Recovery)	การนำข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบสารสนเทศที่เกิดความเสียหายกลับมาใช้งานได้อย่างถูกต้องครบถ้วน
การเข้าถึง (Access)	การอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้น สำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้ (อ้างอิงจาก ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553)
การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Information Assets Classification)	การจัดระดับการป้องกันความมั่นคงปลอดภัย โดยคำนึงถึงความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และการให้บริการ (Availability) ของทรัพย์สินสารสนเทศ
การจ้างงาน (Employment)	การว่าจ้างผู้ปฏิบัติงานหรือผู้รับจ้าง เพื่อปฏิบัติงานหรือให้บริการแก่มหาวิทยาลัยมหาสารคาม
การปฏิบัติงานจากระยะไกล (Teleworking)	การทำงานที่บ้านหรือที่สถานที่ตั้งภายนอกองค์กรอื่น ๆ ที่มีการเชื่อมต่อทาง อิเล็กทรอนิกส์โดยผ่านทาง เครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์พกพา หรือเครื่องโทรสาร ไปยังมหาวิทยาลัยมหาสารคาม หรือสถานที่อื่นอันเป็นสถานที่ทำงานหลัก
การพิสูจน์และยืนยันตัวตน (Identification and Authentication)	กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล (อ้างอิงจาก พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562)
การสำรองข้อมูล (Backup)	การเก็บรักษาข้อมูลคอมพิวเตอร์ลงในสื่อที่ได้เตรียมการไว้แล้วและจะถูกนำมาใช้งานแทนในกรณีที่ข้อมูลหลักที่กำลังถูกใช้ในการปฏิบัติงานอยู่เกิดความเสียหาย

คำศัพท์	ความหมาย
ข้อมูลชีวภาพ (Bio-metrics)	ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ (อ้างอิงจาก พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อมแต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (อ้างอิงจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
ข้อมูลอิเล็กทรอนิกส์ (Electronic Data)	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมาย อิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร เป็นต้น (อ้างอิงจาก พ.ร.บ. ว่า ด้วย ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544)
ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Cyber and Information Security)	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของไซเบอร์ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ (อ้างอิงจาก ประกาศ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติใน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553)
ความเสี่ยงเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber and Information Security Risk)	ความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศในการดำเนินงาน ซึ่งจะมีผลกระทบต่อระบบหรือการปฏิบัติงานของมหาวิทยาลัยมหาสารคาม รวมถึงความเสี่ยงที่เกิดจากภัยคุกคามทางไซเบอร์
เครือข่าย (Network)	ระบบที่เกิดจากการนำเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปมาต่อเชื่อมโยง เข้าด้วยกัน เพื่อแลกเปลี่ยนข้อมูลข่าวสาร หรือใช้ทรัพยากรต่าง ๆ

คำศัพท์	ความหมาย
จุดอ่อนความมั่นคงปลอดภัยทางไซเบอร์ (Cyber and information Security Weaknesses)	จุดบกพร่อง หรือความอ่อนแอซึ่งภัยคุกคามหรือผู้ไม่ประสงค์ดีอาจใช้ประโยชน์เพื่อกระทำการใดๆ ต่อทรัพย์สินสารสนเทศ อันอาจจะนำไปสู่ผลเสียต่อการดำเนินงานและความปลอดภัยทางไซเบอร์ เช่น ข้อบกพร่องในแอปพลิเคชั่นช่องโหว่ทางเทคนิคในระบบปฏิบัติการ การเปิด Network Protocol และ IP Service Port ที่ไม่ได้ใช้งาน การไม่ Lock หน้าจอ หรือการไม่ Log Off ออกจากระบบ เมื่อไม่ได้ใช้งานเป็นระยะเวลานาน
เจ้าของข้อมูลส่วนบุคคล (Personal Data's Owner)	บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล (อ้างอิงจาก พ.ร.บ. คุ้มครองข้อมูลส่วน บุคคล พ.ศ. 2562)
ซอฟต์แวร์ (Software)	โปรแกรมคอมพิวเตอร์หรือโปรแกรมประยุกต์ประเภทใดๆ ก็ได้ เช่น โปรแกรม ระบบปฏิบัติการ โปรแกรมประเภทยูทิลิตี้ โปรแกรมสำเร็จรูป
ไซเบอร์ (Cyber)	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อ กันเป็นการทั่วไป (อ้างอิงจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)
ดัดแปลง (Tamper)	ทำซ้ำโดยเปลี่ยนรูปใหม่ ปรับปรุงแก้ไขเพิ่มเติม หรือจำลองงานต้นฉบับในส่วน อันเป็นสาระสำคัญโดยไม่มีลักษณะเป็นการจัดทำงานขึ้นใหม่ ทั้งนี้ ไม่ว่าทั้งหมด หรือบางส่วน ในส่วนที่เกี่ยวกับโปรแกรมประยุกต์ ให้หมายความรวมถึง ทำซ้ำ โดยเปลี่ยนรูปใหม่ ปรับปรุงแก้ไขเพิ่มเติมโปรแกรมประยุกต์ในส่วนอันเป็นสาระสำคัญโดยไม่มีลักษณะเป็นการจัดทำขึ้นใหม่ (อ้างอิงจาก พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537)
ทรัพย์สิน (Asset)	สิ่งใดก็ตามที่มีคุณค่าสำหรับมหาวิทยาลัยมหาสารคาม (อ้างอิงจากประกาศคณะกรรมการธุรกรรม ทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553)

คำศัพท์	ความหมาย
ทรัพย์สินสารสนเทศ (Information Asset)	1. ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2. ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์ อื่นใด 3. ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (อ้างอิงจาก พระราชกฤษฎีกา ว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรม ทางอิเล็กทรอนิกส์ พ.ศ. 2553)
ทำซ้ำ (Copy)	คัดลอกไม่ว่าโดยวิธีใด ๆ เลียนแบบ ทำสำเนา ทำแม่พิมพ์ บันทึกเสียง บันทึกภาพ หรือ บันทึกเสียงและภาพ จากต้นฉบับ หรือจาการโฆษณาในส่วนอันเป็นสาระสำคัญ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน สำหรับในส่วนที่เกี่ยวกับ โปรแกรมประยุกต์ ให้หมายความถึง คัดลอกหรือทำสำเนาโปรแกรมประยุกต์ จากสื่อบันทึกใด ๆ ไม่ว่าด้วยวิธีใด ๆ ในส่วนอันเป็นสาระสำคัญ โดยไม่มี ลักษณะเป็นการจัดทำงานขึ้นใหม่ ทั้งนี้ไม่ว่าทั้งหมดหรือบางส่วน (อ้างอิงจาก พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537)
ธุรกรรม (Business)	การกระทำใด ๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐ อันประกอบไปด้วย คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ (อ้างอิงจาก พ.ร.บ. ว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544)
เปลี่ยนแปลงการจ้างงาน (Change of Employment)	เปลี่ยนแปลงหน้าที่รับผิดชอบของผู้ปฏิบัติงานในหน่วยงานต้นสังกัด หรือเงื่อนไขการว่าจ้างของผู้รับจ้าง
โปรแกรมประยุกต์ (Program)	คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่ทำไปใช้กับเครื่องคอมพิวเตอร์ เพื่อให้เครื่อง คอมพิวเตอร์ทำงานหรือเพื่อให้ได้รับผลอย่างหนึ่งอย่างใด ทั้งนี้ไม่ว่าจะเป็นภาษาโปรแกรมในลักษณะใด
โปรแกรมประเภท Peer-to-Peer	วิธีจัดการเครือข่ายคอมพิวเตอร์ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่อง

คำศัพท์	ความหมาย
โปรแกรมประเภทยูทิลิตี้ (System Utilities)	โปรแกรมเฉพาะ เพื่อใช้สำหรับงานบำรุงรักษาและเพิ่มประสิทธิภาพการทำงาน ของระบบคอมพิวเตอร์
โปรแกรมไม่พึงประสงค์ (Malicious Software)/มัลแวร์ (Malware)	โปรแกรมหรือชุดโปรแกรมที่ทำให้สารสนเทศ หรือระบบสารสนเทศเกิดความ เสียหายโดยตั้งใจ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) สปายแวร์ (Spyware)
ผู้ควบคุมข้อมูลส่วนบุคคล (Personal Data Controller)	ผู้ที่ได้รับมอบหมายให้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้บุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ดูแลระบบที่จัดเก็บข้อมูลส่วนบุคคล
ผู้ใช้งาน (Users)	เจ้าหน้าที่ ผู้ปฏิบัติงาน ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารมหาวิทยาลัย ผู้รับบริการ ผู้ใช้งานทั่วไป (อ้างอิงจาก ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553)
ผู้ดูแลพื้นที่ควบคุม (Control Area Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลพื้นที่ควบคุม
ผู้ดูแลระบบ (Administrator)	ผู้ที่ได้รับมอบหมายให้บริหารจัดการบัญชีรายชื่อผู้มีสิทธิในการเข้าถึงระบบงานรวมทั้งการปรับปรุงดูแลรักษาระบบ
ผู้ดูแลระบบเครือข่าย (Network Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่าย
ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail System Administrator)	ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษาระบบจดหมายอิเล็กทรอนิกส์
ผู้ดูแลห้องบริการคอมพิวเตอร์ (Computer Room Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลห้องบริการคอมพิวเตอร์
ผู้ตรวจประเมิน (Auditor)	หน่วยงานภายในหรือภายนอกที่ทำหน้าที่ในการตรวจสอบการควบคุมภายในที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นอิสระจากผู้รับตรวจ
ผู้ปฏิบัติงาน (Employee)	ข้าราชการ พนักงาน และลูกจ้างของมหาวิทยาลัยมหาสารคาม

คำศัพท์	ความหมาย
ผู้ดูแลระบบที่จัดเก็บข้อมูลส่วนบุคคล (Personal Data Administrator)	ผู้ที่ได้รับมอบหมายให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
ผู้พัฒนาระบบ (Developer)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุงระบบงานสารสนเทศ
ผู้ส่งมอบ (Supplier)	ผู้ผลิต ผู้ขาย ผู้รับจ้าง บุคคลภายนอกและหน่วยงานภายนอกที่ดำเนินงานหรือ ให้บริการที่อาจได้รับสิทธิเข้าถึงทรัพย์สินสารสนเทศของมหาวิทยาลัยมหาสารคาม ซึ่งครอบคลุมถึง ผู้รับจ้างปฏิบัติงานให้กับมหาวิทยาลัยมหาสารคาม (Outsource) เช่น ผู้รับจ้างติดตั้งระบบงาน ผู้รับจ้างพัฒนาระบบงานหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ (Supplier) เช่น ผู้พัฒนาระบบงานควบคุมการผลิต ผู้จำหน่ายอุปกรณ์คอมพิวเตอร์ ผู้ให้บริการต่าง ๆ (Service Provider) เช่น ผู้ติดตั้งและบำรุงรักษา ทรัพย์สินต่าง ๆ ผู้ให้บริการโครงข่ายสื่อสาร ผู้ให้บริการอินเทอร์เน็ต
พื้นที่ควบคุม (Secure Area)	พื้นที่ซึ่งมีระบบสารสนเทศที่สำคัญของมหาวิทยาลัยมหาสารคาม เช่น ห้องศูนย์กลางข้อมูล
ภัยคุกคามทางไซเบอร์ (Cyber Threats)	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบ คอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อ ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็น ภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการ ทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง (อ้างอิง จาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)
ระบบคอมพิวเตอร์ (Computer System)	อุปกรณ์คอมพิวเตอร์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ (อ้างอิงจาก พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550)

คำศัพท์	ความหมาย
ระบบสารสนเทศ (Information System)	ระบบคอมพิวเตอร์และการเก็บบันทึกข้อมูลซึ่งมีการประมวลผลด้วยระบบคอมพิวเตอร์
ลิขสิทธิ์ (Copyright)	สิทธิแต่ผู้เดียวที่จะทำการใด ๆ ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น (อ้างอิงจาก พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537)
สำนักคอมพิวเตอร์ (Computer Center)	สถานที่ที่ใช้ในการจัดวางอุปกรณ์สารสนเทศที่ประมวลผลหรือจัดเก็บสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด”
สถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber and Information Security Incident)	สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือ โจมตี และความมั่นคงปลอดภัยถูกคุกคาม (อ้างอิงจาก ประกาศคณะกรรมการ ธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553)
สารสนเทศ (Information)	ข้อมูลคอมพิวเตอร์หรือข้อความที่ได้มีการประมวลผล เช่น ทรัพย์สินประเภท ฐานข้อมูล (Database) และไฟล์ข้อมูล (Data File) สัญญา (Contract) และ ข้อตกลง (Agreement) เอกสารและคู่มือระบบสารสนเทศ (System Document) ข้อมูลวิจัย (Research Document) คู่มือผู้ใช้งาน (User Manual) เอกสารการฝึกอบรม (Training Document) ขั้นตอนการปฏิบัติงาน (Operational or Support Procedure) และข้อมูลจัดเก็บสำรอง (Archived Information) เป็นต้น (อ้างอิงจาก พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553)
สิทธิของผู้ใช้งาน (User Rights)	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบ สารสนเทศของมหาวิทยาลัยมหาสารคาม(อ้างอิงจาก ประกาศคณะกรรมการธุรกรรมทาง อิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553)

คำศัพท์	ความหมาย
สิทธิพิเศษ (Privileged Access Right)	สิทธิสูงสุดของระบบ หรือสิทธิสำหรับผู้ดูแลระบบหรือเทียบเท่า เช่น บัญชีผู้ใช้ Administrators (Windows) หรือ SYSTEM (Oracle)
สื่อบันทึกข้อมูล (Removable Media Device)	เอกสารที่เป็นกระดาษ หรืออุปกรณ์สารสนเทศที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ เช่น เทป ดิสก์ CD, DVD, Thumb drive
หน่วยงานภายนอก (External Parties)	บุคคลหรือนิติบุคคลภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศหรือที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยมหาสารคาม หรือที่สามารถเข้าถึงข้อมูล สำคัญของมหาวิทยาลัยมหาสารคาม ซึ่งครอบคลุมถึง -ผู้ผลิต ผู้ขาย ผู้รับจ้าง -บริษัทที่ให้บริการโครงข่ายการสื่อสาร -ที่ปรึกษา (Consultant) เช่น ที่ปรึกษาระบบงานการวางแผนความมั่นคงปลอดภัยทางไซเบอร์ -เจ้าหน้าที่ของหน่วยงานต่าง ๆ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และ คอมพิวเตอร์แห่งชาติ (NECTEC) สำนักงานตำรวจแห่งชาติ
ห้องบริการคอมพิวเตอร์ (Computer Room)	สถานที่ที่ใช้ในการจัดวางอุปกรณ์สารสนเทศ ที่ประมวลผลหรือจัดเก็บสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “ปานกลาง”
ผู้อำนวยการสำนักคอมพิวเตอร์ (Director of Computer Center)	ผู้อำนวยการสำนักคอมพิวเตอร์
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัย ทางไซเบอร์ (Cyber and Information Security Event)	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย (อ้างอิงจากประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553)

คำศัพท์	ความหมาย
อิเล็กทรอนิกส์ (Electronic)	การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใด ในลักษณะคล้ายกันและให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็กหรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่า นั้น (อ้างอิงจาก พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544)
อุปกรณ์คอมพิวเตอร์พกพา (Mobile Device)	อุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์สื่อสารที่สะดวกในการพกพา เช่น คอมพิวเตอร์โน้ตบุ๊ค (Notebook/Laptop) โทรศัพท์มือถือ (Smartphone)
อุปกรณ์สารสนเทศ (Information Processing Facilities)	เครื่องมือ เครื่องใช้ วัสดุ และอุปกรณ์ต่าง ๆ ที่ประมวลผลหรือจัดเก็บสารสนเทศ เช่น คอมพิวเตอร์ กล้องดิจิทัล สื่อบันทึกข้อมูล สแกนเนอร์ เครื่องพิมพ์
อุปกรณ์และระบบสนับสนุน (Supporting Utilities)	ระบบไฟฟ้า ระบบการสื่อสาร ระบบแหล่งจ่ายน้ำ ระบบบำบัด ระบบระบายอากาศ และระบบทำความเย็น
แอปพลิเคชัน (Application)	โปรแกรมประยุกต์หรือกลุ่มของโปรแกรม ซึ่งทำหน้าที่เพื่อจุดประสงค์อย่างใด อย่างหนึ่ง เช่น โปรแกรมประมวลผลคำ (Word Processor) โปรแกรมการ คำนวณแบบตาราง (Spreadsheet) โปรแกรมนำเสนอ (Presentation) ฐานข้อมูล (Database) โปรแกรมประยุกต์ที่อยู่บนอุปกรณ์พกพาต่าง ๆ

นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy)

รหัสเอกสาร:	MSUP-01
ชื่อเอกสาร:	นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
หมายเลขปรับปรุงเอกสาร:	2566-V1
วันที่เอกสารมีผลบังคับใช้:	1 เมษายน 2566
เจ้าของเอกสาร:	สำนักคอมพิวเตอร์

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุง เอกสาร (version) :	คำอธิบายและเหตุผลในการแก้ไข
2566-V1.0	เอกสารเผยแพร่ฉบับแรก

รายการบันทึก

ลำดับ	รายการบันทึก	ผู้รับผิดชอบ	อายุการ จัดเก็บหลักฐาน	วิธีการจัดเก็บ หลักฐาน

หมวด 1 นโยบายความมั่นคงปลอดภัยทางไซเบอร์

(Cyber and Information Security Policies)

นโยบายความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคามกำหนดขึ้นโดย คณะกรรมการดำเนินงานจัดทำแผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 และได้รับการอนุมัตินโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์โดยอธิการบดีมหาวิทยาลัย และมีการประกาศ เผยแพร่และสื่อสารไปยังนิสิต บุคลากรและบุคคลภายนอกที่เกี่ยวข้อง มีการทบทวนนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ตามรอบระยะเวลาการทบทวนที่กำหนดไว้ เพื่อให้นโยบายมีความเหมาะสมกับสถานการณ์ปัจจุบันและมีประสิทธิผลต่อการนำไปใช้งาน

วัตถุประสงค์

เพื่อกำหนดทิศทางและสนับสนุนเรื่องความมั่นคงปลอดภัยทางไซเบอร์ให้สอดคล้องกับการดำเนินงานตามพันธกิจของมหาวิทยาลัยมหาสารคาม กฎหมาย และระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้อง

มาตรการ

1. นโยบายความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคามพร้อมเอกสารประกอบ กำหนดโดยคณะกรรมการดำเนินงานจัดทำแผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 และมีการประกาศ เผยแพร่ และสื่อสารให้กับผู้ปฏิบัติงานและบุคคลที่เกี่ยวข้อง

2. ทบทวนนโยบายความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคามตามรอบระยะเวลาการทบทวนที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อมหาวิทยาลัย ทั้งนี้เพื่อให้นโยบายมีความเหมาะสมเพียงพอและมีประสิทธิผลต่อการนำไปใช้งาน

แนวทางการดำเนินงาน

การดำเนินงานในระดับนโยบายต้องกำหนด “นโยบายความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม” โดยได้รับการอนุมัติจากอธิการบดีมหาวิทยาลัย เพื่อกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยโดยมีแนวทางการดำเนินงาน ดังนี้

1. จัดทำนโยบายความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยเป็นลายลักษณ์อักษรและประกาศให้นิสิต บุคลากร และบุคคลภายนอกที่เกี่ยวข้อง ทั้งหมดทราบ เข้าถึง เข้าใจและปฏิบัติตามแนวนโยบาย มาตรฐาน และแนวปฏิบัติ

2. กำหนดผู้รับผิดชอบตามแนวนโยบาย มาตรฐาน และแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์อย่างชัดเจน

3. ทบทวนและปรับปรุงนโยบาย มาตรฐาน และแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ให้เป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

4. ประเมินความเสี่ยง และกำหนดมาตรการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งต้องจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ โดยผู้ตรวจสอบภายในอย่างน้อย
ปีละ 1 ครั้ง

5. สร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่ให้แก่นิสิต บุคลากร และบุคคลภายนอกที่เกี่ยวข้อง

หมวด 2 การจัดการความมั่นคงปลอดภัยทางไซเบอร์ภายในมหาวิทยาลัย

(Organization of Cyber Security)

มหาวิทยาลัยมหาสารคาม จะต้องมีการกำหนดกรอบการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัย โดยต้องมีการกำหนดบทบาท หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างชัดเจน มีการกำหนดนโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพาและนโยบายและมาตรการสนับสนุนการปฏิบัติงานจากระยะไกล

วัตถุประสงค์

เพื่อกำหนดทิศทางการดำเนินงาน กรอบการบริหารจัดการ การจัดทำนโยบาย การควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ภายในมหาวิทยาลัยมหาสารคาม และเพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและของการใช้งานอุปกรณ์คอมพิวเตอร์พกพา โดยมีการกำหนดมาตรการและแนวทางการดำเนินงานแบ่งเป็น 2 องค์ประกอบคือ โครงสร้างการจัดการภายในมหาวิทยาลัย และอุปกรณ์คอมพิวเตอร์ชนิดพกพาและการปฏิบัติงานจากระยะไกล

1. โครงสร้างการจัดการภายในมหาวิทยาลัย

มาตรการ

1. กำหนดและแบ่งหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยทางไซเบอร์

2. แบ่งแยกงานและหน้าที่ความรับผิดชอบของบุคลากรอย่างเหมาะสม เพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาตหรือโดยไม่ได้ตั้งใจ หรือลดโอกาสในการใช้ทรัพย์สินสารสนเทศขององค์กรผิดวัตถุประสงค์

3. จัดการเกี่ยวกับการติดต่อหน่วยงานผู้มีอำนาจหน้าที่อย่างเหมาะสม เช่น ช่องทางการติดต่อแบบทางการและข้อมูลสำหรับการติดต่อแบบทางการ

4. จัดการเกี่ยวกับการติดต่อและแลกเปลี่ยนข้อมูลกับกลุ่มผู้สนใจ กลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยอย่างเหมาะสม

5. บริหารจัดการโครงการทุกประเภท องค์กรควรพิจารณาถึงความมั่นคงปลอดภัยทางไซเบอร์

แนวทางการดำเนินงาน

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม ดำเนินงานได้อย่างเป็นระบบ จึงกำหนดให้มีการบริหารจัดการ 4 ระยะ ดังนี้

1. ระยะวางแผนการบริหาร (Plan)

กิจกรรมการวางแผนการบริหาร โดยกิจกรรมในระยะนี้ ประกอบด้วย

1.1 พิจารณา และทบทวนนโยบายความมั่นคงปลอดภัยทางไซเบอร์ และเอกสารที่เกี่ยวข้อง

1.2 ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

1.3 จัดทำแผนการอบรมผู้เกี่ยวข้องให้สามารถปฏิบัติตามแผน และนโยบายได้

1.4 จัดทำแผนการสร้างความรู้ความตระหนักเรื่องความมั่นคงปลอดภัยทางไซเบอร์แก่ผู้ปฏิบัติงาน

1.5 จัดทำแผนส่งเสริมผู้ปฏิบัติงานที่ได้รับมอบหมายสิทธิหรือบทบาทพิเศษในงานความมั่นคงปลอดภัยทางไซเบอร์ ให้ได้ใบรับรองความสามารถทางวิชาชีพ

2. ระยะการดำเนินงาน และปฏิบัติการ (Do)

กิจกรรมระยะดำเนินงาน ประกอบด้วย

2.1 ปฏิบัติตามนโยบาย มาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม

2.2 ประเมินความสามารถและข้อจำกัดต่าง ๆ ในการปฏิบัติตามมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม

2.3 วิเคราะห์ผลการประเมิน เพื่อบ่งชี้ช่องโหว่และตรวจสอบประสิทธิผลของมาตรการควบคุมที่มีอยู่

3. ระยะการติดตามตรวจสอบ และทบทวน (Check)

กิจกรรมระยะการติดตามตรวจสอบ และทบทวน โดยกิจกรรมในระยะนี้ ประกอบด้วย

3.1 จัดตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์

3.2 สรุปผลการตรวจสอบ

3.3 นำเสนอผลการปฏิบัติในที่ประชุมคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มหาวิทยาลัยมหาสารคาม

4. ระยะการแก้ไข และปรับปรุง (Act)

กิจกรรมระยะการแก้ไข และปรับปรุง โดยกิจกรรมในระยะนี้ ประกอบด้วย

4.1 พิจารณาแนวทางการปรับปรุงการปฏิบัติ เพื่อให้เป็นไปตามเป้าหมาย หรือตามที่คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคามกำหนด

4.2 แจ้งผลการตรวจสอบและแนวทางการแก้ไขให้กับหน่วยงานต่าง ๆ

4.3 ปฏิบัติตามแนวทางการปรับปรุงที่กำหนด พร้อมบันทึกผลการปฏิบัติ

4.4 ตรวจสอบและติดตามผลการปรับปรุงแก้ไข

โครงสร้างของมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม

องค์ประกอบของมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม แบ่งเป็น 12 หัวข้อ ดังต่อไปนี้

หมวด	เรื่อง
1	นโยบายความมั่นคงปลอดภัยทางไซเบอร์ (Cyber and Information Security Policies)
2	การจัดการความมั่นคงปลอดภัยทางไซเบอร์ภายในมหาวิทยาลัย (Organization of Cyber and Information Security)
3	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
4	การบริหารจัดการทรัพย์สิน (Asset Management)
5	ความมั่นคงปลอดภัยในการดำเนินงาน (Operations Security)
6	การควบคุมอุปกรณ์คอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกล (Mobile Device Control and Remote Access Control)
7	การควบคุมการเข้าถึง (Access Control)
8	การเข้ารหัสข้อมูล (Cryptography)
9	ความมั่นคงปลอดภัยในการสื่อสาร (Communications Security)
10	การจัดหา พัฒนา และบำรุงรักษาระบบ
11	นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางการดำเนินงาน (Information security continuity policy)
12	การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

2. โครงสร้างผู้รับผิดชอบและบทบาทหน้าที่

คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม คณะกรรมการดำเนินงานจัดทำแผนการปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยามหาสารคาม พ.ศ. 2566-2569

2.1 กำหนดทิศทางความมั่นคงปลอดภัยทางไซเบอร์

2.2 ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยทางไซเบอร์ (Cyber and Information Security Policy)

2.3 ดูแลให้มีมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม และมีการทบทวนและประเมินประสิทธิภาพนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

2.4 ดูแลให้มีการติดตามและตรวจสอบในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ผลการทดสอบและการปฏิบัติตามแผนบริหารจัดการความต่อเนื่องในการดำเนินงานตามพันธกิจด้านเทคโนโลยีดิจิทัลและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

3. คณะทำงาน Computer Security Incident Response Team (งานระบบเครือข่ายและการสื่อสาร สำนักคอมพิวเตอร์)

3.1 จัดให้มีช่องทางการติดต่อสื่อสารสำหรับใช้รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

3.2 รายงานการติดตามและเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งแนวโน้มความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้นและส่งผลกระทบต่อมหาวิทยาลัยมหาสารคาม

4. การแบ่งแยกหน้าที่ความรับผิดชอบ

เพื่อให้เกิดความชัดเจนในการปฏิบัติงานของผู้ปฏิบัติงานและเป็นการยืนยันตัวบุคคล ซึ่งเป็นการลดความเสี่ยงในการเข้าถึงและใช้งานทรัพย์สินสารสนเทศ ให้หน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่เกี่ยวข้องดำเนินงานดังนี้

4.1 จัดทำ “ทะเบียนรายชื่อผู้มีสิทธิพิเศษและหน้าที่ความรับผิดชอบ” ซึ่งมอบหมายหน้าที่ให้แก่ผู้ปฏิบัติงานในการเข้าถึงส่วนสำคัญของระบบงาน และกำหนดหน้าที่ความรับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติงานอยู่อย่างชัดเจนเป็นลายลักษณ์อักษร ดังนี้

1.1 รายชื่อผู้ดูแลระบบเครือข่าย (Network Administrator)

1.2 รายชื่อผู้พัฒนาระบบ (Developer Administrator)

1.3 ผู้ดูแลระบบงาน (Application Administrator)

1.4 ผู้ดูแลระบบ (System Administrator)

1.5 รายชื่อผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์

1.6 รายชื่อผู้ควบคุมข้อมูลส่วนบุคคล

1.7 รายชื่อผู้ดูแลระบบที่จัดเก็บข้อมูลส่วนบุคคล

4.2 กำหนดบุคลากรสำรองในงานที่สำคัญ เพื่อทำงานทดแทนในกรณีจำเป็น เช่น ผู้ดูแลระบบงาน (Application Administrator) ผู้บริหารระบบ (System Administrator)

4.3 กำหนดบุคลากรผู้ทำหน้าที่ติดต่อหน่วยงานและประสานงานผู้มีอำนาจหน้าที่ในการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ และผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยฯ

4.4 กำหนดหน่วยงานที่มีหน้าที่รับผิดชอบความมั่นคงปลอดภัยทางไซเบอร์ ให้มีหน้าที่ดำเนินงาน ดังนี้

1. เพิ่มเติมความรู้เกี่ยวกับแนวปฏิบัติที่ดี (Best Practices) และติดตามข้อมูลข่าวสารด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

2. กำหนดมาตรการให้สภาพแวดล้อมและสถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคาม มีความทันสมัยและครอบคลุมทุกกระบวนการ

3. รับการแจ้งเตือนเกี่ยวกับการโจมตีและช่องโหว่ รวมถึงคำแนะนำ และการปรับปรุงระบบที่เกี่ยวข้อง

4. เพิ่มช่องทางการเข้าถึงคำแนะนำของผู้เชี่ยวชาญเรื่องความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

5. แบ่งปันและแลกเปลี่ยนข้อมูลเกี่ยวกับเทคโนโลยี ผลิตภัณฑ์ ภัยคุกคามหรือช่องโหว่ใหม่6.

6. จัดเตรียมช่องทางการติดต่อประสานงาน เพื่อรับมือกับสถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์อย่างเหมาะสม

ตารางแสดงหน้าที่ความรับผิดชอบตามมาตรฐานความมั่งคงปลอดภัยทางไซเบอร์

หมวด	หมวด/หัวข้อตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม	หน้าที่ความรับผิดชอบ
1	นโยบายความมั่นคงปลอดภัยทางไซเบอร์ (Cyber and Information Security Policies)	--คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม -ผู้อำนวยการสำนักคอมพิวเตอร์ -ผู้ดูแลระบบเครือข่าย
2	การจัดการความมั่นคงปลอดภัยทางไซเบอร์ภายในมหาวิทยาลัย (Organization of Cyber and Information Security)	-คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม

หมวด	หมวด/หัวข้อตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม	หน้าที่ความรับผิดชอบ
		-ผู้อำนวยการสำนักคอมพิวเตอร์ -ผู้ดูแลระบบเครือข่าย -คณะ/หน่วยงาน -ผู้ปฏิบัติงาน
3	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)	-ผู้อำนวยการสำนักคอมพิวเตอร์ -คณะ/หน่วยงาน -ผู้ปฏิบัติงาน -ผู้ดูแลระบบ -ผู้ควบคุมห้องบริการคอมพิวเตอร์ -ผู้ควบคุมดูแลพื้นที่ควบคุม
4	การบริหารจัดการทรัพย์สิน (Asset Management)	-ผู้อำนวยการสำนักคอมพิวเตอร์ -ผู้ดูแลระบบเครือข่าย -คณะ/หน่วยงาน -ผู้ปฏิบัติงาน
5	ความมั่นคงปลอดภัยในการดำเนินงาน (Operations Security)	-คณะ/หน่วยงาน -ผู้ปฏิบัติงาน
6	การควบคุมอุปกรณ์คอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกล	--คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม -ผู้อำนวยการสำนักคอมพิวเตอร์ -ผู้ดูแลระบบเครือข่าย -คณะ/หน่วยงาน -ผู้ปฏิบัติงาน
7	การควบคุมการเข้าถึง (Access Control)	-ผู้ดูแลระบบเครือข่าย -คณะ/หน่วยงาน -ผู้ปฏิบัติงาน -ผู้พัฒนาระบบ -ผู้ดูแลระบบ
8	การเข้ารหัสข้อมูล (Cryptography)	-ผู้ดูแลระบบเครือข่าย -ผู้ดูแลระบบ -คณะ/หน่วยงาน -ผู้ดูแลจดหมายอิเล็กทรอนิกส์ -ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ -ผู้ปฏิบัติงาน

หมวด	หมวด/หัวข้อตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม	หน้าที่ความรับผิดชอบ
9	ความมั่นคงปลอดภัยในการสื่อสาร (Communications Security)	-คณะ/หน่วยงาน -ผู้ปฏิบัติงาน
10	การจัดหา พัฒนา และบำรุงรักษาระบบ	-ผู้อำนวยการสำนักคอมพิวเตอร์ -ผู้ดูแลระบบเครือข่าย -คณะ/หน่วยงาน -ผู้ปฏิบัติงาน -ผู้ส่งมอบ
11	นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางการดำเนินงาน (Information security continuity policy)	-คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม -ผู้อำนวยการสำนักคอมพิวเตอร์ -ผู้ดูแลระบบเครือข่าย -ผู้ปฏิบัติงาน
12	การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)	-คณะ/หน่วยงาน -ผู้ปฏิบัติงาน

ข้อตกลงการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

1. แต่ละคณะ/หน่วยงานต้องมี “ทะเบียนรายชื่อผู้รับผิดชอบและบทบาทหน้าที่” ซึ่งมอบหมายหน้าที่ให้แก่ผู้ปฏิบัติงานตามมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม เช่น ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ดูแลห้องบริการคอมพิวเตอร์ ผู้ดูแลพื้นที่ควบคุม

2. แต่ละคณะ/หน่วยงานต้องประเมินความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพ

3. แต่ละคณะ/หน่วยงานต้องระบุและตรวจสอบทะเบียนทรัพย์สินสารสนเทศของหน่วยงาน รวมทั้งทบทวนปรับปรุงให้ทันสมัยอยู่เสมอ

4. แต่ละคณะ/หน่วยงานต้องทำการประเมินความสามารถและข้อจำกัดต่าง ๆ ในการปฏิบัติตามมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคามตาม “แบบประเมินและตรวจสอบการปฏิบัติตามมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์”

หมวด 3 ความมั่นคงปลอดภัยทางกายภาพของคณะ/หน่วยงานและสภาพแวดล้อม
(Physical and Environmental Security)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย การก่อกวนหรือการแทรกแซงการทำงานที่มีต่อทรัพย์สินสารสนเทศของมหาวิทยาลัยมหาสารคาม สถานที่ อุปกรณ์เครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ ระบบสารสนเทศ และระบบสนับสนุนสำหรับการประมวลผลสารสนเทศ และเพื่อป้องกันทรัพย์สินสารสนเทศจากการสูญหาย ความเสียหาย การโจรกรรมหรืออันตราย และการรบกวนการดำเนินงานตามพันธกิจของมหาวิทยาลัย ซึ่งประกอบด้วย 2 เรื่องดังต่อไปนี้

3.1 พื้นที่ควบคุม สำนักงาน และทรัพย์สินอื่น ๆ

3.1.1 พื้นที่ควบคุม

3.1.2 สำนักคอมพิวเตอร์

3.1.3 ห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน

3.1.4 ห้องบริการคอมพิวเตอร์สำหรับการสืบค้นข้อมูล

3.1.5 สำนักงาน ห้องทำงาน และทรัพย์สินอื่น ๆ

3.1.6 บริเวณสำหรับการเข้าถึง หรือการส่งมอบพัสดุโดยผู้ส่งมอบ

3.2 อุปกรณ์เครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ และระบบสารสนเทศ

โดยมีรายละเอียดการดำเนินงานในแต่ละเรื่อง ดังต่อไปนี้

3.1 พื้นที่ควบคุม สำนักงาน และทรัพย์สินอื่น ๆ

มาตรการ

1. กำหนดและใช้งานแนวกั้นทางกายภาพหรือขอบเขตความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันพื้นที่ที่มีทรัพย์สินสารสนเทศที่ละเอียดอ่อนหรือสำคัญ และสถานที่หรือสิ่งอำนวยความสะดวกสำหรับการประมวลผลและการเข้าถึงสารสนเทศ

2. ป้องกันพื้นที่ควบคุม โดยมีการควบคุมการเข้าออกที่เหมาะสม เพื่อให้มั่นใจได้ว่า เข้าถึงได้เฉพาะบุคคลที่มีสิทธิเท่านั้น

3. ออกแบบและรักษาความมั่นคงปลอดภัยทางกายภาพต่อสำนักงาน ห้องทำงาน และอาคารสถานที่อย่างเหมาะสม

4. ออกแบบและป้องกันทางกายภาพ เพื่อป้องกันภัยธรรมชาติ การโจมตีที่เป็นอันตรายหรืออุบัติเหตุ

5. ออกแบบและดำเนินงานตามขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการความมั่นคงปลอดภัยทางด้านระบบเครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ และระบบสารสนเทศ

6. ควบคุมบริเวณที่มีการเข้าถึง เช่น พื้นที่ส่งมอบและขนถ่ายวัสดุ พื้นที่อื่นที่บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้ หากเป็นไปได้ควรแยกจากสถานที่และสิ่งอำนวยความสะดวกสำหรับการประมวลผลสารสนเทศเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

3.1.1 **พื้นที่ควบคุม (ห้องศูนย์กลางข้อมูล)**

คุณสมบัติของพื้นที่ควบคุม

1. กั้นบริเวณและจัดทำผนังหรือกำแพงล้อมรอบ

2. กำแพงชั้นนอกของอาคาร ต้องมีโครงสร้างที่แข็งแรง ประตูชั้นนอกทั้งหมดต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอย่างแน่นหนาด้วยกลไกควบคุม เช่น สัญญาณเตือนผู้บุกรุก (Alarms) ประตูและหน้าต่างที่อยู่ชั้นล่างต้องใส่กุญแจ (Lock) อยู่ตลอดเวลา

3. บริเวณทางเข้า-ออกของอาคาร ต้องจัดตั้งโต๊ะทำการของผู้รักษาความปลอดภัย โดยกำหนดให้เข้าอาคารได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

4. ประตูหนีไฟของอาคาร ต้องไม่สามารถเปิดประตูจากภายนอกอาคารได้ หรือมีระบบแจ้งเตือนการบุกรุกพร้อมทั้งทดสอบระบบแจ้งเตือนอย่างน้อยปีละ 1 ครั้ง

5. มีอุปกรณ์ดับเพลิงอย่างพอเพียงและติดตั้งอยู่ในจุดที่สำคัญ มีความสะดวกและมีความพร้อมแก่การใช้งาน

6. มีระบบดับเพลิงอัตโนมัติ

7. มีระบบป้องกันไฟฟ้าขัดข้อง เช่น ระบบสำรองไฟฟ้า (UPS) และหรือระบบกำเนิดไฟฟ้า(Generator)

8. มีระบบกรองกระแสไฟฟ้า (Stabilizer System) เพื่อป้องกันความเสียหายอันเกิดจากระบบไฟฟ้า

9. มีบริเวณสำหรับการเข้าถึงหรือการส่งมอบพัสดุโดยผู้ส่งมอบ เพื่อให้หน่วยงานที่ส่งมอบสามารถส่งมอบพัสดุโดยไม่จำเป็นต้องเข้าถึงในบริเวณอื่น ๆ ของพื้นที่ควบคุม หรืออนุญาตเฉพาะบุคลากรที่ได้ระบุไว้

แนวปฏิบัติสำหรับผู้ดูแลพื้นที่ควบคุม

1. กำหนดสิทธิผู้ปฏิบัติงานและหน่วยงานภายนอกที่มีสิทธิผ่านเข้า–ออกพื้นที่ควบคุมและช่วงเวลาที่มีสิทธิผ่านเข้า – ออกพื้นที่ควบคุมอย่างเป็นลายลักษณ์อักษร รวมทั้งต้องมีผู้ดูแลหรือผู้ปฏิบัติงานของคณะ/หน่วยงาน อยู่ร่วมในการปฏิบัติงานดังกล่าว

2. จัดให้มีบันทึกผู้มาติดต่อ (Visitor Log Book)

3. ควบคุมดูแลให้เข้าพื้นที่ควบคุมได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น และทำการลงบันทึกข้อมูลในบันทึกผู้มาติดต่อ

4. ควบคุมไม่ให้นำอุปกรณ์สารสนเทศที่บันทึกรูปภาพ วีดีทัศน์หรือเสียง และสื่อบันทึกชนิดเคลื่อนที่เข้าไปภายในพื้นที่ควบคุม ยกเว้นเมื่อรับอนุญาตอย่างเป็นลายลักษณ์อักษรจากผู้บริหารคณะ/หน่วยงาน

5. ตรวจสอบความถูกต้องครบถ้วนของบันทึกผู้มาติดต่อเป็นประจำทุกเดือน และลงรายชื่อรับรองความถูกต้องโดยผู้ดูแลพื้นที่ควบคุม

6. จัดเก็บบันทึกผู้มาติดต่อไว้อย่างน้อย 90 วัน

7. ทบทวนสิทธิผ่านเข้า – ออกบริเวณพื้นที่ควบคุมเป็นประจำทุกไตรมาส

จัดให้มีการป้องกันไฟไหม้ เช่น เครื่องตรวจจับความร้อน และเครื่องตรวจจับควัน

8. ควบคุมให้มีการทดสอบระบบดับเพลิงอัตโนมัติ ระบบป้องกันไฟฟ้าขัดข้อง เป็นประจำอย่างน้อยปีละ 1 ครั้ง

9. ระมัดระวังไม่ให้มีวัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้และวัสดุที่ติดไฟได้ง่าย ตั้งอยู่ในพื้นที่ควบคุม

10. ควบคุมไม่ให้สูบบุหรี่ รับประทานอาหาร และดื่มน้ำภายในพื้นที่ควบคุม นอกจากบริเวณที่ได้จัดไว้ให้

11. ตรวจสอบวัสดุว่า มีความถูกต้องตามทะเบียนที่แจ้งไว้หรือไม่ ก่อนนำเข้าพื้นที่ควบคุม เพื่อป้องกันการปลอมแปลง

12. ตรวจสอบวัสดุว่า จะก่อให้เกิดความเสียหายต่อพื้นที่ควบคุมหรือไม่ ก่อนจะเคลื่อนย้ายวัสดุจากบริเวณสำหรับการเข้าถึงหรือการส่งมอบไปยังจุดที่ติดตั้งใช้งานจริง โดยเฉพาะอย่างยิ่งควรตรวจสอบไม่ให้มีวัตถุระเบิด สารเคมี หรือวัตถุอันตรายอื่น ๆ

3.1.2 สำนักคอมพิวเตอร์

คุณสมบัติของสำนักคอมพิวเตอร์

1. อยู่ในพื้นที่เฉพาะซึ่งมีผนังล้อมรอบและมีประตูทางเข้า–ออกอีกชั้นหนึ่ง โดยประตูทางเข้า–ออกของสำนักคอมพิวเตอร์ต้องมีการป้องกันการเข้าถึงอย่างแน่นหนาด้วยกลไกควบคุม เช่น สัญญาณเตือนผู้บุกรุก (Alarms) ระบบตรวจจับการบุกรุก

2. บริเวณทางเข้า-ออกของอาคาร ต้องจัดตั้งโต๊ะทำการของผู้รักษาความปลอดภัย โดยกำหนดให้เข้าอาคารได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

3. ประตูหนีไฟของอาคาร ต้องไม่สามารถเปิดประตูจากภายนอกอาคารได้ หรือมีระบบแจ้งเตือนการบุกรุก พร้อมทั้งทดสอบระบบแจ้งเตือนอย่างน้อยปีละ 1 ครั้ง

4. ภายในสำนักคอมพิวเตอร์ ต้องแบ่งพื้นที่ให้เป็นสัดส่วน โดยแบ่งเป็นส่วนระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server zone) ส่วนระบบเครือข่าย (Network zone) และส่วนพื้นที่ปฏิบัติงานสำหรับเจ้าหน้าที่สำนัก

คอมพิวเตอร์ ทั้งนี้ต้องมีประตูทางเข้า–ออก เฉพาะสำหรับส่วนระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server zone) และส่วนระบบเครือข่าย (Network zone)

5. ภายในสำนักคอมพิวเตอร์ ต้องแบ่งพื้นที่ให้เป็นสัดส่วน โดยแยกอุปกรณ์สารสนเทศที่ดูแลโดยมหาวิทยาลัย ออกจากอุปกรณ์สารสนเทศที่ดูแลโดยหน่วยงานภายนอกอย่างชัดเจน

6. ภายในสำนักคอมพิวเตอร์ ต้องมีการติดตั้งกล้องวงจรปิดให้ครอบคลุมพื้นที่ที่สำคัญทั้งหมดภายในอาคารของสำนักคอมพิวเตอร์

7. มีอุปกรณ์ดับเพลิงอย่างพอเพียง และติดตั้งอยู่ในจุดที่สำคัญ มีความสะดวกและมีความพร้อมแก่การใช้งาน

8. มีระบบดับเพลิงอัตโนมัติ เช่น ระบบดับเพลิงแบบใช้สาร IG541, ระบบดับเพลิงด้วยน้ำชนิด Dry Pipe

9. มีระบบป้องกันไฟฟ้าขัดข้อง เช่น ระบบสำรองไฟฟ้า (UPS) ระบบกำเนิดไฟฟ้า (Generator) สำหรับห้องศูนย์ข้อมูลกลาง (Data Center) เป็นการเฉพาะ ของสำนักคอมพิวเตอร์

10. มีระบบควบคุมอุณหภูมิและความชื้น โดยอุณหภูมิและความชื้นต้องอยู่ในระดับที่เหมาะสมกับอุปกรณ์เครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ และระบบสารสนเทศ ที่จัดอยู่ในสำนักคอมพิวเตอร์

11. มีระบบตรวจจับน้ำรั่วและมีการยกระดับพื้นสำหรับห้องศูนย์ข้อมูลกลาง (Data Center) ของสำนักคอมพิวเตอร์

12. มีระบบกรองกระแสไฟฟ้า (Stabilizer System) เพื่อป้องกันความเสียหายอันเกิดจากระบบไฟฟ้า

13. มีบริเวณสำหรับการเข้าถึงหรือการส่งมอบพัสดุโดยผู้ส่งมอบ เพื่อให้หน่วยงานที่ส่งมอบ สามารถส่งมอบพัสดุโดยไม่จำเป็นต้องเข้าถึงในบริเวณอื่น ๆ ของสำนักคอมพิวเตอร์ หรืออนุญาตเฉพาะบุคลากรที่ได้ระบุไว้

14. บริเวณทางเข้า-ออกของอาคารและห้องศูนย์ข้อมูลกลาง (Data Center) ต้องติดตั้งระบบกล้องวงจรปิดและทำการบันทึกการเข้าออกตลอด 24 ชั่วโมง และมีการจัดเก็บข้อมูลผู้เข้า-ออกไว้เป็นเวลาไม่น้อยกว่า 90 วัน

แนวปฏิบัติสำหรับผู้อำนวยการสำนักคอมพิวเตอร์

1. กำหนดสิทธิผู้ปฏิบัติงานและหน่วยงานภายนอกที่มีสิทธิผ่านเข้า-ออกสำนักคอมพิวเตอร์และช่วงเวลาที่มีสิทธิผ่านเข้า–ออกสำนักคอมพิวเตอร์อย่างเป็นลายลักษณ์อักษร สำหรับหน่วยงานภายนอกจะต้องได้รับการอนุมัติจากผู้บริหารคณะ/หน่วยงาน รวมทั้งต้องมีผู้ดูแลสำนักคอมพิวเตอร์หรือผู้ปฏิบัติงานของคณะ/หน่วยงาน อยู่ร่วมในการปฏิบัติงานดังกล่าว

2. จัดให้มีบันทึกผู้มาติดต่อ (Visitor Log Book)

3. ควบคุมดูแลให้เข้าสำนักคอมพิวเตอร์ได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น และทำการลงบันทึกข้อมูลในบันทึกผู้มาติดต่อ

4. ตรวจสอบความถูกต้องครบถ้วนของบันทึกผู้มาติดต่อเป็นประจำทุกเดือน และลงรายชื่อรับรองความถูกต้อง

5. จัดเก็บบันทึกผู้มาติดต่อไว้อย่างน้อย 90 วัน

6. ทบทวนสิทธิผ่านเข้า – ออกสำนักคอมพิวเตอร์เป็นประจำทุกไตรมาส

7. ในระหว่างการบำรุงรักษาอุปกรณ์เครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ และระบบสารสนเทศ หรือระบบสนับสนุนต่าง ๆ ต้องประสานงานเจ้าของระบบสารสนเทศ จัดให้มีการควบคุมที่เหมาะสม เพื่อป้องกันการปฏิบัติงานอันก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

8. จัดให้มีการป้องกันไฟไหม้ เช่น เครื่องตรวจจับความร้อน เครื่องตรวจจับควัน เป็นต้น

9. ควบคุมให้มีการทดสอบระบบดับเพลิงอัตโนมัติ ระบบป้องกันไฟฟ้าขัดข้อง ระบบควบคุมอุณหภูมิและความชื้น และระบบตรวจจับน้ำรั่ว เป็นประจำอย่างน้อยปีละ 1 ครั้ง

10. ควบคุมให้มีระบบหรือกระบวนการ ในการปิดการทำงานฉุกเฉินสำหรับอุปกรณ์เครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ และระบบสารสนเทศ เมื่อระบบไฟฟ้าสำรองมีกระแสไฟฟ้าเหลืออยู่ในจำนวนจำกัด เพื่อป้องกันความเสียหายอันเกิดจากอุปกรณ์เครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ และระบบสารสนเทศ ไม่ได้รับการปิดการทำงานได้ทันท่วงทีระมัดระวังไม่ให้มีวัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้และวัสดุที่ติดไฟได้ง่าย ตั้งอยู่ในสำนักคอมพิวเตอร์

11. ควบคุมไม่ให้สูบบุหรี่ ภายในสำนักคอมพิวเตอร์

12. ตรวจสอบวัสดุว่า มีความถูกต้องตามทะเบียนที่แจ้งไว้หรือไม่ ก่อนนำเข้าสำนักคอมพิวเตอร์ เพื่อป้องกันการปลอมแปลง ทั้งนี้ควรรายงานให้ผู้บริหารคณะ/หน่วยงาน ทราบทันที ในกรณีที่มีการค้นพบการปลอมแปลงดังกล่าว

13. ตรวจสอบวัสดุว่า จะก่อให้เกิดความเสียหายต่อสำนักคอมพิวเตอร์หรือไม่ ก่อนจะเคลื่อนย้ายวัสดุจากบริเวณสำหรับการเข้าถึงหรือการส่งมอบไปยังจุดที่ติดตั้งใช้งานจริง โดยเฉพาะอย่างยิ่งควรตรวจสอบไม่ให้มีวัตถุระเบิด สารเคมี หรือวัตถุอันตรายอื่น ๆ

14. ประสานงานคณะ/หน่วยงานที่เป็นเจ้าของระบบสารสนเทศ เพื่อจัดทำทะเบียนทรัพย์สินที่อยู่ในสำนักคอมพิวเตอร์ และทบทวนทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง และปรับปรุงให้ทันสมัยอยู่เสมอ

15. ตรวจสอบทะเบียนทรัพย์สินโดยต้องมีการระบุเจ้าของ ช่องทางการติดต่อเจ้าของ และระดับการป้องกันความมั่นคงปลอดภัยให้ชัดเจน

3.1.3 ห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน

คุณสมบัติของห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน

1. อยู่ในอาคารที่มีการกั้นบริเวณและจัดทำผนังหรือกำแพงล้อมรอบ โดยต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2. ประตูหนีไฟของอาคาร ต้องไม่สามารถเปิดประตูจากภายนอกอาคารได้ หรือมีระบบแจ้งเตือนการบุกรุก พร้อมทั้งทดสอบระบบแจ้งเตือนเป็นประจำอย่างน้อยปีละ 1 ครั้ง

3. มีอุปกรณ์ดับเพลิงอย่างพอเพียงและติดตั้งอยู่ในจุดที่สำคัญ มีความสะดวกและมีความพร้อมแก่การใช้งาน

4. มีบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์ เพื่อให้ผู้ส่งมอบสามารถส่งมอบผลิตภัณฑ์โดยไม่จำเป็นต้องเข้าถึงในบริเวณอื่น ๆ ของห้องบริการคอมพิวเตอร์ หรืออนุญาตเฉพาะบุคลากรที่ได้ระบุไว้

5. บริเวณทางเข้า-ออกของห้องบริการคอมพิวเตอร์ ต้องติดตั้งระบบกล้องวงจรปิดและทำการบันทึกการเข้าออกตลอดการให้บริการ และมีการจัดเก็บข้อมูลผู้เข้า-ออกไว้เป็นเวลาไม่น้อยกว่า 3 เดือน

แนวปฏิบัติสำหรับผู้ดูแลห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน

1. กำหนดสิทธิผู้ปฏิบัติงานและหน่วยงานภายนอกที่มีสิทธิผ่านเข้า–ออกห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอนและช่วงเวลาที่มีสิทธิผ่านเข้า – ออกห้องบริการคอมพิวเตอร์อย่างเป็นลายลักษณ์อักษร

2. จัดให้มีบันทึกข้อมูลการเข้าใช้ห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอนตามตารางการใช้งาน

3. มีมาตรการควบคุมห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน เช่น มีกุญแจล็อค หรือระบบล็อคประตูดิจิทัล

4. จัดให้มีการป้องกันไฟไหม้ เช่น เครื่องตรวจจับความร้อน เครื่องตรวจจับควัน

5. ระมัดระวังไม่ให้มีวัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้และวัสดุที่ติดไฟได้ง่าย ตั้งอยู่ในห้องบริการคอมพิวเตอร์

6. ควบคุมไม่ให้สูบบุหรี่ รับประทานอาหารภายในห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน

7. ตรวจสอบวัสดุว่า มีความถูกต้องตามทะเบียนที่แจ้งไว้หรือไม่ ก่อนนำเข้าห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน เพื่อป้องกันการปลอมแปลง ทั้งนี้ควรรายงานให้ผู้บริหารคณะ/หน่วยงาน ทราบทันที ในกรณีที่มีการค้นพบการปลอมแปลงดังกล่าว

8. ประสานงานหน่วยงานที่เป็นเจ้าของระบบสารสนเทศ เพื่อจัดทำทะเบียนทรัพย์สินที่อยู่ในห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอนและทบทวนทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง และปรับปรุงให้ทันสมัยอยู่เสมอ

9. ตรวจสอบทะเบียนทรัพย์สินโดยต้องมีการระบุเจ้าของ ช่องทางการติดต่อเจ้าของ และระดับการป้องกันความมั่นคงปลอดภัยให้ชัดเจน

3.1.4 ห้องบริการคอมพิวเตอร์สำหรับการสืบค้นข้อมูล

คุณสมบัติของห้องบริการคอมพิวเตอร์สำหรับการสืบค้นข้อมูล

1. อยู่ในอาคารที่มีการกั้นบริเวณและจัดทำผนังหรือกำแพงล้อมรอบ โดยต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2. ประตูหนีไฟของอาคาร ต้องไม่สามารถเปิดประตูจากภายนอกอาคารได้ หรือมีระบบแจ้งเตือนการบุกรุก พร้อมทั้งทดสอบระบบแจ้งเตือนเป็นประจำอย่างน้อยปีละ 1 ครั้ง

3. พื้นที่ห้องบริการคอมพิวเตอร์สำหรับการสืบค้นข้อมูล ต้องมีผนังล้อมรอบและมีประตูทางเข้า–ออกอีกชั้นหนึ่ง โดยประตูทาง เข้า–ออกของห้องบริการคอมพิวเตอร์ต้องมีการป้องกันการเข้าถึงอย่างแน่นหนา

4. มีอุปกรณ์ดับเพลิงอย่างพอเพียงและติดตั้งอยู่ในจุดที่สำคัญ มีความสะดวกและมีความพร้อมแก่การใช้งาน

5. มีบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์ เพื่อให้ผู้ส่งมอบสามารถส่งมอบผลิตภัณฑ์โดยไม่จำเป็นต้องเข้าถึงในบริเวณอื่น ๆ ของห้องบริการคอมพิวเตอร์หรืออนุญาตเฉพาะบุคลากรที่ได้ระบุไว้

6. บริเวณทางเข้า-ออกของห้องบริการคอมพิวเตอร์ต้องติดตั้งระบบกล้องวงจรปิดและทำการบันทึกการเข้าออกตลอดการให้บริการ และมีการจัดเก็บข้อมูลผู้เข้า-ออกไว้เป็นเวลาไม่น้อยกว่า 3 เดือน

แนวปฏิบัติสำหรับผู้ดูแลห้องบริการคอมพิวเตอร์

1. กำหนดสิทธิผู้ปฏิบัติงานและหน่วยงานภายนอกที่มีสิทธิผ่านเข้า–ออกห้องบริการคอมพิวเตอร์และช่วงเวลาที่มีสิทธิผ่านเข้า – ออกห้องบริการคอมพิวเตอร์อย่างเป็นลายลักษณ์อักษร

2. จัดให้มีบันทึกผู้มาติดต่อ (Visitor Log Book)

3. มีมาตรการควบคุมการเข้าออก เช่น มีกุญแจล็อค หรือระบบล็อคประตูดิจิทัล หรือใช้บัตรผ่านเฉพาะบุคคล (Access Card)

4. ตรวจสอบความถูกต้องครบถ้วนของบันทึกผู้มาติดต่อเป็นประจำทุกเดือน และลงรายชื่อรับรองความถูกต้อง

5. จัดเก็บบันทึกผู้มาติดต่อไว้อย่างน้อย 90 วัน

6. ทบทวนสิทธิระบบการผ่านเข้า–ออกห้องบริการคอมพิวเตอร์เป็นประจำทุกไตรมาส

7. จัดให้มีการป้องกันไฟไหม้ เช่น เครื่องตรวจจับความร้อน เครื่องตรวจจับควัน

8. ระมัดระวังไม่ให้มีวัตถุที่เป็นอันตรายอันอาจจะก่อให้เกิดเพลิงไหม้และวัสดุที่ติดไฟได้ง่าย ตั้งอยู่ในห้องบริการคอมพิวเตอร์

9. ควบคุมไม่ให้สูบบุหรี่ รับประทานอาหารภายในห้องบริการคอมพิวเตอร์

10. ตรวจสอบวัสดุว่า มีความถูกต้องตามทะเบียนที่แจ้งไว้หรือไม่ ก่อนนำเข้าห้องบริการคอมพิวเตอร์ เพื่อป้องกันการปลอมแปลง ทั้งนี้ควรรายงานให้ผู้บริหารคณะ/หน่วยงาน ทราบทันที ในกรณีที่มีการค้นพบการปลอมแปลงดังกล่าว

11. ประสานงานหน่วยงานที่เป็นเจ้าของระบบสารสนเทศ เพื่อจัดทำทะเบียนทรัพย์สินที่อยู่ในห้องบริการคอมพิวเตอร์ และทบทวนทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง และปรับปรุงให้ทันสมัยอยู่เสมอ

12. ตรวจสอบทะเบียนทรัพย์สินโดยต้องมีการระบุเจ้าของ ช่องทางการติดต่อเจ้าของ และระดับการป้องกันความมั่นคงปลอดภัยให้ชัดเจน

3.1.5 สำนักงาน ห้องทำงาน และทรัพย์สินอื่น ๆ

แนวปฏิบัติสำหรับหน่วยงาน

1. ควบคุมดูแลไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลภายใน ที่บ่งชี้ถึงสถานที่ตั้งของอุปกรณ์สารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด”

2. ควบคุมดูแลให้มีผู้รับผิดชอบตามที่ได้รับมอบหมาย ในสถานที่ที่มีการรับ-ส่ง อุปกรณ์เครือข่ายอุปกรณ์เทคโนโลยีดิจิทัลอื่น ๆ และสารสนเทศ โดยทำการบันทึกการเข้า-ออก

3. ควบคุมดูแลอุปกรณ์สารสนเทศสำนักงาน โดยจัดวางอยู่ในพื้นที่ตามหน่วยงานที่ได้รับการจัดสรร และอนุญาตให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

4. ควบคุมดูแลในระหว่างการบำรุงรักษาอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ และสารสนเทศ เช่น การเคลื่อนย้ายหรือส่งอุปกรณ์ไปตรวจซ่อม ต้องนำข้อมูลสำคัญซึ่งอาจมีผลกระทบต่อการดำเนินงานตามพันธกิจของมหาวิทยาลัย ออกจากอุปกรณ์หรือเครื่องก่อนเสมอ

5. ควบคุมดูแลให้หน่วยงานภายนอกปฏิบัติตามมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์มหาวิทยาลัยมหาสารคาม หากพบเห็นพฤติกรรมที่น่าสงสัยต้องแจ้งผู้บริหารคณะ/หน่วยงาน ผู้ดูแลพื้นที่ควบคุมห้องศูนย์กลางข้อมูล ผู้อำนวยการสำนักคอมพิวเตอร์ หรือผู้ดูแลห้องบริการคอมพิวเตอร์ โดยทันที

3.1.6 บริเวณสำหรับการเข้าถึง หรือการส่งมอบพัสดุโดยผู้ส่งมอบ

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. ตรวจสอบรายการอุปกรณ์จากผู้ส่งมอบทุกครั้งที่มีการนำอุปกรณ์เข้า–ออก พื้นที่
2. ทำการลงทะเบียนพัสดุที่รับเข้าตามแนวปฏิบัติหมวด 4 การบริหารจัดการทรัพย์สิน

ข้อปฏิบัติในการเข้าถึงพื้นที่ควบคุม สำนักงาน และทรัพย์สินต่าง ๆ

แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

1. ผู้ปฏิบัติงานที่ไม่มีความเกี่ยวข้องจะต้องไม่เข้าไปในพื้นที่ควบคุม เนื่องจากเหตุผลด้านความปลอดภัยและเพื่อป้องกันโอกาสที่จะเกิดกิจกรรมที่เป็นอันตราย

2. ไม่สูบบุหรี่ รับประทานอาหารภายในพื้นที่ควบคุม ห้องศูนย์กลางข้อมูล ห้องบริการคอมพิวเตอร์ ยกเว้นบริเวณที่ได้จัดไว้

3. ห้องทำงานส่วนตัว ต้องมีการปิดใส่กุญแจ (Lock) เมื่อไม่อยู่ภายในห้องทำงาน

4. เมื่อพบเห็นผู้ที่มีพฤติกรรมน่าสงสัยอยู่ภายในพื้นที่ควบคุมหรือสำนักงาน ต้องแจ้งผู้รักษาความปลอดภัยทราบโดยทันที

แนวปฏิบัติสำหรับหน่วยงานภายนอก

1. ทำหนังสือถึงผู้บริหารคณะ/หน่วยงาน เพื่อขออนุญาตเข้าพื้นที่พื้นที่ควบคุม ห้องศูนย์กลางข้อมูล และห้องบริการคอมพิวเตอร์

2. แลกบัตรอนุญาตหรือบัตรผู้มาติดต่อ และต้องติดบัตรให้สามารถเห็นได้อย่างชัดเจนตลอดเวลาที่อยู่ในสถานที่ ตามกฎระเบียบการเข้าพื้นที่อย่างเคร่งครัด

3. สำหรับพื้นที่ควบคุม ห้องศูนย์กลางข้อมูล และห้องบริการคอมพิวเตอร์ ต้องได้รับการอนุญาตตามข้อกำหนดของแต่ละสถานที่ และปฏิบัติตามกฎระเบียบการเข้าพื้นที่ควบคุมอย่างเคร่งครัด

4. ห้ามบันทึกภาพ วิดีโอ เสียง ในพื้นที่ควบคุม ห้องศูนย์กลางข้อมูล ยกเว้นเมื่อได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

5. ห้ามสูบบุหรี่ รับประทานอาหารภายในพื้นที่ควบคุม ห้องศูนย์กลางข้อมูล และห้องบริการคอมพิวเตอร์ ยกเว้นบริเวณที่ได้จัดไว้

6. แสดงรายการอุปกรณ์ที่นำเข้า-ออกพื้นที่อย่างเป็นลายลักษณ์อักษร

3.2 อุปกรณ์เครือข่าย เทคโนโลยีดิจิทัลอื่น ๆ และระบบสารสนเทศ

มาตรการ

1. จัดวางและป้องกันอุปกรณ์ เพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายทางสภาพแวดล้อม และโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

2. ป้องกันอุปกรณ์ต่าง ๆ จากปัญหากระแสไฟฟ้าล้มเหลว และการหยุดชะงักอื่น ๆ ซึ่งมีสาเหตุมาจากความล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานของระบบ

3. ป้องกันการเดินสายไฟฟ้า สายสื่อสาร และสายสัญญาณอื่น ๆ ที่มีข้อมูลหรือสนับสนุนบริการสารสนเทศจากการสกัดกั้น การรบกวนหรืออันตราย

4. บำรุงรักษาอุปกรณ์อย่างถูกต้อง เพื่อให้มั่นใจว่าอุปกรณ์มีความพร้อมใช้งานและมีความสมบูรณ์อย่างต่อเนื่อง

5. ไม่นำอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ หรือซอฟต์แวร์ต่าง ๆ ออกนอกคณะ/หน่วยงาน โดยไม่ได้รับอนุญาตก่อน

6. รักษาความมั่นคงปลอดภัยกับทรัพย์สินที่ใช้งานอยู่นอกคณะ/หน่วยงาน โดยคำนึงถึงความเสี่ยงต่าง ๆ ของการปฏิบัติงานนอกคณะ/หน่วยงาน

7. ตรวจสอบรายการอุปกรณ์ทั้งหมดที่บรรจุสื่อบันทึกข้อมูล เพื่อให้มั่นใจว่า มีการลบหรือเขียนทับข้อมูลที่อ่อนไหวและซอฟต์แวร์ลิขสิทธิ์อย่างปลอดภัย ก่อนกำจัดหรือนำอุปกรณ์กลับมาใช้งานอีกครั้ง

8. อุปกรณ์ที่ไม่มีผู้ดูแลจะต้องมีการป้องกันที่เหมาะสม

9. ปรับใช้นโยบายการเก็บรักษาทรัพย์สินไว้ในที่ที่ปลอดภัยสำหรับกระดาษและสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ และนโยบายการป้องกันหน้าจอเครื่องคอมพิวเตอร์สำหรับสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศให้เหมาะสม

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. ควบคุมให้มีการจัดวางอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ในพื้นที่ ให้สอดคล้องกับระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดังตารางต่อไปนี้

การควบคุมการจัดวางอุปกรณ์สารสนเทศ ตามระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์	
ระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์	**พื้นที่จัดวาง**
สูงสุด	พื้นที่ควบคุม หรือ ห้องศูนย์กลางข้อมูล (Data Center)
สูง	สำนักคอมพิวเตอร์
ปานกลาง	ห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน ห้องบริการคอมพิวเตอร์สำหรับการสืบค้นข้อมูล
ต่ำ	สำนักงาน

1.1 อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ที่ถูกจัดไว้ในระดับการป้องกันความมั่นคงปลอดภัย ทางไซเบอร์ “สูง” และ “สูงสุด” ต้องจัดวางอยู่ในสำนักคอมพิวเตอร์ หรือพื้นที่ควบคุม หรือ ห้องศูนย์กลางข้อมูล หรือมีมาตรการควบคุมการเข้าถึงอุปกรณ์สารสนเทศตามความเหมาะสม เช่น ให้มีการพิสูจน์และยืนยันตัวตนโดยใช้วิธีการพิสูจน์และยืนยันตัวตนแบบ 2 Factors

1.2 อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ที่ถูกจัดไว้ในระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ “ปานกลาง” ให้จัดวางอยู่ในห้องบริการคอมพิวเตอร์สำหรับการเรียนการสอน ห้องบริการคอมพิวเตอร์สำหรับการสืบค้นข้อมูล

1.3 อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ที่ถูกจัดไว้ในระดับการป้องกันความมั่นคงปลอดภัย ทางไซเบอร์ “ต่ำ” ควรจัดวางอยู่ในสำนักงาน

2. ควบคุมให้อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ถูกจัดวางอยู่ในพื้นที่ของหน่วยงานตามที่ได้รับการจัดสรร โดยอนุญาตให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

3. ควบคุมให้อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ถูกจัดวางอยู่ในสภาพแวดล้อมที่เหมาะสมตามคู่มือการใช้งานของเจ้าของผลิตภัณฑ์

4. ควบคุมให้อุปกรณ์แสดงผลสารสนเทศ เช่น จอคอมพิวเตอร์และเครื่องพิมพ์ ถูกจัดวางอย่างเหมาะสมเพื่อลดความเสี่ยงจากการเข้าถึงหรือเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต

5. ควบคุมให้อุปกรณ์คอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์พกพา และอุปกรณ์สำนักงาน มีการป้องกันการสูญหาย อย่างเหมาะสม เช่น การใช้สายล็อคอุปกรณ์ การเก็บในตู้ที่มีการล็อค

6. ควบคุมให้มีการรักษาความปลอดภัยพื้นที่จัดวางอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

7. มีมาตรการควบคุม เพื่อลดความเสี่ยงต่อภัยคุกคามทางกายภาพและสภาพแวดล้อมที่เป็นไปได้ เช่น การโจรกรรม ไฟไหม้ การรั่วไหล วัตถุระเบิด ควัน น้ำ หรือระบบจ่ายน้ำล้มเหลว ฝุ่น การสั่นสะเทือน การรบกวนแหล่งจ่ายไฟฟ้า การรบกวนการสื่อสาร และการทำลายทรัพย์สิน

8. ควบคุมให้มีการบำรุงรักษาอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ“สูงสุด” เป็นประจำ อย่างน้อยปีละ 1 ครั้ง หรือตามที่ได้ระบุในคู่มือการใช้งานของอุปกรณ์สารสนเทศ

9. ควบคุมให้มีสัญญาการว่าจ้างอย่างเป็นทางการ ในการว่าจ้างผู้ส่งมอบ เพื่อบำรุงรักษาอุปกรณ์สารสนเทศต่าง ๆ โดยกำหนดระยะเวลา ขอบเขต และระดับการให้บริการ (Service Level Agreement) อย่างชัดเจน

10. ควบคุมให้มีการบันทึกประวัติการบำรุงรักษาอุปกรณ์สารสนเทศอย่างเป็นลายลักษณ์อักษร

11. ทบทวนสัญญาบำรุงรักษาอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ เป็นประจำอย่างน้อยปีละ 1 ครั้ง

12. ควบคุมไม่ให้การบำรุงรักษาอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ผิดเงื่อนไขต่อการสิ้นสุดการประกัน

13. ในกรณีที่ต้องส่งมอบอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ เพื่อบำรุงรักษา ต้องจัดให้มีการควบคุมบุคลากรที่ดำเนินการบำรุงรักษาให้ปฏิบัติงานภายใต้ข้อกำหนดการรักษาความลับ และในกรณีที่มีสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ต้องล้างสารสนเทศดังกล่าวออกจากอุปกรณ์ก่อนส่งมอบ

14. ระหว่างการบำรุงรักษา ต้องควบคุมดูแลให้ปฏิบัติตามข้อกำหนดด้านการบำรุงรักษาทั้งหมดที่กำหนดในขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะ

15. ตรวจสอบอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ หลังบำรุงรักษา เพื่อให้มั่นใจว่าอุปกรณ์ทำงานได้ถูกต้องและไม่ได้ถูกดัดแปลงหรือมีการติดตั้งโปรแกรมไม่พึงประสงค์ ก่อนนำอุปกรณ์กลับมาใช้งาน

16. ควบคุมให้มีการบันทึกรายละเอียดเป็นลายลักษณ์อักษร และต้องตรวจสอบสภาพของทรัพย์สินของมหาวิทยาลัย หลังจากได้รับคืน ในกรณีที่เป็นการนำทรัพย์สินออกนอกพื้นที่ชั่วคราว

17. ควบคุมดูแลให้การประกันอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ที่ใช้งานอยู่ทั้งในและนอกสำนักงาน ครอบคลุมเพียงพอตามความเหมาะสมและเห็นสมควร

18. ควบคุมดูแลให้มีการลบหรือเขียนทับข้อมูลอุปกรณ์สารสนเทศที่บรรจุข้อมูล ก่อนกำจัดหรือนำอุปกรณ์กลับมาใช้งานอีกครั้ง

19. มีมาตรการป้องกันไม่ให้ผู้ปฏิบัติงานและหน่วยงานภายนอกที่ไม่มีสิทธิสามารถเข้าถึง อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ที่ไม่มีผู้รับผิดชอบโดยตรง

แนวปฏิบัติสำหรับผู้ดูแลพื้นที่ควบคุม ผู้อำนวยการสำนักคอมพิวเตอร์ ผู้ดูแลห้องบริการคอมพิวเตอร์

1. บริหารจัดการอุปกรณ์และระบบสนับสนุนสำหรับพื้นที่ควบคุม ห้องศูนย์กลางข้อมูล สำนักคอมพิวเตอร์และห้องบริการคอมพิวเตอร์ ดังต่อไปนี้

1.1 ให้เป็นไปตามข้อกำหนดของผู้ผลิตอุปกรณ์ และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

1.2 จัดให้มีอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ อย่างเพียงพอ เพื่อสนับสนุนการทำงานของอุปกรณ์ประมวลผลสารสนเทศ และมีการประเมินความสามารถของอุปกรณ์และระบบสนับสนุนเพื่อรองรับการทำงานในอนาคตอย่างน้อยปีละ 1 ครั้ง

1.3 จัดให้มีช่องทางสื่อสารอย่างน้อย 2 ช่องทาง เพื่อให้มีช่องทางสื่อสารสำรอง เมื่อช่องทางสื่อสารช่องทางใดช่องทางหนึ่งไม่สามารถใช้งานได้ตามปกติ

1.4 จัดเตรียมระบบแสงสว่างฉุกเฉินและระบบการสื่อสารฉุกเฉินไว้ รวมทั้งติดตั้งสวิตช์ฉุกเฉินและอุปกรณ์สำหรับตัดกระแสไฟฟ้า น้ำ แก๊ส หรืออุปกรณ์สนับสนุนอื่น ๆ ไว้ใกล้ทางออกฉุกเฉินหรือห้องอุปกรณ์

1.5 จัดให้มีการทดสอบความพร้อมใช้ของอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ เป็นประจำ

1.6 จัดให้มีระบบสัญญาณเตือนเมื่อตรวจพบความผิดปกติของการทำงาน ในกรณีที่จำเป็น

2. บริหารจัดการสายสื่อสาร สายเคเบิ้ลอื่น ๆ และการเดินสายไฟฟ้า ดังต่อไปนี้

2.1 สายไฟฟ้าและสายสื่อสารสำหรับอุปกรณ์ต่าง ๆ ต้องวางสายภายในท่อรางร้อยสาย หรือได้รับการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อหลีกเลี่ยงจากการเกิดความเสียหาย หรือการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

2.2 สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญา

2.3 สายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ต้องได้รับการทำสัญลักษณ์อย่างชัดเจนเพื่อป้องกันความสับสน

2.4 ในกรณีที่มีความจำเป็นต้องวางสายไฟฟ้าและสายสื่อสารสำหรับอุปกรณ์ต่าง ๆ ไว้ใต้ดิน ต้องมีป้ายบ่งชี้ถึงแนวสาย เพื่อป้องกับความเสียหายที่เกิดจากการขุดเจาะ

2.5 จัดทำเอกสารรายการการเข้าสาย (Patch List) เพื่อป้องกันความสับสน

3. บริหารจัดการระบบและอุปกรณ์ที่มีความสำคัญ (Sensitive or Critical Systems) ดังต่อไปนี้

3.1 ใช้สายสัญญาณที่มีคุณสมบัติป้องกันสนามแม่เหล็กไฟฟ้า หรือ ใช้สายใยแก้วนำแสง (Fiber Optic)

3.2 ติดตั้งท่อหุ้มสายชนิดพิเศษ (Armored Conduit) โดยจุดเชื่อมต่อของสายสัญญาณต่าง ๆ ต้องอยู่ภายในห้องหรือกล่องที่ใส่กุญแจได้

3.3 ควบคุมการเข้าถึงแผงพักปลายสาย (Patch Panel) และห้องพักสาย (Cable Room)

3.4 มีการตรวจสอบระบบสายสัญญาณ เพื่อตรวจจับอุปกรณ์แปลกปลอม

4. จัดให้มีการบำรุงรักษาอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ เป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือตามที่ได้ระบุในคู่มือการใช้งานของอุปกรณ์

5. จัดให้มีการบันทึกประวัติการบำรุงรักษาอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ อย่างเป็นลายลักษณ์อักษร

6. ทบทวนสัญญาบำรุงรักษาอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ เป็นประจำอย่างน้อยปีละ 1 ครั้ง

แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

1. การนำทรัพย์สินขององค์กรออกนอกพื้นที่มหาวิทยาลัยมหาสารคาม

1.1 นำเอกสารแบบฟอร์มใบนำสิ่งของออกนอกบริเวณมหาวิทยาลัยมหาสารคาม นำเสนอผู้บังคับบัญชา เพื่อขออนุมัติและให้หน่วยงานเก็บเป็นหลักฐาน

1.2 นำสำเนาเอกสารแบบฟอร์มใบนำสิ่งของออกนอกบริเวณมหาวิทยาลัยมหาสารคาม ที่ผ่านการอนุมัติ ให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบลักษณะของทรัพย์สินของมหาวิทยาลัยมหาสารคามให้ตรงตามรายการในแบบฟอร์ม

2. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน

2.1 ขณะเคลื่อนย้ายหรือเดินทาง ต้องจัดเตรียมอุปกรณ์ให้อยู่ในสัมภาระที่ปกปิดมิดชิดและห่อหุ้มในขณะเดินทาง เพื่อป้องกันความเสียหายต่ออุปกรณ์

2.2 ปฏิบัติตามคำแนะนำจากผู้ผลิตของอุปกรณ์อย่างเคร่งครัด เพื่อป้องกันไม่ให้เกิดความเสียหายของอุปกรณ์ เช่น ไม่วางอุปกรณ์ไว้ใกล้กับอุปกรณ์อื่น ๆ ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง ไม่เก็บอุปกรณ์ไว้ในที่ที่มีอุณหภูมิสูง

2.3 ทำการสำรองข้อมูลในอุปกรณ์อย่างสม่ำเสมอ

2.4 ไม่วางอุปกรณ์ทิ้งไว้ในที่สาธารณะ

2.5 ในกรณีที่มีความจำเป็นต้องวางอุปกรณ์ในที่สาธารณะ อุปกรณ์ดังกล่าวต้องสามารถใช้สายเข้ากุญแจล็อคกับอุปกรณ์สำนักงานหรืออุปกรณ์อื่น ๆ ที่ไม่สามารถเคลื่อนย้ายได้ หรือมีมาตรการป้องกันการสูญหาย

2.6 จดบันทึกการแลกเปลี่ยนหรือการครอบครองอุปกรณ์ โดยระบุรายละเอียดของผู้รับผิดชอบขณะมีการใช้งานนอกสถานที่

3. การป้องกันอุปกรณ์ที่ไม่มีผู้รับผิดชอบโดยตรง

3.1 ปลดการเชื่อมต่อ (Log-off) จากโปรแกรมหรือบริการเครือข่ายเมื่อไม่มีการใช้งาน

3.2 ล็อคหน้าจอ เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์

4. การเก็บรักษาทรัพย์สินและอุปกรณ์สารสนเทศ

4.1 นำข้อมูลสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ออกจากเครื่องพิมพ์โดยเร็วและหากเอกสารนั้นมีข้อผิดพลาด ต้องได้รับการทำลายทางกายภาพผ่านทางเครื่องทำลายกระดาษหรือวิธีการอื่นใดที่ทำให้ไม่สามารถเข้าถึงสารสนเทศนั้นได้

4.2 อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ที่อยู่ในระยะเวลารับประกัน ห้ามถอด หรือเปลี่ยนแปลงแก้ไขส่วนประกอบภายใน ซึ่งจะมีผลให้อุปกรณ์ดังกล่าวผิดเงื่อนไขการรับประกัน

4.3 อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ และโปรแกรมที่มหาวิทยาลัยอนุญาตให้ใช้งาน เป็นทรัพย์สินของมหาวิทยาลัยสำหรับใช้งานในภารกิจของมหาวิทยาลัยเท่านั้น

4.4 การเคลื่อนย้ายหรือส่งอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ไปตรวจซ่อม ต้องนำข้อมูลสำคัญ ซึ่งอาจมีผลกระทบต่อการดำเนินงานของมหาวิทยาลัย ออกจากเครื่องก่อนเสมอ

4.5 ปิดการทำงานของอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ทุกครั้งหลังจากเลิกใช้งาน

4.6 ไม่วางอุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ในพื้นที่ที่มีความเสี่ยงต่อการตกหล่น หรือถูกกระแทก

หมวด 4 การบริหารจัดการทรัพย์สิน

(Asset Management)

วัตถุประสงค์

เพื่อระบุทรัพย์สินสารสนเทศของมหาวิทยาลัยมหาสารคาม และกำหนดหน้าที่ความรับผิดชอบในการป้องกันอย่างเหมาะสม ซึ่งประกอบด้วย

1. หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ
2. การจัดหมวดหมู่ทรัพย์สินสารสนเทศ
3. การจัดการสื่อบันทึกข้อมูล

4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ

มาตรการ

1. ระบุทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและสถานที่และสิ่งอำนวยความสะดวกสำหรับการประมวลผลสารสนเทศให้ชัดเจน และจัดทำเป็นบัญชีทรัพย์สิน รวมทั้งปรับปรุงให้มีความทันสมัย

2. ทรัพย์สินแต่ละรายการในบัญชีทรัพย์สิน จะต้องระบุผู้รับผิดชอบ

3. กำหนด จัดทำเอกสาร และนำข้อกำหนดการใช้งานทรัพย์สินอย่างเหมาะสมไปสู่การปฏิบัติโดยผู้ปฏิบัติงานและผู้เกี่ยวข้อง เพื่อความมั่นคงปลอดภัยทางไซเบอร์ ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ และสถานที่หรือสิ่งอำนวยความสะดวกสำหรับประมวลผลสารสนเทศ

4. เรียกคืนทรัพย์สินที่ผู้ปฏิบัติงานและผู้ใช้งานของหน่วยงานภายนอกถือครองหรือใช้งานอยู่ เมื่อสิ้นสุดการจ้างงาน สัญญา หรือข้อตกลง

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. ระบุและตรวจสอบ “ทะเบียนทรัพย์สินสารสนเทศ” ของคณะ/หน่วยงาน ภายในมหาวิทยาลัย โดยรายการทรัพย์สินสารสนเทศประกอบไปด้วย สารสนเทศและอุปกรณ์สารสนเทศ ซึ่งจัดแบ่งตามประเภท ดังนี้

1.1 สารสนเทศ (Information) เช่น ข้อมูลในฐานข้อมูล ข้อมูลอิเล็กทรอกนิกส์ ไฟล์ข้อมูล สัญญา เอกสาร/คู่มือระบบข้อมูลที่สนับสนุนพันธกิจมหาวิทยาลัย คู่มือผู้ใช้งาน ทรัพยากรในการฝึกอบรม ขั้นตอนการปฏิบัติงานหรือสนับสนุน แผนการกู้คืนสภาพ ประวัติการตรวจสอบ สารสนเทศที่สำคัญอื่น ๆ

1.2 ทรัพย์สินทางซอฟต์แวร์ (Software Assets) เช่น ซอฟต์แวร์สำเร็จรูป ระบบสารสนเทศที่สนับสนุนพันธกิจมหาวิทยาลัย โปรแกรมระบบ เครื่องมือสำหรับพัฒนา โปรแกรมประเภทยูทิลิตี้ (System Utilities)

1.3 ทรัพย์สินทางฮาร์ดแวร์ (Hardware Assets) เช่น อุปกรณ์สารสนเทศ อุปกรณ์ติดต่อสื่อสาร อุปกรณ์เครือข่ายคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครื่องบันทึกข้อมูล สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

1.4 การบริการด้านการประมวลผล การติดต่อสื่อสาร และสาธารณูปโภคอื่น ๆ (Services) เช่น บริการอินเทอร์เน็ต บริการการเข้าถึงระบบสารสนเทศ บริการควบคุมการเข้าถึงอาคาร บริการแสงสว่าง บริการไฟฟ้าและพลังงาน

2. ทบทวนทะเบียนทรัพย์สินสารสนเทศของคณะ/หน่วยงานและปรับปรุงให้ทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง

3. กำหนดผู้รับผิดชอบในทรัพย์สินสารสนเทศ หรือจัดการให้สิทธิการใช้งานทรัพย์สินสารสนเทศ

4. กำหนดกระบวนการจัดการให้สิทธิการใช้งานทรัพย์สินสารสนเทศ โดยแบ่งแยกหน้าที่ให้เหมาะสมเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาตหรือโดยไม่ได้ตั้งใจ เช่น แบ่งแยกบุคคลที่มีหน้าที่ในขั้นตอนการร้องขอ (Request) และขั้นตอนการอนุมัติ (Approve) ออกจากกัน

5. กำหนดมาตรการดูแลรักษาความมั่นคงปลอดภัยที่สอดคล้องเหมาะสมกับทรัพย์สินสารสนเทศแต่ละประเภทที่ได้จำแนกไว้ เช่น การควบคุมการเข้าถึง การจัดให้มีการเข้ารหัสข้อมูลที่เป็นความลับหรือความถูกต้องในระดับสูง เป็นต้น

4.2 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ

มาตรการ

1. จัดหมวดหมู่ทรัพย์สินสารสนเทศตามข้อกำหนดของกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

2. จัดทำขั้นตอนปฏิบัติสำหรับการทำป้ายบ่งชี้ทรัพย์สินสารสนเทศ และนำไปปฏิบัติให้สอดคล้องกับรูปแบบการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

3. จัดทำขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สิน และนำไปปฏิบัติให้สอดคล้องกับรูปแบบจัดหมวดหมู่ทรัพย์สินสารสนเทศ

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. การจัดหมวดหมู่ทรัพย์สินสารสนเทศ

1.1 จัดหมวดหมู่ทรัพย์สินสารสนเทศ โดยคำนึงถึงการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของทรัพย์สินสารสนเทศ (ดูรายละเอียดที่ภาคผนวก เรื่องเกณฑ์การจัดระดับการป้องกันความมั่นคงปลอดภัย) ซึ่งหมวดหมู่สารสนเทศที่ได้รับการจัดจะแบ่งเป็นระดับการป้องกันความมั่นคงปลอดภัย 4 ระดับ คือ ต่ำ ปานกลาง สูง และ สูงสุด

1.2 ทบทวนการจัดหมวดหมู่ ปรับปรุงหมวดหมู่ให้ทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง

2. การจัดหมวดหมู่ทรัพย์สินสารสนเทศ

2.1 พิจารณาจัดทำป้ายบ่งชี้อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ รวมถึงสื่อบันทึกข้อมูลแบบอิเล็กทรอนิกส์ เช่น ซีดี อุปกรณ์บันทึกข้อมูลแบบพกพา โดยต้องไม่แสดงวัตถุประสงค์ของอุปกรณ์ดังกล่าวอย่างชัดแจ้ง

3. การจัดการทรัพย์สินสารสนเทศ

3.1 จัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ เพื่อป้องกันความเสียหายต่อทรัพย์สิน

3.2 เก็บสารสนเทศที่อยู่ในระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ที่อยู่ในรูปแบบเอกสารหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ โดยใส่กุญแจ (วิธีที่ดีที่สุด คือ เก็บไว้ในตู้นิรภัย หรือตู้ใส่ของ หรือครุภัณฑ์รูปแบบอื่น ๆ ที่รักษาความปลอดภัยได้)

3.3 ควบคุมดูแลให้ผลิตภัณฑ์ที่ได้รับการส่งมอบ ต้องได้รับการลงทะเบียนในทะเบียนรายการทรัพย์สินของคณะ/หน่วยงาน ก่อนเคลื่อนย้ายไปยังจุดที่ติดตั้งใช้งานจริง

3.4 ทบทวนแผนการบำรุงรักษาทรัพย์สินสารสนเทศของหน่วยงานอย่างน้อยปีละ 1 ครั้ง

4.3 การจัดการสื่อบันทึกข้อมูล

มาตรการ

1. จัดทำขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ให้สอดคล้องกับรูปแบบการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

2. สื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไป ควรกำจัดด้วยวิธีที่ปลอดภัยตามขั้นตอนปฏิบัติที่เป็นทางการ ปฏิบัติตามกฎหมาย

3. สื่อบันทึกข้อมูลควรได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์หรือการเกิดความเสียหายในระหว่างการขนส่ง

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. จัดทำทะเบียนสื่อบันทึกข้อมูล โดยระบุชนิด วันที่ได้มา ข้อมูลที่จัดเก็บ และชื่อผู้รับผิดชอบ

2. อนุญาตให้ใช้สื่อบันทึกข้อมูลกับระบบงานที่เกี่ยวข้องเท่านั้น

3. กรณีมีความจำเป็นต้องมีการแลกเปลี่ยนข้อมูลที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ให้ส่งผ่านช่องทางระบบงานสารบรรณอิเล็กทรอนิกส์มหาวิทยาลัยมหาสารคาม (Electronic Document System)

4. ตรวจสอบอายุของสื่อบันทึกข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้คงสภาพความสามารถในการเก็บข้อมูลบนอุปกรณ์

5. ลงบันทึกวันที่ทำลายสื่อบันทึกข้อมูลลงใน “ทะเบียนสื่อบันทึกข้อมูล” เพื่อใช้เป็นหลักฐานอ้างอิงสำหรับการตรวจสอบในภายหลัง

6. กำหนดขั้นตอนกระบวนการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูลและไม่ให้สามารถกู้คืนข้อมูลได้ในกรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล

7. ควบคุมและตรวจสอบการถอดถอนหรือทำลายสารสนเทศของมหาวิทยาลัยมหาสารคาม ออกจากอุปกรณ์ดังกล่าวเมื่อเลิกใช้งานสื่อบันทึกข้อมูล หรือโอนให้หน่วยงานอื่น หรือจำหน่ายออกจากคณะ/หน่วยงาน

7.1 สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่ใช้บันทึกสารสนเทศ ซึ่งหมดอายุการใช้งานแล้ว ต้องได้รับการทำลายทางกายภาพ หรือทำลาย ลบ เขียนทับข้อมูลโดยใช้หลักการทางเทคนิคที่มั่นใจได้ว่า จะไม่สามารถนำสารสนเทศเดิมกลับมาได้ (Non-Retrievable)

7.2 สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่ใช้บันทึกสารสนเทศ ซึ่งต้องการนำกลับมาใช้ใหม่ ต้องได้รับการลบ เขียนทับข้อมูลโดยใช้หลักการทางเทคนิคที่มั่นใจได้ว่าจะไม่สามารถนำสารสนเทศเดิมกลับมาได้ (Non-Retrievable) โดยพิจารณาตามระดับการป้องกันความมั่นคงปลอดภัยของสารสนเทศ

7.3 คำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน

การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
1	- แฟลชไดรฟ์ (Flash Drive) - ฮาร์ดดิสก์ (Hard disk) - ฮาร์ดดิสก์พกพา (External Hard disk)	- ทำลายข้อมูลตามแนวทางของ DOD 5220.22-M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูล เดิมหลายๆ รอบ - ดำเนินการตามข้อกฎหมายและระเบียบ
2	แผ่นซีดี/ดีวีดี (CD/DVD)	- ดำเนินการตามข้อกฎหมายและระเบียบ
3	เทป	- ดำเนินการตามข้อกฎหมายและระเบียบ
4	กระดาษ	- ดำเนินการตามข้อกฎหมายและระเบียบ

8. เอกสารที่เป็นกระดาษซึ่งใช้บันทึกสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” เมื่อไม่มีความจำเป็นต้องใช้งานแล้ว ต้องได้รับการทำลายทางกายภาพผ่านทางเครื่องทำลายกระดาษหรือวิธีการอื่นใดที่ทำให้ไม่สามารถเข้าถึงสารสนเทศนั้นได้

9. ในกรณีที่มีการใช้บริการจากหน่วยงานภายนอกในการทำลายเอกสาร อุปกรณ์สารสนเทศ หรือสื่อบันทึกข้อมูล ต้องกำกับดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อตกลงหรือสัญญาการให้บริการ

10. กำหนดขั้นตอนกระบวนการดูแลรักษาความปลอดภัยกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่นอกมหาวิทยาลัยมหาสารคาม ต้องจัดให้มีการป้องกันข้อมูลที่มีการส่งถึงกันระหว่างหน่วยงาน ดังต่อไปนี้

10.1 บรรจุหีบห่ออย่างเหมาะสม และเป็นไปตามคำแนะนำของผู้ผลิต เพื่อป้องกันความเสียหายทางกายภาพที่อาจเกิดขึ้นในช่วงขนส่ง เช่น การถูกความร้อน ความชื้น หรือคลื่นแม่เหล็กไฟฟ้า

10.2 ป้องกันการเปิดเผยหรือดัดแปลงสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” โดยไม่ได้รับอนุญาต เช่น ใช้บรรจุภัณฑ์ที่มีกุญแจป้องกัน การส่งมอบถึงผู้รับโดยตรง

10.3 ใช้ผู้ส่งที่น่าเชื่อถือ

10.4 กำหนดกระบวนการในการระบุตัวตนของผู้ส่งและจดบันทึกไว้ เช่น แสดงบัตรประจำตัวผู้ปฏิบัติงาน หรือบัตรประจำตัวประชาชน

10.5 จดบันทึกรายละเอียดการจัดส่ง เช่น สิ่งที่จัดส่ง ผู้ส่ง วัน/เวลา หน่วยงานผู้รับ ผู้รับ วัน/เวลา

แนวปฏิบัติสำหรับผู้ปฏิบัติงานและหน่วยงานภายนอก

1. ตรวจสอบโปรแกรมไม่พึงประสงค์ก่อนนำสื่อบันทึกข้อมูลมาใช้งาน และตรวจสอบข้อมูลภายในสื่อบันทึกข้อมูลเป็นประจำ

2. ใช้สื่อบันทึกข้อมูลกับงานที่เกี่ยวข้องเท่านั้น

3. ไม่ใช้สื่อบันทึกข้อมูลกับข้อมูลที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” กรณีมีความจำเป็นต้องมีการแลกเปลี่ยนข้อมูล ให้ส่งผ่านช่องทางระบบบริการจัด ส่งข้อมูล หรือจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยมหาสารคาม

4. ทำลายข้อมูลภายในสื่อบันทึกข้อมูลโดยดำเนินการตามข้อกฎหมายและระเบียบ เมื่อไม่มีความจำเป็นต้องใช้งานสื่อบันทึกข้อมูลอีกต่อไป

หมวด 5 ความมั่นคงปลอดภัยในการดำเนินงาน

(Operations Security)

วัตถุประสงค์

เพื่อดำเนินงานที่เกี่ยวข้องกับสถานที่ อุปกรณ์และระบบสนับสนุนสำหรับประมวลผลสารสนเทศอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการทำลายสารสนเทศ อุปกรณ์และระบบสนับสนุนสำหรับประมวลผลสารสนเทศ ซึ่งประกอบด้วย 7 หัวข้อ ดังนี้

1. ขั้นตอนปฏิบัติสำหรับการดำเนินงานและหน้าที่ความรับผิดชอบ
2. การป้องกันโปรแกรมไม่พึงประสงค์
3. การสำรองข้อมูล
4. การลงบันทึกเหตุการณ์และการเฝ้าระวัง
5. การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ
6. การบริหารจัดการช่องโหว่ทางเทคนิค
7. การพิจารณาการตรวจสอบระบบ

5.1 ขั้นตอนปฏิบัติสำหรับการดำเนินงานและหน้าที่ความรับผิดชอบ

มาตรการ

1. จัดทำขั้นตอนปฏิบัติสำหรับการดำเนินงานไว้เป็นลายลักษณ์อักษร และพร้อมให้ผู้ใช้งานทุกคนที่ต้องการนำไปใช้งานได้

2. ควบคุมการเปลี่ยนแปลงกระบวนการการดำเนินงาน สิ่งอำนวยความสะดวก ระบบสำหรับประมวลผลสารสนเทศ และระบบที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์

3. เฝ้าระวังและปรับแต่งการใช้ทรัพยากร รวมทั้งคาดการณ์ความต้องการขีดความสามารถของระบบในอนาคต เพื่อให้มั่นใจในประสิทธิภาพของระบบที่ต้องการ

4. แยกระบบสำหรับการพัฒนา การทดสอบ และให้บริการออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสารสนเทศสำหรับให้บริการโดยไม่ได้รับอนุญาต

แนวปฏิบัติสำหรับหน่วยงาน

1. ควบคุมให้มีคู่มือสำหรับการปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์หรือระบบประมวลสารสนเทศ (Operation Manual) ที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” โดยคู่มือต้องประกอบด้วย เรื่องดังต่อไปนี้

1.1 ขั้นตอนหรือลำดับในการปฏิบัติงานประจำวัน

1.2 การสำรองข้อมูลสำหรับระบบต่าง ๆ

1.3 ตารางการจัดการการทำงาน (Job Scheduling)

1.4 กระบวนการในการแก้ไขปัญหาที่อาจจะเกิดขึ้นในขณะปฏิบัติงาน

1.5 รายชื่อบุคคลที่สามารถติดต่อได้ในกรณีที่เกิดเหตุการณ์ฉุกเฉินเกิดขึ้น

1.6 กระบวนการในการจัดการเอกสารรายงานของข้อมูล (Printing Report) ที่มีความสำคัญและการจัดการสื่อที่ใช้ในการบันทึกข้อมูล ซึ่งรวมถึงการทำลายเอกสารรายงานหรือสื่อที่ใช้ในการบันทึกข้อมูล

1.7 กระบวนการในการกู้คืนสภาพ ในกรณีที่ระบบเกิดการผิดพลาด (System Restart and Recovery)

1.8 การจัดการหลักฐานการตรวจสอบ (Audit Trail) และข้อมูลบันทึกเหตุการณ์ของระบบ (System Log)

2. ควบคุมการเข้าถึงคู่มือการปฏิบัติงาน เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยคู่มือการปฏิบัติงานดังกล่าว จะอนุญาตให้เข้าถึงได้เฉพาะผู้ปฏิบัติงานที่เกี่ยวข้องเท่านั้น

3. จัดทำ “ทะเบียนคู่มือการปฏิบัติงาน” เพื่อความเป็นระเบียบในการจัดเก็บคู่มือการปฏิบัติงานต่าง ๆโดยมีรายละเอียดดังนี้

3.1 ชื่อคู่มือ

3.2 คำอธิบาย

3.3 ชื่อผู้เป็นเจ้าของทรัพย์สินสารสนเทศ

3.4 หมวดหมู่ทรัพย์สินสารสนเทศ

3.5 บันทึกการเปลี่ยนแปลง (Version Control) โดยรวมถึง วันที่จัดทำและวันที่แก้ไขคู่มือการปฏิบัติงาน

3.6 สถานที่จัดเก็บเอกสารต้นฉบับ

3.7 จำนวนและสถานที่จัดเก็บสาเนาเอกสาร

4. ทบทวน “ทะเบียนคู่มือการปฏิบัติงาน” อย่างน้อยปีละ 1 ครั้ง

5. มีมาตรการในการเปลี่ยนแปลงซอฟต์แวร์ ระบบสารสนเทศ ข้อมูลในระบบประมวลผลสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศอย่างเคร่งครัด โดยขั้นตอนในการแจ้งความประสงค์ขอเปลี่ยนแปลงต้องมีการระบุรายละเอียดดังต่อไปนี้

5.1 วัตถุประสงค์ในการเปลี่ยนแปลง

5.2 รายละเอียดการเปลี่ยนแปลง

5.3 ผลกระทบที่อาจเกิดขึ้น รวมทั้งผลกระทบความมั่นคงปลอดภัยทางไซเบอร์ของการเปลี่ยนแปลงนั้น ๆ

5.4 ผู้ขออนุมัติการเปลี่ยนแปลง และผู้อนุมัติการเปลี่ยนแปลง (ผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายหรือเทียบเท่าขึ้นไป)

5.5 วันและเวลาที่จะทำการเปลี่ยนแปลง

5.6 การสื่อสารการเปลี่ยนแปลงให้ผู้เกี่ยวข้องรับทราบ

5.7 ขั้นตอนในการถอยกลับ (Fallback Procedure) รวมทั้งหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการกู้คืนระบบ ในกรณีที่การเปลี่ยนแปลงไม่เป็นไปตามแผน

6. ควบคุมให้มีการทบทวนหรือปรับปรุงเอกสารระบบที่เปลี่ยนแปลงและแก้ไข เช่น เอกสารการออกแบบ คู่มือการปฏิบัติงาน คู่มือการใช้งาน อย่างน้อยปีละ 1 ครั้ง

7. จัดเก็บข้อมูลบันทึกเหตุการณ์ เมื่อซอฟต์แวร์ ระบบสารสนเทศ ข้อมูลในระบบประมวลผลสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศมีการเปลี่ยนแปลง

8. ควบคุมให้มีการแยกระบบสำหรับการพัฒนา และระบบสำหรับการทดสอบ ออกจากระบบที่ใช้งานจริง เพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูล หรือการประมวลผลของระบบที่ใช้งานจริง
โดยต้องจัดให้มีการควบคุม ดังต่อไปนี้

8.1 จัดทำขั้นตอนการปฏิบัติสำหรับการย้ายโปรแกรมคอมพิวเตอร์ จากระบบสำหรับการพัฒนา หรือระบบสำหรับการทดสอบ ไปยังระบบที่ใช้งานจริง

8.2 ในการแยกระบบออกจากกัน ต้องมีการแยกการทำงานแบบกายภาพ (Physical) เช่น การแยกเครื่องคอมพิวเตอร์แม่ข่าย การแยกระบบสำหรับการพัฒนาหรือระบบสำหรับการทดสอบออกจากเครื่องคอมพิวเตอร์แม่ข่ายระบบที่ใช้งานจริง ทั้งนี้ในกรณีที่ไม่สามารถทำได้เนื่องจากมีข้อจำกัด ต้องทำการแยกการทำงานแบบตรรกะ (Logical) เช่น แยก Directories, แยก Logical Partition ออกจากกัน

8.3 ระบบสำหรับการทดสอบต้องจำลองมาจากระบบที่ใช้งานจริง โดยต้องให้มีความคล้ายคลึงกันมากที่สุด

8.4 ในการเข้าถึงระบบสำหรับการทดสอบ ผู้ปฏิบัติงานต้องใช้บัญชีผู้ใช้งานที่แตกต่างจากระบบที่ใช้งานจริง และต้องมีข้อความหรือสัญลักษณ์ที่แสดงประเภทของระบบอย่างชัดเจน เพื่อลดความเสี่ยงจากการผิดพลาดในการเข้าถึงระบบ

8.5 นำสำเนาของซอร์สโค้ด (Source Code) ล่าสุดที่ใช้ในระบบสารสนเทศที่ให้บริการจริง มาจำลองบนระบบสำหรับการทดสอบ ก่อนทำการเปลี่ยนแปลงและแก้ไขบนระบบที่ให้บริการจริง

8.6 ซอร์สโค้ด (Source Code) ของระบบสารสนเทศ ต้องไม่เก็บอยู่ในระบบที่ใช้งานจริง ในกรณีที่มีความจำเป็นต้องเก็บซอร์สโค้ด (Source Code) ในระบบที่ใช้งานจริง เนื่องจากข้อจำกัดของภาษาที่ใช้ในการพัฒนาระบบ ให้มีการกำหนดสิทธิในการเข้าถึงซอร์สโค้ดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

8.7 Compilers เครื่องมือในการแก้ไข (Editor Tools) และเครื่องมือที่ใช้ในการพัฒนาอื่น ๆ รวมทั้งโปรแกรมประเภทยูทิลิตี้ (System Utilities) ต้องไม่ติดตั้งในระบบที่ใช้งานจริง

แนวปฏิบัติสำหรับผู้ดูแลระบบ

1. กำหนดให้มีการติดตามการปรับปรุงระบบ (Patch) ของระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องอยู่เสมอ

2. จัดทำแผนการเปลี่ยนแปลง และแก้ไขซอฟต์แวร์ ระบบสารสนเทศ และระบบปฏิบัติการล่วงหน้า เพื่อใช้ในการดูแลและบำรุงรักษาระบบในอนาคต และให้ผู้เกี่ยวข้องมีเวลาในการทดสอบก่อนการเปลี่ยนแปลงและแก้ไข

3. แจ้งผลการตรวจสอบและประเมินแนวโน้มระดับการใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Capacity) และสรุปประเด็นปัญหาให้กับผู้บริหารอย่างสม่ำเสมอทุกเดือน เพื่อที่จะสามารถปรับปรุงประสิทธิภาพและความเพียงพอของอุปกรณ์ประมวลผลสารสนเทศให้ตอบสนองความต้องการของผู้เป็นเจ้าของสารสนเทศทั้งในปัจจุบันและในอนาคต ทั้งนี้การตรวจสอบและประเมินต้องพิจารณาในเรื่องดังต่อไปนี้

3.1 ความสามารถในการประมวลผล (Processing Power)

3.2 ความต้องการหน่วยความจำ (Memory Requirement)

3.3 ขนาดและการใช้งานของหน่วยเก็บข้อมูล (Disk Usage and Size)

3.4 ปริมาณข้อมูลในระบบเครือข่ายที่สามารถรองรับได้ (Network Traffic Load)

5.2 การป้องกันโปรแกรมไม่พึงประสงค์

มาตรการ

จัดทำมาตรการการตรวจหา ป้องกัน และกู้คืน เพื่อป้องกันโปรแกรมไม่พึงประสงค์ รวมทั้งสร้างความตระหนักแก่ผู้ใช้งานอย่างเหมาะสม

แนวปฏิบัติสำหรับหน่วยงาน

1. เตรียมแผนความต่อเนื่องเหมาะสม เพื่อรับมือกับการถูกโจมตีโดยไวรัสคอมพิวเตอร์มัลแวร์ โปรแกรมไม่พึงประสงค์อื่น ๆ ทั้งนี้รวมถึงกระบวนการในการสำรองและกู้คืนข้อมูล

2. ควบคุมให้ปฏิบัติตามกระบวนการที่กำหนด เมื่อตรวจพบโปรแกรมไม่พึงประสงค์ซึ่งรวมถึงการรายงานและการกู้ข้อมูลจากการถูกโจมตี โดยโปรแกรมไม่พึงประสงค์

แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

1. ตรวจสอบและปรับปรุงโปรแกรมที่ตรวจจับและแก้ไขโปรแกรมไม่พึงประสงค์บนอุปกรณ์ประมวลผลสารสนเทศที่รับผิดชอบให้ทันสมัยอยู่เสมอ โดยให้ทำการตรวจสอบอย่างน้อยสัปดาห์ละ 1 ครั้ง หากพบว่าอุปกรณ์ประมวลผลสารสนเทศทำงานผิดปกติ ให้รีบแจ้งหน่วยงานที่เกี่ยวข้อง เช่น HelpDesk เพื่อดำเนินการแก้ไขโดยทันที

2. ตรวจสอบไฟล์ที่อยู่ในอุปกรณ์ประมวลผลสารสนเทศและไฟล์ที่ได้รับผ่านเครือข่าย เพื่อตรวจหาโปรแกรมไม่พึงประสงค์ก่อนเปิดใช้งาน

3. ตรวจสิ่งแนบที่ส่งมากับจดหมายอิเล็กทรอนิกส์ เพื่อตรวจหาโปรแกรมไม่พึงประสงค์ก่อนเปิดใช้

4. ไม่เปิดสิ่งแนบที่ส่งมากับจดหมายอิเล็กทรอนิกส์จากผู้ส่งที่ไม่รู้จัก

5. หลีกเลี่ยงการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย

6. ไม่สร้าง เก็บ หรือเผยแพร่โปรแกรมไม่พึงประสงค์เข้าสู่ระบบคอมพิวเตอร์

7. ไม่ขัดขวาง หรือรบกวนการทำงานของโปรแกรมป้องกันไวรัส

5.3 การสำรองข้อมูล

มาตรการ

สำรองข้อมูล ซอฟต์แวร์ และชุดข้อมูลจำลองระบบ พร้อมทดสอบ อย่าสม่ำเสมอตามนโยบายการสำรองข้อมูลที่ตกลงไว้ในแนวปฏิบัติ

แนวปฏิบัติสำหรับผู้ดูแลระบบ

1. จัดทำแผนสำรองข้อมูล ตามความเหมาะสมของระดับการป้องกันความมั่นคงปลอดภัย ดังนี้

1.1 ระบบที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ “สูงสุด” ให้จัดทำแผนสำรองข้อมูลและมีการทบทวนแผนทุก 1 ปี

1.2 ระบบที่มีระดับการป้องกันความมั่นคงปลอดภัย “ปานกลาง” ให้พิจารณาจัดทำแผนสำรองข้อมูลตามความเหมาะสม

1.3 ระบบที่มีระดับการป้องกันความมั่นคงปลอดภัย “ต่ำ” ไม่ต้องจัดทำแผนสำรองข้อมูล

2. จัดทำแผนการทดสอบการสำรองข้อมูลและการกู้คืน เพื่อให้มั่นใจว่าสามารถใช้งานได้ในกรณีฉุกเฉินเมื่อมีความจำเป็น

3. มีการทดสอบความสามารถในการเรียกคืนข้อมูลที่สำรองไว้บนสื่อบันทึกข้อมูลที่ใช้เฉพาะสำหรับการทดสอบเท่านั้น โดยไม่เขียนทับสื่อบันทึกข้อมูลต้นฉบับ เนื่องจากในกรณีที่กระบวนการสำรองข้อมูลหรือการกลับสู่สภาวะปกติล้มเหลว จะทำให้เกิดความเสียหายหรือสูญหายของข้อมูลที่ไม่สามารถแก้ไขได้

4. จัดทำขั้นตอนปฏิบัติสำหรับการเฝ้าระวังการสำรองข้อมูลและการจัดการความล้มเหลวของการสำรองข้อมูลตามกำหนดการ เพื่อให้มั่นใจว่าการสำรองข้อมูลเสร็จสมบูรณ์ตามแผนการสำรองข้อมูล

5. มีระบบการสำรองข้อมูลที่มีความมั่นคงปลอดภัย

6. มีระบบการสำรองข้อมูลที่ถูกติดตั้งอยู่นอกอาคาร หรือบริเวณอื่นนอกเหนือจากห้องศูนย์ข้อมูลกลาง

7. ระบบการสำรองข้อมูลต้องเป็นมาตรฐานสากล ตามมาตรฐานการสำรองข้อมูล

5.4 การลงบันทึกเหตุการณ์และการเฝ้าระวัง

มาตรการ

1. จัดทำและเก็บรักษาบันทึกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ และควรทบทวนอย่างสม่ำเสมอ

2. ป้องกันสิ่งอำนวยความสะดวกในการลงบันทึกเหตุการณ์และข้อมูลบันทึกเหตุการณ์จากการปลอมแปลงและการเข้าถึงโดยไม่ได้รับอนุญาต

3. ลงบันทึกเหตุการณ์กิจกรรมของผู้ดูแลระบบและผู้ปฏิบัติงาน มีการป้องกันรวมถึงทบทวนอย่างสม่ำเสมอ

4. กำหนดข้อมูลเวลาของระบบประมวลผลสารสนเทศทั้งหมดให้ตรงกับแหล่งเวลาอ้างอิง

แนวปฏิบัติสำหรับผู้ดูแลระบบ

1. จัดทำและเก็บรักษาบันทึกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น ข้อผิดพลาด และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ โดยบันทึกเหตุการณ์ (event logs) ประกอบด้วย

1.1 บัญชีผู้ใช้งาน (User IDs)

1.2 วันที่ เวลา และรายละเอียดของเหตุการณ์สำคัญ เช่น เมื่อเข้าสู่ระบบ (Log-on) เมื่อออกจากระบบ (Log-off)

1.3 สิ่งยืนยันตนหรือตำแหน่งของอุปกรณ์ (หากเป็นไปได้) และตัวระบุระบบ

1.4 บันทึกการพยายามเข้าถึงระบบที่ประสบความสำเร็จและถูกปฏิเสธ

1.5 บันทึกการพยายามเข้าถึงข้อมูลและทรัพยากรอื่น ๆ ที่ประสบความสำเร็จและถูกปฏิเสธ

1.6 การเปลี่ยนแปลงการกำหนดค่าระบบ (System Configuration)

1.7 การใช้งานสิทธิพิเศษ

1.8 การเข้าถึงไฟล์และชนิดของการเข้าถึง

1.9 ที่อยู่ของเครือข่าย เช่น IP address, MAC address

1.10 Protocol ที่ใช้งาน

1.11 สัญญาณเตือนภัยที่เกิดขึ้นโดยระบบควบคุมการเข้าถึง

1.12 การเปิดการใช้งาน (Activation) และการระงับการใช้งาน (De-Activation) ของระบบป้องกัน เช่น ระบบป้องกันไวรัส ระบบตรวจจับการบุกรุก (Intrusion Detection System)

2. กำหนดให้มีรายละเอียดในการบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศ อย่างน้อยดังต่อไปนี้

2.1 เวลาที่เหตุการณ์ได้เกิดขึ้น

2.2 สารสนเทศที่เกี่ยวกับเหตุการณ์ เช่น การจัดการไฟล์ (File) ข้อผิดพลาดอันเกิดจากความผิดพลาดและมีการแก้ไขให้ถูกต้อง

2.3 บัญชีผู้ใช้ ผู้ดูแลระบบ (Administrator) หรือโอเปอเรเตอร์ (Operator) ที่เกี่ยวข้อง

2.4 การประมวลผลคอมพิวเตอร์ (Processing) ที่เกี่ยวข้อง

3. จัดให้มีการป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลบันทึกเหตุการณ์โดยไม่ได้รับอนุญาตและป้องกันปัญหาที่เกิดกับการบันทึกเหตุการณ์ ดังต่อไปนี้

3.1 การเปลี่ยนแปลงแก้ไขประเภทของข้อความ (Message Types) ที่ได้รับการบันทึก

3.2 การแก้ไขหรือลบไฟล์ (File) ข้อมูลบันทึกเหตุการณ์ (Log)

3.3 ข้อผิดพลาดของเหตุการณ์ที่บันทึกหรือการเขียนทับเหตุการณ์ที่บันทึก อันเนื่องมาจากความจุของสื่อที่เก็บไฟล์ (File) บันทึกเหตุการณ์ (Log File)ไม่เพียงพอ

4. ตรวจสอบและจัดทำรายงานบันทึกเหตุการณ์ อย่างน้อยเดือนละ 1 ครั้ง

5. เทียบข้อมูลนาฬิกาของระบบประมวลผลสารสนเทศทั้งหมดให้ตรงกับแหล่งเวลาการอ้างอิง โดยใช้ NTP Server ของมหาวิทยาลัยมหาสารคาม เพื่อให้เวลาที่ปรากฏในประวัติเหตุการณ์ (Log) ของระบบสารสนเทศถูกต้องตรงกัน และสามารถนาไปใช้ในการตรวจสอบวัน เวลา ได้อย่างถูกต้องและมีประสิทธิภาพ

5.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ

มาตรการ

ควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ

แนวปฏิบัติสำหรับผู้ดูแลระบบ

1. ควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ ให้ดำเนินงานโดยผู้ดูแลระบบที่ได้รับอนุญาต พร้อมทั้งจัดเก็บบันทึกเหตุการณ์ (Audit Log) เพื่อใช้ในการตรวจสอบ

5.6 การจัดการช่องโหว่ทางเทคนิค

มาตรการ

1. รับข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้ในเวลาที่เหมาะสม มีการประเมินความเสี่ยงดังกล่าวและมีมาตรการที่เหมาะสม เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง

2. กำหนดและนำกฎระเบียบเกี่ยวกับการติดตั้งซอฟต์แวร์โดยผู้ใช้งานไปปฏิบัติ

แนวปฏิบัติสำหรับผู้ดูแลระบบ

1. เมื่อมีแนวโน้มในการเกิดช่องโหว่ทางเทคนิค ต้องระบุถึงความเสี่ยงที่เกี่ยวข้องและการกระทำที่จะต้องดำเนินงาน ทั้งนี้การกระทำดังกล่าวอาจเกี่ยวข้องกับการปรับปรุงระบบ (Patch) ที่มีช่องโหว่ หรือการใช้การ

ควบคุมอื่น ๆ ควรดำเนินงานตามมาตรการควบคุมที่เกี่ยวข้องกับการบริหารจัดการการเปลี่ยนแปลง หรือตามขั้นตอนการตอบสนองต่อความมั่นคงปลอดภัยทางไซเบอร์ โดยขึ้นอยู่กับความจำเป็นเร่งด่วนที่จะต้องจัดการช่องโหว่ทางเทคนิค

2. ประเมินความเสี่ยงและทดสอบการปรับปรุงระบบ (Patch) ก่อนติดตั้งบนอุปกรณ์ที่ใช้งานจริง (Production) เพื่อให้มั่นใจได้ว่าการติดตั้งมีประสิทธิภาพและไม่ส่งผลกระทบข้างเคียงอย่างรุนแรงในกรณีที่ไม่มีการปรับปรุงระบบ (Patch) ต้องจัดให้มีการควบคุมอื่น ๆ เช่น

2.1 การปิดบริการที่เกี่ยวข้องกับช่องโหว่ทางเทคนิค

2.2 การปรับเปลี่ยนหรือเพิ่มการควบคุมในการเข้าถึง เช่น Firewalls/IDS/IPS

2.3 การเพิ่มการเฝ้าระวัง เพื่อตรวจจับหรือป้องกันการจู่โจม

2.4 การเพิ่มความตระหนักถึงช่องโหว่ทางเทคนิค

3. บันทึกเหตุการณ์เพื่อการตรวจสอบ (Audit Log) ในทุก ๆ ขั้นตอนปฏิบัติงาน

4. ตรวจสอบและประเมินกระบวนการในการบริหารจัดการช่องโหว่ทางเทคนิคอย่างสม่ำเสมอ เพื่อให้มั่นใจว่า กระบวนการดังกล่าวมีประสิทธิภาพและประสิทธิผล

5. จัดการช่องโหว่ทางเทคนิคกับระบบที่มีความเสี่ยงสูงก่อน

แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

1. ไม่ติดตั้งซอฟต์แวร์ใด ๆ บนอุปกรณ์ที่มหาวิทยาลัยมหาสารคาม เป็นเจ้าของ โดยไม่ได้รับอนุญาต

5.7 การพิจารณาการตรวจสอบระบบ

มาตรการ

1. วางแผนข้อกำหนดและกิจกรรมสำหรับการตรวจสอบระบบให้บริการอย่างรอบคอบ พร้อมทำข้อตกลงเพื่อลดการหยุดชะงักของกระบวนการ

แนวปฏิบัติสำหรับหน่วยงาน

1. สนับสนุนการทดสอบเจาะระบบ (Penetration Test) สำหรับระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด”

หมวด 6 การควบคุมอุปกรณ์คอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกล
(Mobile Device Control and Remote Access Control)

6.1 การควบคุมอุปกรณ์คอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกล

มาตรการ

1. กำหนดนโยบายและมาตรการควบคุมความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงที่มาจากการใช้งานอุปกรณ์คอมพิวเตอร์พกพาคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ

2. กำหนดนโยบายและมาตรการควบคุมความมั่นคงปลอดภัย เพื่อป้องกันข้อมูลที่มีการเข้าถึงประมวลผลหรือจัดเก็บไว้ในพื้นที่ปฏิบัติงานจากระยะไกล

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. กำหนดและมอบหมายผู้รับผิดชอบในการดูแลคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ให้ชัดเจนในทะเบียนทรัพย์สินสารสนเทศ

2. แจ้งถอดถอนสิทธิในการเข้าถึงของผู้ปฏิบัติงานจากระยะไกล เมื่อเสร็จสิ้นการปฏิบัติงานที่ได้รับมอบหมายและเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

แนวปฏิบัติสำหรับผู้ดูแลระบบเครือข่าย

1. กำหนดให้คอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ มีการพิสูจน์และยืนยันตัวตนก่อนเชื่อมต่อเครือข่ายมหาวิทยาลัยมหาสารคาม

2. ควบคุมการให้สิทธิในการปฏิบัติงานจากระยะไกล โดยผู้ใช้งานต้องได้รับการอนุมัติจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร และแจ้งทบทวนสิทธิกับหน่วยงานอย่างน้อยปีละ 1 ครั้ง

3. พิจารณาเงื่อนไขในการจัดเตรียมการปฏิบัติงานจากระยะไกล ดังต่อไปนี้

3.1 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของการปฏิบัติงานจากระยะไกล

3.2 ความมั่นคงปลอดภัยทางการสื่อสาร โดยยึดจากระดับความสำคัญ (Sensitivity) ของข้อมูลที่จะถูกเข้าถึงและส่งผ่านช่องทางการเชื่อมต่อสื่อสาร (Communication Link) รวมถึงระดับความสำคัญ (Sensitivity) ของระบบภายในมหาวิทยาลัยมหาสารคาม

แนวปฏิบัติสำหรับผู้ปฏิบัติงานและหน่วยงานภายนอก

1. ควบคุมดูแลให้มีการใส่รหัสผ่านก่อนเข้าถึงข้อมูลหรือแอปพลิเคชัน (Application) บนคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ที่มีข้อมูลของมหาวิทยาลัยมหาสารคาม เช่น ต้องมีการพิสูจน์และยืนยันตัวตนก่อนเข้าถึงอุปกรณ์หรือข้อมูลดังกล่าว

2. ต้องกำหนดให้มีการปิดหน้าจอหากไม่มีการใช้งานเกิน 10 นาที

3. ผู้ใช้งานคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ของมหาวิทยาลัยมหาสารคามชนิดที่รองรับการติดตั้งโปรแกรมป้องกันไวรัสได้ ต้องจัดให้มีโปรแกรมป้องกันไวรัสที่มหาวิทยาลัยได้ทำการเช่าใช้บริการ และต้องปรับปรุงให้โปรแกรมดังกล่าวทันสมัยอยู่เสมอ

4. ติดตั้งโปรแกรมป้องกันไวรัสและ Personal Firewall/IDS/IPS สำหรับคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ส่วนตัวที่ใช้เชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัยมหาสารคามจากภายนอก

5. คอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ที่เชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัย ต้องไม่เชื่อมต่ออินเทอร์เน็ตผ่านช่องทางอื่นนอกเหนือจากช่องทางที่มหาวิทยาลัยมหาสารคามจัดให้

6. ระมัดระวังในการใช้งานคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ พกพาในที่สาธารณะ ห้องประชุม และพื้นที่อื่น ๆ ที่ไม่มีการป้องกัน

7. ไม่วางคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ไมโครเวฟ ตู้เย็น

8. นำคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ติดตัวไปด้วยเสมอ ไม่ละทิ้งคอมพิวเตอร์พกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม ในกรณีที่มีความจำเป็นต้องทิ้งไว้ในรถยนต์ต้องเก็บไว้ในท้ายรถ หรือล็อคคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ไว้ในสถานที่มั่นคงปลอดภัย

9. จัดเก็บคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ ในกระเป๋าที่ปลอดภัยและเหมาะสม เพื่อป้องกันการกระแทก กันน้ำ หรือความชื้น

10. สำรองข้อมูลของคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่อื่น ๆ อย่างสม่ำเสมอ และมีการเข้ารหัสข้อมูลที่สำรองอย่างเหมาะสม

11. การปฏิบัติจากระยะไกล ต้องจัดเก็บเอกสารที่เป็นความลับ ในบริเวณการทำงานและจัดเก็บในอุปกรณ์บรรจุภัณฑ์ที่มีกุญแจ โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในมหาวิทยาลัยมหาสารคาม

หมวด 7 การควบคุมการเข้าถึง

(Access Control)

วัตถุประสงค์

เพื่อจำกัดการเข้าถึงสารสนเทศ สถานที่ อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ รวมทั้งระบบสนับสนุนสำหรับการประมวลผลสารสนเทศ ซึ่งประกอบด้วย 4 หัวข้อ ดังนี้

1. ข้อกำหนดการควบคุมการเข้าถึง
2. การบริหารจัดการการเข้าถึงระบบโดยผู้ใช้งาน
3. หน้าที่ความรับผิดชอบของผู้ใช้งาน
4. การควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ

7.1 ข้อกำหนดการควบคุมการเข้าถึง

มาตรการ

1. จัดทำเอกสารนโยบายควบคุมการเข้าถึงตามข้อกำหนดความมั่นคงปลอดภัยทางไซเบอร์ และมีการทบทวนนโยบายอย่างสม่ำเสมอ

2. จัดการให้ผู้ใช้งานสามารถเข้าถึงเครือข่ายและบริการเครือข่ายได้เฉพาะส่วนบุคคลนั้นได้รับอนุมัติเท่านั้น

แนวปฏิบัติสำหรับหน่วยงาน

1. กำหนดมาตรการการควบคุมการเข้าถึง สิทธิ และข้อจำกัดในการเข้าถึงทรัพย์สินสารสนเทศ โดยพิจารณาจาก หมวด 4 การบริหารจัดการทรัพย์สิน (Asset Management) และหมวด 3 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

2. ทบทวนมาตรการอย่างน้อยทุก 1 ปี

แนวปฏิบัติสำหรับผู้ดูแลระบบเครือข่าย

1. กำหนดมาตรการขอใช้บริการเครือข่าย

2. กำหนดมาตรการควบคุมการเล่นเกม ดูภาพยนตร์ หรือฟังเพลงผ่านทางระบบเครือข่าย

3. ควบคุมการใช้งานระบบเครือข่าย เพื่อป้องกันการเข้าถึงระบบเครือข่ายและบริการของระบบเครือข่ายโดยไม่ได้รับอนุญาต

4. ควบคุมไม่ให้เข้าถึงเว็บไซต์ที่ไม่เหมาะสม

    4.1 การพนัน

    4.2 การบ่อนทำลายต่อความมั่นคงของชาติ

    4.3 การลามก อนาจาร

    4.4 อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือจริยธรรม

5. ควบคุมการเชื่อมต่อเครือข่ายภายนอก ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบสารสนเทศของมหาวิทยาลัยมหาสารคามได้โดยไม่ได้รับอนุญาต

6. ควบคุมไม่ให้ใช้โปรแกรมประเภท Peer-to-Peer (P2P) เพื่อแลกเปลี่ยนข้อมูลทางเครือข่ายกับผู้ใช้งานอื่น

7. ควบคุมการเผยแพร่แผนผังระบบเครือข่าย (Network Diagram) ซึ่งรวมไปถึงโครงสร้างการจัดการระบบไอพีแอดเดรส ชื่อระบบ และชื่ออุปกรณ์เครือข่ายและเทคโนโลยีดิจิทัลอื่น ๆ ให้แก่ผู้ที่ไม่ได้รับอนุญาต

แนวปฏิบัติสำหรับผู้ปฏิบัติงานและหน่วยงานภายนอก

1. ขออนุมัติเข้าใช้บริการงานระบบสารสนเทศตามเงื่อนไขการให้บริการของระบบ

2. ขออนุมัติเข้าใช้งานระบบบริการเครือข่ายตามขั้นตอนการปฏิบัติในการขอใช้บริการ

3. ไม่ใช้ระบบเครือข่ายของมหาวิทยาลัยมหาสารคาม เพื่อทำกิจกรรมต่าง ๆ ที่ไม่เหมาะสม ดังต่อไปนี้

3.1 เจาะระบบ (Hacking) หรือสแกนช่องโหว่ของระบบเครือข่ายมหาวิทยาลัยโดยไม่ได้รับอนุญาต

3.2 เข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม

3.3 ดาวน์โหลดหรือส่งไฟล์ประเภทสื่อลามกอนาจาร หรือซอฟต์แวร์ หรือข้อมูลใด ๆ ที่เป็นการละเมิดลิขสิทธิ์

3.4 นำเข้าข้อมูลใด ๆ ที่มีลักษณะอันเป็นเท็จ กระทาผิดกฎหมายหรือก่อให้เกิดความเสียหายแก่บุคคลอื่น

3.5 เผยแพร่ข้อมูลสารสนเทศที่เป็นความลับของของบุคคล คณะ/หน่วยงาน หรือมหาวิทยาลัย

3.6 กระทำสิ่งที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี

3.7 แพร่กระจายไวรัส หนอน โทรจัน สปายแวร์ หรือซอฟต์แวร์ประสงค์ร้ายอื่น ๆ ที่สร้างความเสียหายหรือลดทอนประสิทธิภาพและความถูกต้องในการทำงานของระบบเครือข่าย

7.2 การบริหารจัดการการเข้าถึงระบบโดยผู้ใช้งาน

มาตรการ

1. จัดทำกระบวนการที่เป็นทางการสำหรับการลงทะเบียนและเพิกถอนผู้ใช้งาน เพื่อใช้ในการกำหนดสิทธิการเข้าถึงระบบเครือข่ายของมหาวิทยาลัย

2. จัดทำขั้นตอนปฏิบัติสำหรับการจัดเตรียมการเข้าถึงของผู้ใช้งาน เพื่อกำหนดหรือเพิกถอนสิทธิในการเข้าถึงระบบเครือข่ายของมหาวิทยาลัยและบริการทั้งหมดสำหรับผู้ใช้งานทุกประเภท

3. จำกัดและควบคุมการจัดสรรและการใช้งานสิทธิพิเศษ

4. ควบคุมการจัดสรรข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งานผ่านกระบวนการบริหารจัดการอย่างเป็นทางการ

5. ทบทวนสิทธิการเข้าถึงของผู้ใช้งานเป็นประจำ

6. เพิกถอนสิทธิการเข้าถึงระบบเครือข่ายของมหาวิทยาลัย สารสนเทศและสิ่งอำนวยความสะดวกสำหรับการประมวลผลสารสนเทศของผู้ปฏิบัติงานและผู้ใช้งานที่เป็นบุคคลภายนอกทุกคนออกจากระบบ เมื่อสิ้นสุดการจ้างงาน สัญญาหรือข้อตกลงที่ได้ทำไว้กับคณะ/หน่วยงาน หรือปรับปรุงสิทธิดังกล่าวเมื่อมีการเปลี่ยนแปลงสัญญาหรือข้อตกลงใหม่

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. จัดทำแนวปฏิบัติในการขออนุมัติและเพิกถอนสิทธิการใช้งานแต่ละระบบสารสนเทศ

2. จัดทำทะเบียนควบคุมสิทธิที่เหมาะสม รวมถึงรายชื่อหรือกลุ่มผู้มีสิทธิใช้งานทั้งที่ต้องขออนุมัติและไม่ต้องขออนุมัติก่อนเริ่มใช้งานอย่างเป็นลายลักษณ์อักษรในแต่ละระบบสารสนเทศ โดยการเข้าถึงของผู้ใช้งานทั้งหมดต้องสอดคล้องกับการดำเนินงานของมหาวิทยาลัยมหาสารคาม และหน้าที่ความรับผิดชอบของผู้ใช้งาน

3. ดูแลกำกับ สิทธิการเข้าถึง ไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้น

4. ควบคุมให้จำกัดจำนวนผู้ปฏิบัติงานที่มีสิทธิพิเศษทำหน้าที่เป็นผู้ให้สิทธิกับผู้ใช้งาน ไม่เกิน 3 คนต่อระบบงาน

5. ควบคุมไม่ให้ผู้ปฏิบัติงานที่มีสิทธิพิเศษเปิดเผยรหัสผ่านของผู้ใช้งานคนอื่น ๆ

6. จัดทำ “ทะเบียนรายชื่อบัญชีผู้ใช้งานร่วมกัน” โดยลงทะเบียนชื่อผู้ใช้งานเหล่านั้นทั้งหมดที่มีการใช้งานบัญชีเดียวกัน

7. ควบคุมการใช้บัญชีผู้ใช้งานร่วมกัน โดยจัดทำบันทึกการเข้าใช้งาน ระบุคณะ/หน่วยงาน ระบุผู้เข้าใช้ วัน/เวลา และการเข้าใช้งาน

8. ควบคุมดูแลให้มีการเพิกถอนสิทธิในการเข้าถึงบัญชีผู้ใช้งานร่วมกัน เมื่อบุคคลนั้นสิ้นสุดสัญญาหรือเปลี่ยนแปลงตำแหน่ง/การจ้างงาน และต้องเปลี่ยนรหัสผ่านของผู้ใช้งานทันที

9. แจ้งสมาชิกที่เหลือของผู้ใช้บัญชีผู้ใช้งานร่วมกัน เพื่อให้ทราบถึงจำนวนสมาชิกที่เหลือและรหัสผ่านใหม่ โดยต้องไม่ให้ผู้ที่ถูกเพิกถอนสิทธิรับทราบรหัสผ่านใหม่และเข้าถึงบัญชีผู้ใช้งานได้อีก

10. ทบทวนตารางแสดงสิทธิ อย่างน้อยปีละ 1 ครั้ง สำหรับระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ “สูงสุด” ให้ทบทวนตารางแสดงสิทธิทุก 90 วัน

11. ทบทวนและพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัย เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญาและข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ

12. ควบคุมดูแลการถอดถอนสิทธิในการเข้าถึงของผู้ปฏิบัติงาน ผู้ส่งมอบ และหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการปฏิบัติงาน ทั้งทางกายภาพ (Physical) และทางตรรกะ (Logical) เช่น กุญแจ บัตรแสดงตน บัตรประจำตัวผู้ปฏิบัติงาน และบัญชีผู้ใช้งาน

13. แสดงรายละเอียดการให้บริการระบบสารสนเทศกับผู้เกี่ยวข้อง เพื่อแจ้งให้ทราบถึงรายละเอียดการให้บริการสิทธิการเข้าใช้งาน การขออนุมัติ เปลี่ยนแปลงสิทธิและเพิกถอนสิทธิใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และอื่น ๆ

7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน

มาตรการ

ผู้ใช้งานปฏิบัติตามระเบียบปฏิบัติในการใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตน

แนวปฏิบัติสำหรับผู้ปฏิบัติงานและหน่วยงานภายนอก

1. รักษารหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ รวมถึงผู้ดูแลระบบ

2. ไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ปฏิบัติงานคนอื่น

3. ไม่เก็บรหัสผ่านในที่ที่เปิดเผย เช่น บันทึกรหัสผ่านบนกระดาษหรือในไฟล์ที่อ่านได้โดยง่าย

4. ไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านของผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม

5. เปลี่ยนแปลงรหัสผ่านอย่างเป็นประจำหรือเมื่อมีเหตุการณ์ที่มีนัยสำคัญสมควรจะต้องเปลี่ยนแปลงรหัสผ่าน เช่น เมื่อสงสัยว่ารหัสผ่านล่วงรู้โดยบุคคลอื่น เมื่อมีการแจ้งเตือนจากระบบหรือผู้ดูแลระบบ

6. ไม่กำหนดรหัสผ่านที่สามารถคาดเดาได้ง่าย ได้แก่

6.1 ข้อมูลส่วนตัว เช่น ชื่อ ชื่อเล่น วันเดือนปีเกิด เลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์

6.2 ตัวเลขหรือตัวอักษรเรียงต่อเนื่องกัน หรือเป็นตัวเลขหรือตัวอักษรทั้งหมด เช่น abcdefgh, aaaaaaaa หรือ 12345678 เป็นต้น

7. ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

8. ในกรณีที่มีการใช้งานบัญชีผู้ใช้งานร่วมกัน ต้องมีความตระหนักว่าหากมีความเสียหายเกิดขึ้น ผู้ใช้งานร่วมกันนั้นจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

9. ปิดโปรแกรมเว็บเบราเซอร์เมื่อเลิกใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

7.4 การควบคุมการเข้าถึงระบบสารสนเทศ

มาตรการ

1. จำกัดการเข้าถึงสารสนเทศและฟังก์ชันของระบบหรือโปรแกรมประยุกต์ให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

2. ควบคุมการเข้าถึงระบบงานและโปรแกรมประยุกต์ต่าง ๆ ผ่านขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบอย่างมั่นคงปลอดภัยตามที่กำหนดไว้ในนโยบายควบคุมการเข้าถึง

3. ระบบบริหารจัดการรหัสผ่านควรเป็นแบบโต้ตอบ และควรรับรองรหัสผ่านที่มีคุณภาพ

4. จำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้อย่างเข้มงวด เนื่องจากโปรแกรมประเภทยูทิลิตี้อาจมีความสามารถที่จะเปลี่ยนแปลงแก้ไขมาตรการควบคุมของระบบและโปรแกรมประยุกต์

5. จำกัดการเข้าถึงซอร์สโค้ดของโปรแกรม

แนวปฏิบัติสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ

1. ควบคุมให้ผู้ใช้งานเฉพาะระบบสารสนเทศที่ได้รับอนุญาตจากเจ้าของระบบสารสนเทศ และตามสิทธิที่พึงได้เท่านั้น

2. สอบทานสิทธิในการเข้าถึงระบบสารสนเทศกับคณะ/หน่วยงานเจ้าของระบบ อย่างน้อยปีละ 1 ครั้ง พร้อมทั้งเพิกถอนสิทธิ เมื่อพบเห็นสิทธิที่ไม่ถูกต้องตามตารางแสดงสิทธิในการเข้าถึง (Authorization Matrix) โดยต้องทบทวนผู้ใช้งานที่มีสิทธิพิเศษ (Privileged User) ด้วยรอบระยะเวลาที่ถี่กว่าปกติ

3. ควบคุมให้ระบบไม่แสดงข้อมูลของระบบ หากกระบวนการเข้าสู่ระบบสารสนเทศนั้นไม่สำเร็จ

4. ควบคุมให้ระบบไม่มีข้อความช่วยเหลือในระหว่างการเข้าสู่ระบบ เช่น ชื่อผู้ใช้งานให้ใช้หมายเลขบัตรประจำตัวประชาชนเท่านั้น หรือใช้บัญชีรายชื่อด้วยอีเมลแอดเดรส เพื่อป้องกันผู้ใช้งานที่ไม่ได้รับอนุญาตสามารถเข้าสู่ระบบได้

5. ควบคุมให้ระบบตรวจสอบข้อมูลการเข้าสู่ระบบเมื่อเสร็จสิ้นการป้อนข้อมูลนำเข้า ทั้งหมดแล้ว ทั้งนี้หากมีข้อผิดพลาดเกิดขึ้น ระบบไม่ควรระบุว่า เกิดข้อผิดพลาดที่ส่วนใดของชุดข้อมูล

6. ควบคุมให้ระบบตัดการเชื่อมต่อช่วงที่ไม่มีการใช้งานเมื่อครบระยะเวลาที่ไม่มีการใช้งานตามที่กำหนดไว้ รวมทั้งประกาศให้ผู้ใช้งานได้รับทราบว่าระบบจะมีการตัดการเชื่อมต่อเมื่อผู้ใช้งานไม่ได้ใช้งานเกินกว่าระยะเวลาดังกล่าว

7. ควบคุมให้ระบบบันทึกเหตุการณ์ (Log) การพยายามเข้าสู่ระบบทั้งกรณีที่สำเร็จและไม่สำเร็จ

8. มีแนวทางป้องกันการพยายามเข้าสู่ระบบโดยวิธีการสุ่มรหัสผ่าน (Brute Force)

9. ลบหรือระงับการใช้งานสิทธิของผู้ใช้งานที่มากับระบบ (Default User) ในกรณีที่มีความจำเป็นต้องใช้งาน ต้องมีการกำหนดรหัสผ่านใหม่

10. ควบคุมดูแลบัญชีผู้ใช้งานและรหัสผ่านให้มีความเหมาะสม ถูกต้องและปลอดภัย โดยประเภทของบัญชีผู้ใช้งาน ได้แก่ บัญชีผู้ใช้งานส่วนบุคคล บัญชีผู้ใช้งานร่วมกัน (Shared User ID) และบัญชีสิทธิพิเศษ (Privileged User)

11. กำหนดคุณสมบัติของระบบสารสนเทศ ดังนี้

11.1 สำหรับระบบที่มีการสร้างรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ต้องบังคับให้มีการเปลี่ยนแปลงรหัสผ่านชั่วคราว (Temporary Password) ในครั้งแรกของการเข้าสู่ระบบ

11.2 ควรมีฟังก์ชันการทำงานให้ผู้ใช้งานสามารถเปลี่ยนแปลงรหัสผ่านของตนเอง พร้อมทั้งมีขั้นตอนในการยืนยันรหัสผ่านเดิม และการตั้งรหัสผ่านใหม่

11.3 กำหนดให้มีการเปลี่ยนแปลงรหัสผ่านในการเข้าถึงระบบทุก 90 วัน สำหรับระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด”

11.4 กำหนดให้มีการระงับการใช้งานชั่วคราวตามความเหมาะสมของหมวดหมู่ทรัพย์สินสารสนเทศสำหรับบัญชีผู้ใช้ที่ใส่รหัสผ่านผิดเกินที่ทำการกำหนดไว้ในข้อปฏิบัติ

11.5 ไม่แสดงรหัสผ่านที่ผู้ใช้งานพิมพ์ในขณะเข้าสู่ระบบ โดยอาจมีการแสดงสัญลักษณ์แทนรหัสผ่านจริงในขณะที่ผู้ใช้งานพิมพ์

11.6 มีรูปแบบที่ป้องกันในการจัดเก็บและส่งรหัสผ่าน เช่น การเข้ารหัสข้อมูลหรืออื่น ๆ

12. กำหนดคุณสมบัติของรหัสผ่านอย่างน้อย ดังนี้

12.1 รหัสผ่านต้องมีความยาวอย่างน้อย 8 หลัก

12.2 รหัสผ่านต้องประกอบด้วย ตัวอักษร (ทั้งตัวพิมพ์เล็กและตัวพิมพ์ใหญ่) ตัวเลข และอักขระพิเศษหรือสัญลักษณ์ต่าง ๆ เช่น (A-Z), (a-z), (0-9), (@ , # , & , “ , ‘ , *, =, < , > , % , $, + , ?)

12.3 รหัสผ่านต้องไม่ตรงกับชื่อผู้ใช้งานระบบ (User Login) และชื่อผู้ใช้งานจริง (User Name)

13. ระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ “สูงสุด” ต้องจัดเก็บและควบคุมให้แสดงข้อมูล วันและเวลาของการเข้าสู่ระบบที่ประสบความสำเร็จในครั้งก่อน หลังจากทำการเข้าสู่ระบบเสร็จสมบูรณ์

14. ระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ต้องควบคุมให้มีการพิสูจน์และยืนยันตัวตนโดยการใช้วิธีการพิสูจน์และยืนยันตัวตนแบบ Two-factor Authentication (2FA)

15. ควบคุมจำกัดการเข้าถึงอุปกรณ์เครือข่าย ระบบปฏิบัติการ ฐานข้อมูล และระบบสารสนเทศที่เก็บบัญชีผู้ใช้งานและรหัสผ่าน โดยผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น

16. ไม่เก็บคลังซอร์สโค้ดไว้ในระบบที่ดำเนินการปฏิบัติงานอยู่ (Production Systems)

17. ปฏิบัติตามแนวทางการเข้าถึงซอร์สโค้ดของระบบสารสนเทศ ไม่นำเข้าฟังก์ชันการทำงานหรือเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

18. บริหารจัดการซอร์สโค้ดและคลังซอร์สโค้ดตามขั้นตอนปฏิบัติที่จัดทำขึ้น

19. จำกัดการเข้าถึงคลังซอร์สโค้ดของบุคลากรผู้สนับสนุนการทำงาน

20. ปรับปรุงคลังซอร์สโค้ดและรายการที่เกี่ยวข้อง รวมถึงแจกจ่ายซอร์สโค้ดไปยังผู้พัฒนาระบบ หลังจากได้รับการอนุมัติเท่านั้น

21. เก็บซอร์สโค้ดที่จัดพิมพ์ออกมาเอาไว้ในสภาพแวดล้อมที่มีความปลอดภัย

22. ควบคุมให้มีบันทึกเหตุการณ์ (Log) ในการเข้าถึงคลังซอร์สโค้ด

23. เก็บรักษาและคัดลอกคลังซอร์สโค้ดตามขั้นตอนปฏิบัติในการควบคุมการเปลี่ยนแปลงแก้ไขอย่างเคร่งครัด

24. แจ้งคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม หรือผู้อำนวยสำนักคอมพิวเตอร์ เมื่อตรวจพบการละเมิดมาตรการควบคุมการเข้าสู่ระบบ หรือสงสัยว่าอาจเป็นเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

หมวด 8 การเข้ารหัสข้อมูล

(Cryptography)

วัตถุประสงค์

เพื่อให้มั่นใจว่า มีการใช้งานการเข้ารหัสข้อมูลที่เหมาะสมและมีประสิทธิภาพ

มาตรการ

1. จัดทำและนำนโยบายการใช้มาตรการการเข้ารหัสข้อมูลไปสู่การปฏิบัติ

2. จัดทำและนำนโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจสำหรับการเข้ารหัสข้อมูลตลอดวงจรชีวิตของกุญแจดังกล่าวไปสู่การปฏิบัติ

8.1 มาตรการการเข้ารหัสข้อมูล

แนวปฏิบัติสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ

1. จัดให้มีการเข้ารหัสข้อมูล โดยพิจารณาตามระดับการป้องกันความมั่นคงปลอดภัย
2. จัดทำบัญชีการใช้งานการเข้ารหัส

8.2 มาตรการการใช้กุญแจสำหรับการเข้ารหัสข้อมูล

แนวปฏิบัติสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ

1. ในระบบที่มีความสำคัญ ต้องจัดเก็บกุญแจคู่ (Key Pair) ในการเข้ารหัสแบบสมมาตร (Asymmetric Encryption) หรือ กุญแจลับ (Secret Keys) ในการเข้ารหัสแบบสมมาตร (Symmetric Encryption) ด้วยวิธีการที่ปลอดภัย เช่น เก็บแยกในเครื่องอื่นหรืออุปกรณ์อื่นที่มีการควบคุมการเข้าถึงที่อย่างแน่นหนา หรือเก็บในสื่อที่เคลื่อนย้ายได้ที่มีกุญแจป้องกันอย่างแน่นหนา

2. จัดเก็บกุญแจสาธารณะ (Public Keys) ในเครือข่ายกลาง ซึ่งสามารถเข้าถึงโดยผู้ที่ได้รับอนุญาตเท่านั้น

3. จัดเก็บกุญแจหลัก (Master Keys) กุญแจของผู้ดูแลระบบ (Administrators' Keys) หรือกุญแจฉุกเฉิน (Emergency Keys) ในสื่อที่แยกกันและมีการควบคุมการเข้าถึงที่เข้มงวด

4. บริหารจัดการกุญแจเข้ารหัสข้อมูล โดยมีการแบ่งแยกหน้าที่ ดังนี้

    4.1 ในการเบิกหรือใช้งานกุญแจหลัก (Master Keys) ต้องกระทำโดยบุคคลตั้งแต่สองคนขึ้นไป

    4.2 บุคคลคนเดียวกัน ต้องไม่สามารถสร้างและเปิดการใช้งาน (Activate) กุญแจชุดเดียวกัน

5. ผู้ดูแลระบบหรือผู้พัฒนาระบบทำหน้าที่สร้างกุญแจในการเข้ารหัส และส่งมอบกุญแจเข้ารหัสอย่างปลอดภัยให้กับเจ้าของกุญแจเท่านั้น

6. เรียกคืนหรือทำลายกุญแจส่วนบุคคล (Private Keys) และกุญแจลับ (Secret Keys) ในกรณีต่อไปนี้

    6.1 ผู้ใช้งานพ้นสภาพการเป็นผู้ปฏิบัติงานของมหาวิทยาลัยมหาสารคาม

6.2 ผู้ใช้งานไม่มีความจำเป็นต้องใช้กุญแจ

6.3 กุญแจถูกทำลายหรือล้าสมัยแล้ว

6.4 กุญแจถูกล่วงรู้โดยบุคคลอื่น หรือกุญแจสูญหาย

7. สร้างกุญแจส่วนบุคคล (Private Keys) หรือกุญแจลับ (Secret Keys) ใหม่ในกรณีต่อไปนี้

7.1 กุญแจถูกทำลายหรือล้าสมัยแล้ว

7.2 กุญแจถูกล่วงรู้โดยบุคคลอื่น หรือกุญแจสูญหาย

8. กำหนดกระบวนการในการกู้คืนกุญแจ เพื่อลดความเสี่ยงในการสูญหาย หรือเสียหายของกุญแจ

9. กำหนดอายุการใช้งานของกุญแจ เพื่อให้กุญแจนั้นถูกใช้ในช่วงเวลาที่จำกัด เช่น

9.1 กุญแจหลัก (Master Keys) ควรเปลี่ยนแปลงทุก ๆ 1 ปี หรือเป็นไปตามที่เจ้าของผลิตภัณฑ์แนะนำ

9.2 กุญแจที่ใช้เข้ารหัสกุญแจ เช่น การใช้กุญแจส่วนบุคคล (Private Keys) เข้ารหัสกุญแจลับ (Secret Keys) ควรเปลี่ยนแปลงอย่างน้อยทุก ๆ 6 เดือน หรือเป็นไปตามที่เจ้าของผลิตภัณฑ์แนะนำ

แนวปฏิบัติสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ

1. ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบการเข้ารหัส (Cryptographic) ต้องไม่ส่งกุญแจส่วนบุคคล (Private Keys) ไปยังผู้อื่น

2. พิสูจน์และยืนยันตัวตนของเจ้าของกุญแจสาธารณะ (Public Keys) โดยแบบการยืนยันโดยตรงจากผู้ส่ง หรือการยืนยันในรูปแบบของใบรับรองกุญแจจาก Certification Authority (CA) ที่เชื่อถือได้

3. ทดสอบความถูกต้องของกุญแจที่รับผิดชอบก่อนที่จะใช้งานจริง เช่น ทดสอบการส่งข้อความที่มีการเข้ารหัส ทดสอบการเข้ารหัสและการถอดรหัสไฟล์

4. เก็บกุญแจส่วนบุคคล (Private Keys) ในสถานที่ที่ปลอดภัย ซึ่งควรจัดเก็บในอุปกรณ์สารสนเทศที่สามารถเคลื่อนย้ายได้ เช่น Token, Smart Card

5. ในกรณีที่พบว่ากุญแจถูกล่วงรู้โดยบุคคลอื่น ต้องแจ้งผู้บริหารหน่วยงานทราบทันที

หมวด 9 ความมั่นคงปลอดภัยในการสื่อสาร

(Communications Security)

วัตถุประสงค์

เพื่อให้มั่นใจว่า มีการป้องกันสารสนเทศในระบบเครือข่าย และอุปกรณ์สำหรับการประมวลผลสารสนเทศที่สนับสนุนการทำงานของระบบเครือข่าย และป้องกันสารสนเทศที่มีการแลกเปลี่ยนกันภายในคณะ/หน่วยงานของมหาวิทยาลัย รวมถึงแลกเปลี่ยนกับหน่วยงานภายนอก เพื่อป้องกันปัญหาต่าง ๆ ที่อาจเกิดขึ้น เช่น ข้อมูลสำคัญรั่วไหล ข้อมูลถูกดักจับระหว่างการแลกเปลี่ยน ข้อมูลติดโปรแกรมไม่พึงประสงค์ โดยผ่านทางช่องทางการสื่อสารทุกชนิด ซึ่งประกอบด้วย 2 หัวข้อ ดังนี้

1. มาตรการควบคุมทางระบบเครือข่าย
2. การแลกเปลี่ยนสารสนเทศ

9.1 มาตรการควบคุมทางระบบเครือข่าย

มาตรการ

1. ป้องกันสารสนเทศในระบบเครือข่ายและสิ่งอำนวยความสะดวกสำหรับการประมวลผลสารสนเทศที่สนับสนุนการทำงานของเครือข่าย

2. ระบุวิธีการหรือเครื่องมือสำหรับความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของฝ่ายบริหารเกี่ยวกับการให้บริการเครือข่ายไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าจะเป็นบริการที่หน่วยงานดำเนินงานเอง (In-house) หรือการให้หน่วยงานอื่นดำเนินงานแทน (Outsource)

3. แบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบสารสนเทศ

แนวปฏิบัติสำหรับคณะ/หน่วยงาน

1. มอบหมายผู้รับผิดชอบควบคุมการใช้งานเครือข่ายของหน่วยงานภายนอก และประสานงานกับผู้ดูแลระบบเครือข่าย

2. ควบคุมไม่ให้มีการใช้งานบัญชีผู้ใช้งานร่วมกัน (Shared ID) เพื่อเชื่อมต่อกับเครือข่ายมหาวิทยาลัยมหาสารคาม

แนวปฏิบัติสำหรับผู้ดูแลระบบเครือข่าย

1. กำหนดหน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่าย

2. กำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบของบุคคลในการปฏิบัติงานด้านเครือข่าย

3. จัดให้มีมาตรการควบคุมพิเศษสำหรับการรักษาความลับ (Confidentiality) และความสมบูรณ์ (Integrity) ของข้อมูลที่ส่งผ่านระบบเครือข่ายสาธารณะหรือเครือข่ายไร้สาย และสำหรับป้องกันระบบและแอปพลิเคชันที่เชื่อมต่อกับระบบเครือข่าย เช่น การเข้ารหัสข้อมูล นอกจากนี้ให้พิจารณานำมาตรการควบคุมพิเศษมาใช้สำหรับดูแลรักษาความพร้อมใช้งาน (Availability) ของการให้บริการระบบเครือข่ายและคอมพิวเตอร์ที่เชื่อมต่อ

กับระบบเครือข่าย เช่น มีเส้นทางสำรองในการเชื่อมต่อระหว่างอาคารที่สำคัญกับศูนย์ข้อมูลกลาง (Data Center) หรือมีเส้นทางสำรองการเชื่อมต่อระบบเครือข่ายของมหาวิทยาลัยกับเครือข่ายอินเทอร์เน็ต

4. กำหนดให้มีการลงบันทึกเหตุการณ์และมีการเฝ้าระวังอย่างเหมาะสม เพื่อบันทึกและตรวจหาการกระทำที่อาจส่งผลกระทบหรือเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

5. มีการจำกัดช่องทางการเชื่อมต่อของระบบไปยังเครือข่าย โดยต้องถูกกำหนดให้ใช้เฉพาะที่จำเป็นเท่านั้น เช่น การเข้าถึงระบบสารสนเทศที่สำคัญของมหาวิทยาลัย ต้องเข้าถึงได้เฉพาะผู้ใช้บริการในเครือข่ายของมหาวิทยาลัย (MSUNet) เท่านั้น

6. จัดทำข้อกำหนดและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยของการให้บริการระบบเครือข่าย และดำเนินงานให้สอดคล้องกับข้อกำหนดดังกล่าว

7. ระบุข้อตกลงด้านความมั่นคงปลอดภัยที่จำเป็นสำหรับแต่ละการให้บริการบนระบบเครือข่ายของมหาวิทยาลัย ตามคุณลักษณะด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของสำนักคอมพิวเตอร์หรือผู้บริหารมหาวิทยาลัย เช่น ข้อตกลง Service Level Agreement (SLA)

8. ติดตามผลอย่างสม่ำเสมอว่า ผู้ให้บริการระบบเครือข่ายสามารถจัดการงานบริการได้อย่างปลอดภัยเป็นไปตามข้อตกลง และมีข้อตกลงที่ให้สิทธิกับมหาวิทยาลัยมหาสารคาม ในการตรวจประเมินการดำเนินงานของผู้ให้บริการระบบเครือข่าย

9. ควบคุมดูแลให้ระบบเครือข่ายมีคุณลักษณะด้านความมั่นคงปลอดภัยของการให้บริการระบบเครือข่าย เช่น

9.1 มีเทคโนโลยีดิจิทัลที่นำมาใช้รักษาความมั่นคงปลอดภัยของการให้บริการระบบเครือข่าย เช่น การพิสูจน์และยืนยันตัวตน การเข้ารหัสข้อมูล การตรวจจับสิ่งผิดปกติ และการควบคุมและตรวจสอบการเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัย ทั้งเครือข่ายสายสัญญาณและเครือข่ายไร้สาย

9.2 การจัดหาอุปกรณ์เครือข่าย อุปกรณ์เทคโนโลยีดิจิทัลอื่น ๆ และการพัฒนาระบบสารสนเทศต้องสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยของการให้บริการระบบเครือข่าย

9.3 กำหนดขั้นตอนปฏิบัติในการใช้บริการระบบเครือข่ายของมหาวิทยาลัย สำหรับควบคุมการเข้าถึงการให้บริการระบบเครือข่ายหรือระบบสารสนเทศต่าง ๆ ตามความจำเป็น

10. ตั้งค่าอุปกรณ์เครือข่าย โดยจำกัดสิทธิการเข้าถึงพอร์ตสำหรับตั้งค่าการทำงาน (Console Port) ด้วยวิธีการพิสูจน์และยืนยันตัวตน

11. ระบบเครือข่ายของมหาวิทยาลัย ทั้งเครือข่ายสายสัญญาณและเครือข่ายไร้สาย ต้องควบคุมการเชื่อมต่อได้เฉพาะเครื่องที่ผ่านการพิสูจน์และยืนยันตัวตนแล้วเท่านั้น

12. เพิกถอนบัญชีผู้ใช้งานระบบเครือข่าย เมื่อสิ้นสุดระยะเวลาที่ขอใช้งาน หรือสิ้นสุดการจ้างงาน หรือลาออก หรือเสียชีวิต

13. จัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้ หรือกลุ่มของระบบสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อย (Virtual LAN) ได้อย่างเหมาะสม ทั้งนี้การแบ่งแยกเครือข่าย ต้องมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall, Core Switch หรือ Access Switch ที่สามารถแบ่ง Virtual LAN ได้ โดยหลักเกณฑ์การแบ่งแยกเครือข่าย ต้องสอดคล้องกับมาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ ความต้องการในการเข้าถึงข้อมูล ระดับการป้องกันความมั่นคงปลอดภัยของข้อมูล รวมถึงการพิจารณาประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

13.1 ระบบเครือข่ายที่อนุญาตให้สามารถเข้าถึงจากภายนอกได้ กับระบบเครือข่ายที่ใช้ภายในมหาวิทยาลัยมหาสารคามเท่านั้น

13.2 ระบบเครือข่ายร่วมกันระหว่างคณะ/หน่วยงาน ภายในมหาวิทยาลัยมหาสารคาม

13.3 เครือข่ายของแอปพลิเคชัน (Application) ที่มีความสำคัญภายในมหาวิทยาลัย กับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า

13.4 เครือข่ายสำหรับศูนย์ข้อมูลกลาง (Data Center) ที่ให้บริการกับเครือข่ายของผู้ใช้งานในมหาวิทยาลัย

14. กำหนดเส้นทางบนระบบเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงจากระยะไกลเฉพาะเครือข่ายหรืออุปกรณ์เครือข่ายที่กำหนด

15. ตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall, Router, Core Switch หรือ Access Switch Layer 3 ที่มีการตั้งค่าไว้ ไม่ให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉินเท่านั้น ซึ่งต้องได้รับการอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์ รองผู้อำนวยการที่มีหน้าที่ควบคุมและบริหารงานระบบเครือข่าย หรือหัวหน้างานระบบเครือข่ายและการสื่อสาร

แนวปฏิบัติสำหรับหน่วยงานภายนอก

1. ในกรณีที่มีความจำเป็นต้องใช้งานระบบเครือข่ายมหาวิทยาลัยมหาสารคาม หรือขอเปลี่ยนแปลงรายละเอียด ให้ขออนุมัติผ่านผู้อำนวยการสำนักคอมพิวเตอร์ หรือรองผู้อำนวยการสำนักคอมพิวเตอร์ ที่มีหน้าที่ควบคุมและบริหารงานระบบเครือข่าย โดยมีรายละเอียดดังนี้

1.1 ผู้รับผิดชอบ

1.2 ระยะเวลาการใช้งานระบบเครือข่าย

1.3 คอมพิวเตอร์หรือเครือข่ายปลายทางที่จำเป็นต่อการใช้งาน

1.4 รูปแบบการเชื่อมต่อระบบเครือข่าย เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายภายในมหาวิทยาลัยมหาสารคาม หรือการเข้าถึงจากระยะไกล

2. ในกรณีที่มีการเข้าถึงระบบเครือข่ายมหาวิทยาลัยมหาสารคามจากระยะไกลในรูปแบบ Client to Site หรือ VPN Server ซึ่งมีลักษณะเป็นการเชื่อมต่อจากบุคคลสู่เครือข่ายภายในมหาวิทยาลัยมหาสารคาม ต้องได้รับอนุมัติจากผู้อำนวยการมหาวิทยาลัยมหาสารคามเท่านั้น

9.2 การแลกเปลี่ยนสารสนเทศ

มาตรการ

1. กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการควบคุมอย่างเป็นทางการสำหรับการแลกเปลี่ยนสารสนเทศ เพื่อป้องกันการแลกเปลี่ยนสารสนเทศผ่านการใช้งานสิ่งอำนวยความสะดวกด้านการสื่อสารทุกประเภท

2. ป้องกันสารสนเทศที่รับส่งในรูปแบบข้อความทางอิเล็กทรอนิกส์อย่างเหมาะสม

3. ระบุข้อกำหนดสำหรับข้อตกลงการรักษาความลับหรือการไม่เปิดเผยข้อมูล ซึ่งเหมาะสมกับระดับความจำเป็นในการป้องกันสารสนเทศ โดยมีการจัดทำเป็นลายลักษณ์อักษร รวมถึงให้มีการทบทวนอย่างสม่ำเสมอ ทุก 1 ปี

แนวปฏิบัติสำหรับหน่วยงาน

1. จัดทำขั้นตอนปฏิบัติงานสำหรับการแลกเปลี่ยนสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” โดยขั้นตอนดังกล่าวต้องได้รับการอนุมัติจากบริหารหน่วยงานเพื่อควบคุมการแลกเปลี่ยนสารสนเทศในช่องทางการสื่อสาร ดังต่อไปนี้

    1.1 จดหมายอิเล็กทรอนิกส์

    1.2 ระบบเครือข่าย

    1.3 สื่อบันทึกข้อมูลต่าง ๆ

    1.4 เอกสาร จดหมายและบันทึก

2. ควบคุมให้การแลกเปลี่ยนสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ผ่านช่องทางบริการจัดส่งข้อมูล หรือระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยมหาสารคาม

3. ควบคุมให้ผู้ปฏิบัติงานดำเนินงานตามขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศในข้อ 1 โดยต้องได้รับการอนุมัติจากผู้อำนวยการสำนักคอมพิวเตอร์ หรือรองผู้อำนวยการสำนักคอมพิวเตอร์ที่ได้รับมอบหมายขึ้นไปก่อนดำเนินงาน

4. จัดทำข้อกำหนดการเก็บรักษาและการกำจัดเอกสารที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ตามกฎหมายและกฎระเบียบของมหาวิทยาลัยมหาสารคาม

5. จัดทำข้อตกลงเกี่ยวกับการแลกเปลี่ยนสารสนเทศด้วยวิธีการที่ปลอดภัยกับหน่วยงานภายนอก และควรมีรายละเอียดในประเด็นดังนี้

    5.1 หน้าที่ความรับผิดชอบในการบริหารจัดการกระบวนการควบคุมและแจ้งสถานะการส่ง (Transmission) การกระจายไปยังผู้รับ (Dispatching) และการรับ (Receipt)

    5.2 ขั้นตอนปฏิบัติเพื่อให้มั่นใจในการสอบทวนแหล่งที่มา (Traceability) และการไม่สามารถปฏิเสธความรับผิดชอบ (Non-Repudiation)

    5.3 สัญญาการดูแลผลประโยชน์ของคู่สัญญา (Escrow Agreement)

5.4 มาตรการระบุตัวตนของผู้ส่งสารสนเทศ

5.5 หน้าที่ความรับผิดชอบและความรับผิดเมื่อเกิดสถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์ เช่น ข้อมูลสูญหาย หรืออื่นๆ

5.6 มาตรการด้านเทคนิคสำหรับการบันทึกและการอ่านสารสนเทศรวมถึงซอฟต์แวร์และเทคโนโลยีดิจิทัลอื่น ๆ

5.7 มาตรการควบคุมพิเศษที่จำเป็นสำหรับป้องกันสารสนเทศที่อ่อนไหว เช่น การเข้ารหัสข้อมูล

5.8 มาตรการควบคุมการเข้าถึงในระดับที่ยอมรับได้

แนวปฏิบัติสำหรับผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์

1. มีการแจ้งความประสงค์ขอใช้งานอย่างเป็นลายลักษณ์อักษรและสามารถใช้งานได้เมื่อได้รับการอนุมัติจากผู้บังคับบัญชาของผู้แจ้งความประสงค์ใช้งานและผู้อำนวยการสำนักคอมพิวเตอร์ หรือรองผู้อำนวยการสำนักคอมพิวเตอร์ที่ได้รับมอบหมาย

2. กำหนดสิทธิการเข้าถึงระบบส่งจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการใช้บริการและหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึง อย่างน้อยปีละ 1 ครั้ง

3. กำหนดให้ผู้ที่ได้รับมอบหมายเท่านั้นที่จะเข้าแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงต่าง ๆ ได้

4. บันทึกรายละเอียดการเข้าถึงระบบส่งจดหมายอิเล็กทรอนิกส์ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ ไว้เพื่อเป็นหลักฐานการตรวจสอบในกรณีเกิดปัญหา

5. จัดให้มีวิธีการตรวจสอบตัวตนและสิทธิในการใช้บริการของผู้ปฏิบัติงานก่อนอนุญาตให้ใช้บริการ

6. จัดให้มีการทดสอบระบบส่งจดหมายอิเล็กทรอนิกส์ อย่างน้อยปีละ 1 ครั้ง เพื่อหาจุดอ่อนและข้อผิดพลาดในเรื่องความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ เช่น การประเมินช่องโหว่ทางเทคนิค (Vulnerability Assessment) การทำให้การให้บริการล้มเหลว (Denial of Service)

7. พิจารณาทบทวนข้อกฎหมายต่าง ๆ เช่น ข้อกำหนดสำหรับลายเซ็นทางอิเล็กทรอนิกส์

แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

1. ตรวจสอบความถูกต้องของข้อมูลในเอกสารหรือรายงานต่าง ๆ ที่จัดทำขึ้นให้เรียบร้อย ก่อนที่จะนำไปใช้งานหรือส่งต่อให้กับผู้อื่น หากพบข้อผิดพลาดให้ตรวจสอบและแก้ไข

2. ใช้บริการจดหมายอิเล็กทรอนิกส์ตามนโยบายการใช้จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยมหาสารคาม

3. ผู้ปฏิบัติงานที่เป็นเจ้าของบัญชีผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของมหาวิทยาลัยมหาสารคามหากเกิดกรณีที่ทำให้มหาวิทยาลัยมหาสารคามหรือผู้อื่นได้รับความเสียหายจะต้องเป็นผู้รับผิดชอบ

4. ไม่ส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) หรือจดหมายลูกโซ่ (Chain Letter) และไม่ปลอมแปลงจดหมายอิเล็กทรอนิกส์ของบุคคลอื่น

5. ไม่ส่งจดหมายอิเล็กทรอนิกส์ที่เป็นการละเมิดต่อกฎหมาย เช่น กฎหมายทรัพย์สินทางปัญญาหรืออื่นๆ

6. ไม่ส่งจดหมายอิเล็กทรอนิกส์ที่มีโปรแกรมไม่พึงประสงค์ให้กับบุคคลอื่น

หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบ
(System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อบริหารจัดการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศของมหาวิทยาลัยมหาสารคาม และสร้างความมั่นคงปลอดภัยให้กับสารสนเทศและระบบสารสนเทศให้มีประสิทธิภาพ ซึ่งประกอบด้วย 3 เรื่อง ดังต่อไปนี้

1. ข้อกำหนดความมั่นคงปลอดภัยทางไซเบอร์สำหรับระบบสารสนเทศ
2. ความมั่นคงปลอดภัยในกระบวนการพัฒนาและกระบวนการสนับสนุนอื่น ๆ
3. ข้อมูลสำหรับการทดสอบ

10.1 ข้อกำหนดความมั่นคงปลอดภัยทางไซเบอร์สำหรับระบบสารสนเทศ

มาตรการ

1. รวมข้อกำหนดความมั่นคงปลอดภัยทางไซเบอร์ไว้ในข้อกำหนดสำหรับระบบใหม่หรือการปรับปรุงระบบที่มีอยู่

2. ป้องกันสารสนเทศที่เกี่ยวข้องกับธุรกรรม/รายการเปลี่ยนแปลงการให้บริการโปรแกรมประยุกต์ เพื่อป้องกันไม่ให้มีการส่งที่ไม่สมบูรณ์ การส่งผิดเส้นทาง การเปลี่ยนแปลงแก้ไขข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การทำสำเนาหรือเปิดฟังข้อความโดยไม่ได้รับอนุญาต

แนวปฏิบัติสำหรับหน่วยงาน

1. ระบุคุณสมบัติ (Specification) ด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับระบบสารสนเทศที่มีการจัดซื้อหรือมีการพัฒนาขึ้น โดยข้อกำหนดดังกล่าวต้องครอบคลุมตั้งแต่ขั้นตอนการออกแบบจนถึงขั้นตอนการนำระบบไปติดตั้ง โดยคุณสมบัติ (Specification) ด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับระบบสารสนเทศขึ้นอยู่กับระดับการป้องกันความมั่นคงปลอดภัยของระบบสารสนเทศ ภัยคุกคามทางไซเบอร์ และการพิจารณาดังนี้

1.1 ปัจจัยเสี่ยง

1.1.1 ระดับความสำคัญ (Criticality) รวมไปถึงความถูกต้องครบถ้วนและความพร้อมใช้ ของกระบวนการในระบบสารสนเทศ

1.1.2 คุณค่า (Value) ระดับความลับ (Sensitivity) หรือระดับความสำคัญ (Criticality) รวมไปถึงความถูกต้องครบถ้วนและความพร้อมใช้ของสารสนเทศที่เกี่ยวข้อง

1.1.3 ประสบการณ์ในอดีตเกี่ยวกับการใช้ระบบสารสนเทศ หรือการใช้ระบบสารสนเทศไปในทางที่ไม่ถูกต้อง

1.1.4 ขอบเขตสำหรับการเชื่อมต่อระบบสารสนเทศ

1.1.5 ผลกระทบที่อาจเกิดขึ้นกับระบบสารสนเทศอื่น ๆ และภาพรวมของระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ของมหาวิทยาลัยมหาสารคาม

6.2 กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

1.2.1 โครงสร้างระบบและการเชื่อมต่อระบบเครือข่าย เช่น ระบบแบบกระจายศูนย์ (Distributed System) ระบบแบบรวมศูนย์ (Centralized System) หรือระบบแบบปิด (Closed System)

1.2.2 การเข้าถึงจากสถานที่กำหนดให้เฉพาะ เช่น การเข้าถึงจากภายในและภายนอกสำนักงาน

1.2.3 ผู้ใช้งานที่ได้รับอนุญาตให้เข้าถึงระบบ

1.2.4 วิธีการพิสูจน์และยืนยันตัวตน

1.2.5 การควบคุมการเข้าถึง

1.2.6 วิธีการมอบสิทธิ (Authorization)

1.2.7 การแบ่งแยกหน้าที่ในกระบวนการที่สำคัญ เช่น ผู้ที่สามารถกำหนดค่าของระบบ (Configuration) ต้องไม่สามารถสร้างรายการธุรกรรมของผู้ใช้งานได้

1.2.8 วิธีการตรวจสอบข้อมูลนำเข้า การประมวลผล และข้อมูลนาออก

1.2.9 การรองรับและความสามารถสูงสุดในการทำงานของระบบที่ประมาณการ

1.2.10 ความมั่นคงปลอดภัยในการส่งผ่านข้อมูล

1.2.11 ความจำเป็นของการใช้เครื่องมือการเข้ารหัส (Cryptographic Tools) เพื่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ของข้อมูล หรือการป้องกันการปฏิเสธความรับผิด (Non-Repudiation)

1.2.12 ข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศในระดับระบบสารสนเทศ (Application) ระดับโครงสร้าง (Infrastructure) ระดับระบบปฏิบัติการ (Operating System) และระดับฐานข้อมูล (Database System)

1.2.13 วิธีการตรวจสอบและการควบคุม

1.2.14 การสำรองและการกู้คืนระบบ

1.2.15 การคุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติสำหรับผู้ดูแลระบบ

1. ควบคุมให้หน้าแรกของเว็บไซต์หรือระบบงานที่หน่วยงานรับผิดชอบ ระบุผู้รับผิดชอบ และช่องทางการติดต่อผู้รับผิดชอบ

2. บันทึกเหตุการณ์ (Log) การเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ ไว้ เพื่อเป็นหลักฐานการตรวจสอบในกรณีเกิดปัญหา

3. ควบคุมดูแลให้เอกสารระบบถูกจัดเก็บในที่ปลอดภัยตามความเหมาะสม

4. ควบคุมดูแลการพัฒนาระบบให้มีความมั่นคงปลอดภัยทางไซเบอร์ตามคุณสมบัติ (Specification) ด้านความมั่นคงปลอดภัยทางไซเบอร์

5. ควบคุมให้มีการทดสอบความมั่นคงปลอดภัยทางไซเบอร์ของอุปกรณ์ประมวลสารสนเทศหลัก เช่น การค้นหาช่องโหว่ของระบบปฏิบัติการ, Router, Firewall, ฐานข้อมูล ก่อนนำระบบใช้งานจริง

6. ควบคุมดูแลสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ ดังต่อไปนี้

6.1 จัดให้มีกระบวนการอนุมัติที่เป็นทางการก่อนจะมีการเผยแพร่สารสนเทศ ในการรักษาความถูกต้องเชื่อถือได้

6.2 มีการรักษาความถูกต้องเชื่อถือได้ของสารสนเทศ โดยกลไกที่เหมาะสม เช่น Digital Signatures

6.3 กำหนดสิทธิการเข้าถึงสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานและหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

6.4 กำหนดให้ผู้ที่ได้รับมอบหมายเท่านั้น ที่จะเข้าแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงต่าง ๆ ได้

6.5 จัดให้มีการทดสอบ เพื่อหาจุดอ่อนและข้อผิดพลาด เช่น การประเมินช่องโหว่ทางเทคนิค (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) อย่างน้อยปีละ 1 ครั้ง

7. ควบคุมให้มีความมั่นคงปลอดภัยสำหรับการทำธุรกรรมอิเล็กทรอนิกส์ ดังต่อไปนี้

7.1 กำหนดสิทธิการเข้าถึงระบบธุรกรรมอิเล็กทรอนิกส์ให้เหมาะสมกับการเข้าใช้บริการและหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสม

7.2 กำหนดให้ผู้ที่ได้รับมอบหมายเท่านั้นที่จะเข้าแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงต่าง ๆ ได้

7.3 บันทึกรายละเอียดการเข้าถึงระบบธุรกรรมอิเล็กทรอนิกส์ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ ไว้เพื่อเป็นหลักฐานการตรวจสอบในกรณีเกิดปัญหา

7.4 จัดให้มีวิธีการตรวจสอบตัวตนและสิทธิในการใช้บริการของผู้ใช้บริการก่อนอนุญาตให้ใช้บริการ

7.5 จัดให้มีวิธีการตรวจสอบตัวตนและป้องกันการปฏิเสธความรับผิด ให้มีความเหมาะสมกับระดับความเสี่ยง รูปแบบและมูลค่าของธุรกรรมที่ให้บริการ

7.6 จัดให้มีการควบคุมการเข้าถึงและการแก้ไขเปลี่ยนแปลงข้อมูล ในฐานข้อมูลที่จัดเก็บข้อมูลที่ใช้ในการตรวจสอบตัวตน (Authentication Database)

7.7 จัดให้มีการบันทึกรายละเอียดการเข้าทำธุรกรรมของผู้ใช้บริการ (Transaction Log) ไว้ เพื่อใช้เป็นหลักฐานการตรวจสอบ

7.8 จัดให้มีวิธีการรับส่ง ประมวลผล และจัดเก็บสารสนเทศในลักษณะ ที่ปลอดภัยตามหมวดหมู่สารสนเทศ ทั้งนี้สารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ต้องมีวิธีในการรักษาความถูกต้องเชื่อถือได้และการรักษาความลับของข้อมูล เช่น

6.8.1 เทคโนโลยีการเข้ารหัสลับสำหรับข้อมูลลับ เช่น การเข้ารหัสลับข้อมูลที่อยู่ระหว่างการรับส่งการเข้ารหัสลับข้อมูลตั้งแต่ต้นทางถึงปลายทาง (End-to-End Encryption) การเข้ารหัสลับข้อมูลในช่วงจัดเก็บ

6.8.2 การใช้ช่องทางที่มีความปลอดภัยสูงในการรับส่งข้อมูลลับ เช่น Secure Sockets Layer (SSL)

7.9 จัดให้มีการทดสอบระบบธุรกรรมอิเล็กทรอนิกส์ เพื่อหาจุดอ่อนและข้อผิดพลาด เช่น การประเมินช่องโหว่ทางเทคนิค (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Testing) อย่างน้อยปีละ 1 ครั้ง

7.10 จัดให้มีวิธีการตรวจสอบตัวตนและป้องกันการปฏิเสธความรับผิด ให้มีความเหมาะสมกับระดับความเสี่ยง รูปแบบและมูลค่าของธุรกรรม ในการทำธุรกรรมออนไลน์

10.2 ความมั่นคงปลอดภัยในกระบวนการพัฒนาและกระบวนการสนับสนุนอื่น ๆ

มาตรการ

1. เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานที่ใช้งาน ควรมีการทบทวนและทดสอบโปรแกรมประยุกต์ที่สำคัญ เพื่อให้มั่นใจว่า ไม่มีผลกระทบทางลบต่อการดำเนินงานหรือความมั่นคงปลอดภัยทางไซเบอร์

2. จำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่ซื้อมาจากผู้ผลิตให้สามารถเปลี่ยนแปลงแก้ไขได้เท่าที่จำเป็นและควรมีการควบคุมการเปลี่ยนแปลงแก้ไขทั้งหมดอย่างเข้มงวด

3. กำหนดหลักการสำหรับวิศวกรรมระบบอย่างปลอดภัย จัดทำเป็นเอกสาร ปรับปรุงให้ทันสมัย และประยุกต์ใช้กับการจัดทำระบบใด ๆ

4. จัดทำสภาพแวดล้อมที่มีการป้องกันอย่างเหมาะสมสำหรับกระบวนการพัฒนาและเชื่อมโยงระบบเพื่อให้เกิดความมั่นคงปลอดภัยตลอดวงจรชีวิตของการพัฒนาระบบ

5. ควบคุมและเฝ้าระวัง ติดตามกิจกรรมของการพัฒนาระบบที่ให้หน่วยงานอื่นดำเนินงานแทน (Outsource)

6. ทดสอบความสามารถในการรักษาความมั่นคงปลอดภัยของระบบตั้งแต่ช่วงการพัฒนา

7. สร้างแผนการทดสอบ การตรวจรับ และหลักเกณฑ์ที่เกี่ยวข้อง สำหรับระบบใหม่ และการปรับปรุงระบบ

แนวปฏิบัติสำหรับหน่วยงาน

1. ขออนุมัติการพัฒนาระบบสารสนเทศจากผู้บริหารหน่วยงานก่อนดำเนินการพัฒนาระบบ

2. ทบทวนและตรวจสอบระดับของสิทธิ (Authorization Levels) ของผู้ใช้งาน เมื่อมีการเปลี่ยนแปลงของระบบที่ใช้งานจริง ให้สอดคล้องกับระดับสิทธิที่ได้ตกลงกัน

3. ควบคุมให้มีการจัดทำเอกสารทางเทคนิค คู่มือการใช้งานระบบ หรือเอกสารที่เกี่ยวข้องสำหรับผู้ใช้งานและผู้ดูแลระบบ ภายหลังจากที่ได้พัฒนาแล้วเสร็จ ตลอดจนจัดให้มีการอบรมผู้ใช้งานตามความเหมาะสม

4. ในกรณีที่ผู้ขายหรือผู้เป็นเจ้าของผลิตภัณฑ์ให้บริการหลังการขายในการดูแลและบำรุงรักษาซอฟต์แวร์และระบบสารสนเทศ ต้องควบคุมดูแลการเข้าถึงซอฟต์แวร์และระบบสารสนเทศเพียงเท่าที่จำเป็นต่อการให้บริการหลังการขายเท่านั้น พร้อมทั้งจัดเก็บบันทึกเหตุการณ์ (Audit Log) เพื่อใช้ในการตรวจสอบ

5. ในกรณีที่ผู้ขายหรือผู้เป็นเจ้าของผลิตภัณฑ์ให้บริการหลังการขายในการดูแลและบำรุงรักษาซอฟต์แวร์และระบบสารสนเทศจากภายนอก (Remote Maintenance) ต้องกำหนดให้มีการขออนุมัติจากผู้บริหารหน่วยงานโดยระบุขอบเขต วัตถุประสงค์ และแผนงานการดูแลและบำรุงรักษาระบบจากภายนอก และประสานงานกับผู้ดูแลระบบหรือผู้ที่เกี่ยวข้องให้มีมาตรการควบคุม ดังนี้

5.1 จำกัดสิทธิการเข้าถึงเพียงเท่าที่จำเป็นต่อการให้บริการตามขอบเขตและวัตถุประสงค์ที่ระบุ

5.2 ถอดถอนสิทธิหรือเปลี่ยนแปลงรหัสผ่านทันที ภายหลังการให้บริการแล้วเสร็จหรือภายหลังที่สัญญาการให้บริการสิ้นสุด

5.3 จัดเก็บบันทึกเหตุการณ์ เพื่อใช้ในการตรวจสอบ (Audit Log) กิจกรรมของผู้ขาย

แนวปฏิบัติสำหรับผู้พัฒนาระบบ

1. ประสานงานกับเจ้าของระบบสารสนเทศ ให้มีการขออนุมัติการพัฒนาระบบจากผู้บริหารหน่วยงานก่อนดำเนินการพัฒนาระบบ

2. ประสานงานกับเจ้าของระบบสารสนเทศ ให้มีการขออนุมัติการเปลี่ยนแปลงระบบจากผู้บริหารหน่วยงานก่อนดำเนินการเปลี่ยนแปลงระบบ

3. ต้องมีการทดสอบการปรับปรุงระบบ ซึ่งรวมถึงการปรับปรุงระบบปฏิบัติการ ระบบสนับสนุนต่าง ๆก่อนดำเนินการปรับปรุงระบบที่ให้บริการ

4. ห้ามตั้งค่าปรับปรุงระบบโดยอัตโนมัติ (Auto Update) บนระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ “สูงสุด”

5. หลีกเลี่ยงการปรับแต่ง เปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่ซื้อมาจากผู้ผลิต หากจำเป็นต้องเปลี่ยนแปลงแก้ไขซอฟต์แวร์ จะต้องพิจารณาประเด็นดังต่อไปนี้

5.1 ความเสี่ยงของการควบคุมและกระบวนการความสมบูรณ์แบบ

5.2 การได้รับความยินยอมจากผู้จำหน่าย

5.3 ความเป็นไปได้ของการเปลี่ยนแปลงแก้ไข โดยปรับปรุงโปรแกรมให้ทันสมัยตามมาตรฐานจากผู้ผลิต

5.4 ผลกระทบในการบำรุงรักษาซอฟต์แวร์อันเป็นผลมาจากการเปลี่ยนแปลงแก้ไข

5.5 ความเข้ากันได้กับซอฟต์แวร์อื่น ๆ ที่ใช้งานอยู่

6. นำเทคนิควิศวกรรมความมั่นคงปลอดภัยทางไซเบอร์มาใช้ในขั้นตอนการพัฒนาระบบสารสนเทศที่มีช่องทางการรับเข้า (Input) และการส่งออก (Output) เช่น เทคนิคการพิสูจน์และยืนยันตัวตนผู้ใช้งาน การควบคุมเซสชัน (Session) การกรองข้อมูล (Sanitisation) การยืนยันความถูกต้องของข้อมูล (Data Validation) การลบชุดคำสั่งสำหรับแก้ไขข้อบกพร่อง (Debugging Code)

7. พัฒนาระบบสารสนเทศ ให้สอดคล้องกับการจัดทำขั้นตอนการพิสูจน์และยืนยันตัวตน เพื่อเข้าใช้งานระบบให้มีความปลอดภัย

8. ให้ตรวจสอบว่า การนำซอร์สโค้ดหรือซอฟต์แวร์ไลบรารี่ของผู้อื่นมาใช้งานจะไม่เป็นการละเมิดลิขสิทธิ์ของเจ้าของนั้น รวมทั้งให้ตรวจสอบด้วยโปรแกรมป้องกันโปรแกรมไม่พึงประสงค์

9. ตรวจสอบความถูกต้องของรายงานหรือข้อมูลต่าง ๆ ในระหว่างที่ทำการพัฒนาและหากพบข้อผิดพลาดให้ตรวจสอบหาสาเหตุและแก้ไข

10. ทำการทดสอบระบบบนเครื่องทดสอบที่ไม่ใช่เครื่องเซิร์ฟเวอร์สำหรับให้บริการจริง

11. จัดให้มีการทดสอบระบบ โดยผู้ใช้งานที่ต้องเกี่ยวข้องกับระบบนั้นเข้าร่วมทำการทดสอบ ก่อนโอนย้ายระบบขึ้นเครื่องที่ให้บริการจริง

10.3 ข้อมูลสำหรับการทดสอบ

มาตรการ

เลือกข้อมูลสำหรับการทดสอบอย่างระมัดระวัง มีการป้องกันและควบคุมอย่างเหมาะสม

แนวปฏิบัติสำหรับหน่วยงาน

1. จัดทำทะเบียนบันทึกเหตุการณ์ของการสำเนาข้อมูลจากระบบที่ให้บริการจริง เพื่อใช้ในการทดสอบ

2. ควบคุมดูแลสิทธิการเข้าถึงระบบสำหรับการทดสอบในระดับเดียวกับระบบที่ให้บริการจริง

แนวปฏิบัติสำหรับผู้พัฒนาระบบ

1. ประสานงานกับเจ้าของระบบสารสนเทศ เพื่อขออนุญาตในการทำสำเนาข้อมูลจากระบบที่ให้บริการจริงไปใช้ทดสอบ

2. ไม่นำข้อมูลจริง (Live Data) ที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ “สูงสุด” มาใช้ทดสอบระบบ

3. ลบข้อมูลที่ใช้ในการทดสอบทันทีภายหลังการทดสอบเสร็จสิ้น

หมวด 11 นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางการดำเนินงาน

(Information security continuity policy)

วัตถุประสงค์

เพื่อบริหารจัดการความต่อเนื่องทางการดำเนินงานและเพื่อให้มั่นใจว่าสถานที่และสิ่งอำนวยความสะดวกสำหรับการประมวลผลสารสนเทศมีความพร้อมใช้งาน ดังต่อไปนี้

11.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยทางไซเบอร์

มาตรการ

1. ต้องมีการกำหนดแนวทางในการสร้างความต่อเนื่องด้านการบริหารจัดการความมั่นคง ปลอดภัยสารสนเทศ ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ เช่น เหตุฉุกเฉิน หรือ วิกฤต
2. จัดให้ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งของกระบวนการ ในการบริหารจัดการความต่อเนื่องทางการดำเนินงานหรือ กระบวนการในการกู้คืนระบบในภาวะ วิกฤต
3. พิจารณาด้านความมั่นคงปลอดภัยสารสนเทศ ระหว่างการวางแผนความต่อเนื่องทางการดำเนินงานหรือการกู้คืนระบบในภาวะวิกฤต

11.2 การดำเนินการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

1. มีแนวทางปฏิบัติการรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ
2. มีการประเมินความเสี่ยงและการควบคุม
3. มีการวางกลยุทธ์สำหรับรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ
4. มีการพัฒนาแนวทางการรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ
5. มีการประชาสัมพันธ์และการฝึกอบรม
6. มีการทดสอบปรับปรุงแนวทางปฏิบัติรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ แนวทางปฏิบัติในการจัดทำแนวทางรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ
7. มีการเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินภารกิจและการให้บริการ
8. มีการตอบสนองต่อสถานการณ์ฉุกเฉินเพื่อควบคุมและจำกัดขอบเขตของ ความเสียหาย เช่น กำหนดแนวทางการควบคุมการแก้ไขสถานการณ์ฉุกเฉิน
9. มีการดำเนินการเพื่อให้สามารถดำเนินภารกิจได้อย่างต่อเนื่อง เช่น การสำรอง ข้อมูลและอุปกรณ์สำคัญการกู้ระบบงานและข้อมูลที่เสียหาย

10. ดำเนินการให้ระบบกลับคืนสู่การทำงานปกติ เพื่อให้ภารกิจกลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงาน ตามปกติ

11. แนวทางปฏิบัติของการเก็บรักษาข้อมูล เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลผู้ใช้งานควรปฏิบัติตามแนวปฏิบัติการสำรองข้อมูล การกู้คืนและรักษาความลับของข้อมูล

11.1 เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบซึ่งได้แก่ ข้อมูลเกี่ยวกับ ระบบปฏิบัติการ, ซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบ นั้นกำหนดจำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าว ต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้น ๆ

11.2 ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบ ต้องทำการสำรองข้อมูลของระบบทุกครั้ง

11.3 การสำรองข้อมูลควรดำเนินการสำรองกับเครื่องที่มิใช่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลัก

11.4 ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลัก และเป็นข้อมูลของระบบงานที่สำคัญจะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

11.5 ข้อมูลที่มีความสำคัญมากจะต้องทำการสำรองข้อมูลไว้ทุกวัน และข้อมูลสำรองดังกล่าวต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งหลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมี ความปลอดภัย

11.6 ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

11.7 ต้องบันทึกรายละเอียดการสำรองข้อมูล โดยมีรายละเอียดเวลาเริ่มต้นและสิ้นสุด ชื่อผู้ทำการสำรอง ข้อมูลและชนิดของข้อมูลที่บันทึก

11.8 กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล ผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

11.9 ต้องมีการสำรองข้อมูลภายนอกอาคารที่ตั้งตามความเหมาะสม เพื่อให้สามารถกู้ข้อมูลกลับคืนได้ ป้องกันระบบจากการถูกโจมตีหรือความเสียหายที่อาจเกิดขึ้น

11.10 ต้องควบคุมความปลอดภัยของข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสมเพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

11.11 ต้องจัดให้มีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ และการทดสอบควรดำเนินการบนสื่อที่จัดเตรียมไว้แยกจากสื่อที่ใช้สำหรับสำรองข้อมูลตามปกติ เพื่อป้องกันกรณีการทดสอบการกู้คืน ข้อมูลไม่สำเร็จซึ่งอาจจะทำให้ข้อมูลที่สำรองไว้เสียหายและไม่สามารถนำกลับมาใช้งานได้

11.12 ระบบข้อมูลที่สำคัญทั้งหมด ควรมีระบบการประมวลผลสำรองระบบ เครือข่ายสำรองเพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ ระบบหนึ่งไม่สามารถทำงาน ได้สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้ ภารกิจหลักดำเนินต่อไปได้

11.13 ข้อมูลที่ถูกจัดประเภทเป็นข้อมูลธรรมดาซึ่งไม่ส่งผลกระทบต่อการดำเนิน จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูล และข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ ๆ มีความปลอดภัย

11.14 การตรวจสอบสอบทาน และวัดผลความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ โดยต้องมีการสอบทานและปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่งครั้ง

หมวด 12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(Information Security Incident Management)

วัตถุประสงค์

เพื่อกำหนดวิธีการที่สอดคล้องและมีประสิทธิภาพในการบริหารจัดการสถานการณ์ความมั่นคงปลอดภัยไซเบอร์

การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัย

มาตรการ

1. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Management of Information Security Incidents and Improvements) เพื่อให้มีวิธีการที่สอดคล้อง และได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย

2. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และขั้นตอนดังกล่าวต้องมีความรวดเร็วได้ผลและมีความเป็นระบบระเบียบที่ดี

3. การรายงานเหตุการณ์น่าสงสัย / จุดอ่อนด้านความมั่นคงปลอดภัย

3.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

3.2 ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้แจ้งต่อผู้รับผิดชอบทันทีเช่น เหตุการณ์ ต่อไปนี้

3.2.1 พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อคโดยไม่ทราบสาเหตุ

3.2.2 เวลาการเข้าใช้งานระบบครั้งล่าสุดที่ผิดปกติ

3.2.3 พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จักการเปลี่ยนแปลงของค่าต่าง ๆ

3.2.4 มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

3.2.5 พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

3.2.6 พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไขหรือลบทิ้ง

3.2.7 มีความพยายามที่จะเข้าใช้ระบบบอย่างผิดวิธีไม่ว่าจะสำเร็จหรือไม่

3.2.8 การให้บริการของระบบเกิดการชะงักหรือไม่สามารถให้บริการ

3.2.9 เกิดการละเมิดสิทธิ์เข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บ ข้อมูล

3.2.10 การแก้ไขค่าความปลอดภัยในระบบเช่น Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

4. การประเมินเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ดูแลระบบต้องประเมินขอบเขต และความรุนแรงของปัญหาหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรงหรือมีผลต่อชื่อเสียงจะต้องรายงานให้ผู้บริหารทราบโดยด่วนเพื่อหาแนวทางแก้ไข และป้องกันไม่ให้เกิดในครั้งต่อไปควรมีการแบ่งประเภทของปัญหาอย่างเหมาะสม

5. การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟต์แวร์ เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและระบบทำงานบกพร่อง เช่น ไวรัสคอมพิวเตอร์ แพร่กระจาย ระบบถูกบุกรุก

6. หากผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย และ/หรือจุดอ่อน ช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และ/หรือการทำงานที่บกพร่อง หรือการทำงานผิดปกติของซอฟต์แวร์ผู้ใช้งานต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบทราบโดยเร่งด่วน

7. ในกรณีที่ไม่สามารถติดต่อผู้รับผิดชอบได้ให้รายงานกับผู้บริหารหน่วยงาน

8. ในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย ให้ปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ดังนี้

8.1 ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง มีความเสี่ยงอย่างมีนัยสำคัญ ที่ทำให้ระบบคอมพิวเตอร์หรือการให้บริการของมหาวิทยาลัยด้อยประสิทธิภาพลง

8.2 ภัยคุกคามทางไซเบอร์ระดับร้ายแรง ถูกโจมตีอย่างมีนัยสำคัญทำให้เกิดความเสียหายกับระบบคอมพิวเตอร์หรือการให้บริการของมหาวิทยาลัย จนไม่สามารถทำงานหรือให้บริการได้

8.3 ภัยคุกคามทางไซเบอร์ระดับร้ายแรงวิกฤติถูกโจมตีในระดับสูง ส่งผลกระทบรุนแรงเป็นวงกว้างทำให้ระบบคอมพิวเตอร์ หรือการให้บริการที่มหาวิทยาลัยล้มเหลว

9. การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

9.1 ต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อนช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศรวมทั้งวิธีการแก้ไข เพื่อจะได้ เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2 ระบบต้องจัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้รับทราบอย่างน้อยเดือนละ 1 ครั้ง

10. การเก็บรวบรวมหลักฐาน

10.1 ต้องกำหนดให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์ สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์สืบสวนหรือเป็นหลักฐานในกระบวนการทางศาลที่เกี่ยวข้องเมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

10.2 ส่วนงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบหรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูลและกฎหมาย เช่น 90 วัน หรือ 1 ปี

ภาคผนวก

เกณฑ์การจัดระดับการป้องกันความมั่นคงปลอดภัย

การจัดระดับการป้องกันความมั่นคงปลอดภัย ให้ประเมินในด้านความลับ (Confidential) ความสมบูรณ์ (Integrity) และการให้บริการ (Availability) ของทรัพย์สินสารสนเทศ โดยเกณฑ์ที่ได้รับสูงสุดให้ถือเป็นผลระดับการป้องกันความมั่นคงปลอดภัย

1. ข้อมูล

ระดับ	ความลับ Confidential	ความสมบูรณ์ Integrity	ความพร้อมใช้งาน Availability
สูงสุด	ข้อมูลส่วนบุคคล/ข้อมูลลับ/ข้อมูลที่เปิดเผยแล้วเป็นการผิดข้อกฎหมาย/ข้อมูลสำคัญขององค์กร	ข้อมูลห้ามแก้ไข ใช้เป็นหลักฐาน/ข้อกฎหมาย	ข้อมูลต้องมีความพร้อมใช้งานภายใน 1 ชม.
สูง	ข้อมูลที่ใช้/รับรู้เฉพาะภายในหน่วยงาน	ข้อมูลที่ต้องมีการตรวจสอบ/อนุมัติความถูกต้องของข้อมูล	ข้อมูลที่ต้องจัดเก็บเข้าระบบภายใน 7 ชม.
ปานกลาง	ข้อมูลที่ใช้/รับรู้เฉพาะภายในองค์กร	ข้อมูลที่ใช้ในการดำเนินงาน	ข้อมูลที่ต้องจัดเก็บเข้าระบบ ภายใน 24 ชม.
ต่ำ	ข้อมูลสาธารณะ ข้อมูลที่สามารถเปิดเผยได้	ข้อมูลเกี่ยวกับความรู้ความเข้าใจต่อสาธารณะ	ข้อมูลทั่วไป สามารถรอเข้าระบบได้

2. แอปพลิเคชันและซอฟต์แวร์

ระดับ	ความลับ Confidential	ความสมบูรณ์ Integrity	ความพร้อมใช้งาน Availability
สูงสุด	ซอฟต์แวร์/ระบบที่ดูแลเกี่ยวกับการเข้ารหัส หรือการพิสูจน์ตัวตน	ซอฟต์แวร์/ระบบที่รับข้อมูลแล้วห้ามมีการแก้ไขข้อมูล เช่น Log System	ซอฟต์แวร์/ระบบที่ใช้ควบคุมระบบ หรืออุปกรณ์ในการดำเนินงานหลัก
สูง	ซอฟต์แวร์/ระบบที่ใช้เฉพาะมหาวิทยาลัยเท่านั้น หรือใช้ในการดำเนินงานหลัก	ซอฟต์แวร์/ระบบที่มีการรับข้อมูล แก้ไขข้อมูล	ซอฟต์แวร์/ระบบที่ใช้ในการดำเนินงานหลัก

ระดับ	ความลับ Confidential	ความสมบูรณ์ Integrity	ความพร้อมใช้งาน Availability
ปานกลาง	ซอฟต์แวร์/ระบบที่มีการใช้งานร่วมกับหน่วยงานอื่น หรือสามารถให้หน่วยงานอื่นร่วมใช้งานได้	ซอฟต์แวร์/ระบบที่สนับสนุนการ ทำงานของระบบข้อมูล เช่น ระบบฐานข้อมูล	ซอฟต์แวร์/ระบบที่ใช้ในส่วนของการสนับสนุนการดำเนินงาน
ต่ำ	ซอฟต์แวร์ Open Source	ซอฟต์แวร์/ระบบทั่วไป หรือแสดงข้อมูลเท่านั้น ไม่มีการรับค่าข้อมูลจากผู้ใช้งาน เช่น เว็บไซต์	ซอฟต์แวร์สำนักงาน หรือซอฟต์แวร์ทั่วไป

3. ฮาร์ดแวร์

ประเมินเฉพาะด้านความสมบูรณ์เท่านั้น

ระดับ	ความสมบูรณ์ Integrity
สูงสุด	อุปกรณ์ที่ใช้ในการจัดเก็บและประมวลผลของระบบ เมื่อมีข้อผิดพลาด ส่งผลกระทบต่อการดำเนินงาน/ต่อชีวิต/ต่อทรัพย์สินอื่น ๆ
สูง	อุปกรณ์สนับสนุนการทำงานของระบบ เมื่อมีข้อผิดพลาด ส่งผลกระทบต่อการดำเนินงาน/ต่อชีวิต/ต่อทรัพย์สินอื่น ๆ เช่น อุปกรณ์เครือข่าย
ปานกลาง	อุปกรณ์สนับสนุนการทำงาน เมื่อมีข้อผิดพลาด ไม่มีผลกระทบต่อการให้บริการขององค์กร เช่น PC Notebook
ต่ำ	อุปกรณ์ทั่วไป ไม่เกี่ยวข้องกับการประมวลผลข้อมูล เช่น Printer Scanner

เกณฑ์ประเมินเหตุการณ์ภัยคุกคามทางไซเบอร์

การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ แบ่งออกเป็น 3 ระดับ ดังต่อไปนี้

1. ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ที่สำคัญของมหาวิทยาลัยหรือการให้บริการของมหาวิทยาลัยด้อยประสิทธิภาพลง

2. ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของมหาวิทยาลัยและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์ที่สำคัญหรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของมหาวิทยาลัยไม่สามารถทำงานหรือให้บริการได้

3. ภัยคุกคามทางไซเบอร์ในระดับวิกฤต

มีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศของมหาวิทยาลัย ในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของมหาวิทยาลัยหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของมหาวิทยาลัยล้มเหลวทั้งระบบ จนมหาวิทยาลัยไม่สามารถทำงาน ควบคุมการส่วนกลางของระบบคอมพิวเตอร์ของมหาวิทยาลัยได้

หัวข้อในรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

ทรัพย์สินสารสนเทศประเภทฮาร์ดแวร์ (Hardware)							
ลำดับ	ประเภทฮาร์ดแวร์	ลักษณะการใช้งาน	ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง)	ผู้รับผิดชอบ	ที่ตั้ง	วันที่เริ่มสัญญาบำรุงรักษา (วว/ดด/ปป)	หมายเหตุ

ทรัพย์สินสารสนเทศประเภทซอฟต์แวร์ (Software)										
ลำดับ	ชื่อซอฟต์แวร์	ผู้พัฒนา	จำนวนลิขสิทธิ์	ประเภทซอฟต์แวร์	รายละเอียดซอฟต์แวร์	ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง/ต่ำ)	ผู้รับผิดชอบ	ที่เก็บซอฟต์แวร์	วันที่หมดอายุทรัพย์สินซอฟต์แวร์	เลขทะเบียนทรัพย์สินซอฟต์แวร์ (ถ้ามี)

ทรัพย์สินสารสนเทศประเภทข้อมูล (Information)							
ลำดับ	ประเภทของข้อมูล	รายละเอียดของ สารสนเทศ	ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง/ต่ำ)	ผู้รับผิดชอบ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	เลขทะเบียนทรัพย์สินซอฟต์แวร์ (ใช้อ้างอิง)	หมายเหตุ

ตัวอย่างหัวข้อในรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

ทรัพย์สินสารสนเทศประเภทฮาร์ดแวร์ (Hardware)							
ลำดับ	ประเภทฮาร์ดแวร์	ลักษณะการใช้งาน	ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง/ต่ำ)	ผู้รับผิดชอบ	ที่ตั้ง	วันที่เริ่มสัญญาบำรุงรักษา (วว/ดด/ปปปป)	หมายเหตุ
1	Switch	Switch Net App Intercluster	ปานกลาง	นาย ก	Data Center ชั้น 3 Computer Center	1 เมษายน 2566	NS-OS 1.1.0.5
2	UCS Blade Server	Blade Server	สูง	นาย ก	Data Center ชั้น 3 Computer Center	1 เมษายน 2566	NS-OS 1.1.0.5

ทรัพย์สินสารสนเทศประเภทซอฟต์แวร์ (Software)										
ลำดับ	ชื่อซอฟต์แวร์	ผู้พัฒนา	จำนวนลิขสิทธิ์	ประเภทซอฟต์แวร์	รายละเอียดซอฟต์แวร์	ระดับความมั่นคงปลอดภัย	ผู้รับผิดชอบ	ที่ติดตั้งซอฟต์แวร์	วันที่ลงทะเบียน	เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (ใช้อ้างอิง)
1	VM Ware	VM Ware	1	Virtual Machine	VM Ware Management	สูง	นายก	Computer Center	1 เมษายน 2566	VM66010102

ทรัพย์สินสารสนเทศประเภทข้อมูล (Information)							
ลำดับ	ประเภทของข้อมูล	รายละเอียดของสารสนเทศ	ระดับความมั่นคงปลอดภัย (สูงสุด/สูง/ปานกลาง/ต่ำ)	ผู้รับผิดชอบ	ที่เก็บสารสนเทศ (ชื่อสถานที่)	เลขทะเบียนทรัพย์สินซอฟต์แวร์ (ใช้อ้างอิง)	หมายเหตุ
1	Infomation	ข้อมูล Log ของระบบ	สูง	CC Comcenter	Computer Center	CC ชั้น 3	851006

ตัวอย่างฟอร์มการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม

แบบฟอร์มบันทึกข้อมูลภัยคุกคาม				
ชื่อเหตุการณ์ภัยคุกคาม			**หมายเลขของเหตุการณ์ภัยคุกคาม**	
วันที่บันทึกเหตุการณ์ภัยคุกคาม			**หมายเลขของเหตุการณ์ภัยคุกคามอื่น ๆ ที่เกี่ยวข้องกับเหตุการณ์นี้**	
ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม			**ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม**	
ชื่อ-นามสกุล			**ชื่อ-นามสกุล**	
หน่วยงาน			**โทรศัพท์**	
โทรศัพท์		**อีเมล**	**อีเมล**	
วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม				
วันที่และเวลาพบเหตุการณภัยคุกคาม				
วันที่และเวลารายงานเหตุภัยคุกคาม				

รายละเอียดเหตุการณ์ภัยคุกคาม
- สิ่งที่เกิดขึ้น -เกิดขึ้นอย่างไร -ทำไมจึงเกิดขึ้น -การประเมินทรัพย์สินสารสนเทศที่เสียหาย -ผลกระทบต่อการดำเนินงาน -ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม

การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้	**การดำเนินการขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้**
ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ	**รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม**

สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม

เอกสารอ้างอิง

1. แผนการพัฒนาดิจิทัลเพื่อเป็น Smart University ของมหาวิทยาลัยมหาสารคาม ระยะ 5 ปี (พ.ศ.2565-2569)

2. แผนพัฒนาการศึกษา มหาวิทยาลัยมหาสารคาม ฉบับที่ 13 (พ.ศ. 2565-2569)

3. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

4. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2544

5. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2544

6. มาตรฐานและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ กฟผ. ฉบับที่ 3 2013

7. แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงคมนาคม พ.ศ.2562-2566

8. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy)

คำสั่งมหาวิทยาลัยมหาสารคาม

ที่ 1231 /2566

เรื่อง แต่งตั้งคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคาม

เพื่อให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยมหาสารคามเป็นไปด้วยความเรียบร้อย เพื่อรองรับกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และให้สอดคล้องกับการดำเนินงานตามแผนการพัฒนาดิจิทัลเพื่อเป็น Smart University ของมหาวิทยาลัยมหาสารคาม ระยะ 5 ปี (พ.ศ. 2565-2569) อาศัยอำนาจตามความในมาตรา 17 และมาตรา 20 (1) แห่งพระราชบัญญัติมหาวิทยาลัยมหาสารคาม พ.ศ. 2537 จึงแต่งตั้งคณะกรรมการดำเนินงานการจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 ดังรายชื่อต่อไปนี้

1. คณะกรรมการฝ่ายอำนวยการ

1.1 อธิการบดีมหาวิทยาลัยมหาสารคาม	ประธานกรรมการ
1.2 รองอธิการบดีฝ่ายบริหารและพัฒนาศักยภาพองค์กร	กรรมการ
1.3 รองอธิการบดีฝ่ายพัฒนาโครงสร้างพื้นฐาน วิจัย และนวัตกรรม	กรรมการ
1.4 รองอธิการบดีฝ่ายแผนงานและพัฒนาองค์กรดิจิทัล	กรรมการ
1.5 รองอธิการบดีฝ่ายการคลังและพัสดุ	กรรมการ
1.6 คณบดีคณะแพทยศาสตร์	กรรมการ
1.7 คณบดีคณะวิศวกรรมศาสตร์	กรรมการ
1.8 คณบดีคณะวิทยาศาสตร์	กรรมการ
1.9 คณบดีคณะศึกษาศาสตร์	กรรมการ
1.10 รองศาสตราจารย์สุชาติ คุ้มมะณี	กรรมการ
1.11 รองศาสตราจารย์พยุง มีสัจ	กรรมการ
1.12 ผู้ช่วยศาสตราจารย์มณีรัตน์ วงษ์ชิ้ม	กรรมการ
1.13 ผู้ช่วยศาสตราจารย์อนัตต์ เจ่าสกุล	กรรมการ
1.14 ผู้อำนวยการสำนักคอมพิวเตอร์	กรรมการและเลขานุการ
1.15 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายพัฒนาระบบนวัตกรรมดิจิทัล	กรรมการและผู้ช่วยเลขานุการ
1.16 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้	กรรมการและผู้ช่วยเลขานุการ

หน้าที่.../2

หน้าที่รับผิดชอบ

กำกับดูแล ให้คำปรึกษาในการดำเนินงานตามแผนปฏิบัติการด้านความมั่นคงปลอดภัยทางไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ

2. คณะกรรมการฝ่ายดำเนินงาน

2.1 ผู้อำนวยการสำนักคอมพิวเตอร์	ประธานกรรมการ
2.2 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายพัฒนาระบบนวัตกรรมดิจิทัล	รองประธานกรรมการ
2.3 รองผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้	รองประธานกรรมการ
2.4 ผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย	กรรมการ
2.5 ผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายนโยบายและแผนพัฒนาดิจิทัล	กรรมการ
2.6 รองศาสตราจารย์สุชาติ คุ้มมะณี	กรรมการ
2.7 อาจารย์สมโภช ทองน้ำเที่ยง	กรรมการ
2.8 อาจารย์อิทธิพล เอี่ยมภูงา	กรรมการ
2.9 นางสิริวรรณ ดติยรัตน์	กรรมการ
2.10 นายสิทธิ์ เอมดี	กรรมการ
2.11 นายวงศวัฒน์ เทพาศักดิ์	กรรมการ
2.12 นางสาวสุกัญญา สิดวัน	กรรมการ
2.13 นายสุรเชษฐ์ ตั้งทรัพย์สกุล	กรรมการ
2.14 นายวีระศักดิ์ ศรีวงยาง	กรรมการ
2.15 ผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์ ฝ่ายพัฒนาระบบดิจิทัลและถ่ายทอดเทคโนโลยี	กรรมการและเลขานุการ

หน้าที่รับผิดชอบ

1. ตรวจสอบและให้คำแนะนำในการดำเนินการตามแผนปฏิบัติการด้านความมั่นคงไซเบอร์ มหาวิทยาลัยมหาสารคาม พ.ศ. 2566-2569 กับหน่วยงานภายในมหาวิทยาลัย
2. ป้องกันและแก้ไขปัญหาด้านความมั่นคงไซเบอร์ ให้กับหน่วยงานภายในมหาวิทยาลัยมหาสารคาม
3. เผยแพร่องค์ความรู้ด้านความมั่นคงไซเบอร์ให้กับบุคลากรและนิสิต มหาวิทยาลัยมหาสารคาม
4. สร้างความตระหนักรู้ด้านความมั่นคงไซเบอร์ให้กับบุคลากรและนิสิต มหาวิทยาลัยมหาสารคาม

ทั้งนี้.../3

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ 12 พฤษภาคม พ.ศ. 2566

(รองศาสตราจารย์ประยุกต์ ศรีวิไล)
อธิการบดีมหาวิทยาลัยมหาสารคาม

ผู้จัดทำ

นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Policy)

ที่ปรึกษา

รองศาสตราจารย์ ดร.ประยุกต์ ศรีวิไล	อธิการบดีมหาวิทยาลัยมหาสารคาม
ผู้ช่วยศาสตราจารย์ ดร.จรวย สาวิถี	ผู้อำนวยการสำนักคอมพิวเตอร์
อาจารย์ ดร.ณัฐกานต์ ชุติมารังสรรค์	รองผู้อำนวยการฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้
อาจารย์ ดร.สมหมาย ขันทอง	รองผู้อำนวยการฝ่ายพัฒนาระบบนวัตกรรมดิจิทัล
นางสาวพัตชบูล กิ่งพุ่ม	หัวหน้าสำนักงานเลขานุการ

ผู้จัดทำ

อาจารย์ ดร.ณัฐกานต์ ชุติมารังสรรค์	รองผู้อำนวยการฝ่ายบริการวิชาการและนวัตกรรมการเรียนรู้
นางสิรีวรรณ ตติยรัตน์	หัวหน้ากลุ่มงานบริหาร

ออกแบบปก

นางสาวพรพรรณ โตจำเริญ

ปีที่พิมพ์

ธันวาคม 2566 จำนวน 40 เล่ม

นโยบายและแนวปฏิบัติ ความมั่นคงปลอดภัยทางไซเบอร์

มหาวิทยาลัยมหาสารคาม

Cybersecurity Policy