ประกาศคณะแพทยศาสตร์

เรื่อง นโยบายการใช้งานระบบคอมพิวเตอร์ และเครือข่ายคณะแพทยศาสตร์

มหาวิทยาลัยเชียงใหม่ พ.ศ. ๒๕๕๙

.....

ตามที่คณะแพทยศาสตร์ ได้ประกาศนโยบายการใช้งานระบบคอมพิวเตอร์ และเครือข่ายคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ พ.ศ. ๒๕๕๕ ตั้งแต่วันที่ ๒๙ กุมภาพันธ์ พ.ศ. ๒๕๕๕ เป็นต้นมานั้น

เพื่อให้การใช้งานระบบคอมพิวเตอร์ และเครือข่ายมีความเป็นปัจจุบัน ทันสมัย สอดคล้องกับระบบเทคโนโลยีสารสนเทศในปัจจุบัน อาศัยอำนาจตามความในมาตรา ๔๐ แห่งพระราชบัญญัติมหาวิทยาลัยเชียงใหม่ พ.ศ. ๒๕๕๑ จึงยกเลิกประกาศนโยบายการใช้งานระบบคอมพิวเตอร์ และเครือข่ายคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ พ.ศ. ๒๕๕๕ และให้ประกาศใช้นโยบายการใช้งานระบบคอมพิวเตอร์ และเครือข่ายคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ พ.ศ. ๒๕๕๙ แทน รายละเอียดดังต่อไปนี้

บทนำ

๑. นโยบายนี้จัดทำขึ้นสำหรับผู้ใช้ที่จะเข้าใช้งานระบบคอมพิวเตอร์ของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ รวมไปถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต โดยผ่านทางเครือข่ายของคณะแพทยศาสตร์ โดยให้ผู้ใช้ต้องถือปฏิบัติโดยเคร่งครัด

๒. คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ขอสงวนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามีการละเมิดนโยบายการใช้งานระบบคอมพิวเตอร์ และการเชื่อมต่ออินเทอร์เน็ตของคณะแพทยศาสตร์

๓. นิยามของระบบคอมพิวเตอร์ และอุปกรณ์ประกอบของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่มีดังนี้

๓.๑ ระบบคอมพิวเตอร์และเครือข่าย หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือ ชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติที่อยู่ภายใต้การดูแลของงานเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

๓.๒ ทรัพยากร หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของงานเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

๓.๓ ผู้ใช้ หมายความว่า บุคลากร นักศึกษา หน่วยงานของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ หรือบุคลากร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้ระบบคอมพิวเตอร์และเครือข่ายของคณะแพทยศาสตร์

๓.๔ คณะแพทยศาสตร์ หมายความว่า คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

หมวด ๑ นโยบายการควบคุมการใช้ระบบสารสนเทศ (Information Security Policy)

๑.๑ จัดให้มีนโยบายการควบคุมการใช้งานสารสนเทศที่เป็นลายลักษณ์อักษร ซึ่งได้รับการอนุมัติจากผู้บริหารระดับสูง รวมถึงการแก้ไขเปลี่ยนแปลงนโยบายทุกครั้งต้องได้รับการอนุมัติด้วย

๑.๒ มีการทบทวนและปรับปรุงนโยบายที่ไม่เหมาะสม ให้สอดคล้องกับความต้องการของคณะแพทยศาสตร์

๑.๓ มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ในระบบสารสนเทศ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง

๑.๔ มีการจัดเก็บนโยบายให้เป็นลายลักษณ์อักษรไว้ในที่ผู้ใช้งาน และผู้เกี่ยวข้องเข้าถึงได้ง่าย

๑.๕ นโยบายที่จัดทำต้องมีการกำหนดวัตถุประสงค์ ขอบเขต ความรับผิดชอบ และเนื้อหาอย่างชัดเจน รวมถึงบทลงโทษ

๑.๖ มีการเผยแพร่นโยบายความปลอดภัยสารสนเทศให้ทุกคนในคณะแพทยศาสตร์ ทราบเพื่อปฏิบัติได้

๑.๗ มีรายงานอุบัติการณ์ในการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศอย่างต่อเนื่องตามกรอบมาตรฐานในการตรวจสอบ

๑.๘ มีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละครั้ง

๑.๙ มีการรายงานผู้บริหารระดับสูงของคณะแพทยศาสตร์ ทราบโดยเร็ว เมื่อมีกรณีที่นโยบายส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญ

๑.๑๐มีขั้นตอนหรือวิธีปฏิบัติเพื่อรองรับให้มีการปฏิบัติตามนโยบายที่ได้กำหนดไว้

๑.๑๑มีการกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และหน่วยงานที่เกี่ยวข้องอย่างชัดเจนในรายละเอียดของนโยบาย และผ่านความเห็นชอบจากหน่วยวินัยและนิติการ งานบริหารงานบุคคล

หมวด ๒ นโยบายการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

๒.๑ จัดให้มีคำอธิบายลักษณะงาน (Job Description) ซึ่งระบุหน้าที่และความรับผิดชอบระบบสารสนเทศของแต่ละหน้าที่งานอย่างชัดเจน

๒.๒ มีการแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบงานหลัก (Production environment)

๒.๓ จัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีที่จำเป็น

๒.๔ มีการกำหนดเจ้าของระบบงานสารสนเทศภายในคณะแพทยศาสตร์ (Information owner) เพื่อควบคุม และกำหนดการเข้าใช้ข้อมูล ยกเว้นระบบงานหลักที่มีการใช้งานร่วมกันจากหลายหน่วยงาน กำหนดให้คณะแพทยศาสตร์เป็นผู้ระบุความรับผิดชอบให้กับผู้ได้รับมอบหมายในการดูแล (System administrator) และการอนุมัติในการใช้งาน (Authorized owner)

๒.๕ กรณีที่เจ้าของระบบสารสนเทศ/ผู้ได้รับมอบหมายในการอนุมัติสารสนเทศไม่อยู่ หรือไม่สามารถปฏิบัติงานได้ และไม่มีการมอบหมายล่วงหน้า ผู้บังคับบัญชาของเจ้าของระบบสารสนเทศ/ผู้ได้รับมอบหมายในการอนุมัติสารสนเทศต้องเป็นผู้รับผิดชอบแทนหรือเป็นผู้มอบหมายให้บุคคลอื่นรับผิดชอบต่อ

หมวด ๓ นโยบายการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing Policy)

๓.๑ มีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ

๓.๒ มีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Non-disclosure Agreement) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน โดยผู้รับมอบงาน จะเป็นผู้รับผิดชอบต่อการดำเนินการทั้งหมดที่เกิดขึ้น

๓.๓ ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Development environment) เท่านั้น หากให้เข้าใช้ระบบงานจริง (Production environment) ต้องมีการควบคุม และการตรวจสอบผู้ให้บริการอย่างเข้มงวด

๓.๔ มีการกำหนดให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๓.๕ มีการกำหนดให้ผู้ให้บริการรายงานปัญหาต่าง ๆ และแนวทางการแก้ไขในการปฏิบัติงานเมื่อมีการร้องขอ หรือมีการปรับปรุงเทคโนโลยีที่เกี่ยวข้องกับระบบงาน

๓.๖ มีการจัดทำขั้นตอนในการตรวจรับงานของผู้ให้บริการ

หมวด ๔ นโยบายการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Policy)

๔.๑ มีการกำหนดผู้รับผิดชอบในเหตุการณ์ผิดปกติแต่ละประเภทอย่างชัดเจน

๔.๒ มีการกำหนดขั้นตอนในการรับมือเหตุการณ์ต่าง ๆ โดยมีการตรวจสอบ และวิเคราะห์ผู้เข้ามาจู่โจมระบบ

๔.๓ มีการกำหนดขั้นตอนปฏิบัติการกู้คืนระบบงานต่าง ๆ

๔.๔ มีการจัดทำบันทึกเหตุการณ์ที่ผิดปกติ ประกอบด้วยรายละเอียดไม่น้อยกว่า ประเภทเหตุการณ์ วันเวลา สถานที่ ลำดับความสำคัญ บุคคลที่ติดต่อ

๔.๕ เมื่อพบเหตุการณ์ที่น่าสงสัย ให้แจ้งเจ้าหน้าที่ที่รับผิดชอบทราบทันที

๔.๖ มีการเลือกยุทธวิธีที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้โจมตี เพื่อยุติปัญหาที่เกิดขึ้นได้อย่างทันเวลา และถูกต้อง

๔.๗ ระบบงานต่างๆ ที่มีความสำคัญ ต้องมีการเตรียมอุปกรณ์ และเครื่องมือสำหรับการสำรองเพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

หมวด ๕ นโยบายการปฏิบัติตามความมั่นคงปลอดภัยสารสนเทศ (Compliance Policy)

๕.๑ มีการกำหนดหน้าที่รับผิดชอบต่อผู้ตรวจสอบความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน

๕.๒ มีการกำหนดเกณฑ์วัดประสิทธิภาพการทำงานด้านความปลอดภัยสารสนเทศอย่างชัดเจน

๕.๓ มีการดำเนินการตรวจสอบการปฏิบัติตามนโยบายอย่างรัดกุม และมีรอบการตรวจสอบที่ชัดเจน

๕.๔ หน่วยงานที่รับผิดชอบต่อการตรวจสอบการปฏิบัติตามนโยบาย สงวนสิทธิในการเข้าตรวจสอบการปฏิบัติเมื่อมีการร้องขอจากผู้มีอำนาจ

๕.๕ ผู้ใช้งานที่ไม่ปฏิบัติตามนโยบายที่คณะแพทยศาสตร์กำหนด จะถูกดำเนินการตามบทลงโทษทางวินัยของคณะแพทยศาสตร์

๕.๖ ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดในการใช้ระบบสารสนเทศ ว่าด้วยการใช้ทรัพย์สินที่ถูกตามลิขสิทธิ์ทั้งที่เป็นซอฟต์แวร์ และฮาร์ดแวร์

๕.๗ ผู้ใช้งานต้องรับทราบกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศ และปฏิบัติตามกฎหมายเหล่านั้นอย่างเคร่งครัด กรณีที่มีการละเมิด ผู้ทำละเมิดจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๕.๘ ผู้ใช้งานต้องปฏิบัติต่อข้อกำหนดที่ระบุในนโยบายหลักของคณะแพทยศาสตร์

๕.๙ งานเทคโนโลยีสารสนเทศและฝ่ายงานที่เกี่ยวข้อง ต้องร่วมกันศึกษากฎเกณฑ์ที่เกี่ยวข้องในการจัดเก็บหลักฐานข้อมูลของระบบสารสนเทศ เพื่อใช้ในการอ้างอิงและตรวจสอบภายหลัง

หมวด ๖ นโยบายรหัสผ่าน (Password Policy)

๖.๑ รหัสผ่านเป็นข้อมูลสารสนเทศระดับชั้นความลับของคณะแพทยศาสตร์ กรณีผู้ใช้งานดังกล่าวเป็นผู้ใช้ที่มีระดับสิทธิพิเศษ ต้องมีการควบคุมรหัสผ่านในการเข้าใช้อย่างรัดกุม มีรายละเอียดดังนี้

๖.๑.๑ ได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร

๖.๑.๒ มีการควบคุมการใช้งานของผู้ใช้ที่มีสิทธิพิเศษอย่างเข้มงวด

๖.๑.๓ มีการกำหนดระยะเวลาในการใช้งาน และระงับทันทีเมื่อพ้นระยะเวลาดังกล่าว

๖.๑.๕ มีการเปลี่ยนรหัสผ่านใหม่ภายหลังจากการขออนุมัติใช้งาน หรืออย่างน้อยเดือนละครั้ง

๖.๒ รหัสผ่านที่ใช้ ต้องกำหนดให้มีระดับความปลอดภัยที่เหมาะสม คือ มีความซับซ้อน การควบคุมการใส่รหัสผ่านที่ผิดเกินจำนวนครั้งที่กำหนด และรหัสผ่านปรับเปลี่ยน ไม่ซ้ำของเดิม

๖.๓ รหัสผู้ใช้ที่ไม่มีการใช้งานแล้ว ต้องดำเนินการนำออก หรือระงับการใช้งาน

๖.๔ รหัสผ่านไม่ทำการเขียน หรือจดบันทึกไว้ในที่มองเห็นได้โดยง่าย ยกเว้นแต่มีรูปแบบการเขียนที่ไม่สามารถอ่านได้ง่าย หรือจัดเก็บไว้ในพื้นที่ส่วนตัว

๖.๕ การจัดส่งรหัสผ่านให้ผู้ใช้ ต้องมีการดำเนินการอย่างรัดกุม เช่น ใส่ซองปิดผนึกเป็นต้น และเมื่อผู้ใช้ได้รับรหัสผ่านให้ทำการปรับเปลี่ยนทันที

๖.๖ ในระบบที่มีความสำคัญ รหัสผ่านต้องมีการจัดเก็บไว้ในสถานที่ที่เข้าถึงได้ยาก หรือมีระบบสอบทานกัน

๖.๗ ผู้ปฏิบัติงานต้องเก็บรหัสผ่านเป็นความลับ

๖.๘ คณะแพทยศาสตร์ ควรมีการจัดเตรียมเครื่องมือเพื่อใช้ตรวจสอบความเหมาะสมของรหัสผ่าน และมีการกำหนดรอบระยะเวลาตรวจสอบ

หมวด ๗ นโยบายไฟร์วอลล์ (Firewall Policy)

๗.๑ มีการระบุบุคคลรับผิดชอบในการกำหนด แก้ไข เปลี่ยนแปลงค่าพารามิเตอร์ต่างๆ ของไฟร์วอลล์ และการเชื่อมต่อระบบเครือข่ายอย่างชัดเจน

๗.๒ มีการกำหนดขั้นตอนและวิธีปฏิบัติในการเปลี่ยนแปลงค่าพารามิเตอร์ ของไฟร์วอลล์ และระบบสนับสนุนงานด้านความปลอดภัยต่างๆ

๗.๓ มีการแบ่งแยกระบบเครือข่ายให้เหมาะสมตามการใช้งาน เช่น เครือข่ายภายใน เครือข่ายภายนอก และเครือข่าย DMZ เป็นต้น โดยใช้อุปกรณ์ไฟร์วอลล์

๗.๔ จัดให้มีระบบป้องกันการบุกรุกทางเครือข่ายเพื่อสนับสนุนการทำงานของไฟร์วอลล์ เช่น IPS/IDS Antivirus Gateway เป็นต้น

๗.๕ มีการตรวจสอบการบุกรุกการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย การเปลี่ยนแปลงแก้ไขค่าพารามิเตอร์ และการปรับเปลี่ยนขอบเขตของเครือข่าย

๗.๖ มีการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ให้เป็นปัจจุบันทันสมัยอยู่เสมอ

๗.๗ มีการตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ ก่อนเชื่อมต่อกับระบบเครือข่าย เช่นตรวจสอบไวรัส ตรวจสอบการกำหนดค่าพารามิเตอร์ต่างๆ เกี่ยวกับความปลอดภัย รวมไปถึงการตัดการเชื่อมต่ออุปกรณ์คอมพิวเตอร์ออกจากระบบเครือข่าย

๗.๘ การใช้เครื่องมือต่างๆ (tool) ในการตรวจสอบระบบเครือข่าย ต้องได้รับอนุมัติจากผู้มีอำนาจหน้าที่

๗.๙ เครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดของคณะแพทยศาสตร์ ต้องวางไว้หลังไฟร์วอลล์

๗.๑๐ เทคนิครับข้อมูลแบบนำเข้าจากภายนอกโดยไม่ได้ระบุ URL จะต้องผ่านความเห็นชอบจากผู้บังคับบัญชา

๗.๑๑ ทุกไฟร์วอลล์ต้องมีระบบป้องกันผู้บุกรุก

๗.๑๒ ไฟร์วอลล์ที่อยู่ระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน ต้องมีรหัสผ่านไม่เหมือนกัน

๗.๑๓ เจ้าหน้าที่ ที่รับผิดชอบระบบไฟร์วอลล์ ต้องเตรียมและจัดทำแผนรับมือเหตุการณ์ภัยพิบัติตามที่ได้รับอนุมัติจากผู้มีอำนาจ

๗.๑๔ เจ้าหน้าที่ ที่รับผิดชอบไฟร์วอลล์ต้องลงทะเบียนเป็นสมาชิกของเว็บ Computer Emergency Response Team และเว็บไซต์อื่นๆ ที่เหมือนกันนี้ เพื่อที่ติดตามข่าวสารช่องโหว่ไฟร์วอลล์ และวิธีการอุดช่องโหว่ของไฟร์วอลล์ที่คณะแพทยศาสตร์ใช้งาน

๗.๑๕ ทุกการเปลี่ยนแปลงค่ากำหนดของไฟร์วอลล์ การเปิดบริการ และการกำหนดเส้นทางที่เชื่อมต่อ ต้องถูกจัดเก็บบันทึกลงล็อก (Log)

๗.๑๖ ผู้ใช้งาน และผู้ดูแลระบบต้องไม่แจ้งช่องโหว่ที่พบไปยังบุคคลภายนอก หรือบุคคลภายในที่ไม่เกี่ยวข้อง นอกจากจะถูกกำหนดให้เป็นผู้รับผิดชอบในการแก้ปัญหานั้นๆ

๗.๑๗ มีระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึกล็อก (Log) ต่างๆ และกำหนดสิทธิการเข้าถึงบันทึกเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวด ๘ นโยบายการตรวจสอบ และป้องกันการบุกรุกระบบเครือข่าย (Intrusion Detection /Prevention system Policy – IDS/IPS Policy)

๘.๑ อุปกรณ์ IDS/IPS ต้องตั้งไว้ในพื้นที่ที่มีความปลอดภัย

๘.๒ จัดให้มีบุคคลรับผิดชอบในการกำหนด แก้ไข เปลี่ยนแปลงค่าพารามิเตอร์ต่างๆ ของอุปกรณ์ IDS/IPS และการเชื่อมต่อระบบเครือข่ายอย่างชัดเจน

๘.๓ มีการออกแบบ และกำหนดตำแหน่งในการตั้ง IDS/IPS ให้เหมาะสม โดยเฉพาะเครือข่ายที่เชื่อมต่อกับภายนอก

๘.๔ มีการตรวจสอบเกี่ยวกับความปลอดภัยอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย

๘.๕ มีการทดสอบทุกการปรับเปลี่ยนค่ากำหนดทั้งการอัพเดตฮาร์ดแวร์ ซอฟต์แวร์ และเหตุการณ์ ในการตรวจสอบ

๘.๖ มีการติดตั้งซอฟต์แวร์ตรวจสอบไวรัสที่ได้รับการอนุมัติจากผู้มีอำนาจบนเครื่องที่ติดตั้ง IDS/IPS ทั้งหมด ยกเว้นที่เป็นอุปกรณ์ฮาร์ดแวร์

๘.๗ กรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้โมเด็ม (Dial out) ต้องมีการจัดตั้ง IDS/IPS เพื่อตรวจสอบการละเมิดการใช้งาน

๘.๘ ทีมงานของคณะแพทยศาสตร์ ที่รับผิดชอบต่อการจัดการ IDS/IPS ต้องลงทะเบียนเป็นสมาชิกของเว็บ Computer Emergency Response Team หรือเว็บไซต์อื่นๆ ที่เหมือนกันนี้ เพื่อที่ตามข่าวสารช่องโหว่ IDS/IPS ให้เป็นปัจจุบัน

๘.๙ ทุกช่องโหว่ที่พบใน IDS/IPS ต้องถูกส่งตรงไปยังกลุ่มงานที่รับผิดชอบ

๘.๑๐ มีระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึก (Log) ต่างๆ และกำหนดสิทธิการเข้าถึงบันทึกเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวด ๙ นโยบายการเชื่อมต่อระบบสารสนเทศสู่ภายนอก (External Policy)

๙.๑ การใช้งานจากภายนอกที่นอกเหนือจากที่กำหนดไว้ ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา และตัวแทนของคณะแพทยศาสตร์

๙.๒ มีขั้นตอนในการตรวจสอบการเข้าใช้อินเทอร์เน็ตที่ไม่เหมาะสม และดำเนินการปิดเมื่อพบว่ามีปัญหาต่อระบบงานภายในคณะแพทยศาสตร์

๙.๓ การสมัครรับข่าวสารสารสนเทศอัตโนมัติแบบเรียลไทม์จากอินเทอร์เน็ต เช่น การดูภาพยนตร์ ฟังเพลง จากอินเทอร์เน็ต ต้องได้รับการอนุมัติจากผู้มีอำนาจ ยกเว้นการรับข่าวสารผ่านจดหมายอิเล็กทรอนิกส์

๙.๔ ห้ามสร้างการเชื่อมต่อเครือข่ายกับกลุ่มภายนอก ก่อนได้รับอนุญาตจากผู้มีอำนาจ ซึ่งผู้รับผิดชอบจะเฝ้าดูหรือติดตามการเชื่อมต่อนั้นอย่างใกล้ชิด

๙.๕ ผู้ใช้ต้องไม่ประกาศข้อความใดๆ ในนามขององค์กรบนเว็บบอร์ดหรือห้องสนทนาบนกลุ่มสาธารณะใดๆ บนอินเทอร์เน็ต ยกเว้นจะได้รับอนุญาตจากหน่วยงาน

๙.๖ ผู้ใช้ไม่ใช้นามสมมุติ นามผู้อื่น บนอินเทอร์เน็ต หรือบนระบบสารสนเทศใดๆ ของคณะแพทยศาสตร์ ทุกรายการที่ใช้ต้องเป็นชื่อผู้ใช้ที่อยู่ในจดหมายอิเล็กทรอนิกส์หรือระบบลงทะเบียนผู้ใช้ที่มีการผูกกับจดหมายอิเล็กทรอนิกส์

๙.๗ การเปิดเผยสารสนเทศต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ

หมวด ๑๐ นโยบายการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

๑๐.๑ มีขั้นตอนหรือวิธีปฏิบัติในการพัฒนา การแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

๑๐.๒ มีขั้นตอน หรือวิธีปฏิบัติในการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉินและมีบันทึกเหตุผลความจำเป็น รวมทั้งการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

๑๐.๓ มีการชี้แจงรายละเอียดขั้นตอนในการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ให้กับผู้ใช้งาน และบุคคลที่เกี่ยวข้อง ได้รับทราบอย่างทั่วถึง พร้อมทั้งมีกลไกการควบคุมในการปฏิบัติตาม

๑๐.๔ ระบบงานหลัก ต้องมีการแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Development environment) ออกจากส่วนที่ใช้งานจริง (Production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้เกี่ยวข้องในแต่ละส่วนเท่านั้น

๑๐.๕ ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ต้องมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

๑๐.๖ การพัฒนา หรือการแก้ไขเปลี่ยนแปลงระบบงาน ต้องตระหนักถึงระบบรักษาความปลอดภัย และเสถียรภาพการทำงานของระบบงาน

๑๐.๗ การร้องขอให้มีการพัฒนา หรือการเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำอย่างเป็นลายลักษณ์อักษรจากผู้มีอำนาจหน้าที่

๑๐.๘ มีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (Functionality) ของระบบงานหลัก

๑๐.๙ มีการสอบทานกฎเกณฑ์ของทางการในการแก้ไขเปลี่ยนแปลงระบบงาน เพื่อให้สอดคล้องกับกฎเกณฑ์ที่ระบุ

๑๐.๑๐ ผู้ร้องขอและงานเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นๆ ที่เกี่ยวข้อง ต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับพัฒนา หรือแก้ไขเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ และประมวลผลได้ครบถ้วนถูกต้อง

๑๐.๑๑ ในระบบงานสำคัญต้องมีหน่วยงาน หรือทีมงานอิสระเข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนา และการทดสอบระบบก่อนที่จะโอนย้ายไปใช้งานจริง

๑๐.๑๒ จัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ให้เป็นปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

๑๐.๑๓ มีการปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้รับพัฒนา หรือแก้ไขเปลี่ยนแปลงให้ทันสมัยอยู่เสมอ

๑๐.๑๔ มีการจัดเก็บโปรแกรมเวอร์ชั่นก่อนการพัฒนาไว้ใช้ในกรณีที่เวอร์ชั่นปัจจุบันทำงานผิดพลาด หรือไม่สามารถทำงานได้

๑๐.๑๕ มีการชี้แจงรายละเอียดการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

๑๐.๑๖ กำหนดให้มีการสอบทานระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

๑๐.๑๗ มีการจัดทำขั้นตอนการตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วน เพื่อใช้ในการดำเนินการได้อย่างมีประสิทธิภาพ

หมวด ๑๑ นโยบายด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ (Data Security Policy)

๑๑.๑ มีการแบ่งแยกข้อมูลที่เป็นชั้นความลับ (Secret, Confidential) ข้อมูลที่ใช้เปิดเผยได้

๑๑.๒ ข้อมูลสารสนเทศที่มีความสำคัญ ต้องถูกกำหนดป้ายชื่อ (Label) ข้อมูล กรณีที่ไม่มีการกำหนด จะถือว่าเป็นข้อมูลสารสนเทศที่ใช้เฉพาะภายในคณะแพทยศาสตร์ (Internal Use Only)

๑๑.๓ มีการเข้ารหัสข้อมูลที่เป็นชั้นความลับในหน่วยจัดเก็บของเครื่อง และการติดต่อระหว่างเครือข่าย

๑๑.๔ ข้อมูลที่เป็นชั้นความลับระดับสูง เมื่อมีการนำข้อมูลออกจากเครื่อง หรือออกจากคณะแพทยศาสตร์ ต้องผ่านการอนุมัติจากผู้มีอำนาจทุกครั้ง

๑๑.๕ กำหนดให้บันทึกล็อก (Log) การเข้าสู่ข้อมูลต่างๆ ที่มีระดับความสำคัญของข้อมูลสารสนเทศที่ไม่เปิดเผย

๑๑.๖ กรณีที่มีการเปิดเผยข้อมูลสู่สาธารณะ ต้องดำเนินการโดยผู้รับผิดชอบซึ่งได้รับอนุมัติจากผู้มีอำนาจ

๑๑.๗ กรณีที่มีความจำเป็นต้องเปิดเผยข้อมูลในระดับชั้นความลับระดับสูงสู่ภายนอก ผู้รับข้อมูลดังกล่าวต้องมีการเซ็นสัญญาไม่เปิดเผยความลับ (NDA)

๑๑.๘ มีการกำหนดคณะกรรมการที่รับผิดชอบในการทำลายข้อมูลเอกสาร และสื่อจัดเก็บข้อมูลอย่างชัดเจน โดยมีความเข้าใจในการทำลายอย่างถูกต้อง

๑๑.๙ มีการกำหนดขั้นตอนการทำลายข้อมูลสารสนเทศที่เป็นชั้นความลับ ซึ่งต้องมีการดำเนินการอย่างรัดกุม โดยเฉพาะเมื่อมีการนำข้อมูลสารสนเทศออกนอกสถานที่

หมวด ๑๒ นโยบายการรักษาความลับข้อมูลของคณะแพทยศาสตร์ (Privacy Policy)

๑๒.๑ เจ้าหน้าที่ของคณะแพทยศาสตร์ ต้องไม่จัดเก็บข้อมูลที่ไม่เกี่ยวข้องกับกิจการของคณะฯ ไว้ในระบบสารสนเทศของคณะฯ ระบบและข้อมูลสารสนเทศที่ใช้ภายในคณะฯ ถือเป็นทรัพย์สินของคณะฯ

๑๒.๒ มีการจัดทำระบบตรวจสอบล็อก (Log) ในการใช้งานจดหมายอิเล็กทรอนิกส์ และเครือข่าย เพื่อพิจารณากรณีที่มีการละเมิดต่อนโยบายของคณะแพทยศาสตร์

๑๒.๓ การจัดเก็บข้อมูลต่างๆ ของลูกค้าหรือคู่ค้า ต้องได้รับอนุญาตจากลูกค้าหรือคู่ค้าก่อนดำเนินการทุกครั้ง กรณีที่เป็นข้อมูลลูกค้าที่เข้าสู่ระบบของคณะแพทยศาสตร์ ต้องมีการเซ็นรับทราบในแบบฟอร์มดำเนินการทุกครั้ง

๑๒.๔ มีการแจ้งให้บุคคลหรือองค์กรที่ใช้เทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ ได้รับทราบเกี่ยวกับนโยบายการใช้ระบบสารสนเทศ

๑๒.๕ กลุ่มงานภายนอกที่เข้าใช้สารสนเทศภายในชั้นความลับจำเป็น ต้องมีการเซ็นสัญญาการไม่เปิดเผยข้อมูล (Non-disclosure agreement) ก่อนดำเนินการทุกครั้ง

๑๒.๖ ผู้ที่ละเมิดต่อการปฏิบัตินโยบายการรักษาความลับข้อมูลของคณะแพทยศาสตร์ จะได้รับการพิจารณาบทลงโทษตามวินัยของคณะแพทยศาสตร์

หมวด ๑๓ นโยบายลิขสิทธิ์และการรักษาความลับข้อมูลของคณะแพทยศาสตร์ ในเว็บ (Web Privacy Policy)

๑๓.๑ ผู้ที่ไม่มีหน้าที่เกี่ยวข้องในการดูแลบริหารระบบและเครือข่าย หากต้องการใช้บริการต่างๆ นอกเหนือจากเว็บไซต์ และเว็บเพจของคณะแพทยศาสตร์ ต้องมีการขออนุญาตพิเศษ

๑๓.๒ เว็บที่มีการเก็บข้อมูลของคณะแพทยศาสตร์ ต้องมีการกำหนดสิทธิและควบคุมการเข้าถึงเว็บไซต์ของคณะแพทยศาสตร์ กรณีเว็บทั่วไป ไม่จำเป็นต้องระบุการเข้าถึง

๑๓.๓ เว็บไซต์ต่างๆ ของคณะแพทยศาสตร์ ต้องมีข้อความประกาศให้ทราบเกี่ยวกับลิขสิทธิ์และทรัพย์สินของคณะแพทยศาสตร์

๑๓.๔ การสื่อสารข้อมูลในระดับชั้นความลับที่สำคัญผ่านอินเทอร์เน็ต ต้องมีกระบวนการเข้ารหัส

๑๓.๕ มีการกำหนดผู้รับผิดชอบต่อการปรับปรุงเว็บไซต์อย่างชัดเจน กรณีข้อมูลที่นำมาใช้จัดทำเว็บไซต์มีแหล่งที่มาไม่ชัดเจน ห้ามนำลงสู่เว็บไซต์ของคณะแพทยศาสตร์

๑๓.๖ แหล่งที่มาของข้อมูลต่างๆ ที่ไม่ได้มาจากคณะแพทยศาสตร์ ต้องมีการระบุแหล่งที่มาอย่างชัดเจน

๑๓.๗ เว็บไซต์ของคณะแพทยศาสตร์ ต้องมีการระบุผู้รับผิดชอบและผู้รับเรื่องไว้ในหน้าของเว็บไซต์ เพื่อใช้ติดต่อกรณีที่ผู้ใช้งานมีข้อสงสัยหรือต้องการข้อมูลเพิ่ม

หมวด ๑๔ นโยบายการควบคุมการเข้าถึงข้อมูลสารสนเทศ (Access Control)

๑๔.๑ มีการกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์หลักของคณะแพทยศาสตร์

๑๔.๒ การกำหนดสิทธิให้กับผู้ใช้ ต้องกำหนดเท่าที่จำเป็น โดยจัดทำทะเบียนควบคุมการเข้าใช้ระบบสารสนเทศ (Access Control List)

๑๔.๓ มีระบบตรวจสอบตัวตน และสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานหลัก โดยผู้ใช้ทุกคนต้องมีบัญชีรายชื่อของตนเอง

๑๔.๔ มีการกำหนดรหัสผ่านที่มีระบบควบคุมพิเศษเพิ่มเติมนอกเหนือจากชื่อผู้ใช้และรหัสผ่านในระบบงานสำคัญ

๑๔.๕ มีการจัดทำระบบควบคุมการเข้าใช้ด้วยผู้ใช้ในเวลาเดียวกันเพียงหนึ่งเดียว (Single session)

๑๔.๖ ค่ากำหนดเริ่มต้นของระบบไฟล์ และข้อมูลสารสนเทศต่างๆ ต้องถูกกำหนดควบคุมไม่อนุญาตให้ใช้ก่อนเสมอ

๑๔.๗ ในกรณีที่ไม่มีผู้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ ต้องมีการป้องกันการใช้งานโดยบุคคลอื่นๆ ที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง

๑๔.๘ ระบบงานต่างๆ ต้องมีการติดตั้งระบบให้มีระบบความปลอดภัยสูงสุดในปัจจุบันเท่าที่เป็นไปได้

๑๔.๙ ในกรณีที่มีความจำเป็นให้ผู้ใช้งานเป็นเจ้าของข้อมูล และมีการให้สิทธิแก่ผู้อื่นเข้าใช้งานต้องมีการระบุเฉพาะราย หรือเฉพาะกลุ่มเท่านั้น และมีการกำหนดอายุการใช้งาน รวมทั้งมีการระงับใช้ทันทีเมื่อพ้นระยะเวลาในการใช้งาน

๑๔.๑๐ ระบบงานต่างๆ ต้องมีการควบคุมการเข้าถึงเครื่องแม่ข่าย และมีการควบคุมไฟล์ที่เปิดเข้าใช้งาน

๑๔.๑๑ ไฟล์ฐานข้อมูล หรือข้อมูลสารสนเทศที่มีชั้นความลับที่สำคัญ และมีความสัมพันธ์ระหว่างกัน ที่ติดต่อข้ามเครื่อง หรือมีการทำซ้ำในต่างเครื่อง ต้องมีการเข้ารหัสในการติดต่อและจัดเก็บทุกครั้ง

๑๔.๑๒ ต้องมีการกำหนดระยะเวลารอบในการตรวจสอบระบบงาน เพื่อตรวจสอบสิ่งที่ผิดปกติ

๑๔.๑๓ เมื่อมีการปรับเปลี่ยนระดับข้อมูล ต้องมีการแจ้งให้ผู้ใช้งานทราบทันที

หมวด ๑๕ นโยบายการใช้งานระบบเครือข่ายระบบอินทราเน็ต และระบบเอ็กทราเน็ต (Intranet/Extranet)

๑๕.๑ ระบบงานต่างๆ ต้องมีการกำหนดสิทธิ และระบุผู้ใช้งานอย่างชัดเจน และรัดกุม โดยเครื่องแม่ข่ายต้องเก็บไว้ในที่ปลอดภัย ทั้งทางด้าน physical และ logical

๑๕.๒ มีการกำหนดชั้นความลับข้อมูล รวมถึงการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ

๑๕.๓ ข้อมูลที่อยู่ในระดับชั้นความลับสำคัญ ต้องมีการเข้ารหัสในการติดต่อ และการจัดเก็บ

๑๕.๔ มีการระบุผู้รับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่ากำหนดต่างๆ ที่ใช้ในระบบ

๑๕.๕ มีขั้นตอนตรวจสอบ หรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์ และเมื่อพบว่าระบบผิดปกติ ต้องรีบดำเนินการแก้ไขทันที

๑๕.๖ ต้องเปิดเฉพาะบริการ (service) เท่าที่จำเป็น และมีมาตรการป้องกันและการตรวจสอบอย่างรัดกุม

๑๕.๗ มีการดำเนินการปรับปรุงเช่น Patch และ Hot fix ของโปรแกรมระบบ (System software) อย่างสม่ำเสมอ โดยต้องไม่ส่งผลกระทบต่อการทำงานของระบบงานหลัก

๑๕.๘ มีการทดสอบโปรแกรมระบบงานที่จะนำมาใช้ทางด้านความปลอดภัย ก่อนการติดตั้งและหลังจากที่ติดตั้งไปแล้ว

๑๕.๙ มีการบริหารจัดการ และการตรวจสอบความปลอดภัยระบบเครือข่ายอยู่สม่ำเสมอ

๑๕.๑๐ การรับส่งข้อมูลชั้นความลับสำคัญผ่านเครือข่ายสาธารณะ ต้องผ่านช่องทางที่มีการเข้ารหัสข้อมูล (Encryption)

๑๕.๑๑ มีมาตรการควบคุมความถูกต้องของข้อมูลสำคัญที่จัดเก็บ นำเข้า ประมวลผล และแสดงผล นอกจากนี้ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมตรวจสอบความถูกต้องด้วย

๑๕.๑๒ มีมาตรการรักษาความปลอดภัยข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของคณะแพทยศาสตร์ เช่น การส่งซ่อมทำลายข้อมูลที่เก็บอยู่ในเครื่องก่อนที่จะนำออกจากคณะแพทยศาสตร์ เป็นต้น

๑๕.๑๓ การเข้าถึงระบบเครือข่ายในลักษณะ Remote access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้โมเด็ม (Dial out) ต้องได้รับอนุมัติจากผู้รับผิดชอบอย่างเป็นลายลักษณ์อักษร

๑๕.๑๔ มีการประเมินผลกระทบที่เกี่ยวข้องทุกครั้งที่มีการเปลี่ยนแปลงระบบ และอุปกรณ์คอมพิวเตอร์ และมีการบันทึกรายละเอียดการเปลี่ยนแปลง

๑๕.๑๕ ซอฟต์แวร์ที่ติดตั้งใช้งานเพื่อกิจการของคณะแพทยศาสตร์ ต้องมีลิขสิทธิ์ถูกต้อง หรือได้รับอนุมัติจากเจ้าของผลิตภัณฑ์ หรือตกลงกับตัวแทนผู้ขายภายในประเทศล่วงหน้า

๑๕.๑๖ มีตรวจสอบและวัดประสิทธิภาพการทำงานของระบบงานสำคัญ เพื่อรองรับการใช้งานในอนาคต

๑๕.๑๗ มีการบันทึกล็อก (Log) การทำงานของระบบคอมพิวเตอร์แม่ข่าย เครือข่าย การใช้งานของโปรแกรม ระบบงาน และระบบป้องกันการบุกรุก

๑๕.๑๘ มีระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึก (Log) ต่างๆ และกำหนดสิทธิการเข้าถึงบันทึกเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวด ๑๖ นโยบายเครือข่ายไร้สาย (Wireless Policy)

๑๖.๑ เครื่องที่ใช้ในเครือข่ายไร้สาย กำหนดเท่าที่จำเป็นเท่านั้น กรณีที่จำเป็นใช้งาน ให้ขออนุมัติจากผู้มีอำนาจ

๑๖.๒ ห้ามเปิดเผยข้อมูลเกี่ยวกับค่ากำหนดในเครือข่ายไร้สายกับบุคคลที่ไม่เกี่ยวข้อง

๑๖.๓ มีการกำหนดพื้นที่ใช้บริการเฉพาะจุด โดยมีการระบุควบคุมการใช้งานเครือข่ายไร้สายเป็นพิเศษ

๑๖.๔ เครือข่ายไร้สายต้องไม่มีระบบแจกหมายเลข IP โดยอัตโนมัติ

๑๖.๕ มีระบบตรวจสอบตัวตนก่อนเข้าใช้เครือข่ายไร้สาย

๑๖.๖ ระบบเครือข่ายไร้สายภายในคณะแพทยศาสตร์ ต้องมีระบบการตรวจสอบตัวตน (Authentication) และการเข้ารหัส (Encryption) รับรองอีกระดับหนึ่ง

๑๖.๗ มีการบันทึกล็อก (Log) การทำงานของระบบเครือข่ายไร้สาย

๑๖.๘ มีการจัดเตรียมเครื่องมือตรวจสอบการใช้งานอุปกรณ์ไร้สาย และระบุให้กับบุคคลที่รับผิดชอบเท่านั้น

๑๖.๙ มีระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึก (Log) ต่างๆ และกำหนดสิทธิการเข้าถึงบันทึกเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวด ๑๗ นโยบายการป้องกันไวรัส (Virus Protection Policy)

๑๗.๑ เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ของผู้ใช้งาน ทุกเครื่องที่นำมาใช้ในคณะแพทยศาสตร์ ต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ที่มีประสิทธิภาพที่เหมาะสม และต้องมีการปรับปรุงอัพเดตไฟล์ที่เก็บ Virus signature ให้เป็นปัจจุบันอยู่เสมอ

๑๗.๒ เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ของผู้ใช้งาน มีการติดตั้งไฟร์วอลล์ส่วนบุคคล (Personal Firewall) และได้รับการปรับปรุง Patch และ Hot fix อย่างสม่ำเสมอโดยอัตโนมัติ แต่การดำเนินการดังกล่าวต้องไม่ส่งผลกระทบต่อระบบงานหลัก

๑๗.๓ ห้ามผู้ใช้งานคอมพิวเตอร์ทำการเชื่อมต่อเครือข่ายภายนอกคณะแพทยศาสตร์ ก่อนได้รับอนุญาตจากผู้รับผิดชอบ

๑๗.๔ มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีการสำรองเครื่องคอมพิวเตอร์สำหรับระบบงานสำคัญ เพื่อป้องกันปัญหาจากไวรัสคอมพิวเตอร์

๑๗.๕ มีการจัดทำคู่มือในการป้องกันไวรัสคอมพิวเตอร์ เพื่อใช้เป็นแนวทางปฏิบัติให้แก่ผู้ใช้งาน รวมถึงการเผยแพร่ข่าวสารเกี่ยวกับไวรัสคอมพิวเตอร์ชนิดใหม่อยู่เสมอ

๑๗.๖ ผู้ใช้งานเครื่องคอมพิวเตอร์ต้องไม่ทำการติดตั้งโปรแกรมใดๆ ที่ไม่ทราบแหล่งที่มา หรือไม่ได้มาจากแหล่งตัวแทนที่ถูกแต่งตั้งจากคณะแพทยศาสตร์

๑๗.๗ ห้ามพัฒนาโปรแกรมไวรัสคอมพิวเตอร์ หรือนำโปรแกรมไวรัสคอมพิวเตอร์หรือไวรัสมาเผยแพร่โดยเจตนา

๑๗.๘ มีการเฝ้าระวังระบบเครือข่ายและคอมพิวเตอร์ เพื่อป้องกันปัญหาด้านไวรัสคอมพิวเตอร์

๑๗.๙ เมื่อพบว่าเครื่องต้องสงสัยว่าติดไวรัส ให้ปฏิบัติตามแนวทางปฏิบัติที่ทางคณะแพทยศาสตร์ กำหนด

๑๗.๑๐ ไม่ถอดถอน (Remove/Uninstall) หรือปิดบริการซอฟต์แวร์ป้องกันไวรัสบนเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

หมวด ๑๘ นโยบายอุปกรณ์คอมพิวเตอร์พกพา (Mobile Computing Policy)

๑๘.๑ ข้อมูลในระดับชั้นความลับที่สำคัญที่อยู่ในอุปกรณ์พกพา ต้องมีการเข้ารหัสหรือมีวิธีการป้องกันการเข้าใช้อย่างรัดกุม เช่น การใช้รหัสผ่านในการบูตเครื่อง เป็นต้น

๑๘.๒ ผู้ใช้งานคอมพิวเตอร์พกพาต้องได้รับทราบ มีความรู้และความเข้าใจในการใช้งานคอมพิวเตอร์ที่ถูกต้อง และมีความตระหนักถึงความปลอดภัยในการใช้งานอยู่ตลอดเวลา

๑๘.๓ โดยค่ากำหนดของเครื่องต้องระบุห้ามแชร์ไฟล์ข้อมูลในอุปกรณ์พกพา นอกจากมีความจำเป็นในการสำเนาหรือย้ายไฟล์ เมื่อดำเนินการเสร็จเรียบร้อยแล้ว ให้ทำการยกเลิกการแชร์ไฟล์ดังกล่าวทันที

๑๘.๔ ห้ามติดตั้งโมเด็มที่เครื่องลูกข่ายใดๆ รวมถึงกรณีที่เครื่องคอมพิวเตอร์มีอุปกรณ์โมเด็มรวมอยู่ด้วยกับเครื่อง ต้องถูกกำหนดห้ามใช้ ยกเว้นแต่จะได้รับการอนุมัติจากผู้มีอำนาจ

๑๘.๕ การป้องกันไวรัสคอมพิวเตอร์บนเครื่องคอมพิวเตอร์พกพา ให้ปฏิบัติตามนโยบายการป้องกันไวรัสของคณะแพทยศาสตร์

๑๘.๖ เครื่องคอมพิวเตอร์พกพาของคณะแพทยศาสตร์ ต้องใช้งานผ่านเครือข่ายสื่อสารที่หน่วยงานกำหนดไว้เท่านั้น

๑๘.๗ การเข้าใช้คอมพิวเตอร์ทางไกลจากภายนอก ต้องได้รับการอนุญาตจากผู้มีอำนาจ มีการกำหนดอายุการใช้งาน และมีรอบการตรวจสอบในทุกปี

๑๘.๘ ห้ามเก็บรหัสผู้ใช้งานและรหัสผ่าน หรือระบบกลไกควบคุมการเข้าใช้อื่นๆ ในอุปกรณ์คอมพิวเตอร์พกพา นอกเสียจากอยู่ในรูปแบบการเข้ารหัส หรือไม่สามารถเข้าถึงได้จากภายนอก

๑๘.๙ ห้ามกำหนดการเข้าสู่ระบบโดยอัตโนมัติ (Auto logon) บนเครื่องคอมพิวเตอร์พกพา

๑๘.๑๐ ต้องมีการจัดเตรียมอุปกรณ์ล็อค (Lock) คอมพิวเตอร์พกพาเมื่อไปอยู่ในที่สาธารณะและไม่มีผู้ดูแล หรือให้มีการจัดเก็บคอมพิวเตอร์พกพาในพื้นที่ควบคุมบุคคลภายนอกเข้าถึงได้

๑๘.๑๑ อนุญาตให้ผู้ใช้งาน มีอุปกรณ์คอมพิวเตอร์พกพาส่วนตัว ที่สามารถเข้าสู่ระบบเครือข่ายอินเทอร์เน็ต ได้ไม่เกิน ๕ เครื่อง

หมวด ๑๙ นโยบายการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

๑๙.๑ มีการระบุผู้รับผิดชอบในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญอย่างชัดเจน

๑๙.๒ มีขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator) ทราบ

๑๙.๓ มีการกำหนดให้เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ปฏิบัติงานโดยผ่านเมนู และจำกัดการปฏิบัติงานโดยใช้คำสั่งของระบบโดยตรง (Command line) เท่าที่จำเป็น

๑๙.๔ มีการกำหนดให้มีการบันทึกล็อก (log book) หรือเทียบเท่า ซึ่งมีรายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่างๆ ดังนี้ ผู้ปฏิบัติงาน เวลาปฏิบัติงาน รายละเอียดการปฏิบัติงาน ปัญหาที่เกิดขึ้น การแก้ไข สถานะของระบบ และผู้ตรวจสอบการปฏิบัติงาน

๑๙.๕ มีการติดตามสถานะการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

๑๙.๖ มีการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่างๆ ให้อยู่ในสภาพที่ดี และพร้อมใช้งานอยู่เสมอ

๑๙.๗ มีการกำหนดรายชื่อ หน้าที่ และความรับผิดชอบในการแก้ปัญหาอย่างชัดเจน รวมถึงหมายเลขโทรศัพท์ของผู้เกี่ยวข้อง เพื่อใช้ในการติดต่อเมื่อเกิดปัญหาทุกระดับ

๑๙.๘ มีระบบจัดเก็บบันทึกปัญหาและเหตุการณ์ผิดปกติที่เกิดขึ้น และรายงานให้ผู้บังคับบัญชาได้ทราบอย่างสม่ำเสมอ เพื่อประโยชน์ในการรวบรวมปัญหา และตรวจสอบถึงสาเหตุที่เกิดขึ้น รวมทั้งเพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาในอนาคต

๑๙.๙ การขอให้จัดพิมพ์รายงานต่างๆ ที่นอกเหนือจากที่กำหนดไว้ของระบบงานที่สำคัญ ต้องได้รับความเห็นชอบจากเจ้าของข้อมูลสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๑๙.๑๐ การพิมพ์และการจัดส่งรายงานในหัวข้อที่ ๑๙.๙ ต้องมีทะเบียนควบคุม มีการจัดเก็บไว้อย่างรัดกุม และกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน ส่วนรายงานที่ไม่ใช้ให้มีการทำลายทิ้ง

๑๙.๑๑ ข้อมูลสารสนเทศที่มีการส่งออกสู่ภายนอก ต้องมีการควบคุมอย่างรัดกุม และมีระบบยืนยันผู้รับ โดยให้มีการทำลายข้อมูลสารสนเทศเมื่อไม่มีการใช้งาน

หมวด ๒๐ นโยบายการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และการป้องกันความเสียหายกับอุปกรณ์คอมพิวเตอร์ (Physical security)

๒๐.๑ มีการกำหนดพื้นที่ควบคุมในระดับต่างๆ เพื่อใช้ในการระบุขั้นตอนในการควบคุมการเข้าสู่สถานที่ได้อย่างเหมาะสม

๒๐.๒ มีการจัดเตรียมห้องคอมพิวเตอร์เพื่อจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ที่สำคัญในระบบสารสนเทศ

๒๐.๓ มีการกำหนดผู้รับผิดชอบในการดูแลห้องคอมพิวเตอร์อย่างชัดเจน โดยมีรายละเอียดของสถานที่ เวลาที่ปฏิบัติงาน ในห้องคอมพิวเตอร์

๒๐.๔ จัดให้มีระบบตรวจสอบผู้เข้าออกห้องคอมพิวเตอร์ และมีการตรวจสอบอย่างรัดกุม

๒๐.๕ กรณีที่มีบุคคลภายนอก หรือบุคคลที่ไม่มีส่วนเกี่ยวข้องกับการเข้าใช้ศูนย์คอมพิวเตอร์ แต่จำเป็นที่ต้องเข้าไปสู่ศูนย์คอมพิวเตอร์ ต้องมีการจัดทำขั้นตอนในการดำเนินการอย่างรัดกุม

๒๐.๖ แผนผังแสดงรายละเอียดโครงสร้างระบบเครือข่าย และโครงสร้างการจัดเก็บอุปกรณ์ภายในห้องคอมพิวเตอร์ ถือว่าเป็นข้อมูลความลับ (Confidential) ห้ามเผยแพร่สู่บุคคลภายนอกโดยไม่ได้รับอนุญาต

๒๐.๗ แผนผังแสดงรายละเอียดโครงสร้างระบบเครือข่าย และโครงสร้างการจัดเก็บอุปกรณ์ภายในห้องคอมพิวเตอร์ต้องมีการปรับปรุงให้มีความทันสมัยอยู่เสมอ

๒๐.๘ ห้องคอมพิวเตอร์ ต้องมีอุปกรณ์แจ้งเหตุ ควบคุม และป้องกันไฟไหม้

๒๐.๙ ระบบป้องกันอัคคีภัยต่างๆ ต้องมีการกำหนดรอบตรวจสอบ และการบำรุงรักษาระบบอย่างเหมาะสม

๒๐.๑๐ ห้องคอมพิวเตอร์ต้องมีระบบสำรองไฟฟ้า และระบบปั่นไฟฟ้า (Generator)

๒๐.๑๑ ระบบไฟฟ้าสำรอง และระบบปั่นไฟฟ้า ต้องมีการกำหนดรอบในการตรวจสอบ และบำรุงรักษาระบบอย่างเหมาะสม

๒๐.๑๒ ห้องคอมพิวเตอร์ต้องมีระบบควบคุมอุณหภูมิ

๒๐.๑๓ ห้องคอมพิวเตอร์ต้องมีระบบป้องกันความชื้น

๒๐.๑๔ ระบบควบคุมอุณหภูมิ และระบบป้องกันความชื้น ต้องมีการกำหนดรอบตรวจสอบ และบำรุงรักษาระบบอย่างเหมาะสม

๒๐.๑๕ ห้องคอมพิวเตอร์ ต้องมีระบบเตือนภัยน้ำรั่ว

๒๐.๑๖ ระบบเตือนภัยน้ำรั่ว ต้องมีการกำหนดรอบตรวจสอบ และบำรุงรักษาระบบอย่างเหมาะสม

๒๐.๑๗ ผู้ดูแลห้องคอมพิวเตอร์ ต้องให้ความร่วมมือในการจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง ทั้งในด้านการจัดทำขั้นตอนปฏิบัติ และความร่วมมือในการฝึกแผนฉุกเฉิน

๒๐.๑๘ มีการกำหนดผู้ดูแลระบบกล้องวงจรปิดที่ชัดเจน (เช่น รปภ.) การบันทึกกิจกรรมที่เกิดขึ้น ต้องไม่ละเมิดสิทธิ์ส่วนบุคคลหรือเข้าไปดูกิจกรรมที่เกิดขึ้นผ่านหน้าจอ

หมวด ๒๑ นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

๒๑.๑ จดหมายอิเล็กทรอนิกส์ที่คณะแพทยศาสตร์จัดให้ใช้งาน ห้ามใช้ในงานส่วนตัว

๒๑.๒ มีการกำหนดให้มีการควบคุมการจัดเก็บของระบบจดหมายอิเล็กทรอนิกส์ เพื่อให้ระบบจดหมายอิเล็กทรอนิกส์ที่คณะแพทยศาสตร์จัดให้ใช้งาน มีประสิทธิภาพสูงสุด เช่น กำหนดเนื้อที่ในการจัดเก็บจดหมายอิเล็กทรอนิกส์ (Mailbox) เป็นต้น

๒๑.๓ ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ต้องรับทราบ มีความรู้และความเข้าใจในการใช้งานจดหมายอิเล็กทรอนิสก์ที่ถูกต้อง และมีความตระหนักถึงความปลอดภัยในการใช้งานอยู่ตลอดเวลา

๒๑.๔ ผู้ใช้งานต้องไม่เขียนหรือพิมพ์ข้อความที่ไม่เหมาะสมในจดหมายอิเล็กทรอนิกส์ หลังจากรับทราบนโยบายด้านความปลอดภัยสารสนเทศของคณะแพทยศาสตร์

๒๑.๕ มีกระบวนการตรวจสอบข้อความในจดหมายอิเล็กทรอนิกส์ ทั้งรับเข้าและส่งออกของคณะแพทยศาสตร์ โดยได้รับอนุญาตจากผู้มีอำนาจ

๒๑.๖ มีการควบคุมขนาดไฟล์ที่ส่ง เพื่อให้เกิดประสิทธิภาพในการทำงานสูงสุด

๒๑.๗ เมื่อพบว่ามีจดหมายสแปม (Spam mail) หรือสิ่งผิดปกติที่แนบมาพร้อมกับจดหมายอิเล็กทรอนิกส์เข้ามาในระบบ ให้ลบทิ้งทันที

๒๑.๘ มีการกำหนดให้มีการเข้ารหัสจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาสาระที่สำคัญตามที่ระบุไว้ในข้อตกลง

๒๑.๙ เครื่องที่ใช้งานจดหมายอิเล็กทรอนิกส์ ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์หรือโค้ดที่มุ่งหวังร้าย รวมถึงการปฏิบัติตามข้อปฏิบัติในการป้องกันไวรัสของคณะแพทยศาสตร์

๒๑.๑๐ ผู้ไม่ปฏิบัติตามกฎเกณฑ์ในการใช้งานจดหมายอิเล็กทรอนิกส์ จะถูกระงับการใช้งานจดหมายอิเล็กทรอนิกส์และระบบอินเทอร์เน็ต จนกว่าจะได้รับอนุญาตจากผู้รับผิดชอบ

หมวด ๒๒ นโยบายความปลอดภัยอินเทอร์เน็ต (Internet Policy)

๒๒.๑ ผู้ใช้งานอินเทอร์เน็ต ต้องได้รับอนุมัติจากผู้มีอำนาจ

๒๒.๒ ผู้ใช้งานอินเทอร์เน็ต ต้องได้รับทราบ มีความรู้และความเข้าใจในการใช้งานอินเทอร์เน็ตที่ถูกต้อง และมีความตระหนักถึงความปลอดภัยในการใช้งานอยู่ตลอดเวลา

๒๒.๓ มีการพิจารณาเนื้อหา และบริการ (service) ในอินเทอร์เน็ต ที่เหมาะสมกับความจำเป็นของคณะแพทยศาสตร์

๒๒.๔ มีระบบตรวจสอบเนื้อหา และข้อมูลที่รับเข้า-ส่งออกจากเครือข่ายของคณะแพทยศาสตร์ เพื่อตรวจสอบโค้ดที่มุ่งร้าย (Malicious code) และข้อความที่ไม่เหมาะสม

๒๒.๕ กรณีที่มีการกำหนดการเชื่อมต่อเครือข่ายอินเทอร์เน็ตแบบเรียลไทม์กับคอมพิวเตอร์ภายในสำนักงาน ที่ใช้ผ่าน Virtual Private Network (VPN) ต้องได้รับการรับรองจากผู้รับผิดชอบ

๒๒.๖ กรณีที่มีการติดต่อแลกเปลี่ยนข้อมูลจากอินเทอร์เน็ตเข้าสู่คณะแพทยศาสตร์ ต้องกำหนดให้มีการเข้ารหัสตลอดเวลา และมีระบบตรวจสอบตัวตน (Authentication) ก่อนการเข้ามาใช้งานเครือข่ายภายใน

๒๒.๗ เมื่อพบหรือสงสัยว่ามีสิ่งผิดปกติในการใช้งาน แจ้งให้งานเทคโนโลยีสารสนเทศทราบทันที

หมวด ๒๓ นโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

๒๓.๑ มีการสำรองข้อมูลสำคัญ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating system) โปรแกรมระบบงานคอมพิวเตอร์ (Application system) และชุดคำสั่งที่ใช้งานให้ครบถ้วน พร้อมทั้งให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

๒๓.๒ มีการกำหนดผู้รับผิดชอบในการสำรองระบบงานต่างๆ อย่างชัดเจน

๒๓.๓ มีขั้นตอน หรือวิธีปฏิบัติในการสำรองข้อมูล เพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยมีรายละเอียดอย่างน้อยดังนี้

๒๓.๓.๑ ข้อมูลที่สำรอง และความถี่ในการสำรอง

๒๓.๓.๒ ประเภทสื่อที่บันทึก (media)

๒๓.๓.๓ จำนวนที่ใช้ในการสำเนา (copy)

๒๓.๓.๔ ขั้นตอน และวิธีการสำรองโดยละเอียด

๒๓.๓.๕ สถานที่ และวิธีการเก็บรักษาสื่อบันทึก

๒๓.๓.๖ วิธีการทำลายสื่อบันทึก

๒๓.๔ มีการบันทึกการปฏิบัติงาน (Log) เกี่ยวกับการสำรองข้อมูล ของเจ้าหน้าที่ เพื่อตรวจสอบความถูกต้องครบถ้วน และมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

๒๓.๕ ในระบบงานหลัก ต้องมีการทดสอบข้อมูลสำรองอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าข้อมูล รวมทั้งโปรแกรมต่างๆ ที่สำรองไว้ มีความถูกครบถ้วน และใช้งานได้

๒๓.๖ มีการกำหนดขั้นตอน หรือวิธีปฏิบัติในการทดสอบ และการนำข้อมูลสำรองจากสื่อที่บันทึกมาใช้งาน

๒๓.๗ มีการจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ทำงานปัจจุบันไม่สามารถเข้าใช้งานได้

๒๓.๘ ในกรณีที่จำเป็นต้องเก็บข้อมูลไว้เป็นระยะเวลานาน ให้พิจารณาถึงวิธีการนำข้อมูลกลับมาใช้งานได้ในอนาคต

๒๓.๙ มีการติดป้ายชื่อที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

๒๓.๑๐ การขอใช้งานสื่อบันทึกข้อมูลสำรอง ต้องได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยมีรายละเอียดที่เกี่ยวข้องกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภท ข้อมูล และเวลา

๒๓.๑๑ มีขั้นตอนการทำลายข้อมูลสำคัญ และสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ในระบบกู้คืนข้อมูล

๒๓.๑๒ มีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์ หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว เพื่อให้เกิดความเสียหายน้อยที่สุด โดยแผนฉุกเฉินมีรายละเอียดดังนี้

๒๓.๑๒.๑ การจัดลำดับความสำคัญของระบบงาน และความสัมพันธ์ของระบบงาน และระยะเวลาในการกู้คืนในแต่ละระบบงาน

๒๓.๑๒.๒ กำหนดสถานการณ์ หรือลำดับความรุนแรงของปัญหา

๒๓.๑๒.๓ ขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

๒๓.๑๒.๔ กำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

๒๓.๑๒.๕ รายชื่อ และเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

๒๓.๑๒.๖ รายละเอียดของอุปกรณ์ และซอฟต์แวร์ที่จำเป็นในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ค่ากำหนดค่าติดตั้ง และอุปกรณ์เครือข่าย เป็นต้น

๒๓.๑๒.๗ กรณีที่มีศูนย์คอมพิวเตอร์สำรอง ให้ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่นสถานที่ตั้ง และแผนที่ เป็นต้น

๒๓.๑๒.๘ ปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และต้องมีสำเนาอย่างน้อย ๑ ชุดเก็บไว้แยกจากกัน

๒๓.๑๓ ในระบบงานหลัก ต้องมีการทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยเป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้งานได้จริงในทางปฏิบัติ และให้ทีมงานมีความเข้าใจในการดำเนินงาน พร้อมบันทึกผลการทดสอบด้วย

๒๓.๑๔ ชี้แจงแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องได้รับทราบ

๒๓.๑๕ ในกรณีที่เกิดเหตุการณ์ฉุกเฉิน ต้องมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหาไว้ด้วย

จึงประกาศมาเพื่อทราบ และถือปฏิบัติโดยทั่วกัน ทั้งนี้ รายละเอียดในการปฏิบัติตามนโยบายนี้ให้ดูจากระเบียบคณะแพทยศาสตร์ ว่าด้วยการใช้ และความมั่นคงของระบบคอมพิวเตอร์ พ.ศ. ๒๕๕๙

ประกาศ ณ วันที่ ๑๘ กุมภาพันธ์ พ.ศ. ๒๕๕๙

(ศาสตราจารย์คลินิก นายแพทย์วัฒนา นาคาเจริญ)
คณบดีคณะแพทยศาสตร์