ประกาศมหาวิทยาลัยศรีนครินทรวิโรฒ
เรื่อง นโยบายความมั่นคงปลอดภัยของสารสนเทศ
มหาวิทยาลัยศรีนครินทรวิโรฒ

มหาวิทยาลัยศรีนครินทรวิโรฒ ตระหนักถึงความสำคัญของสารสนเทศซึ่งนับเป็นสินทรัพย์ที่มีคุณค่าสูงสุดขององค์กร มหาวิทยาลัยจึงได้จัดทำนโยบายความมั่นคงปลอดภัยของสารสนเทศขึ้น เพื่อให้มั่นใจว่าสารสนเทศรวมทั้งระบบสารสนเทศและการสื่อสารของมหาวิทยาลัยมีการดูแลด้านการบริหารจัดการอย่างมีประสิทธิภาพ โดยอาศัยกรอบตามมาตรฐานสากลด้านความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 รวมทั้งข้อกำหนดตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาสินทรัพย์ด้านสารสนเทศของมหาวิทยาลัยจากภาวะคุกคามทุกประเภทที่อาจจะเกิดขึ้นทั้งจากภายในและภายนอกมหาวิทยาลัย โดยเจตนาหรือโดยรู้เท่าไม่ถึงการณ์ ซึ่งครอบคลุมด้านการรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ อาศัยอำนาจตามความในมาตรา 34 แห่งพระราชบัญญัติมหาวิทยาลัยศรีนครินทรวิโรฒ พ.ศ. 2559 มหาวิทยาลัยศรีนครินทรวิโรฒ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยศรีนครินทรวิโรฒ เรื่อง นโยบายความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยศรีนครินทรวิโรฒ”

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 ในประกาศนี้

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยศรีนครินทรวิโรฒ

“ส่วนงาน” หมายความว่า ส่วนงานตามพระราชบัญญัติมหาวิทยาลัยศรีนครินทรวิโรฒ

“หน่วยงานภายนอก” หมายความว่า องค์กรซึ่งมหาวิทยาลัยศรีนครินทรวิโรฒอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูลหรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัย โดยจะได้รับสิทธิตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของมหาวิทยาลัยโดยมิได้รับอนุญาต

“สารสนเทศ” หมายความว่า ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้

“ข้อมูล” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“เทคโนโลยีสารสนเทศและการสื่อสาร” (Information and communication technology) หมายความว่า เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ 3 ส่วนคือ คอมพิวเตอร์ การสื่อสาร และสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบสารสนเทศ” หมายถึง ชุดขององค์ประกอบที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บและแจกจ่ายสารสนเทศ เพื่อช่วยการตัดสินใจและการควบคุมในองค์กร ในการทำงานของระบบสารสนเทศประกอบไปด้วยกิจกรรม 3 อย่าง คือ การนำข้อมูลเข้าสู่ระบบ (Input) การประมวลผล (Processing) และการนำเสนอผลลัพธ์ (Output)

“ระบบงาน” หมายความว่า การนำระบบสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบงานบุคคล ระบบจัดเก็บเอกสาร

“ระบบปฏิบัติการ” (operating system) หมายความว่า ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

“ระบบเครือข่าย” (network) หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยศรีนครินทรวิโรฒ

“เครื่องคอมพิวเตอร์แม่ข่าย” (server) หมายความว่า เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์ สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่น ๆ หรือควบคุมการทำงานในเครือข่าย

“สินทรัพย์” (asset) หมายความว่า เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย ข้อมูล และระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

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

“ความลับ” (confidentiality) หมายความว่า การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

“ความถูกต้องครบถ้วน” (integrity) หมายความว่า การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

“สภาพพร้อมใช้งาน” (availability) หมายความว่า การรับรองได้ว่าข้อมูล หรือระบบสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

“เหตุการณ์ด้านความมั่นคงปลอดภัย” (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“ความเสี่ยง” หมายความว่า โอกาสของสินทรัพย์สารสนเทศในการถูกละเมิดการรักษาความปลอดภัย

“ช่องโหว่” (vulnerability) หมายความว่า จุดอ่อนของระบบสารสนเทศที่ทำให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบทำให้ประสิทธิภาพของการทำงานลดลง

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” (access control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

“ผู้ใช้งาน” หมายความว่า นิสิตและบุคลากรของมหาวิทยาลัยศรีนครินทรวิโรฒที่ได้รับสิทธิในการใช้งานระบบสารสนเทศของมหาวิทยาลัย รวมถึงบุคคลจากหน่วยงานภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานสารสนเทศของมหาวิทยาลัย

“บัวศรีไอดี” (Buasri ID) หมายความว่า ชื่อและรหัสบัญชีผู้ใช้งานเพื่อใช้ในการพิสูจน์ตัวตนก่อนการเข้าใช้เครือข่ายและบริการระบบสารสนเทศของมหาวิทยาลัย

“รหัสผ่าน” (password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของส่วนงาน

“Idle Timeout” หมายความว่า ระยะเวลาที่ผู้ใช้งานเชื่อมต่อกับระบบสารสนเทศ และไม่มีการใช้งานเกินระยะเวลาที่กำหนด ระบบสารสนเทศจะทำการตัดการเชื่อมต่อผู้ใช้งานออกจากระบบ

”Session Timeout” หมายความว่า ระยะเวลาที่ผู้ใช้สามารถเชื่อมต่อกับระบบสารสนเทศได้

ข้อ 4 วัตถุประสงค์ของการกำหนดนโยบาย

นโยบายความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยศรีนครินทรวิโรฒได้กำหนดขึ้นโดยมีวัตถุประสงค์ดังต่อไปนี้

(1) เพื่อให้มีนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศมหาวิทยาลัยศรีนครินทรวิโรฒ ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

(2) เพื่อเป็นกรอบและแนวปฏิบัติในการกำหนดมาตรฐาน ขั้นตอนการปฏิบัติงาน ผู้รับผิดชอบ รวมถึงสิ่งอำนวยความสะดวกด้านคอมพิวเตอร์สำหรับการติดตั้งและใช้งานระบบเพื่อการรักษาความมั่นคงปลอดภัยของสารสนเทศ

(3) เพื่อกำหนดให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ มีแผนเตรียมความพร้อมสำหรับกรณีฉุกเฉิน และให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม เพื่อให้ระบบสารสนเทศและการสื่อสารของมหาวิทยาลัย สามารถใช้งานได้เป็นปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องตามภารกิจ

(4) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของสารสนเทศ รวมทั้งระบบสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

(5) เพื่อส่งเสริมให้มีการเผยแพร่ความรู้แก่นิสิต และบุคลากรของมหาวิทยาลัยศรีนครินทรวิโรฒ รวมถึงบุคคลที่เกี่ยวข้อง เพื่อสร้างความเข้าใจ ให้เกิดความตระหนัก และมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

หมวด 1
นโยบายความมั่นคงปลอดภัย

ข้อ 5 นโยบายความมั่นคงปลอดภัย (Security policy)

กำหนดขึ้นเพื่อใช้เป็นกรอบและทิศทางในการสนับสนุนการดำเนินการด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศของมหาวิทยาลัย เพื่อให้เกิดการดำเนินการตามมาตรฐานระดับสากลหรือสอดคล้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ข้อ 6 ข้อกำหนดตามกฎหมาย

ความมั่นคงปลอดภัยของสารสนเทศบางประเด็นอาจจะเกี่ยวข้องกับกฎหมายที่ได้มีบัญญัติมีประกาศและมีผลบังคับใช้ อาทิ

(1) กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

(2) กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(3) กฎหมายลิขสิทธิ์

ข้อ 7 มาตรฐานระดับสากล

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

ข้อ 8 ผู้ได้รับผลกระทบจากนโยบาย

นโยบายนี้มีผลบังคับใช้กับนิสิตและบุคลากรทุกคนในมหาวิทยาลัย รวมถึงผู้รับสัญญาและผู้เยี่ยมเยือนซึ่งแม้จะมิได้รับการว่าจ้างจากมหาวิทยาลัย แต่มีส่วนเกี่ยวข้องกับการทำงาน หรือสามารถเข้าถึงสารสนเทศของมหาวิทยาลัย

ข้อ 9 การใช้งานที่ยอมรับได้

มหาวิทยาลัยจัดให้บริการสารสนเทศ รวมทั้งระบบสารสนเทศและการสื่อสารเพื่อการใช้ประโยชน์ตามวัตถุประสงค์ของกิจกรรมตามภารกิจของมหาวิทยาลัย อาทิ

(1) การเรียนการสอน

(2) การวิจัย

(3) การบริหารงานตามภารกิจของมหาวิทยาลัย

(4) การปฏิบัติงานตามภารกิจของมหาวิทยาลัย

(5) การพัฒนาการเรียนรู้ส่วนบุคคล

(6) การให้คำแนะนำปรึกษาซึ่งเป็นงานตามข้อสัญญาหรือข้อตกลงกับมหาวิทยาลัย

(7) การติดต่อสื่อสารตามวัตถุประสงค์ดังกล่าวข้างต้น

การใช้งานสารสนเทศ รวมถึงระบบสารสนเทศและการสื่อสารตามกิจกรรมดังกล่าวข้างต้นต้องเป็นไปอย่างเหมาะสม โดยอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของบุคคลอื่น รวมถึงเคารพและปฏิบัติอย่างถูกต้องตามกฎหมาย และต้องไม่เกี่ยวข้องกับการดำเนินธุรกิจการค้าใด ๆ

ข้อ 10 พื้นที่ที่มีผลบังคับใช้

นโยบายนี้มีผลบังคับใช้กับทุกตำแหน่งพื้นที่ที่สามารถเข้าถึงระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ซึ่งรวมถึงการเข้าถึงจากระยะไกลหรือการเชื่อมโยงจากองค์กรภายนอก การอนุญาตและมอบหมายสิทธิในการเข้าถึงระบบของมหาวิทยาลัย ไม่ว่าจะเป็นระบบสารสนเทศด้านวิชาการและระบบสารสนเทศด้านการบริหาร มหาวิทยาลัยต้องมั่นใจว่าได้มีการดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยของสารสนเทศ และได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจจะเกิดขึ้น

ข้อ 11 การตรวจสอบและทบทวน

มหาวิทยาลัยต้องกำหนดให้มีผู้บริหารระดับสูงทำหน้าที่กำกับดูแลนโยบายและรับผิดชอบในการตรวจสอบการดำเนินงานตามนโยบายความมั่นคงปลอดภัยของสารสนเทศอย่างสม่ำเสมอ

และทันเหตุการณ์ โดยให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์แปรเปลี่ยนที่สำคัญ มหาวิทยาลัยต้องติดตามเพื่อให้มั่นใจว่านโยบายเหล่านี้มีความเหมาะสมเพื่อปกป้องผลประโยชน์ของมหาวิทยาลัย

หมวด 2
โครงสร้างการบริหารความมั่นคงปลอดภัยของสารสนเทศ

ข้อ 12 โครงสร้างการบริหารความมั่นคงปลอดภัยของสารสนเทศ (Organization of Information Security) กำหนดขึ้นเพื่อให้การบริหารและการรักษาความมั่นคงปลอดภัยที่เกี่ยวกับสารสนเทศของมหาวิทยาลัยดำเนินการได้อย่างชัดเจน และเพื่อให้มั่นใจว่านิสิตและบุคลากรของมหาวิทยาลัยทุกคนได้ตระหนักถึงความสำคัญในเรื่องความมั่นคงปลอดภัยของสารสนเทศ มีความรู้ความเข้าใจและมีความรับผิดชอบตามภาระหน้าที่ร่วมกันในการจำกัดภาวะความเสี่ยงและภัยคุกคาม ซึ่งมีแนวโน้มของความซับซ้อนและความรุนแรงเพิ่มมากขึ้น

ข้อ 13 วิธีการและความรับผิดชอบ

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

มหาวิทยาลัยจึงจำเป็นต้องมีการกำหนดแนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศ โดยให้มีการจัดทำนโยบายและแนวปฏิบัติ กำกับให้มีการดำเนินการตามข้อกำหนด มีการตรวจสอบและวิเคราะห์ความเสี่ยงอย่างสม่ำเสมอ เพื่อนำมาใช้ในการปรับปรุงนโยบายและแนวปฏิบัติของมหาวิทยาลัยให้สามารถรองรับการเปลี่ยนแปลงของภัยคุกคามที่อาจจะเกิดขึ้น มหาวิทยาลัยต้องดำเนินการรักษาความมั่นคงปลอดภัยอย่างสมเหตุสมผล โดยยึดแนวทางการสร้างความสมดุล ระหว่างความคล่องตัวกับความมั่นคงปลอดภัยของสารสนเทศ และค่าใช้จ่ายที่จะเกิดขึ้น

ข้อ 14 ผู้รับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

(1) ระดับมหาวิทยาลัย

อธิการบดีเป็นผู้รับผิดต่อชอบความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น และทำหน้าที่บริหารจัดการและกำกับดูแลภาพรวมของความมั่นคงปลอดภัยของสารสนเทศของมหาวิทยาลัย และได้มีการแต่งตั้งคณะกรรมการบริหารความมั่นคงปลอดภัยทำหน้าที่รับผิดชอบในส่วนของนโยบาย

การรักษาความมั่นคงปลอดภัย แต่ทั้งนี้ คณะ/สถาบัน/สานัก ที่เป็นเจ้าของข้อมูลที่อยู่ในระบบส่วนกลาง และในระบบที่สร้างขึ้นเอง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย

(2) ระดับส่วนงาน

หัวหน้าส่วนงานต้องกำหนดให้ผู้บริหารของส่วนงานหรือเจ้าหน้าที่ประจำของส่วนงานทำหน้าที่ในฐานะเจ้าของข้อมูล และเป็นผู้รับผิดชอบในการประสานความร่วมมือและกำกับดูแลให้มีการปฏิบัติตามประกาศของมหาวิทยาลัย ที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ ทั้งด้านเทคนิค การตรวจสอบ การเฝ้าระวัง การให้บริการข้อมูล และการประเมินและรายงานความเสี่ยงต่อมหาวิทยาลัย

ข้อ 15 ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

(1) ผู้บริหาร

ผู้บริหารของทุกส่วนงานต้องกำกับดูแลให้นิสิตและบุคลากรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย

(2) นิสิตและบุคลากร

นิสิตและบุคลากรทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย และต้องรายงานต่อมหาวิทยาลัย หากพบปัญหาหรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ

(3) ผู้พัฒนาและผู้ดูแลระบบ

ผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของมหาวิทยาลัยต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรการด้านความมั่นคงปลอดภัยของระบบต้องผ่านการพิจารณาและได้รับคำแนะนำจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

ผู้พัฒนาและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศทุกระบบของมหาวิทยาลัยต้องมีความรับผิดชอบในเรื่องความมั่นคงปลอดภัยของสารสนเทศ

(4) บุคคลภายนอก

บุคคลภายนอก หรือบุคลากรของหน่วยงานภายนอกที่มหาวิทยาลัยอนุญาตให้มีสิทธิในการเข้าถึงข้อมูลสารสนเทศ หรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัย ต้องรับผิดชอบและปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัยอย่างเคร่งครัด โดยการใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการกระทำที่เกิดขึ้นและไม่เปิดเผยความลับของมหาวิทยาลัยโดยมิได้รับอนุญาต

หมวด 3
การจัดการสินทรัพย์สารสนเทศ

ข้อ 16 การจัดการสินทรัพย์สารสนเทศ (Information Asset Management)

กำหนดขึ้นเพื่อป้องกันสินทรัพย์สารสนเทศของมหาวิทยาลัยให้เกิดความมั่นคงปลอดภัย และสามารถใช้งานสินทรัพย์เหล่านั้นได้อย่างเหมาะสม

ข้อ 17 หน้าที่ความรับผิดชอบต่อสินทรัพย์สารสนเทศ

มหาวิทยาลัยต้องกำหนดให้มีผู้รับผิดชอบในการจัดทำบัญชีสินทรัพย์สารสนเทศ และปรับปรุงข้อมูลให้ถูกต้อง โดยให้ความสำคัญกับสินทรัพย์ที่มีผลต่อการดำเนินภารกิจของมหาวิทยาลัย ซึ่งจำแนกเป็น 5 กลุ่ม ดังต่อไปนี้

(1) ข้อมูลสารสนเทศ

(2) บริการและกระบวนการ

(3) ฮาร์ดแวร์

(4) ซอฟต์แวร์

(5) บุคลากร

มหาวิทยาลัยต้องจัดทำกฎ ระเบียบ หรือ หลักเกณฑ์ในการใช้สินทรัพย์อย่างเป็นลายลักษณ์อักษรเพื่อให้เกิดการใช้งานได้อย่างเหมาะสม และเพื่อป้องกันความเสียหายต่อสินทรัพย์เหล่านั้น

ข้อ 18 การจัดหมวดหมู่สารสนเทศ

มหาวิทยาลัยต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของสินทรัพย์สารสนเทศ ตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อมหาวิทยาลัย ทั้งนี้เพื่อให้สามารถกำหนดวิธีการในการป้องกันได้อย่างเหมาะสม รวมทั้งจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการสินทรัพย์สารสนเทศตามหมวดหมู่ที่กำหนดไว้

หมวด 4
ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

ข้อ 19 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (Human Resources Security) กำหนดขึ้นเพื่อให้บุคลากรของมหาวิทยาลัย และบุคลากรของผู้รับสัญญาว่าจ้างจากมหาวิทยาลัยได้เข้าใจในบทบาทและหน้าที่ความรับผิดชอบของตน เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง รวมถึงการใช้สารสนเทศหรือระบบสารสนเทศและการสื่อสารอย่างไม่ถูกต้อง หรือผิดวัตถุประสงค์

ข้อ 20 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน

มหาวิทยาลัยต้องกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นลายลักษณ์อักษร และต้องมีการตรวจสอบคุณสมบัติของผู้สมัคร โดยพิจารณาจากจดหมายรับรอง ประวัติการทำงาน เป็นต้น นอกจากนั้นต้องมีการระบุเงื่อนไขการจ้างงานซึ่งรวมถึงความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

ข้อ 21 การสร้างความมั่นคงปลอดภัยระหว่างการจ้างงาน

บุคลากร หรือผู้ได้รับการว่าจ้างต้องปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของมหาวิทยาลัย โดยต้องมีการให้ความรู้ และฝึกอบรมด้านความปลอดภัยให้แก่บุคลากร ในกรณีที่มีการกระทำความผิดต้องมีกระบวนการสอบสวนและลงโทษตามระเบียบของมหาวิทยาลัย

ข้อ 22 การสิ้นสุดหรือการเปลี่ยนการจ้าง

เมื่อสิ้นสุดการเป็นบุคลากร หรือการเปลี่ยนสัญญาการจ้างงานต้องมีการคืนสินทรัพย์ของมหาวิทยาลัย และถอดถอนสิทธิในการเข้าถึงระบบสารสนเทศของบุคคลนั้น

หมวด 5
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ข้อ 23 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) กำหนดขึ้นเพื่อป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต ป้องกันความเสียหายและการคุกคามสินทรัพย์สารสนเทศของมหาวิทยาลัย

ข้อ 24 การรักษาความปลอดภัยทางกายภาพ

มหาวิทยาลัยต้องกำหนดรายละเอียดของสถานที่และอุปกรณ์ที่จำเป็นต้องมีระบบการป้องกันการเสียหาย และระบบควบคุมการเข้าออกเพื่อรักษาความมั่นคงปลอดภัย อาทิ ห้องคอมพิวเตอร์กลางของมหาวิทยาลัยซึ่งเป็นพื้นที่จัดเก็บเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ด้านเครือข่าย ต้องมีระบบรักษาความปลอดภัยและมีการควบคุมการเข้าถึงอย่างเข้มงวด โดยอนุญาตเฉพาะผู้รับผิดชอบเท่านั้น

ข้อ 25 การควบคุมการเข้าถึงอุปกรณ์

อุปกรณ์ทุกชนิดต้องกำหนดให้มีผู้รับผิดชอบโดยตรง และผู้รับผิดชอบเท่านั้นที่ได้รับสิทธิในการเข้าถึง โดยต้องจัดให้มีระบบสำหรับจัดเก็บข้อมูลการเข้าถึงเพื่อใช้เป็นหลักฐานในการตรวจสอบ

ข้อ 26 การรักษาความปลอดภัยของอุปกรณ์

อุปกรณ์สำคัญที่ถูกจัดเก็บในห้องคอมพิวเตอร์กลาง ต้องมีการจัดวางอย่างถูกต้องและมีการป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต การเดินสายเพื่อเชื่อมโยงระหว่างอุปกรณ์ต้องมีป้ายเพื่อบ่งบอกถึงตำแหน่งในการเชื่อมต่อกับอุปกรณ์ และมีการกำหนดแผนการบำรุงรักษาอุปกรณ์อย่างชัดเจนและต่อเนื่อง

ข้อ 27 การนำอุปกรณ์ออกนอกส่วนงาน

การนำอุปกรณ์ทุกชิ้นออกนอกส่วนงาน ต้องปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยของส่วนงาน และต้องจัดให้มีการตรวจสอบอย่างเคร่งครัด

ข้อ 28 การนำอุปกรณ์ภายนอกเข้ามาเชื่อมต่อภายในส่วนงาน

การนำอุปกรณ์ทุกชิ้นจากภายนอกเข้ามาเชื่อมต่อภายในส่วนงาน ต้องปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยของส่วนงาน และต้องจัดให้มีการตรวจสอบอย่างเคร่งครัด

หมวด 6
การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ

ข้อ 29 การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ (Communication and Operations Management) กำหนดขึ้นเพื่อให้การดำเนินงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านสารสนเทศ อุปกรณ์ประมวลผลที่มีความถูกต้อง เหมาะสม และปลอดภัย ในแต่ละขั้นตอนของการปฏิบัติงานต้องมีการบันทึกและจัดเก็บเป็นลายลักษณ์อักษร เพื่อประโยชน์สำหรับการกู้คืนข้อมูลในกรณีที่เกิดความเสียหาย

ข้อ 30 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน

โครงสร้างพื้นฐานและสารสนเทศทุกระบบต้องมีผู้รับผิดชอบ มีเอกสารขั้นตอนในการปฏิบัติงานที่ได้บันทึกไว้เป็นลายลักษณ์อักษร ในกรณีมีการเปลี่ยนแปลงข้อมูล หรือการปรับเปลี่ยนเวอร์ชั่นของระบบ หรือโปรแกรมภายใน ต้องมีการบันทึกเพื่อให้มั่นใจว่าจัดการกับปัญหาที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นได้ และสามารถกลับคืนสู่สถานะเดิมได้หากแก้ไขไม่สำเร็จ

ข้อ 31 การรับบริการจากหน่วยงานภายนอก

ในการรับบริการจากหน่วยงานภายนอกต้องมีการตรวจสอบและบันทึกการปฏิบัติงานมีการเฝ้าระวังและจัดทำรายงานผลการดำเนินงานที่เกิดขึ้นอย่างสม่ำเสมอ รวมถึงกำหนดแนวทางการบริหารจัดการในกรณีที่มีการเปลี่ยนแปลงซึ่งอาจจะมีผลกระทบต่อมหาวิทยาลัย

ข้อ 32 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ

มหาวิทยาลัยต้องจัดให้มีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถตรวจรับทรัพยากรสารสนเทศตามหลักเกณฑ์กลางที่มหาวิทยาลัยประกาศใช้ และทดสอบการทำงานของทรัพยากรสารสนเทศนั้นเพื่อให้มั่นใจว่าสามารถใช้งานได้ตามข้อกำหนด

ข้อ 33 การป้องกันโปรแกรมที่ไม่ประสงค์ดี

มหาวิทยาลัยต้องจัดให้มีการติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดี รวมทั้งโปรแกรมเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการสำหรับระบบงาน หรือ อุปกรณ์หลักของมหาวิทยาลัย และกำหนดให้มีระเบียบและขั้นตอนวิธีปฏิบัติที่เหมาะสม และสนับสนุนให้ส่วนงานภายในที่มีการใช้งานระบบผ่านเครือข่ายของมหาวิทยาลัยได้ยึดถือและปฏิบัติตาม

ข้อ 34 การสำรองข้อมูล

มหาวิทยาลัยต้องจัดให้มีการสำรองข้อมูลที่สำคัญ โดยต้องกำหนดรูปแบบและวิธีปฏิบัติ รวมทั้งแผนการสำรองข้อมูลที่เหมาะสมตามลำดับความสำคัญของสารสนเทศของมหาวิทยาลัยเพื่อป้องกันการสูญหายอันอาจจะเกิดขึ้นจากภาวะคุกคาม หรือ จากการเกิดภัยพิบัติ โดยต้องกำหนดให้มีผู้รับผิดชอบในการสำรองข้อมูลตามรูปแบบและแผนการดำเนินการที่กำหนดไว้

ข้อ 35 การเฝ้าระวังด้านความมั่นคงปลอดภัย

มหาวิทยาลัยต้องมีการเฝ้าระวังระบบที่สำคัญ เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ ต้องให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ และต้องกำหนดขั้นตอนวิธีปฏิบัติในการติดตั้งเวลาของระบบคอมพิวเตอร์กลางให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง เพื่อช่วยในการตรวจสอบช่วงเวลาในกรณีเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ของมหาวิทยาลัย

หมวด 7
การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย

ข้อ 36 การควบคุมการเข้าถึง (Access Control)

การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย กำหนดขึ้นเพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศ โดยมหาวิทยาลัยต้องมีการกำหนดนโยบายการเข้าถึงระบบ การบริหารการจัดการเข้าถึงของผู้ใช้ และการควบคุมการเข้าถึงเครือข่าย

ข้อ 37 การควบคุมการเข้าถึงระบบ

มหาวิทยาลัยต้องมีนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร และทบทวนตามระยะเวลาที่กำหนดไว้ โดยพิจารณาให้สอดคล้องกับภารกิจของมหาวิทยาลัย และความมั่นคงปลอดภัยในการเข้าถึงสินทรัพย์สารสนเทศ

ข้อ 38 การจัดการการเข้าถึงของผู้ใช้

มหาวิทยาลัยต้องมีการกำหนดมาตรการและแนวปฏิบัติอย่างเป็นระบบเพื่อใช้ในการกำหนดรหัสบัญชีผู้ใช้สำหรับนิสิตและบุคลากร การจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ การจัดการรหัสผ่าน รวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้

ข้อ 39 หน้าที่ความรับผิดชอบของผู้ใช้งาน

เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามมาตรการด้านการรักษาความปลอดภัยในการเข้าถึงอย่างเคร่งครัด เช่น ไม่กำหนดรหัสผ่านแบบที่ไม่ปลอดภัย ไม่เปิดเผยรหัสผ่านให้ผู้อื่นล่วงรู้ เป็นต้น

ข้อ 40 การควบคุมการเข้าถึงเครือข่าย

การเข้าถึงเครือข่ายจากภายในมหาวิทยาลัย หรือการเชื่อมต่อจากภายนอกต้องมีมาตรการควบคุมที่ชัดเจน ต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบต้องยอมให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตผ่านเข้าสู่เครือข่าย และใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

ข้อ 41 การควบคุมการใช้งานระบบปฏิบัติการ

การเข้าถึงระบบปฏิบัติการต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิการปฏิบัติการ และกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้อื่นเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

ข้อ 42 การควบคุมการใช้งานระบบสารสนเทศ

การเข้าถึงระบบสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศ ซึ่งได้แก่ มีการกำหนดสิทธิในการใช้งานระบบสารสนเทศ อาทิ เขียน อ่าน ลบ ได้ มีการกำหนดกลุ่มของผู้ใช้ตามความจำเป็น

ในการปฏิบัติงานได้ มีการแยกการติดตั้งระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้ในบริเวณเครือข่ายที่ปลอดภัย

ข้อ 43 การควบคุมการใช้งานฐานข้อมูลกลาง

การเข้าถึงฐานข้อมูลกลางของมหาวิทยาลัยต้องกำหนดกระบวนการเข้าถึงฐานข้อมูลให้มีความมั่นคงปลอดภัย โดยผ่านการพิสูจน์ตัวตน ตามสิทธิบัญชีผู้ใช้ที่ได้รับ

หมวด 8
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ข้อ 44 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information system acquisition, development, and maintenance) กำหนดขึ้นเพื่อให้การพัฒนาและการบำรุงระบบสารสนเทศสามารถดำเนินการได้โดยสอดคล้องกับนโยบายความมั่นคงปลอดภัย และเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูลในระบบสารสนเทศของมหาวิทยาลัย

ข้อ 45 ข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ

การจัดหา และการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศที่มีอยู่เดิมต้องมีการวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ

ข้อ 46 การตรวจสอบการประมวลผล

ระบบสารสนเทศที่พัฒนาขึ้นต้องผ่านการตรวจสอบการประมวลผลทั้งส่วนข้อมูลนำเข้าและผลลัพธ์จากการประมวลผล รวมทั้งต้องมีกลไกในการตรวจจับข้อผิดพลาดและบันทึกไว้เพื่อการตรวจสอบและแก้ไข

ข้อ 47 การสร้างความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ

ระบบที่ให้บริการต้องมีการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ มีการป้องกันข้อมูลที่ใช้สำหรับการทดสอบ และมีการควบคุมการเข้าถึงซอร์สโค้ดของระบบ

ข้อ 48 การสร้างความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบ

ในการพัฒนาระบบสารสนเทศต้องมีการกำหนดขั้นตอนวิธีปฏิบัติอย่างเป็นทางการเพื่อใช้ควบคุมการเปลี่ยนแปลงหรือแก้ไข และต้องมีการตรวจสอบการทำงานของระบบหลังมีการเปลี่ยนแปลง

ข้อ 49 การจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

ฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ต้องได้รับการดูแลอย่างสม่ำเสมอเพื่อให้สามารถทำงานได้เป็นปกติ และต้องมีการปรับปรุงข้อมูลเพื่อปิดช่องโหว่อย่างเหมาะสมตามแนวปฏิบัติที่ได้ผ่านการทดสอบแล้ว

หมวด 9
การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย

ข้อ 50 การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย (Information security incident management) กำหนดขึ้นเพื่อให้มีระบบการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และใช้เป็นเครื่องมือที่ช่วยในการตรวจสอบและปรับปรุงแก้ไขระบบให้มีประสิทธิภาพมากยิ่งขึ้น

ข้อ 51 การรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัย

เมื่อพบเหตุการณ์ผิดปกติ หรือจุดอ่อนด้านความมั่นคงปลอดภัย ต้องมีการรายงานและบันทึกเหตุการณ์นั้น ๆ ไว้เป็นหลักฐานเพื่อนำมาวิเคราะห์ ทบทวนและแจ้งให้บุคลากรทราบโดยทั่วถึงกัน

ข้อ 52 การจัดการและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

เมื่อได้รับรายงานเหตุการณ์ผิดปกติ หรือจุดอ่อนด้านความมั่นคงปลอดภัยแล้ว ต้องมีการวิเคราะห์และตรวจสอบเพื่อค้นหาที่มาของความผิดปกติ และดำเนินการหาวิธีที่จะใช้ในการป้องกันปัญหาที่อาจจะเกิดขึ้นในอนาคต โดยมหาวิทยาลัยควรกำหนดขั้นตอนการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย อาทิ

(1) ความล้มเหลวของระบบสารสนเทศ
(2) ผลกระทบจากซอฟต์แวร์ที่ไม่ประสงค์ดี
(3) การปฏิเสธการให้บริการ
(4) การละเมิดความลับและความถูกต้องสมบูรณ์
(5) การใช้ระบบสารสนเทศผิดวัตถุประสงค์

หมวด 10
การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย

ข้อ 53 การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย (Business Continuity Management) กำหนดขึ้นเพื่อมิให้การดำเนินงานตามภารกิจของมหาวิทยาลัยต้องเกิดการติดขัดหรือหยุดชะงัก และป้องกันมิให้การปฏิบัติงานตามภารกิจที่สำคัญของมหาวิทยาลัยต้องได้รับผลกระทบ หรือเกิดความเสียหายรุนแรง อันเนื่องจากความผิดพลาดของระบบสารสนเทศ และเพื่อให้มั่นใจได้ว่าหากเกิดผลกระทบกับระบบสารสนเทศขึ้น ระบบสารสนเทศจะสามารถกู้คืนให้สามารถกลับมาใช้งานได้ในระยะเวลาที่เหมาะสม

การบริหารเพื่อความต่อเนื่องในการดำเนินภารกิจของมหาวิทยาลัย ต้องมีการกำหนดมาตรการเพื่อรองรับความเสี่ยงและแนวทางในการจำกัดความเสียหาย รวมถึงการกู้คืนระบบที่มีความสำคัญ

ของมหาวิทยาลัย มาตรการเหล่านั้นมีขึ้นเพื่อให้เชื่อมั่นได้ว่า กระบวนการหลักสามารถฟื้นตัวได้ภายในช่วงเวลาที่ยอมรับได้ และสามารถให้บริการในกิจกรรมหลักที่มีความสำคัญต่อมหาวิทยาลัยได้

ข้อ 54 กระบวนการวางแผน

กระบวนการวางแผนเพื่อให้การดำเนินงานของมหาวิทยาลัยเป็นไปอย่างต่อเนื่องนั้น ต้องพิจารณาและให้ความสำคัญกับประเด็นดังต่อไปนี้

(1) การจัดลำดับความสำคัญของระบบสารสนเทศ

(2) การจัดลำดับความสำคัญของผู้ใช้งานหลัก หรือบริเวณที่ผู้ใช้ปฏิบัติงาน

(3) ข้อตกลงที่เกี่ยวกับลำดับความเร่งด่วนของการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

(4) การจัดทำเอกสารคู่มือและแผนการดำเนินการ หลังเกิดเหตุการณ์ความเสียหาย

ข้อ 55 กรอบการวางแผน

ในการกำหนดแผนการแก้ไขเหตุการณ์ความเสียหายต้องพิจารณาถึงระดับความสำคัญและลำดับก่อนหลังของการจัดการในประเด็นต่าง ๆ อันได้แก่

(1) ความสูญเสียที่เกิดขึ้นกับพื้นที่ที่ใช้งานหลักภายในอาคาร

(2) ความสูญเสียที่เกิดขึ้นกับอาคารหลัก

(3) ความสูญเสียที่เกิดขึ้นกับพื้นที่ปฏิบัติงานหลัก

(4) ความสูญเสียที่เกิดขึ้นกับส่วนของระบบเครือข่ายหลัก

(5) ความสูญเสียที่เกิดขึ้นกับระบบปฏิบัติการของคอมพิวเตอร์

(6) ความสูญเสียที่เกิดขึ้นกับบุคลากรหลัก

และต้องระบุรายละเอียดในประเด็นดังต่อไปนี้

(1) ขั้นตอนการปฏิบัติการฉุกเฉินต้องครอบคลุมวิธีปฏิบัติงานที่สามารถดำเนินการได้อย่างฉับไวทันที เพื่อการแก้ไขและควบคุมสถานการณ์ที่เกิดขึ้น

(2) กระบวนการทดสอบที่จำเป็นต้องดำเนินการเพื่อให้เกิดความมั่นใจว่า แผนการแก้ไขเหตุการณ์ที่จัดทำไว้นั้นสามารถดำเนินการได้จริง

หมวด 11
การปฏิบัติตามข้อกำหนด

ข้อ 56 การปฏิบัติตามข้อกำหนด (Compliance)

กำหนดขึ้นเพื่อให้มั่นใจว่านิสิตและบุคลากรของมหาวิทยาลัยรับทราบ และปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ รวมทั้งกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ โดยจัดทำประกาศผ่านทางเว็บไซต์มหาวิทยาลัยศรีนครินทรวิโรฒ

ข้อ 57 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย

มหาวิทยาลัยต้องมอบหมายให้ส่วนงานที่เกี่ยวข้องดำเนินการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เพื่อประกาศให้นิสิตและบุคลากรได้รับทราบ ทำความเข้าใจ และปฏิบัติตามได้อย่างเคร่งครัด

ข้อ 58 การปฏิบัติตามข้อกำหนดทางด้านเทคนิค

มหาวิทยาลัยต้องจัดให้มีการตรวจสอบระบบสารสนเทศของมหาวิทยาลัย เพื่อให้มีความมั่นใจว่าการดำเนินการทางเทคนิคสอดคล้องตามนโยบายความมั่นคงปลอดภัยของสารสนเทศในช่วงเวลาที่กำหนดไว้

ข้อ 59 การกำหนดการตรวจสอบ

มหาวิทยาลัยต้องกำหนดให้มีการจัดทำแผนและกระบวนการตรวจสอบระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย โดยให้มั่นใจว่าการดำเนินการดังกล่าวจะไม่ส่งผลกระทบต่อระบบและกระบวนการดำเนินงานของมหาวิทยาลัย แต่หากเกิดผลกระทบขึ้นต้องควบคุมให้ส่งผลกระทบต่อระบบน้อยที่สุด ในกรณีที่มีการนำซอฟต์แวร์มาใช้ในการตรวจสอบระบบ ต้องควบคุมป้องกันการนำซอฟต์แวร์หรือข้อมูลสำคัญที่ได้จากการตรวจสอบไปใช้ในทางที่ผิด

ประกาศ ณ วันที่ 17 พฤษภาคม พ.ศ. 2565

(รองศาสตราจารย์ ดร.สมชาย สันติวัฒนกุล)
อธิการบดีมหาวิทยาลัยศรีนครินทรวิโรฒ