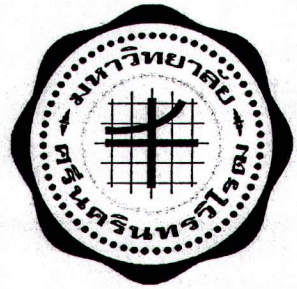

นโยบายความมั่นคงปลอดภัยของสารสนเทศ

มหาวิทยาลัยศรีนครินทรวิโรฒ

พ.ศ. 2557

ข้อมูลเอกสาร

ชื่อเอกสาร:	นโยบายความมั่นคงปลอดภัยของสารสนเทศ
Document Title:	Information Security Policy
รหัสเอกสาร	PolSM01v1-2

ประวัติเอกสาร

รุ่นเอกสาร	ลงวันที่	ประวัติการเปลี่ยนแปลง	หน่วยงานเจ้าของเอกสาร
V1.0	2554		มหาวิทยาลัยศรีนครินทรวิโรฒ

ผู้รับผิดชอบการดำเนินการ

การดำเนินการ	ผู้รับผิดชอบ	ข้อมูลการติดต่อ
▪ การประกาศใช้:	อธิการบดี/ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง	
▪ การจัดทำเอกสาร:	สำนักคอมพิวเตอร์	มหัทธวัฒน์ รักษาเกียรติศักดิ์ โทร 1-7998
▪ การทบทวนเอกสาร	คณะกรรมการบริหารความมั่นคงปลอดภัยของสารสนเทศ	มหัทธวัฒน์ รักษาเกียรติศักดิ์ โทร 1-7998

การเผยแพร่:

ช่องทาง	วันที่	คำอธิบาย
▪ เว็บไซต์:		http://secure.swu.ac.th
▪ หนังสือเวียน:		
▪ เอกสาร/เผยแพร่:		
▪ การอบรม:		
▪ อื่น ๆ		

เอกสารที่เกี่ยวข้อง

▪ เอกสารภายใน:	
▪ เอกสารภายนอก:	พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประวัติการทบทวน

รหัสเอกสาร	วันที่	ผู้จัดทำ/ผู้ทบทวน	คำอธิบาย
PolSM01v0-0			ร่างฉบับแรก
PolSM01v1-0		ISMC	ปรับปรุงตามข้อเสนอแนะ และเสนอที่ประชุมผู้บริหาร
PolSM01v1-1			o ปรับรูปแบบการเขียน เพิ่มเติมคำนิยาม จัดประเด็นเป็นหมวด o เพิ่ม 3 ประเด็น คือ การจัดการสินทรัพย์สารสนเทศ ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร และการปฏิบัติตามข้อกำหนด
PolSM01v1-2		ISBT	o ปรับปรุงตามข้อเสนอแนะที่ประชุม ISMC – 21 ก.พ. 2556

ISMC - คณะกรรมการบริหารความมั่นคงปลอดภัยของสารสนเทศ

ISBT - คณะทำงานจัดทำแนวปฏิบัติที่ดีการบริหารความมั่นคงปลอดภัยของสารสนเทศ

นโยบายความมั่นคงปลอดภัยของสารสนเทศ
มหาวิทยาลัยศรีนครินทรวิโรฒ

มหาวิทยาลัยศรีนครินทรวิโรฒ ตระหนักถึงความสำคัญของสารสนเทศซึ่งนับเป็นสินทรัพย์ที่มีคุณค่าสูงสุดขององค์กร มหาวิทยาลัยจึงได้จัดทำนโยบายความมั่นคงปลอดภัยของสารสนเทศขึ้น เพื่อให้มั่นใจว่าสารสนเทศรวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยมีการดูแลด้านการบริหารจัดการอย่างมีประสิทธิภาพ ถูกต้องตามหลักมาตรฐานสากล และมีการใช้งานอย่างเหมาะสมและปลอดภัย โดยให้ครอบคลุมด้านการรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ

วัตถุประสงค์ของการกำหนดนโยบาย

นโยบายความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยศรีนครินทรวิโรฒได้กำหนดขึ้นโดยมีวัตถุประสงค์ดังต่อไปนี้

1.1. เพื่อให้มีนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยศรีนครินทรวิโรฒ ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

1.2. เพื่อเป็นกรอบและแนวปฏิบัติในการกำหนดมาตรฐาน ขั้นตอนการปฏิบัติงาน ผู้รับผิดชอบ รวมถึงสิ่งอำนวยความสะดวกด้านคอมพิวเตอร์สำหรับการติดตั้งและใช้งานระบบเพื่อการรักษาความมั่นคงปลอดภัยของสารสนเทศ

1.3. เพื่อกำหนดให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ มีแผนเตรียมความพร้อมสำหรับกรณีฉุกเฉิน และให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยสามารถใช้งานได้เป็นปกติอย่างต่อเนื่อง เหมาะสมและสอดคล้องตามภารกิจ

1.4. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

1.5. เพื่อส่งเสริมให้มีการเผยแพร่ความรู้แก่นิสิต และบุคลากรของมหาวิทยาลัยศรีนครินทรวิโรฒ รวมถึงบุคคลที่เกี่ยวข้อง เพื่อสร้างความเข้าใจ ให้เกิดความตระหนัก และมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

องค์ประกอบของนโยบาย

นโยบายนี้จัดทำขึ้นโดยอาศัยกรอบตามมาตรฐานสากลด้านความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 รวมทั้งข้อกำหนดตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาสินทรัพย์ด้านสารสนเทศของมหาวิทยาลัยจากภาวะคุกคามทุกประเภทที่อาจจะเกิดขึ้นทั้งจากภายในและภายนอกมหาวิทยาลัย โดยเจตนาหรือโดยรู้เท่าไม่ถึงการณ์ ซึ่งเป็นแนวนโยบายในภาพรวมเพื่อการจัดการด้านการบริหารความมั่นคงปลอดภัยของสารสนเทศ โดยจัดแบ่งสาระสำคัญออกเป็น 11 หมวด ประกอบด้วย

หมวด 1 นโยบายความมั่นคงปลอดภัย
หมวด 2 โครงสร้างการบริหารความมั่นคงปลอดภัยสารสนเทศและความรับผิดชอบ
หมวด 3 การจัดการสินทรัพย์สารสนเทศ
หมวด 4 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร
หมวด 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
หมวด 6 การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ
หมวด 7 การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย
หมวด 8 การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ
หมวด 9 การดำเนินการกับเหตุการณ์ด้านความมั่นคงปลอดภัย
หมวด 10 การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย
หมวด 11 การปฏิบัติตามข้อกำหนด

คำนิยาม

สารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้

ข้อมูล หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

เทคโนโลยีสารสนเทศและการสื่อสาร (Information and communication technology) หมายถึง เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ 3 ส่วนคือ คอมพิวเตอร์ การสื่อสารและสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบงาน หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบงานบุคคล ระบบจัดเก็บเอกสาร

ระบบปฏิบัติการ (operating system) หมายถึง ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์

ระบบเครือข่าย (network) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยศรีนครินทรวิโรฒ

เครื่องคอมพิวเตอร์แม่ข่าย (server) หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์ สำหรับให้บริการแก่เครื่องคอมพิวเตอร์ อื่น ๆ หรือควบคุมการทำงานในเครือข่าย

สินทรัพย์ (asset) หมายถึง เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย ข้อมูลและระบบสารสนเทศต่างๆที่มหาวิทยาลัยพัฒนาหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

ความมั่นคงปลอดภัยของสารสนเทศ (information security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (reliability)

ความลับ (confidentiality) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

ความถูกต้องครบถ้วน (integrity) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

สภาพพร้อมใช้งาน (availability) หมายถึง การรับรองได้ว่าข้อมูล หรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ความเสี่ยง หมายถึง โอกาสของสินทรัพย์สารสนเทศในการถูกละเมิดการรักษาความปลอดภัย

ช่องโหว่ (vulnerability) หมายถึง จุดอ่อนของระบบสารสนเทศที่ทำให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบทำให้ประสิทธิภาพของการทำงานลดลง

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (access control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

การเข้าถึงจากระยะไกล (remote access) หมายถึง การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสาร หรือสื่อสัญญาณอื่น ๆ อาทิ โมเด็ม (modem) วีพีเอ็น (VPN หรือ Virtual Private Network)

ผู้ใช้งาน หมายถึง นิสิตและบุคลากรของมหาวิทยาลัยศรีนครินทรวิโรฒที่ได้รับสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย รวมถึงบุคคลจากหน่วยงานภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานสารสนเทศของมหาวิทยาลัย

บัวศรีไอดี (Buasri ID) หมายถึง ชื่อและรหัสบัญชีผู้ใช้งานเพื่อใช้ในการพิสูจน์ตัวตนก่อนการเข้าใช้เครือข่ายและบริการระบบสารสนเทศของมหาวิทยาลัย

รหัสผ่าน (password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

มหาวิทยาลัย หมายถึง มหาวิทยาลัยศรีนครินทรวิโรฒ

หน่วยงาน หมายถึง คณะ/สถาบัน/สำนัก/ศูนย์ ซึ่งเป็นส่วนงานตามโครงสร้างของมหาวิทยาลัยศรีนครินทรวิโรฒ

หน่วยงานภายนอก หมายถึง องค์กรซึ่งมหาวิทยาลัยศรีนครินทรวิโรฒอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูลหรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัย โดยจะได้รับสิทธิตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของมหาวิทยาลัยโดยมิได้รับอนุญาต

หมวด 1
นโยบายความมั่นคงปลอดภัย

1.1 วัตถุประสงค์

นโยบายความมั่นคงปลอดภัย (Security policy) กำหนดขึ้นเพื่อใช้เป็นกรอบและทิศทางในการสนับสนุนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศของมหาวิทยาลัยศรีนครินทรวิโรฒ เพื่อให้เกิดการดำเนินการตามมาตรฐานระดับสากล และเพื่อให้เป็นไปตาม หรือ สอดคล้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

1.2 ข้อกำหนดตามกฎหมาย

ความมั่นคงปลอดภัยด้านสารสนเทศบางประเด็นอาจจะเกี่ยวข้องกับกฎหมายที่ได้มีบัญญัติ มีประกาศและมีผลบังคับใช้ อาทิ

(1) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

(2) กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(3) กฎหมายลิขสิทธิ์

1.3 มาตรฐานระดับสากล

มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 จัดเป็นมาตรฐานที่ได้รับการยอมรับจากหลายประเทศในการนำไปใช้บริหารจัดการระบบสารสนเทศขององค์กร และเป็นมาตรฐานที่ถูกใช้เป็นพื้นฐานและอ้างอิงในประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

1.4 ผู้ได้รับผลกระทบจากนโยบาย

นโยบายนี้มีผลบังคับใช้กับนิสิตและบุคลากรทุกคนในมหาวิทยาลัย รวมถึงผู้รับสัญญา และผู้เยี่ยมเยือนซึ่งแม้จะมิได้รับการว่าจ้างจากมหาวิทยาลัย แต่มีส่วนเกี่ยวข้องกับการทำงาน หรือ สามารถเข้าถึงสารสนเทศของมหาวิทยาลัย

1.5 การใช้งานที่ยอมรับได้

มหาวิทยาลัยจัดให้บริการสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการใช้ประโยชน์ตามวัตถุประสงค์ของกิจกรรมตามภารกิจของมหาวิทยาลัย อาทิ

(1) การเรียนการสอน

(2) การวิจัย

(3) การบริหารงานตามภารกิจของมหาวิทยาลัย

(4) การปฏิบัติงานตามภารกิจของมหาวิทยาลัย

(5) การพัฒนาการเรียนรู้ส่วนบุคคล

(6) การให้คำแนะนำปรึกษาซึ่งเป็นงานตามข้อสัญญาหรือข้อตกลงกับมหาวิทยาลัย

(7) การติดต่อสื่อสารตามวัตถุประสงค์ดังกล่าวข้างต้น

การใช้งานสารสนเทศ รวมถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารตามกิจกรรมดังกล่าวข้างต้นต้องเป็นไปอย่างเหมาะสมโดยอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของบุคคลอื่น เคารพและปฏิบัติอย่างถูกต้องตามกฎหมาย และต้องไม่เกี่ยวข้องกับการดำเนินธุรกิจการค้าใด ๆ

1.6 พื้นที่ที่มีผลบังคับใช้

นโยบายนี้มีผลบังคับใช้กับทุกตำแหน่งพื้นที่ที่สามารถเข้าถึงสารสนเทศและเครือข่ายสารสนเทศของมหาวิทยาลัยได้ ซึ่งรวมถึงการเรียกใช้งานจากทางบ้าน หรือ การเข้าถึงจากระยะไกล และการเชื่อมโยงจากองค์กรภายนอก การอนุญาตและมอบหมายสิทธิในการเข้าถึงทุกระบบของมหาวิทยาลัย ไม่ว่าจะเป็นสารสนเทศด้านวิชาการและด้านการบริหาร มหาวิทยาลัยต้องมั่นใจว่าได้มีการดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยของสารสนเทศและได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจจะเกิดขึ้น

1.7 การตรวจสอบและทบทวน

มหาวิทยาลัยต้องกำหนดให้มีผู้บริหารระดับสูงทำหน้าที่กำกับดูแลนโยบายและรับผิดชอบในการตรวจสอบการดำเนินงานตามนโยบายความมั่นคงปลอดภัยของสารสนเทศอย่างสม่ำเสมอและทันเหตุการณ์ โดยให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีเหตุการณ์แปรเปลี่ยนที่สำคัญ มหาวิทยาลัยต้องติดตามเพื่อให้มั่นใจว่านโยบายเหล่านี้มีความเหมาะสมเพื่อปกป้องผลประโยชน์ของมหาวิทยาลัย

หมวด 2
โครงสร้างการบริหารความมั่นคงปลอดภัยของสารสนเทศ

2.1 วัตถุประสงค์

โครงสร้างการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Organization of Information Security) กำหนดขึ้นเพื่อให้การบริหารและการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับสารสนเทศของมหาวิทยาลัยดำเนินการได้อย่างชัดเจน และเพื่อให้มั่นใจว่านิสิตและบุคลากรของมหาวิทยาลัยทุกคนได้ตระหนักถึงความสำคัญในเรื่องความมั่นคงปลอดภัยของสารสนเทศ มีความรู้ความเข้าใจ และมีความรับผิดชอบตามภาระหน้าที่ และร่วมกันในการจำกัดภาวะความเสี่ยงและภัยคุกคามซึ่งมีแนวโน้มของความซับซ้อนและความรุนแรงเพิ่มมากขึ้น

2.2 วิธีการและความรับผิดชอบ

การบริหารความมั่นคงปลอดภัยของสารสนเทศเริ่มต้นจากกระบวนการประเมินความเสี่ยง การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของมหาวิทยาลัย การสร้างมาตรการและข้อกำหนด โดยให้ความสำคัญกับการให้ความรู้และการฝึกทักษะให้แก่นิสิตและบุคลากรเพื่อให้สามารถใช้สารสนเทศ รวมถึงเทคโนโลยีสารสนเทศของมหาวิทยาลัยได้อย่างเหมาะสม มีการติดตามตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อค้นหาช่องโหว่ หรือจุดอ่อน รวมทั้งให้มีการกำหนดแนวทางในการรับมือกับภัยคุกคามที่อาจจะเกิดขึ้นได้อย่างเป็นระบบและมีประสิทธิภาพ โดยดำเนินการอย่างครบวงจรตามวิธีการของการวางแผน/ปฏิบัติ/ตรวจประเมิน/พัฒนา และยึดหลักตามมาตรฐานความมั่นคงปลอดภัยของสารสนเทศ

มหาวิทยาลัยจึงจำเป็นต้องมีการกำหนดแนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศ โดยให้มีการจัดทำนโยบายและแนวปฏิบัติ กำกับให้มีการดำเนินการตามข้อกำหนด มีการตรวจสอบและวิเคราะห์ความเสี่ยงอย่างสม่ำเสมอ เพื่อนำมาใช้ในการปรับปรุงนโยบายและแนวปฏิบัติของมหาวิทยาลัยให้สามารถรองรับการเปลี่ยนแปลงของภัยคุกคามที่อาจจะเกิดขึ้น มหาวิทยาลัยต้องดำเนินการรักษาความมั่นคงปลอดภัยอย่างสมเหตุสมผล โดยยึดแนวทางการสร้างความสมดุล ระหว่างความคล่องตัวกับความมั่นคงปลอดภัยของระบบ และค่าใช้จ่ายที่จะเกิดขึ้น

2.3 ผู้รับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

2.3.1 ระดับมหาวิทยาลัย

ผู้บริหารระดับสูงเป็นผู้รับผิดชอบการบริหารจัดการและกำกับดูแลภาพรวมของความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย และได้มีการแต่งตั้งคณะกรรมการบริหารความมั่นคงปลอดภัยทำหน้าที่รับผิดชอบในส่วนของนโยบายการรักษาความมั่นคงปลอดภัย แต่ทั้งนี้ คณะ/สถาบัน/สำนัก ที่เป็นเจ้าของข้อมูลที่อยู่ในระบบส่วนกลางและในระบบที่สร้างขึ้นเอง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย

2.3.2 ระดับคณะ/สถาบัน/สำนัก

คณะ/สถาบัน/สำนัก ต้องกำหนดให้ผู้บริหารหรือเจ้าหน้าที่ประจำของหน่วยงานทำหน้าที่ในฐานะเจ้าของข้อมูลและเป็นผู้รับผิดชอบในการประสานความร่วมมือและกำกับดูแลให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย

2.4 ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

2.4.1 สำหรับผู้บริหาร

ผู้บริหารของทุกหน่วยงานต้องกำกับดูแลให้นิสิตและบุคลากรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย

2.4.2 สำหรับนิสิตและบุคลากร

นิสิตและบุคลากรทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย และต้องรายงานต่อมหาวิทยาลัย หากพบปัญหาหรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ

2.4.3 สำหรับผู้พัฒนาและผู้ดูแลระบบ

ผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของมหาวิทยาลัยต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรการด้านความมั่นคงปลอดภัยของระบบต้องผ่านการพิจารณาและได้รับคำแนะนำจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

ผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของมหาวิทยาลัยต้องมีภาระงานและความรับผิดชอบในเรื่องความมั่นคงปลอดภัยของสารสนเทศ ทั้งด้านเทคนิค การตรวจสอบ การเฝ้าระวัง และการประเมินและรายงานความเสี่ยงต่อมหาวิทยาลัย

2.4.4 สำหรับบุคคลภายนอก

บุคคลภายนอก หรือ บุคลากรของหน่วยงานภายนอกที่มหาวิทยาลัยอนุญาตให้มีสิทธิในการเข้าถึง หรือใช้ข้อมูลหรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัย ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย ใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการไม่เปิดเผยความลับของมหาวิทยาลัยโดยมิได้รับอนุญาต

หมวด 3
การจัดการสินทรัพย์สารสนเทศ

3.1 วัตถุประสงค์

การจัดการสินทรัพย์สารสนเทศ (Information Asset Management) กำหนดขึ้นเพื่อป้องกันสินทรัพย์สารสนเทศของมหาวิทยาลัยให้เกิดความมั่นคงปลอดภัย และสามารถใช้งานสินทรัพย์เหล่านั้นได้อย่างเหมาะสม

3.2 หน้าที่ความรับผิดชอบต่อสินทรัพย์สารสนเทศ

มหาวิทยาลัยต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำบัญชีสินทรัพย์สารสนเทศ และปรับปรุงข้อมูลให้ถูกต้องอยู่เสมอ โดยให้ความสำคัญกับสินทรัพย์ที่มีผลต่อการดำเนินภารกิจของมหาวิทยาลัย ซึ่งจำแนกเป็น 5 กลุ่ม ได้แก่ (1) ข้อมูลสารสนเทศ (2) บริการและกระบวนการ (3) ฮาร์ดแวร์ (4) ซอฟต์แวร์ และ (5) บุคลากร

มหาวิทยาลัยต้องจัดทำกฎ ระเบียบ หรือ หลักเกณฑ์ในการใช้สินทรัพย์อย่างเป็นลายลักษณ์อักษรเพื่อให้เกิดการใช้งานได้อย่างเหมาะสม และเพื่อป้องกันความเสียหายต่อสินทรัพย์เหล่านั้น

3.3 การจัดหมวดหมู่สารสนเทศ

มหาวิทยาลัยต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของสินทรัพย์สารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อมหาวิทยาลัย ทั้งนี้เพื่อให้สามารถกำหนดวิธีการในการป้องกันได้อย่างเหมาะสม รวมทั้งจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการสินทรัพย์สารสนเทศตามหมวดหมู่ที่กำหนดไว้

หมวด 4
ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

4.1 วัตถุประสงค์

ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (Human Resources Security) เป็นหมวดที่กำหนดขึ้นเพื่อให้บุคลากรของมหาวิทยาลัย และบุคลากรของผู้รับสัญญาว่าจ้างจากมหาวิทยาลัยได้เข้าใจในบทบาทและหน้าที่ความรับผิดชอบ

ของตน เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง รวมทั้งการใช้สารสนเทศ รวมถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างไม่ถูกต้อง หรือผิดวัตถุประสงค์

4.2 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน

มหาวิทยาลัยต้องกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นลายลักษณ์อักษร และต้องมีการตรวจสอบคุณสมบัติของผู้สมัคร โดยพิจารณาจากจดหมายรับรอง ประวัติการทำงาน เป็นต้น นอกจากนั้นต้องมีการระบุเงื่อนไขการจ้างงานซึ่งรวมถึงความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

4.3 การสร้างความมั่นคงปลอดภัยระหว่างการจ้างงาน

บุคลากร หรือ ผู้ได้รับการว่าจ้างต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของมหาวิทยาลัย โดยต้องมีการให้ความรู้ และฝึกอบรมด้านความปลอดภัยให้แก่บุคลากร ในกรณีที่มีการกระทำความผิดต้องมีกระบวนการสอบสวนและลงโทษตามระเบียบของมหาวิทยาลัย

4.4 การสิ้นสุดหรือการเปลี่ยนการจ้าง

เมื่อสิ้นสุดการเป็นบุคลากร หรือ การเปลี่ยนสัญญาการจ้างงานต้องมีการคืนสินทรัพย์ของมหาวิทยาลัย และถอดถอนสิทธิในการเข้าถึงระบบสารสนเทศของบุคคลนั้น

หมวด 5
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

5.1 วัตถุประสงค์

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) เป็นหมวดที่กำหนดขึ้นเพื่อป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต ป้องกันความเสียหายและการคุกคามสินทรัพย์สารสนเทศของมหาวิทยาลัย

5.2 การรักษาความปลอดภัยทางกายภาพ

มหาวิทยาลัยต้องกำหนดรายละเอียดของสถานที่และอุปกรณ์ที่จำเป็นต้องมีระบบการป้องกันการเสียหาย และการควบคุมการเข้าออกในการรักษาความมั่นคงปลอดภัย อาทิ ห้องคอมพิวเตอร์กลางของมหาวิทยาลัยซึ่งเป็นพื้นที่จัดเก็บเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ด้านเครือข่าย ต้องมีระบบรักษาความปลอดภัยและมีการควบคุมการเข้าถึงอย่างเข้มงวด โดยอนุญาตเฉพาะผู้รับผิดชอบเท่านั้น

5.3 การควบคุมการเข้าถึงอุปกรณ์

อุปกรณ์ทุกชนิดต้องกำหนดให้มีผู้รับผิดชอบโดยตรง และผู้รับผิดชอบเท่านั้นที่ได้รับสิทธิในการเข้าถึง โดยต้องจัดให้มีระบบสำหรับจัดเก็บข้อมูลการเข้าถึงเพื่อใช้เป็นหลักฐานในการตรวจสอบ

5.4 การรักษาความปลอดภัยของอุปกรณ์

อุปกรณ์สำคัญที่ถูกจัดเก็บในห้องคอมพิวเตอร์กลาง ต้องมีการจัดวางอย่างถูกต้องและมีการป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต การเดินสายเพื่อเชื่อมโยงระหว่างอุปกรณ์ต้องมีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่อกับอุปกรณ์ และมีการกำหนดแผนการบำรุงรักษาอุปกรณ์อย่างชัดเจนและต่อเนื่อง

5.5 การนำอุปกรณ์ออกนอกหน่วยงาน

การนำอุปกรณ์ทุกชิ้นออกนอกหน่วยงาน ต้องปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยของหน่วยงาน และต้องจัดให้มีการตรวจสอบอย่างเคร่งครัด

หมวด 6
การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ

6.1 วัตถุประสงค์

การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ (Communication and Operations Management) เป็นหมวดที่กำหนดขึ้นเพื่อให้การดำเนินงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านสารสนเทศ และอุปกรณ์ประมวลผลมีความถูกต้อง เหมาะสม และปลอดภัย ในแต่ละขั้นตอนของการปฏิบัติงานต้องมีการบันทึกและจัดเก็บเป็นลายลักษณ์อักษรเพื่อประโยชน์สำหรับการกู้คืนข้อมูลในกรณีที่เกิดความเสียหาย

6.2 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน

โครงสร้างพื้นฐานและสารสนเทศทุกระบบต้องมีผู้รับผิดชอบ มีเอกสารขั้นตอนในการปฏิบัติงานที่ได้บันทึกไว้เป็นลายลักษณ์อักษร ในกรณีมีการเปลี่ยนแปลงข้อมูล หรือ การปรับเปลี่ยนเวอร์ชันของระบบ หรือโปรแกรมภายใน ต้องมีการบันทึกเพื่อให้มั่นใจว่าจัดการกับปัญหาที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นได้ และสามารถกลับคืนสู่สถานะเดิมได้หากแก้ไขไม่สำเร็จ

6.3 การรับบริการจากหน่วยงานภายนอก

ในการรับบริการจากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงาน มีการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอ รวมถึงกำหนดแนวทางการบริหารจัดการ ในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อมหาวิทยาลัย

6.4 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ

มหาวิทยาลัยต้องจัดให้มีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถ ตรวจรับทรัพยากรสารสนเทศตามหลักเกณฑ์กลางที่มหาวิทยาลัยประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้มั่นใจว่าสามารถใช้งานได้ตามข้อกำหนด

6.5 การป้องกันโปรแกรมที่ไม่ประสงค์ดี

มหาวิทยาลัยต้องจัดให้มีการติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งโปรแกรมเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงาน หรือ อุปกรณ์หลักของมหาวิทยาลัย และกำหนดให้มีระเบียบและขั้นตอนวิธีปฏิบัติที่เหมาะสม และสนับสนุนให้หน่วยงานภายในที่มีการใช้งานระบบผ่านเครือข่ายของมหาวิทยาลัยได้ยึดถือและปฏิบัติตาม

6.6 การสำรองข้อมูล

มหาวิทยาลัยต้องจัดให้มีการสำรองข้อมูลที่สำคัญ โดยต้องกำหนดรูปแบบและวิธีปฏิบัติ รวมทั้งแผนการสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของสารสนเทศของมหาวิทยาลัยเพื่อป้องกันการสูญหายอันอาจจะเกิดขึ้นจากภาวะคุกคาม หรือ จากการเกิดภัยพิบัติ โดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบและแผนการดำเนินการที่กำหนดไว้

6.7 **การเฝ้าระวังด้านความมั่นคงปลอดภัย**

มหาวิทยาลัยต้องมีการเฝ้าระวังระบบที่สำคัญ เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ ต้องให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับข้อกำหนดตามพระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ และต้องกำหนดขั้นตอนวิธีปฏิบัติในการติดตั้งเวลาของระบบคอมพิวเตอร์กลางให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ของมหาวิทยาลัย

หมวด 7
การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย

7.1 **วัตถุประสงค์**

การควบคุมการเข้าถึง (Access Control) เป็นหมวดที่กำหนดขึ้นเพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยจำเป็นต้องมีการกำหนดนโยบายการเข้าถึงระบบ การบริหารการจัดการเข้าถึงของผู้ใช้ และการควบคุมการเข้าถึงเครือข่าย

7.2 **การควบคุมการเข้าถึงระบบ**

มหาวิทยาลัยต้องมีนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร และทบทวนตามระยะเวลาที่กำหนดไว้ โดยพิจารณาให้สอดคล้องกับภารกิจของมหาวิทยาลัย และความมั่นคงปลอดภัยในการเข้าถึงสินทรัพย์สารสนเทศ

7.3 **การจัดการการเข้าถึงของผู้ใช้**

มหาวิทยาลัยต้องมีการกำหนดมาตรการและแนวปฏิบัติอย่างเป็นระบบเพื่อใช้ในการกำหนดรหัสบัญชีผู้ใช้สำหรับนิสิตและบุคลากร การจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ การจัดการรหัสผ่าน รวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้

7.4 **หน้าที่ความรับผิดชอบของผู้ใช้งาน**

เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามมาตรการด้านการรักษาความปลอดภัยในการเข้าถึงอย่างเคร่งครัด เช่น ไม่กำหนดรหัสผ่านแบบที่ไม่ปลอดภัย ไม่เปิดเผยรหัสผ่านให้ผู้อื่นล่วงรู้ เป็นต้น

7.5 **การควบคุมการเข้าถึงเครือข่าย**

การเข้าถึงเครือข่ายจากภายในมหาวิทยาลัย หรือ การเชื่อมต่อจากภายนอกต้องมีมาตรการควบคุมที่ชัดเจน ต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบต้องยอมให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตผ่านเข้าสู่เครือข่าย และใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

7.6 **การควบคุมการใช้งานระบบปฏิบัติการ**

การเข้าถึงระบบปฏิบัติการต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิ และมีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

7.7 การควบคุมการใช้งานระบบสารสนเทศ

การเข้าถึงระบบสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศ ซึ่งได้แก่ มีการกำหนดสิทธิในการใช้งานระบบสารสนเทศ อาทิ เขียน อ่าน ลบ ได้ มีการกำหนดกลุ่มของผู้ใช้ตามความจำเป็นในการปฏิบัติงานได้ มีการแยกการติดตั้งระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้ในบริเวณเครือข่ายที่ปลอดภัย

หมวด 8
การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ

8.1 วัตถุประสงค์

การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information system acquisition, development, and maintenance) เป็นหมวดที่กำหนดขึ้นเพื่อให้การพัฒนาและการบำรุงระบบสารสนเทศสามารถดำเนินการได้โดยสอดคล้องกับนโยบายความมั่นคงปลอดภัย และเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูลในระบบสารสนเทศของมหาวิทยาลัย

8.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ

การจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือ การปรับปรุงจากระบบที่มีอยู่เดิม ต้องมีการวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ

8.3 การตรวจสอบการประมวลผล

ระบบสารสนเทศที่พัฒนาขึ้นต้องผ่านการตรวจสอบการประมวลผลทั้งส่วนข้อมูลนำเข้า และผลลัพธ์จากการประมวลผล รวมทั้งต้องมีกลไกในการตรวจจับข้อผิดพลาดและบันทึกไว้เพื่อการตรวจสอบและแก้ไข

8.4 การสร้างความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ

ระบบที่ให้บริการต้องมีการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ มีการป้องกันข้อมูลที่ใช้สำหรับการทดสอบ และมีการควบคุมการเข้าถึงซอร์สโค้ดของระบบ

8.5 การสร้างความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบ

ในการพัฒนาระบบสารสนเทศต้องมีการกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการเพื่อใช้ควบคุมการเปลี่ยนแปลงหรือแก้ไข และต้องมีการตรวจสอบการทำงานหลังการเปลี่ยนแปลงนั้น ๆ

8.6 การจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ต้องได้รับการดูแลอย่างสม่ำเสมอเพื่อให้สามารถทำงานได้เป็นปกติ และต้องมีการปรับปรุงเพื่อปิดช่องโหว่อย่างเหมาะสมตามแนวปฏิบัติที่ได้ผ่านการทดสอบแล้ว

หมวด 9
การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย

9.1 วัตถุประสงค์

การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย (Information security incident management) เป็นหมวดที่กำหนดขึ้นเพื่อให้มีระบบการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และใช้เป็นเครื่องมือที่ช่วยในการตรวจสอบและปรับปรุงแก้ไขระบบให้มีประสิทธิภาพมากยิ่งขึ้น

9.2 **การรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัย**

เมื่อพบเหตุการณ์ผิดปกติ หรือจุดอ่อนด้านความมั่นคงปลอดภัย ต้องมีการรายงานและบันทึกเหตุการณ์นั้น ๆ ไว้เป็นหลักฐานเพื่อนำมาวิเคราะห์ ทบทวนและแจ้งให้บุคลากรทราบโดยทั่วถึงกัน

9.3 **การจัดการและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย**

เมื่อได้รับรายงานเหตุการณ์ผิดปกติ หรือจุดอ่อนด้านความมั่นคงปลอดภัยแล้ว ต้องมีการวิเคราะห์และตรวจสอบเพื่อค้นหาที่มาของความผิดปกติ และดำเนินการหาวิธีที่จะใช้ในการป้องกันปัญหาที่อาจจะเกิดขึ้นในอนาคต โดยมหาวิทยาลัยควรกำหนดขั้นตอนการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย อาทิ

(1) ความล้มเหลวของระบบสารสนเทศ

(2) ผลกระทบจากซอฟต์แวร์ที่ไม่ประสงค์ดี

(3) การปฏิเสธการให้บริการ

(4) การละเมิดความลับและความถูกต้องสมบูรณ์

(5) การใช้ระบบสารสนเทศผิดวัตถุประสงค์

หมวด 10
การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย

10.1 **วัตถุประสงค์**

การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย (Business Continuity Management) เป็นหมวดที่กำหนดขึ้นเพื่อมิให้การดำเนินงานตามภารกิจของมหาวิทยาลัยต้องเกิดการติดขัดหรือหยุดชะงัก และป้องกันมิให้การปฏิบัติงานตามภารกิจที่สำคัญของมหาวิทยาลัยต้องได้รับผลกระทบ หรือเกิดความเสียหายรุนแรง อันเนื่องจากความผิดพลาดของระบบสารสนเทศ และเพื่อให้มั่นใจได้ว่าสามารถกู้ระบบคืนได้ในระยะเวลาที่เหมาะสม

การบริหารเพื่อความต่อเนื่องในการดำเนินภารกิจของมหาวิทยาลัย ต้องมีการกำหนดมาตรการเพื่อรองรับความเสี่ยงและแนวทางในการจำกัดความเสียหาย รวมถึงการกู้คืนระบบที่มีความสำคัญของมหาวิทยาลัย มาตรการเหล่านั้นมีขึ้นเพื่อให้เชื่อมั่นได้ว่า กระบวนการหลักสามารถฟื้นตัวได้ภายในช่วงเวลาที่ยอมรับได้ และสามารถให้บริการในกิจกรรมหลักที่มีความสำคัญต่อมหาวิทยาลัยได้

10.2 **กระบวนการวางแผน**

กระบวนการวางแผนเพื่อให้การดำเนินงานของมหาวิทยาลัยเป็นไปอย่างต่อเนื่องนั้นต้องพิจารณาและให้ความสำคัญกับประเด็นดังต่อไปนี้

(1) การจัดลำดับความสำคัญของระบบสารสนเทศ

(2) การจัดลำดับความสำคัญของผู้ใช้งานหลัก หรือ บริเวณที่ผู้ใช้ปฏิบัติงาน

(3) ข้อตกลงที่เกี่ยวกับลำดับความเร่งด่วนของการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

(4) การจัดทำเอกสารคู่มือและแผนการดำเนินการ หลังเกิดเหตุการณ์ความเสียหาย

10.3 **กรอบการวางแผน**

ในการกำหนดแผนการแก้ไขเหตุการณ์ความเสียหายต้องพิจารณาถึงระดับความสำคัญ และลำดับก่อนหลังของการจัดการในประเด็นต่าง ๆ อันได้แก่

(1) ความสูญเสียที่เกิดขึ้นกับพื้นที่ที่ใช้งานหลักภายในอาคาร

(2) ความสูญเสียที่เกิดขึ้นกับอาคารหลัก

(3) ความสูญเสียที่เกิดขึ้นกับพื้นที่ปฏิบัติงานหลัก

(4) ความสูญเสียที่เกิดขึ้นกับส่วนของระบบเครือข่ายหลัก

(5) ความสูญเสียที่เกิดขึ้นกับระบบปฏิบัติการของคอมพิวเตอร์

(6) ความสูญเสียที่เกิดขึ้นกับบุคลากรหลัก

ในการจัดทำแผนการแก้ไขเหตุการณ์ความเสียหายต้องระบุรายละเอียดในประเด็นดังต่อไปนี้

(1) ขั้นตอนการปฏิบัติการฉุกเฉินต้องครอบคลุมวิธีปฏิบัติงานที่สามารถดำเนินการได้อย่างฉับไวทันทีเพื่อการแก้ไขและควบคุมสถานการณ์ที่เกิดขึ้น

(2) กระบวนการทดสอบที่จำเป็นต้องดำเนินการเพื่อให้เกิดความมั่นใจว่าแผนการแก้ไขเหตุการณ์ที่จัดทำไว้นั้นสามารถดำเนินการได้จริง

หมวด 11
การปฏิบัติตามข้อกำหนด

11.1 วัตถุประสงค์

การปฏิบัติตามข้อกำหนด (Compliance) เป็นหมวดที่กำหนดขึ้นเพื่อให้มั่นใจว่านิสิตและบุคลากรของมหาวิทยาลัยรับทราบ และปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ รวมทั้งกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ

11.2 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย

มหาวิทยาลัยต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบ ข้อบังคับ กฎหมาย หรือ สัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เพื่อให้นิสิตและบุคลากรได้รับทราบ ทำความเข้าใจ และปฏิบัติตามได้อย่างเคร่งครัด

11.3 การปฏิบัติตามข้อกำหนดทางด้านเทคนิค

มหาวิทยาลัยต้องจัดให้มีการตรวจสอบระบบทั้งหมดของมหาวิทยาลัยเพื่อให้มีความมั่นใจว่าได้ดำเนินการสอดคล้องตามนโยบายความมั่นคงปลอดภัยของสารสนเทศในช่วงเวลาที่กำหนดไว้

11.4 การกำหนดการตรวจสอบ

มหาวิทยาลัยต้องกำหนดให้มีการจัดทำแผนและกระบวนการตรวจสอบระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย โดยให้มั่นใจว่าการดำเนินการดังกล่าวนั้นมีผลกระทบต่อระบบและกระบวนการดำเนินงานของมหาวิทยาลัยน้อยที่สุด ในกรณีที่มีการนำซอฟต์แวร์มาใช้ในการตรวจสอบระบบ ต้องป้องกันการนำซอฟต์แวร์ หรือข้อมูลสำคัญที่ได้จากการตรวจสอบไปใช้ในทางที่ผิด