ประกาศคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล
เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ ของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล
พ.ศ. ๒๕๖๘

.....

ตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

เพื่อให้การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความความมั่นคงปลอดภัยทางไซเบอร์ของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล มีความมั่นคงปลอดภัย สอดคล้องกับมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๒๒ และแนวปฏิบัติที่ดีอื่น ๆ ตลอดจนมีการพัฒนาปรับปรุงความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาสินทรัพย์ด้านสารสนเทศของมหาวิทยาลัยจากภาวะคุกคามทุกประเภทที่อาจจะเกิดขึ้นทั้งจากภายในและภายนอกมหาวิทยาลัย อาศัยอำนาจตามความในมาตรา ๓๗ แห่งพระราชบัญญัติมหาวิทยาลัยมหิดล พ.ศ. ๒๕๕๐ คณบดีโดยความเห็นชอบของคณะกรรมการประจำคณะทันตแพทยศาสตร์ ในการประชุมครั้งที่ ๒/๒๕๖๘ เมื่อวันที่ ๖ กุมภาพันธ์ ๒๕๖๘ จึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล ดังนี้

ข้อ ๑ ให้ยกเลิกประกาศคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ ของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล ฉบับลงวันที่ ๒๐ ตุลาคม ๒๕๖๔

ข้อ ๒ ในประกาศนี้

“คณะ” หมายถึง คณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

“แนวปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายด้านเทคโนโลยีสารสนเทศของคณะได้ง่ายขึ้น

“ผู้บริหาร” หมายถึง คณบดี รองคณบดีและรองคณบดีฝ่ายต่าง ๆ หรือผู้มีอำนาจบริหารในระดับสูงของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

“ผู้ดูแลระบบ”.../-๒-

"ผู้ดูแลระบบ" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ ระบบฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์

"ผู้ใช้" หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานมหาวิทยาลัย (คณะทันตแพทยศาสตร์) ลูกจ้างสังกัดคณะ และบุคลากรทุกระดับของคณะ ที่ได้รับมอบหมายจากผู้บริหารให้เป็นผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศใด ๆ รวมถึงบุคคลจากหน่วยงานภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานสารสนเทศของมหาวิทยาลัย

"หน่วยงานภายนอก" หมายถึง องค์กรซึ่งคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล อนุญาตให้มีสิทธิ ในการเข้าถึงหรือใช้ข้อมูลหรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของคณะ โดยจะได้รับสิทธิตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของคณะโดยมิได้รับอนุญาต

"การรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์" (Information and Cyber Security) หมายถึง การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) และการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

"ความมั่นคงปลอดภัยสารสนเทศ" (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"ความลับ" (confidentiality) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้ เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

"ความถูกต้องครบถ้วน" (integrity) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

"สภาพพร้อมใช้งาน" (availability) หมายถึง การรับรองได้ว่าข้อมูล หรือระบบสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

"ไซเบอร์" (Cyber) หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

"เทคโนโลยีปฏิบัติการ" หมายถึง (Operational Technology: OT) ฮาร์ดแวร์ ซอฟต์แวร์ และเทคโนโลยีการสื่อสาร ที่หน่วยงานนำมาใช้เพื่อการตรวจสอบ การควบคุม รวมถึงการจัดการภายในของกระบวนการและการทำงานของอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติงานรวมถึงระบบปฏิบัติการในอากาศยาน

"เทคโนโลยีสารสนเทศ" หมายถึง (Information Technology: IT) ฮาร์ดแวร์ ซอฟต์แวร์ และเทคโนโลยีการสื่อสาร ที่หน่วยงานนำมาใช้เพื่อการประมวลผลข้อมูล การสร้างข้อมูล การจัดเก็บข้อมูล รวมถึงการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ทุกรูปแบบ

"ปัญญาประดิษฐ์" (Artificial Intelligence: AI) หมายถึง ศาสตร์แขนงหนึ่งของวิทยาศาสตร์

คอมพิวเตอร์.../-๓-

คอมพิวเตอร์ ที่เกี่ยวข้องกับวิธีการทำให้คอมพิวเตอร์มีความสามารถคล้ายมนุษย์หรือเลียนแบบพฤติกรรมมนุษย์ โดยเฉพาะความสามารถในการคิดเองได้ หรือมีปัญญา ซึ่งปัญญานี้มนุษย์เป็นผู้สร้างให้คอมพิวเตอร์ จึงเรียกว่าปัญญาประดิษฐ์ มุมมองต่อ AI ที่แต่ละคนมีอาจไม่เหมือนกัน ขึ้นอยู่กับว่าเราต้องการความฉลาดโดยคำนึงถึงพฤติกรรมที่มีต่อสิ่งแวดล้อมหรือคำนึงการคิดได้ของผลผลิต AI

"ภัยคุกคามทางไซเบอร์" (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

"สินทรัพย์" (Assets) หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับคณะ และเป็นสิ่งที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่คณะเป็นเจ้าของหรือผู้ถือลิขสิทธิ์หรือสิทธิการใช้งานอย่างถูกต้องตามกฎหมาย ซึ่งรวมถึงทรัพย์สินทางปัญญาไม่ว่าจะได้มาจากการเช่า การว่าจ้าง การพัฒนาหรือการจัดซื้อ เช่น

- ข้อมูล/สารสนเทศ (Data/Information)
- ด้านกายภาพ (Physical Assets) เช่น อุปกรณ์คอมพิวเตอร์ เราเตอร์ สวิตช์ เป็นต้น
- ด้านซอฟต์แวร์ (Software Assets) เช่น ซอฟต์แวร์ที่จัดซื้อ ซอฟต์แวร์ที่พัฒนาเอง ซอฟต์แวร์ที่เช่าใช้ เป็นต้น
- การบริการและกระบวนการ (Services and Processes Assets) เช่น บริการ Cloud บริการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น
- การติดต่อสื่อสาร (Network/Communication) เช่น ลิงก์การเชื่อมต่ออินเทอร์เน็ต, VPN เป็นต้น
- สาธารณูปโภค (Facility/Heating Ventilation and Air Conditioning: HVAC)
- บุคลากร (People Assets)

"หน่วยงานผู้เป็นเจ้าของสินทรัพย์สารสนเทศ" หมายถึง หน่วยงานผู้รับผิดชอบสินทรัพย์สารสนเทศ

"เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ" (Information Security Event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบาย ด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของมหาวิทยาลัยมหิดลถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"อุปกรณ์คอมพิวเตอร์" (Computer Equipment) หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงและส่วนประกอบต่าง ๆ ทางกายภาพของเครื่องคอมพิวเตอร์ เช่น printer, modem, hard disk, disk drive, sound card.../-๔-

sound card, mouse, keyboard, RAM, CPU และ network card เป็นต้น

"อุปกรณ์คอมพิวเตอร์ประเภทพกพา" (Mobile Computing Device) หมายถึง อุปกรณ์คอมพิวเตอร์ ที่สะดวกในการพกพา เช่นคอมพิวเตอร์โน้ตบุ๊ค (Laptop) และอุปกรณ์พีดีเอ (PDA) เป็นต้น

"บัญชีผู้ใช้" (Account ID) หมายถึง ชื่อและรหัสบัญชีผู้ใช้งานเพื่อใช้ในการพิสูจน์ตัวตนก่อนการเข้าใช้เครือข่ายและบริการระบบสารสนเทศของมหาวิทยาลัยมหิดล

"รหัสผ่าน" (password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของคณะ

"Idle Timeout" หมายถึง ระยะเวลาที่ผู้ใช้งานเชื่อมต่อกับระบบสารสนเทศ และไม่มีการใช้งานเกินระยะเวลาที่กำหนด ระบบสารสนเทศจะทำการตัดการเชื่อมต่อผู้ใช้งานออกจากระบบ

"Session Timeout" หมายถึง ระยะเวลาที่ผู้ใช้สามารถเชื่อมต่อกับระบบสารสนเทศได้

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

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

"ช่องโหว่" (vulnerability) หมายถึง จุดอ่อนของระบบสารสนเทศที่ทำให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบทำให้ประสิทธิภาพของการทำงานลดลง

"ความเสี่ยง" หมายถึง โอกาสของสินทรัพย์สารสนเทศในการถูกละเมิดการรักษาความมั่นคงปลอดภัย

"ระบบเครือข่าย" (network) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยมหิดล

"เครื่องคอมพิวเตอร์แม่ข่าย" (server) หมายความว่า เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์ สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่น ๆ หรือควบคุมการทำงานในเครือข่าย

"ระบบปฏิบัติการ" (operating system) หมายถึง ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำการควบคุม การทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

"ระบบงาน" หมายถึง การนำระบบสารสนเทศมาประยุกต์ใช้ในการทำงาน เพื่อให้งานสำเร็จตามวัตถุประสงค์.../-๕-

วัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบงานบุคคล ระบบจัดเก็บเอกสาร

"ระบบสารสนเทศ" หมายถึง ชุดขององค์ประกอบที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายสารสนเทศ เพื่อช่วยการตัดสินใจและการควบคุมในองค์กรในการทำงานของระบบสารสนเทศ ประกอบไปด้วยกิจกรรม ๓ อย่าง คือ การนำข้อมูลเข้าสู่ระบบ (Input) การประมวลผล (Processing) และการนำเสนอผลลัพธ์ (Output)

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"เทคโนโลยีสารสนเทศและการสื่อสาร"(Information and communication technology) หมายถึง เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ ๓ ส่วนคือ คอมพิวเตอร์ การสื่อสาร และสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

"ข้อมูล" หมายถึง ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

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

ข้อ ๓ วัตถุประสงค์

๓.๑ เพื่อคงไว้ซึ่งการให้บริการเครือข่ายคอมพิวเตอร์คณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล ได้อย่างมีประสิทธิภาพและเสถียรภาพ

๓.๒ เพื่อปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้

๓.๓ เพื่อปกป้องและรักษาซึ่งเอกภาพของข้อมูลและทรัพยากรสารสนเทศของคณะ

๓.๔ เพื่อให้ผู้มีส่วนเกี่ยวข้องเข้าใจถึงหลักปฏิบัติการใช้เครือข่ายคอมพิวเตอร์ตามหลักจริยธรรมและหลักกฎหมาย

๓.๕ เพื่อกำหนดมาตรฐานแนวปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ

ข้อ ๔ คณะต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะ ให้มีสาระสำคัญเพื่อการนำไปดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ดังนี้

หมวดที่ ๑.../-๖-

หมวดที่ ๑
การกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
(Information and Cybersecurity Governance)

ข้อ ๕ การกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information and Cybersecurity Governance)

๕.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และมาตรการที่เกี่ยวข้อง ต้องมีการกำหนดและอนุมัติโดยผู้บริหาร มีการเผยแพร่ รวมทั้งสร้างการรับรู้ให้แก่บุคลากรและบุคคลภายนอกที่เกี่ยวข้อง ตลอดจนทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อคณะ โดยให้ครอบคลุมการรักษาความลับ (Confidentiality), ความถูกต้อง (Integrity), และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๒๒ และเป็นไปตามกฎหมายและกฎระเบียบของที่เกี่ยวข้อง

๕.๒ โครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศ ต้องจัดให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยมอบหมายบทบาทหน้าที่ และความรับผิดชอบให้แก่ผู้บริหาร ผู้ดูแลระบบ และผู้ใช้

๕.๓ คณะต้องดำเนินการ จัดทำแผนการตรวจสอบและประเมินความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และกฎหมายที่เกี่ยวข้อง

๕.๔ คณะต้องดำเนินการ จัดทำรายงานผลการตรวจสอบ พร้อมทั้งวิเคราะห์ปัญหาและนำข้อเสนอแนะไปปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยให้มีประสิทธิภาพยิ่งขึ้น

๕.๕ ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

(๑) ผู้บริหาร

ผู้บริหารของทุกส่วนงานต้องกำกับดูแลให้ผู้ใช้ได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติตามนโยบายและแนวปฏิบัติของคณะ

(๒) ผู้ใช้

ผู้ใช้ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของคณะ และต้องรายงานต่อคณะ หากพบปัญหาหรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ

(๓) ผู้ดูแลระบบ

ผู้ดูแลระบบที่เกี่ยวกับสารสนเทศของคณะต้องตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ โดยมาตรการด้านความมั่นคงปลอดภัยของระบบต้องผ่านการพิจารณาและได้รับคำแนะนำจากผู้บริหารและผู้ดูแลระบบที่เกี่ยวกับสารสนเทศของคณะต้องมีความรับผิดชอบในเรื่องความมั่นคงปลอดภัยของสารสนเทศ

(๔) หน่วยงาน.../-๗-

(๔) หน่วยงานภายนอก

หน่วยงานภายนอกที่คณะอนุญาตให้มีสิทธิในการเข้าถึงข้อมูลสารสนเทศ หรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัยต้องรับผิดชอบและปฏิบัติตามนโยบายและแนวปฏิบัติของคณะอย่างเคร่งครัด โดยการใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการกระทำที่เกิดขึ้นและไม่เปิดเผยความลับของคณะโดยมิได้รับอนุญาต

หมวดที่ ๒
การระบุสินทรัพย์สารสนเทศและการบริหารจัดการความเสี่ยง
(Information Asset Identification and Risk Management)

ข้อ ๖ การระบุสินทรัพย์สารสนเทศและการบริหารจัดการความเสี่ยง (Information Asset Identification Risk Management)

๖.๑ ทะเบียนสินทรัพย์สารสนเทศและการจัดชั้นความลับสารสนเทศ (Information Asset Inventory and Information Classification)

(๑) ทะเบียนสินทรัพย์สารสนเทศทั้งเทคโนโลยีสารสนเทศ (Information Technology: IT) โดยเฉพาะระบบที่สำคัญ (Critical System) พร้อมทั้งผู้รับผิดชอบ ต้องได้รับการจัดทำและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

(๒) การใช้งานสินทรัพย์สารสนเทศ (Acceptable Use Policy: AUP) ต้องมีการกำหนดเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสินทรัพย์เหล่านั้น

(๓) แนวทางการจัดระดับชั้นความลับของสารสนเทศ การบ่งชี้สารสนเทศ และการดูแลสารสนเทศตามระดับชั้นความลับ ต้องมีการกำหนดให้สอดคล้องตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของคณะ

๖.๒ การประเมินความเสี่ยงและกลยุทธ์ในการบริหารจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(๑) คณะต้องดำเนินการ จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง พร้อมทั้งกำหนดมาตรการควบคุมและต้องควบคุมและบริหารจัดการความเสี่ยงที่เกิดขึ้น โดยการประเมินความเสี่ยงจะต้องครอบคลุมทรัพย์สินของคณะ และหน่วยงานภายนอกที่ให้บริการหรือสนับสนุนการดำเนินงานระบบเทคโนโลยีสารสนเทศของคณะ

(๒) คณะต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยง ต้องควบคุมและติดตามการบริหารจัดการความเสี่ยงให้เป็นไปตามแผนการจัดการความเสี่ยงที่กำหนดไว้ และให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้ของคณะ

๖.๓ การบริหาร.../-๘-

๖.๓ การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

(๑) คณะต้องดำเนินการกำหนดเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศในการคัดเลือกผู้ให้บริการภายนอก รวมถึงกระบวนการและขั้นตอนปฏิบัติในการบริหารจัดการผู้ให้บริการภายนอกซึ่งจัดหาผลิตภัณฑ์หรือให้บริการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศแก่คณะต้องมีการกำหนดและนำไปปฏิบัติให้ครอบคลุมตลอดทั้งห่วงโซ่ของผลิตภัณฑ์และบริการ และการถ่ายโอนข้อมูลสารสนเทศ

(๒) คณะทำต้องดำเนินการกำหนดข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information Security) รวมถึงข้อตกลงของระดับการให้บริการ (Service Level Agreement: SLA) ต้องได้รับการระบุในสัญญากับผู้ให้บริการภายนอก

๖.๔ การปฏิบัติตามข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Compliance Management)

(๑) คณะต้องดำเนินการพิจารณา กฎหมาย กฎระเบียบ สัญญาและข้อบังคับที่เกี่ยวข้องในการปฏิบัติงาน ด้านความมั่นคงปลอดภัย ความมั่นคงปลอดภัย ความเป็นส่วนตัว สิทธิในสินทรัพย์ทางปัญญาต้องได้รับการทบทวน และกำหนดให้มีการควบคุมดูแลให้ปฏิบัติตามที่กำหนดไว้

(๒) คณะต้องกำหนดให้มีการดำเนินการตรวจสอบการปฏิบัติตามกฎหมาย มาตรฐานสากล และข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ

(๓) คณะต้องดำเนินการ จัดทำให้มีการประเมินความสอดคล้องกับนโยบาย ความมั่นคงปลอดภัยสารสนเทศ และกฎหมายที่เกี่ยวข้อง

๖.๕ การกำกับดูแลปัญญาประดิษฐ์ (Artificial Intelligence Governance)

การนำเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้งานต้องมีการควบคุม กำกับดูแล และการประเมินความเสี่ยงในการนำระบบ AI มาใช้ในการให้บริการและการดำเนินการภายในคณะ โดยควบคุมผลกระทบจากการใช้ AI ในทุกมิติ รวมถึงผลกระทบต่อผู้มีส่วนได้เสียทั้งหมด โดยต้องควบคุมความเสี่ยงต่าง ๆ ให้อยู่ในระดับที่ยอมรับได้ และมีความชัดเจนตรวจสอบได้

๖.๖ การกำกับดูแลการใช้งานระบบคลาวด์ (Cloud Computing Governance)

(๑) การนำเทคโนโลยีคลาวด์มาใช้งานต้องมีการควบคุม กำกับดูแล และการประเมินความเสี่ยงในการนำระบบคลาวด์มาใช้ในการให้บริการและการดำเนินการภายในคณะ โดยควบคุมผลกระทบจากการใช้คลาวด์ในการใช้บริการและให้บริการและผลกระทบต่อผู้มีส่วนได้เสียทั้งหมด โดยต้องควบคุมความเสี่ยงต่าง ๆ ให้อยู่ในระดับที่ยอมรับได้ และมีความชัดเจนตรวจสอบได้

(๒) คณะต้องดำเนินการจัดการและควบคุมความมั่นคงปลอดภัยของบริการคลาวด์ การจัดเก็บข้อมูลบนระบบคลาวด์ต้องดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัย เช่น การเข้ารหัสข้อมูล การจำกัดสิทธิ์การเข้าถึง และการตรวจสอบผู้ให้บริการคลาวด์อย่างสม่ำเสมอ

หมวดที่ ๓.../-๙-

หมวดที่ ๓
การป้องกันสารสนเทศ
(Information Protection)

ข้อ ๗ การป้องกันสารสนเทศ (Information Protection)

๗.๑ การควบคุมการเข้าถึง (Access Control)

(๑) คณะต้องดำเนินการกำหนดสิทธิการเข้าถึงข้อมูลและสินทรัพย์ที่เกี่ยวข้อง ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานสินทรัพย์แต่ละประเภท โดยใช้หลักการให้สิทธิเท่าที่จำเป็น (Need-to-Know Basis) และหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (Principle of Least Privilege) และต้องทบทวน ปรับปรุง ตามระยะเวลาที่กำหนด และถอดถอน เมื่อไม่มีความจำเป็นในการใช้งาน

(๒) คณะต้องดำเนินการกำหนดมาตรการควบคุมการเข้าถึงก่อนอนุญาตให้เข้าถึงข้อมูลและสินทรัพย์ที่เกี่ยวข้อง ต้องมีการพิสูจน์ตัวตนโดยใช้มาตรการสำหรับการพิสูจน์ตัวตนที่มั่นคงปลอดภัยและต้องมีการสื่อสารแนวปฏิบัติการใช้รหัสผ่านที่ดีไปยังผู้ใช้ที่เกี่ยวข้อง เช่น การใช้ระบบยืนยันตัวตนหลายขั้นตอน (MFA) การใช้รหัสผ่านที่มีความมั่นคงปลอดภัย และการจำกัดสิทธิ์การเข้าถึงตามบทบาท (RBAC) เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๓) คณะต้องดำเนินการใช้มาตรการเข้ารหัสข้อมูลสำคัญ ในระหว่างการจัดเก็บและการส่งผ่าน โดยใช้มาตรฐานการเข้ารหัสที่เหมาะสม เพื่อป้องกันการถูกดักจับหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗.๒ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

๗.๒.๑ การสร้างความมั่นคงปลอดภัยก่อนการว่าจ้าง (Prior to Employment)

(๑) ก่อนการว่าจ้าง บุคลากร คณะต้องดำเนินการตรวจสอบภูมิหลังอย่างละเอียดและความเหมาะสมของบุคลากรก่อนเข้าปฏิบัติงาน เช่น การตรวจสอบประวัติการทำงาน (Background Check), ประวัติอาชญกรรม, สุขภาพ เป็นต้น โดยพิจารณาควบคู่กับกฎหมาย ระเบียบ ข้อบังคับ จริยธรรม และความเสี่ยงที่เกี่ยวข้อง เมื่อประสงค์จะว่าจ้าง

(๒) คณะต้องดำเนินการระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศลงในข้อตกลงการจ้างงาน และต้องควบคุมให้ลงนามในข้อตกลงการรักษาความลับการปฏิบัติงานที่เกี่ยวข้องกับข้อมูลและความลับของคณะ

๗.๒.๒ การสร้างความมั่นคงปลอดภัยในระหว่างการว่าจ้าง (During Employment)

(๑) คณะต้องกำหนดแผนการฝึกอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับบุคลากรภายในและบุคคลภายนอกที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก การให้ความรู้ การฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอเป็นประจำอย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยทางไซเบอร์

(๒) คณะต้อง.../-๑๐-

(๒) คณะต้องกำหนดกระบวนการทางวินัยเพื่อลงโทษผู้ใช้งานที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของคณะต้องมีการกำหนดและสื่อสารไปยังบุคลากรและบุคคลภายนอกที่เกี่ยวข้อง

(๓) คณะต้องกำหนดมาตรการการปฏิบัติงานจากระยะไกลให้กับบุคลากรและบุคคลภายนอกที่เกี่ยวข้องที่จำเป็นต้องปฏิบัติงานและ ต้องได้รับการอนุญาตจากผู้บังคับบัญชา และต้องปฏิบัติตามระเบียบหรือข้อบังคับในการปฏิบัติงานจากระยะไกลอย่างเคร่งครัด

(๔) เมื่อพบจุดอ่อน หรือช่องโหว่ หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ บุคลากรและบุคคลภายนอกที่เกี่ยวข้องต้องรายงานสิ่งที่เกิดขึ้นให้แก่หน่วยงานที่รับผิดชอบทราบโดยทันที โดยผ่านช่องทางที่คณะกำหนดไว้

๗.๒.๓ การสร้างความมั่นคงปลอดภัยเมื่อสิ้นสุดหรือเปลี่ยนแปลงการว่าจ้าง (Termination or Change of Employment)

(๑) คณะต้องดำเนินการกำหนดมาตรการสำหรับบุคลากรที่พ้นสภาพการทำงานเมื่อลาออกหรือพ้นสภาพการทำงาน

(๒) คณะต้องดำเนินการเพิกถอนสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูลสำคัญทันที เช่น การระงับบัญชีผู้ใช้งาน และยืนยันการคืนอุปกรณ์ที่ได้รับไป เป็นต้น

(๓) คณะต้องกำหนดกระบวนการและช่องทางให้กับบุคลากรและบุคคลภายนอกที่เกี่ยวข้องต้องคืนสินทรัพย์ของคณะทั้งหมดที่ตนเองถือครองเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานสิทธิในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องถูกถอดถอนเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงานทันทีหรือภายในระยะเวลาที่กำหนดไว้

๗.๓ การแบ่งปันข้อมูล (Information Sharing)

(๑) คณะต้องจัดทำข้อมูลสำหรับการติดต่อกับหน่วยงานผู้ควบคุม/กำกับดูแล และกลุ่มพิเศษที่มีความสนใจในเรื่องเดียวกัน ต้องมีการจัดทำและปรับปรุงให้เป็นปัจจุบัน เพื่อใช้ในการติดต่อประสานงานในเรื่องที่สำคัญและจำเป็น

(๒) คณะต้องดำเนินการรวบรวม ติดตามข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์จากแหล่งที่น่าเชื่อถือ เจ้าของผลิตภัณฑ์หรือผู้ให้บริการภายนอก สำหรับจัดทำข้อมูลหรือข่าวกรองด้านความมั่นคงปลอดภัย เพื่อกำหนดแนวทางแผนการในการป้องกันและรับมือภัยคุกคามทางไซเบอร์

๗.๔ ความมั่นคงปลอดภัยกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

๗.๔.๑ พื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

(๑) คณะต้องดำเนินการกำหนดพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย หรือพื้นที่สำนักงาน ห้องทำงาน และห้องจัดเก็บอุปกรณ์ต่าง ๆ ต้องมีการกำหนดขอบเขตหรือบริเวณที่ชัดเจน โดย

บริเวณดัง.../-๑๑-

บริเวณดังกล่าว ต้องมีการป้องกันทางกายภาพและด้านสภาพแวดล้อม ต้องมีการควบคุมการเข้า-ออก รวมถึงมีการเฝ้าระวังและติดตามการเข้าถึงพื้นที่

(๒) คณะต้องจัดทำมาตรการรักษาความมั่นคงปลอดภัยสำหรับพื้นที่ปฏิบัติงานและมาตรการรักษาความมั่นคงปลอดภัยต้องครอบคลุมพื้นที่สำคัญ เช่น ศูนย์คอมพิวเตอร์ ห้องเซิร์ฟเวอร์ ห้องควบคุมระบบ และพื้นที่จัดเก็บข้อมูลสำคัญ กำหนดให้การควบคุมการเข้าถึงต้องถูกจำกัดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เช่น การใช้บัตรผ่าน ลายนิ้วมือ หรือระบบสแกนใบหน้า พร้อมบันทึกการเข้า-ออกเพื่อตรวจสอบย้อนหลัง

(๓) คณะต้องดำเนินการติดตั้งระบบเฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) ระบบเตือนภัยอัตโนมัติ หรือสัญญาณเตือนภัยต่าง ๆ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือและมาตรการอื่น ๆ ที่มีความเหมาะสมสำหรับป้องกันข้อมูลและระบบสารสนเทศโดยครอบคลุมพื้นที่สำคัญทั้งหมดของหน่วยงาน และระบบที่ดำเนินการติดตั้งต้องบันทึกข้อมูลอย่างน้อย ๙๐ วัน

(๔) เอกสารหรือสื่อบันทึกข้อมูลแบบพกพา (Removable Storage Media) หรือสื่อบันทึกข้อมูลภายนอก (External Storage Media) ต้องได้รับการจัดเก็บในสถานที่ที่ปลอดภัยและได้รับการควบคุมดูแล

๗.๔.๒ ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

(๑) อุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสารต้องมีการจัดวางและป้องกันโดยคำนึงถึงความมั่นคงปลอดภัย ผู้ใช้งานต้องออกจากระบบหรือทำการล็อคหน้าจอ เมื่อออกห่างจากเครื่องคอมพิวเตอร์ หรือปิดเครื่องหากไม่มีความจำเป็นต้องใช้งาน ซึ่งครอบคลุมถึงอุปกรณ์ที่มีการใช้งานนอกคณะ ระบบสาธารณูปโภคที่สนับสนุนการทำงานของอุปกรณ์ดังกล่าว สายสัญญาณไฟฟ้าและข้อมูลต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้บริการด้านเทคโนโลยีสารสนเทศใช้งานได้อย่างต่อเนื่อง

(๒) ก่อนที่จะจำหน่ายอุปกรณ์ที่มีสื่อบันทึกข้อมูลสารสนเทศ หรือนำอุปกรณ์นั้นกลับมาใช้ใหม่ ต้องได้รับการตรวจสอบว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ถูกลบทิ้ง ย้าย หรือทำลายตามระดับชั้นความลับด้วยวิธีการที่ทำให้มั่นใจได้ว่าจะไม่สามารถกู้คืนข้อมูลเหล่านั้นกลับมาใช้ได้อีก

(๓) คณะต้องกำหนดมาตรการทำลายอุปกรณ์และสื่อจัดเก็บข้อมูลที่ไม่ได้ใช้งาน โดยจัดทำกระบวนการทำลายข้อมูลที่ปลอดภัย เช่น การลบข้อมูลแบบถาวร (Data Wiping) การบดทำลายอุปกรณ์ หรือการเผาทำลาย ตามหลักมาตรฐานด้านความมั่นคงปลอดภัย เพื่อป้องกันไม่ให้ข้อมูลรั่วไหลออกไป

๗.๕ การรักษาความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคล (Information and Personal Data Protection)

๗.๕.๑ การรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Protection)

สารสนเทศของคณะต้องได้รับการควบคุมดูแลโดยสอดคล้องและเป็นไปตามระดับชั้นความลับของสารสนเทศที่คณะกำหนด รวมถึงต้องมีการกำหนดมาตรการการสำรองสารสนเทศและการทดสอบการกู้คืน มาตรการในการป้องกันการรั่วไหลของสารสนเทศ และมาตรการในการลบหรือทำลายสารสนเทศเมื่อ

ไม่มีความ.../-๑๒-

ไม่มีความจำเป็นในการเก็บรักษาหรือใช้งาน

๗.๕.๒ การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Security in Personal Data Protection)

(๑) มาตรการที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ได้แก่ มาตรการสำรองและทดสอบการกู้คืน มาตรการการป้องกันการรั่วไหลของข้อมูลส่วนบุคคล และมาตรการการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ต้องได้รับการกำหนดและนำไปปฏิบัติ โดยครอบคลุมถึงการป้องกันส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in Depth) และการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและโดยค่าเริ่มต้น (Data Protection by Design and by Default)

(๒) บันทึกกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ต้องมีการจัดเก็บและป้องกันเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบข้อมูลส่วนบุคคลได้

๗.๖ ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operation Security)

(๑) ขั้นตอนในการปฏิบัติงานด้านสารสนเทศ ต้องมีการกำหนด ทบทวน และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๒) มาตรการด้านความมั่นคงปลอดภัยในการปฏิบัติงาน ต้องมีการกำหนดให้ครอบคลุมด้านการบริหารการเปลี่ยนแปลง การบริหารจัดการความต้องการทรัพยากรสารสนเทศ การป้องกันโปรแกรมไม่พึงประสงค์ การสำรองข้อมูลและทดสอบข้อมูลที่สำคัญ การเฝ้าระวังความผิดปกติ การจัดเก็บบันทึกเหตุการณ์ (Logging) การตั้งค่านาฬิกาของระบบสารสนเทศให้ตรงกัน การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ การเข้ารหัสลับข้อมูล และการป้องกันอุปกรณ์ปลายทางของผู้ใช้งาน

(๓) คณะต้องกำหนดแนวทางควบคุมการเข้าถึงและการป้องกันการดัดแปลง Log Files การบันทึกกิจกรรมการใช้งานระบบต้องมีการจัดเก็บและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต คณะต้องกำหนดสิทธิ์ในการดูแลรักษาและตรวจสอบ Log Files อย่างเหมาะสม เพื่อให้มั่นใจได้ว่ามีความน่าเชื่อถือ และสามารถใช้เป็นหลักฐานเมื่อมีเหตุการณ์ผิดปกติ

๗.๗ ความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

เครือข่ายและอุปกรณ์เครือข่าย ต้องได้รับการควบคุมและป้องกันด้านความมั่นคงปลอดภัย มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย และระดับของการให้บริการลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายของคณะ รวมถึงต้องมีการเฝ้าระวัง และต้องมีการแบ่งแยกเครือข่ายย่อยเพื่อจำกัดการเข้าถึง โดยพิจารณาจากระดับความสำคัญของข้อมูลที่อยู่บนเครือข่าย และผลกระทบทางด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น

๗.๘ การจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)

๗.๘.๑ ข้อกำหนด.../-๑๓-

๗.๘.๑ ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

(๑) คณะต้องมีการพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems) ในการจัดหาหรือพัฒนาระบบสารสนเทศทั้งที่เป็นระบบใหม่หรือระบบที่มีอยู่เดิม

(๒) คณะต้องกำหนดมาตรการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนาซอฟต์แวร์ต้องดำเนินการตาม Secure Development Lifecycle (SDLC) เช่น การตรวจสอบโค้ด (Code Review) การทดสอบช่องโหว่ และการแก้ไขจุดอ่อนของระบบก่อนใช้งานจริง

๗.๘.๒ การพัฒนาและทดสอบระบบสารสนเทศ (Information Systems Development and Testing)

(๑) การพัฒนาระบบสารสนเทศ ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ต้องมีกระบวนการทดสอบด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงต้องแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน หากเป็นระบบที่พัฒนาโดยบุคคลภายนอก ต้องมีการกำกับดูแล เฝ้าระวัง ติดตาม และทบทวนกิจกรรม เพื่อตรวจสอบให้แน่ใจว่ามีการปฏิบัติตามที่ได้ระบุในสัญญาจ้าง

(๒) คณะต้องดำเนินการติดตั้งระบบป้องกันมัลแวร์และดำเนินการตั้งค่าให้ระบบดำเนินการตรวจสอบเป็นประจำ รวมถึงระบบป้องกันช่องโหว่ (Patch Management) และต้องอัปเดตอย่างสม่ำเสมอ เพื่อป้องกันการโจมตีจากมัลแวร์และภัยคุกคามอื่น ๆ

หมวดที่ ๔
การเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์
(Cyber Threat Monitoring and Detection)

ข้อ ๘ การเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ (Cyber Threat Monitoring and Detection)

ระบบเทคโนโลยีสารสนเทศและระบบเทคโนโลยีปฏิบัติการที่สำคัญ ต้องได้รับการเฝ้าระวังเพื่อตรวจหาช่องโหว่ทางเทคนิค (Technical Vulnerabilities) และพฤติกรรมที่ผิดปกติ รวมถึงต้องมีการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Event) ที่อาจเป็นเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident) และมีการตอบสนองตามที่กำหนดไว้

หมวดที่ ๕.../-๑๔-

หมวดที่ ๕
การตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ
(Information Security Incident Response)

ข้อ ๙ การตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Response)

(๑) ขั้นตอนในการบริหารจัดการ บทบาท และหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Event) และเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident) ต้องได้รับการกำหนดและสื่อสารไปยังบุคลากรที่เกี่ยวข้อง ต้องมีการทดสอบตามขั้นตอนเพื่อให้ใช้ได้จริงในทางปฏิบัติ และบทเรียนที่ได้รับจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นต้องถูกนำมาวิเคราะห์และทบทวนการดำเนินการ เพื่อปรับปรุงมาตรการความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพ

(๒) เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องและจำเป็นต้องดำเนินการทางกฎหมาย หลักฐานของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศดังกล่าวต้องถูกรวบรวมและจัดเก็บให้เป็นไปตามที่กฎหมายกำหนด

(๓) คณะต้องจัดทำแผนการจัดการเหตุการณ์ที่ครอบคลุมขั้นตอนการตรวจจับ การแจ้งเตือน การประเมินผลกระทบ และการกู้คืนระบบ โดยแผนดังกล่าวต้องระบุบทบาทของทีมงานที่เกี่ยวข้องอย่างชัดเจน และต้องจัดทำระบบแจ้งเตือนที่สามารถส่งข้อมูลไปยังทีมรับมือเหตุการณ์ได้อย่างรวดเร็ว

(๔) คณะต้องมีช่องทางในการรายงานเหตุการณ์ เช่น ระบบ Helpdesk หรือ Email ที่สามารถแจ้งเหตุการณ์ได้ตลอด ๒๔ ชั่วโมง ทีมที่เกี่ยวข้องต้องวิเคราะห์เหตุการณ์และจัดทำรายงานสรุปผลเพื่อนำมาปรับปรุงมาตรการป้องกันและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำอีก

หมวดที่ ๖
การฟื้นฟูเพื่อความต่อเนื่องทางธุรกิจ
(Recovery for Business Continuity)

ข้อ ๑๐ การฟื้นฟูเพื่อความต่อเนื่องทางธุรกิจ (Recovery for Business Continuity)

(๑) คณะต้องดำเนินการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) บทบาท และหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการบริหารจัดการความต่อเนื่องทางธุรกิจต้องได้รับการกำหนดโดยคำนึงถึงความมั่นคงปลอดภัย และสื่อสารไปยังบุคลากรที่เกี่ยวข้องและปรับปรุงและทบทวนแผนให้มีความสอดคล้องกับการดำเนินงานเป็นประจำอย่างน้อยปีละ ๑ ครั้ง

(๒) ต้องมีการ.../-๑๕-

(๒) ต้องมีการทดสอบตามแผนเพื่อให้ใช้ได้จริงในทางปฏิบัติอย่างน้อยปีละ ๑ ครั้ง รวมถึงดำเนินการทบทวนและปรับปรุงแผนให้เป็นปัจจุบัน

หมวดที่ ๗ ขอบเขตมีผลบังคับใช้

(Boundary)

ข้อ ๑๑ นโยบายนี้มีผลบังคับใช้กับทุกตำแหน่งพื้นที่ที่สามารถเข้าถึงระบบสารสนเทศและเครือข่ายของคณะ ซึ่งรวมถึงการเข้าถึงจากระยะไกลหรือการเชื่อมโยงจากองค์กรภายนอก การอนุญาตและมอบหมายสิทธิในการเข้าถึงระบบของคณะ ไม่ว่าจะเป็นระบบสารสนเทศด้านวิชาการ และระบบสารสนเทศด้านการบริหารคณะต้องมั่นใจว่าได้มีการดำเนินการตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และได้มีการสร้างความเข้าใจในเรื่องภาวะความเสี่ยงที่อาจจะเกิดขึ้นและการควบคุมความเสี่ยงที่เหมาะสม

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๒๔ ก.พ. ๒๕๖๘

(รองศาสตราจารย์ ทันตแพทย์บัณฑิต จิรจริยาเวช)
คณบดีคณะทันตแพทยศาสตร์
มหาวิทยาลัยมหิดล