ประกาศคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ ของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

พ.ศ.๒๕๖๔

.....

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ให้มีความมั่นคงปลอดภัยและเชื่อถือได้ นั้น

เพื่อให้การดำเนินการทางด้านสารสนเทศ ของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากลและมีการพัฒนาปรับปรุงความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง คณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

อาศัยอำนาจตามความในมาตรา ๓๗ แห่งพระราชบัญญัติมหาวิทยาลัยมหิดล พ.ศ ๒๕๕๐ คณบดีโดยความเห็นชอบของคณะกรรมการประจำคณะกรรมการประจำคณะทันตแพทยศาสตร์ ในการประชุมครั้งที่ ๗ เมื่อวันที่ ๑ กรกฎาคม พ.ศ.๒๕๖๔ จึงเห็นสมควรกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

๑. ในประกาศนี้

“คณะ” หมายถึง คณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

“แนวปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายด้านเทคโนโลยีสารสนเทศของคณะได้ง่ายขึ้น

“ผู้บริหาร”หมายถึง คณบดี และรองคณบดีฝ่ายต่างๆ ผู้อำนวยการโรงพยาบาล หรือคณะกรรมการประจำคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ ระบบฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์

“ผู้ใช้”หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย ลูกจ้าง และบุคลากรทุกระดับของคณะที่ได้รับมอบหมายจากผู้บริหารให้เป็นผู้ปฏิบัติงานเกี่ยวกับระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศใดๆ

“ระบบสารสนเทศ” หมายถึง ระบบงานที่นำเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ เป็นองค์ประกอบหลักในการประมวลผลข้อมูลเพื่อให้ได้ข้อมูลสารสนเทศตรงตามเป้าหมายการดำเนินงานของคณะ

“การควบคุมการเข้าถึง.../-๒-

"การควบคุมการเข้าถึงระบบสารสนเทศ" หมายถึง การตรวจสอบ การอนุมัติ และการกำหนดสิทธิในการผ่านเข้าสู่ระบบสารสนเทศของคณะ

๒. วัตถุประสงค์

๒.๑ เพื่อคงไว้ซึ่งการให้บริการเครือข่ายคอมพิวเตอร์ คณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล อย่างมีประสิทธิภาพและเสถียรภาพ

๒.๒ เพื่อปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวของผู้ใช้

๒.๓ เพื่อปกป้องและรักษาซึ่งเอกภาพของข้อมูลและทรัพยากรสารสนเทศของคณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

๒.๔ เพื่อให้ผู้มีส่วนเกี่ยวข้องเข้าใจถึงหลักปฏิบัติการใช้เครือข่ายคอมพิวเตอร์ตามหลักจริยธรรมและหลักกฎหมาย

๒.๕ เพื่อกำหนดมาตราฐานแนวปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ

๓. คณะต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะ โดยมีสาระสำคัญ ดังนี้

๓.๑. การควบคุมการเข้าถึงสารสนเทศ

๑) คณะต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยกำหนดหลักเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงข้อมูล ประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมถึงระดับชั้นการเข้าถึงข้อมูล เวลาที่เข้าถึงข้อมูลได้ และช่องทางการเข้าถึงข้อมูล

๒) คณะต้องควบคุมการกำหนดสิทธิการใช้งานของผู้ใช้งานตามหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย รวมถึงการบริหารจัดการ การเข้าถึงข้อมูลของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลหรือสารสนเทศ รวมถึงการลักอุปกรณ์ประมวลผลสารสนเทศ

๓) คณะต้องควบคุมการเข้าถึงเครือข่ายเพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๔) คณะต้องควบคุมการเข้าถึงระบบปฏิบัติการเพื่อป้องกันการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์โดยไม่ได้รับอนุญาต

๕) คณะต้องควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศ เพื่อป้องกันการเข้าถึงสารสนเทศอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

๓.๒ การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

คณะต้องจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของบุคลากรเพื่อดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง รวมถึงการจัดทำแผนเตรียมความ

พร้อมกรณีฉุกเฉิน.../-๓-

พร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ทั้งนี้ คณะต้องจัดให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

๓.๓ การตรวจสอบและประเมินความเสี่ยง

คณะต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) เพื่อทราบข้อมูลระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของคณะ

๔. คณะต้องกำหนดแนวปฏิบัติหรือข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศที่ได้ประกาศใช้งานแล้ว โดยได้รับความเห็นชอบจากคณะกรรมการประจำคณะ และประชาสัมพันธ์ให้ผู้เกี่ยวข้องทราบเพื่อสามารถเข้าถึงและปฏิบัติตามแนวปฏิบัติได้ชัดเจน

ทั้งนี้ แนวปฏิบัติจะต้องมีสาระสำคัญครอบคลุมพันธกิจด้านเทคโนโลยีสารสนเทศ ดังนี้

๔.๑ การควบคุมการเข้าถึงระบบสารสนเทศ ประกอบด้วย

๑) การควบคุมการเข้าถึงข้อมูลและสารสนเทศ (Data and Information Access Control)

๒) การจำแนกประเภทข้อมูลและสารสนเทศ (Data and Information Classification)

๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๕) การบริหารจัดการสินทรัพย์ (Assets Management)

๖) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๗) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๘) การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๙) การบริหารจัดการซอฟแวร์และลิขสิทธิ์และการป้องกันโปรแกรมที่ไม่พึงประสงค์ (Software Licensing and intellectual property and Preventing Malwares)

๑๐) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑๑) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑๒) การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

๑๓) การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Control)

๑๔) การควบคุมการใช้อินเทอร์เน็ต (Internet Control)

๑๕) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer Control)

๑๖) การใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ (Computer Notebook and Mobile Device Control)

๑๗) การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

๑๘) การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

๑๙) การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๔.๒ การรักษาความปลอดภัย.../-๔-