ISMS PRACTICE

ขีดความสามารถด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

Photo by Akira Hojo on Unsplash

“ระบบการจัดการ คือ กรอบแนวทางในการขับเคลื่อนสู่เป้าหมายที่วางไว้และเป็นกลไกสนับสนุนที่ทำให้หน่วยงาน วางแผน ดำเนินการ ตรวจทาน และพัฒนาปรับปรุงอย่างต่อเนื่อง”

2569June 17, 2026

คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

ข้อมูลข่าวสารราชการ ประเภท นโยบายภายใน

ที่มาและความสำคัญ

นโยบายฉบับนี้อธิบายถึงกรอบแนวทางการจัดทำระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ให้สอดรับกับยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ แผนปฏิบัติงานดิจิทัล บริบทองค์กร ตลอดจนปัจจัยที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ที่เกี่ยวข้องกับคณะแพทยศาสตร์มหาวิทยาลัยสงขลานครินทร์

Informative Reference: ISO/IEC 27001:2022 Clause 4-10

Document Unique Identification: ISMS-PR

Document Version: 2569

Language: TH

Reviewed By: นายจรูญ แก้วมี และ นายโกเมน เรืองฤทธิ์

Approved By: ผศ.นพ.บุญชัย หวังศุภดิลก

อนุมัติตามหนังสือเลขที่ มอ 104.0135210/69-00410

สารบัญ

ศัพท์และคำนิยามที่ใช้ในเอกสาร

นอกเหนือจากที่ระบุไว้ในเอกสารฉบับนี้ให้ยึดตามมาตรฐานสากล ISO/IEC 27000 เป็นสำคัญ

คำนิยามที่ใช้ในแนวปฏิบัตินี้ประกอบด้วย

“คณะแพทยศาสตร์” หมายถึง คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของคณะแพทยศาสตร์

“ฝ่ายเทคโนโลยีสารสนเทศ” หมายถึง ฝ่ายเทคโนโลยีสารสนเทศเป็นหน่วยงานที่ให้บริการด้าน เทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายของคณะแพทยศาสตร์

“รองคณบดีฝ่ายเวชสารสนเทศ” หมายถึง ผู้มีอำนาจในด้านเทคโนโลยี สารสนเทศและการสื่อสารของคณะแพทยศาสตร์ ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนด นโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศและการสื่อสารของคณะแพทยศาสตร์

“มาตรฐาน” (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย

“วิธีการปฏิบัติ” (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มา ซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้ สามารถบรรลุเป้าหมายได้ง่ายขึ้น

“ผู้ใช้” หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่ง คณะแพทยศาสตร์กำหนดไว้ดังนี้

“ผู้บริหาร” หมายถึง ผู้มีอำนาจบริหารในระดับสูงของคณะแพทยศาสตร์ เช่น หัวหน้าหน่วยงาน เป็นต้น

“ผู้ดูแลระบบ” (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจาก ผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถ เข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานเงินรายได้คณะแพทยศาสตร์ ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการของคณะแพทยศาสตร์

“นักศึกษา” หมายถึง นักศึกษาของคณะแพทยศาสตร์

“หน่วยงานภายนอก” หมายถึง หน่วยงานภายนอกที่คณะแพทยศาสตร์อนุญาตให้มีสิทธิ์ในการ เข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของคณะแพทยศาสตร์ โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจ หน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“ข้อมูลคอมพิวเตอร์” หมายถึงข้อมูลข้อความ คำสั่งชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ใน สภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมาย ว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“สารสนเทศ” (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัด ระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจ ได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดย ได้มีการกำหนดคำสั่ง

ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำ หน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและ สารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆของคณะแพทยศาสตร์ได้เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น

“ระบบ LAN และระบบอินทราเน็ต” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบ คอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการ ติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และสารสนเทศภายในหน่วยงาน

“ระบบอินเทอร์เน็ต” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่ นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและ ควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ระบบเครือข่าย โปรแกรม ข้อมูล และ สารสนเทศ เป็นต้น

“ระบบสารสนเทศโรงพยาบาล” (Hospital Information System: HIS) หมายถึง ระบบงานสารสนเทศส่วนการบริหารและการบริการข้อมูลผู้ป่วย และข้อมูลสุขภาพ ภายใต้การดูแลของโรงพยาบาลสงขลานครินทร์

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

“พื้นที่ทำงานทั่วไป” (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา (Notebook)ที่ประจำโต๊ะทำงาน

“พื้นที่ทำงาน งานบริการโรงพยาบาล” (HIS service area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย ทั้งชนิดส่วนบุคคล (PC) และชนิดพกพา (Notebook) ของระบบงานสารสนเทศโรงพยาบาลสงขลานครินทร์ เช่น หอผู้ป่วย คลินิกผู้ป่วยนอก ห้องจ่ายยา เป็นต้น

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“ทรัพย์สิน” หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของ หน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์เป็นต้น

“จดหมายอิเล็กทรอนิกส์” (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน เครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้มาตรฐานที่ใช้ใน การรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

“รหัสผ่าน” (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

“ชุดคำสั่งไม่พึงประสงค์” หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่ง อื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ” (Information Security Management System: ISMS) หมายถึง กรอบแนวทางอันเป็นองค์ประกอบของ นโยบาย กระบวนการ เทคโนโลยี และบุคลากร ที่ทำให้หน่วยงานบรรลุวัตถุประสงค์ของการสร้างความมั่นคงปลอดภัยสารสนเทศ

“ความมั่นคงปลอดภัยสารสนเทศ” (Information Security) หมายถึง การรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของสารสนเทศ

"ผู้ประมวลผลข้อมูลส่วนบุคคล" (Data Processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเอง เช่น ผู้ให้บริการภายนอก (Vendor) หรือผู้รับจ้างที่เข้าถึงระบบสารสนเทศโรงพยาบาล (HIS)

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” (Data Protection Officer: DPO) หมายถึง ผู้ที่ได้รับแต่งตั้งให้ทำหน้าที่ให้คำปรึกษา ตรวจสอบและติดตามการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ภายในคณะแพทยศาสตร์

“ข้อมูลสุขภาพ” (Health Data) หมายถึง ข้อมูลส่วนบุคคลชั้นความอ่อนไหวที่เกี่ยวกับสุขภาพกายภาพหรือจิตใจ รวมถึงประวัติการบำบัดผลการวินิจฉัยโรค การผ่าตัด และข้อมูลที่บันทึกในระบบ HIS ทั้งหมดถือเป็นข้อมูลสุขภาพที่ต้องได้รับความคุ้มครองตามมาตรา 26 PDPA

ความเข้าใจในบริบทหน่วยงาน

๑. กำหนดบริบทภายในและภายนอกรวมถึงความคาดหวังของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องเพื่อกำหนดวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศขององค์กรและขอบเขตของระบบการจัดการและกระบวนการที่สำคัญ โดยมุ่งเน้นความเข้าใจในสถาปัตยกรรมองค์กร ความสัมพันธ์เชื่อมโยง จากปัจจัยภายในภายนอก ปัญหาอุปสรรค และความต้องการของผู้มีส่วนได้ส่วนเสีย จนนำไปสู่การกำหนดขอบเขตของระบบการจัดการอย่างเหมาะสม โดยเครื่องมือที่ควรพิจารณาประยุกต์ใช้ ได้แก่ PESTEL Analysis, SWOT Analysis, Balance Scorecard เป็นต้น

๒. การวิเคราะห์บริบทองค์กรควรพิจารณาดำเนินการอย่างสม่ำเสมอ อย่างน้อย 1 ครั้งต่อปี หรือเมื่อเกิดการเปลี่ยนแปลงที่สำคัญในระบบการจัดการ ทั้งนี้การเปลี่ยนแปลงทางบริบทถือเป็นหนึ่งในการเปลี่ยนแปลงที่ส่งผลต่อระบบการจัดการอย่างมีนัยสำคัญ

๓. เมื่อหน่วยงานมีระบบการจัดการที่มากกว่า 1 ระบบ ควรพิจารณาบูรณาการระบบการจัดการ (Integrated Management System) โดยให้ยึดโครงสร้างของระบบการจัดการที่เหมือนกัน และสามารถทำงานร่วมกันได้

๔. ปัจจัย ปัญหาอุปสรรค ความต้องการของผู้มีส่วนได้ส่วนเสีย ที่สำคัญอาจมีความเชื่อมโยงสู่การประเมินความเสี่ยงที่เกี่ยวข้อง

๕. ความคาดหวังและความต้องการของผู้มีส่วนได้ส่วนเสียต้องประเมินและวิเคราะห์ในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ในกรณีที่เป็นกฎหมายให้บ่งชี้ตามหน่วยงานที่มีหน้าที่ตรวจสอบหรือบังคับใช้กฎหมายเรื่องนั้น ๆ เมื่อเป็นไปได้ให้นำเสนอแก่นิติกรประจำคณะแพทยศาสตร์ดำเนินการวิเคราะห์ความเกี่ยวข้องต่อระบบการจัดการ

ผลการวิเคราะห์ปัจจัยภายในและภายนอก

ปัจจัยที่มีอิทธิพลต่อระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ จำแนกตามรูปแบบ PESTEL Analysis ได้ ดังนี้

ปัจจัยภายในด้านการเมือง

อิทธิพลของการจัดการโครงสร้างของมหาวิทยาลัย คณะแพทยศาสตร์เป็นหน่วยงานที่มีขนาดใหญ่ และมีขีดความสามารถในการบริหารจัดการภายในหลายเรื่อง อาทิ งานด้านบุคลากร ด้านเทคโนโลยีสารสนเทศ ด้านกฎหมาย ภายใต้กรอบการกำกับของมหาวิทยาลัย ด้วยเหตุนี้การจัดให้มีความมั่นคงปลอดภัยสารสนเทศในระบบสารสนเทศและเครือข่ายของคณะแพทยศาสตร์ที่ครอบคลุมถึงบริการสุขภาพของโรงพยาบาลสงขลานครินทร์ จึงเป็นประเด็นที่คณะแพทยศาสตร์ต้องเร่งดำเนินการ

ผลกระทบ:

- คณะแพทยศาสตร์มีความต้องการให้ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศของคณะแพทยศาสตร์ มีความเป็นมาตรฐานสากล โดยเทียบเคียงมาตรฐานสากล ISO/IEC 27001:2022 เพื่อรองรับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานภายใต้คณะแพทยศาสตร์

ปัจจัยภายในด้านเศรษฐกิจ

การรวมความต้องการพัฒนาฝ่ายเทคโนโลยีสารสนเทศจากหน่วยงานต่าง ๆ ภายใต้คณะแพทยศาสตร์ เป็นแนวความคิดที่จะสามารถลดการลงทุนด้านเทคโนโลยีสารสนเทศ และทำให้การจัดการด้านความมั่นคงปลอดภัยสารสนเทศดำเนินการได้โดยง่ายและเกิดประสิทธิภาพ ผ่านบริการ Colocation เพื่อลดการลงทุนในศูนย์คอมพิวเตอร์และสามารถบริหารจัดการแบบรวมศูนย์

ผลกระทบ:

- คณะแพทยศาสตร์ต้องการให้เกิดการรวมศูนย์การจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ โดยยกระดับให้บริการ

Colocation มีความมั่นคงปลอดภัยสารสนเทศและสามารถให้บริการแก่หน่วยงานภายใต้คณะแพทยศาสตร์ได้ตามวัตถุประสงค์และความต้องการ ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศจึงต้องครอบคลุมบริการ Colocation

ปัจจัยภายในด้านเทคโนโลยี

การเพิ่มศักยภาพและการใช้เทคโนโลยีด้านความมั่นคงปลอดภัยสารสนเทศอย่างเต็มประสิทธิภาพ เพื่อให้เกิดความคุ้มค่าและสร้างเสริมความมั่นคงปลอดภัยสารสนเทศ

ผลกระทบ:

- คณะแพทยศาสตร์มีความประสงค์ให้เกิดการพัฒนาเทคโนโลยีที่เสริมสร้างความมั่นคงปลอดภัยสารสนเทศ ดังนั้นระบบการจัดการความมั่นคงปลอดภัยสารสนเทศจำเป็นต้องพิจารณามาตรการด้านความมั่นคงปลอดภัยสารสนเทศผ่านการใช้เทคโนโลยีที่ทันสมัยและสามารถรองรับภัยคุกคามทางเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

ปัจจัยภายในด้านสิ่งแวดล้อม

การดำเนินงานด้านความมั่นคงปลอดภัยที่ส่งเสริมการลดการใช้ทรัพยากรสิ้นเปลือง โดยการประยุกต์ใช้เทคโนโลยีแทนแบบฟอร์มกระดาษ การใช้ลายมือชื่ออิเล็กทรอนิกส์

ผลกระทบ:

- คณะแพทยศาสตร์ออกแบบให้ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศประยุกต์ใช้เทคโนโลยีดิจิทัล เพื่อลดต้นทุนและการใช้ทรัพยากรสิ้นเปลือง ดังนั้นระบบการจัดการความมั่นคงปลอดภัยสารสนเทศจึงอนุญาตให้ใช้การลงลายมือชื่ออิเล็กทรอนิกส์ และการใช้ระบบสารสนเทศเพื่อการบันทึกข้อมูลทดแทนกระดาษ

ปัจจัยภายนอกด้านเศรษฐกิจ

ภัยคุกคามทางไซเบอร์ที่สร้างผลกระทบด้านการเงิน เนื่องจากกระทบต่อคุณภาพบริการที่สำคัญ บทปรับตามกฎหมาย หรือการละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล กระทบต่อการพิจารณางบประมาณที่เหมาะสมเพื่อเกิดการใช้มาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่เพียงพอต่อความรับผิดชอบในฐานะผู้ให้บริการ

ปัจจัยภายนอกด้านสังคม

การเปลี่ยนแปลงของค่านิยมทางสังคมที่ให้ความสำคัญด้านการคุ้มครองข้อมูลเป็นประเด็นที่ผู้ให้บริการต้องรับผิดชอบและพัฒนาปรับปรุงอย่างต่อเนื่อง โดยเฉพาะคณะแพทยศาสตร์ในฐานะผู้ให้บริการทางการแพทย์และมีข้อมูลสุขภาพของผู้ป่วยจำนวนมากอันเป็นข้อมูลละเอียดอ่อนที่ต้องได้รับการคุ้มครองอย่างปลอดภัย

ผลกระทบ:

- คณะแพทยศาสตร์ต้องการให้ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศในศูนย์คอมพิวเตอร์ที่รองรับระบบ HIS ซึ่งเป็นระบบงานที่สำคัญทางการแพทย์ มีความมั่นคงปลอดภัย การนำมาตรฐานสากล ISO/IEC 27001:2022 มาประยุกต์ใช้จะเพิ่มประสิทธิภาพของการจัดการศูนย์คอมพิวเตอร์และสร้างความเชื่อมั่นให้แก่ผู้ใช้งานระบบสารสนเทศ HIS ได้

ปัจจัยภายนอกด้านเทคโนโลยีสารสนเทศ

ภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงและสามารถสร้างความเสียหายให้แก่ผู้ให้บริการ และภัยคุกคามที่เกิดจากผู้ใช้งานที่ขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและสร้างความเสียหายแก่หน่วยงาน

ผลกระทบ:

- ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องครอบคลุมการใช้มาตรการรับมือต่อภัยคุกคามทางไซเบอร์ที่ทวีรุนแรง อาทิ มาตรการ Threat Intelligence, และ DLP

ปัจจัยภายนอกด้านสิ่งแวดล้อม

การทำงานในรูปแบบ Hybrid Work ที่เป็นพฤติกรรมที่ยังคงเหลืออยู่หลังสถานการณ์โรคระบาด ทำให้ระบบเทคโนโลยีสารสนเทศต้องถูกเข้าถึงได้จากระยะไกลอย่างต่อเนื่อง นอกจากนี้ การใช้ปัญญาประดิษฐ์ (AI) ของผู้โจมตี อาทิ Phishing ที่สร้างด้วย AI และ Deepfake ส่งผลให้เป็นความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่เกิดจากการควบคุมการเข้าถึงระยะไกลที่ไม่มีประสิทธิภาพ

ปัจจัยภายนอกด้านกฎหมาย

คณะแพทยศาสตร์ ต้องดำเนินการให้สอดรับกับกฎหมายดิจิทัลและระเบียบปฏิบัติทางเทคโนโลยีสารสนเทศ รวมถึงกฎหมายที่มีอิทธิพลต่อระบบการจัดการความมั่นคงปลอดภัยสารสนเทศและการใช้เทคโนโลยีของหน่วยงาน อาทิ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์, พ.ร.บ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

ผลกระทบ:

- ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องครอบคลุมการบ่งชี้กฎหมายและระเบียบที่เกี่ยวข้องให้ครบถ้วน

สรุป SWOT Analysis (ปัจจัยภายในและภายนอก)

เพื่อเสริมความเข้าใจและตอบโจทย์การประเมินผลในแต่ละปี ได้ดำเนินการวิเคราะห์ SWOT (Strengths, Weaknesses, Opportunities, Threats) ดังนี้

Strengths (จุดแข็ง)

- การสนับสนุนอย่างชัดเจนจากผู้บริหารระดับสูง
- มีกรอบนโยบายและโครงสร้างกำกับดูแลที่เป็นมาตรฐาน
- ระบบ Colocation และ Data Center มีศักยภาพและประสบการณ์

Weaknesses (จุดอ่อน)

- ข้อจำกัดด้านงบประมาณและบุคลากรผู้เชี่ยวชาญ
- ระบบที่ต้องอัปเดตและปรับปรุงต่อเนื่อง
- ขั้นตอนการบูรณาการระหว่างหน่วยงานยังต้องพัฒนา

Opportunities (โอกาส)

- การบังคับใช้กฎหมายดิจิทัลและมาตรฐานสากลเพิ่มขึ้น
- การพัฒนาระบบ e-Government และ e-Health
- แนวโน้มการพัฒนาเทคโนโลยีใหม่ เช่น AI Security, Zero Trust Architecture และ SIEM/SOAR ที่ช่วยเพิ่มประสิทธิภาพการตรวจจับภัยคุกคาม

Threats (อุปสรรค/ความเสี่ยง)

- ภัยคุกคามไซเบอร์ทวีความรุนแรงมากขึ้น
- การเปลี่ยนแปลงของกฎหมายและนโยบายแบบฉับพลัน
- ผลกระทบจาก Climate Change เช่น น้ำท่วมและไฟฟ้าดับ
- ภัยคุกคาม Supply Chain Attack จาก Vendor/ซอฟต์แวร์ภายนอกที่เชื่อมต่อกับ HIS
- ความเสี่ยงจากการใช้ Generative AI (GenAI) โดยบุคลากรที่อาจนำข้อมูลชั้นความลับเข้าสู่ระบบภายนอกโดยไม่ตั้งใจ

การนำ SWOT ไปใช้ในการทบทวนประจำปี

- **S (Strengths):** พัฒนาและขยายการใช้จุดแข็ง เช่น ใช้ศักยภาพ Data Center เพื่อให้บริการแบบ One-Stop Service
- **W (Weaknesses):** ระบุแผนการเสริมทักษะและปรับโครงสร้างงบประมาณในระยะยาว
- **O (Opportunities):** ต่อยอดโอกาสด้วยโครงการใหม่ เช่น พัฒนาระบบ e-Signature ครอบคลุมทุกหน่วยงาน
- **T (Threats):** อัปเดต BCP, จัดอบรมซ้อมแผนความต่อเนื่อง และเพิ่มการเฝ้าระวังภัยคุกคามใหม่ๆ อย่างต่อเนื่อง

ผลการวิเคราะห์ผู้มีส่วนได้ส่วนเสีย ความคาดหวังและความต้องการ

ผู้บริหารระดับสูงของคณะแพทยศาสตร์ และผู้บริหารระดับสูงของมหาวิทยาลัยสงขลานครินทร์

ผู้บริหารแสดงวิสัยทัศน์และแนวนโยบายสนับสนุนให้เกิดการผลักดันด้านความมั่นคงปลอดภัยสารสนเทศที่มีมาตรฐาน และแพทยศาสตร์สามารถให้บริการฝ่ายเทคโนโลยีสารสนเทศแก่หน่วยงานอื่น ๆ ได้อย่างมีความมั่นคงปลอดภัยผ่านการรับรองมาตรฐานสากล ISO/IEC 27001:2022

เจ้าหน้าที่เทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

เจ้าหน้าที่มีความมุ่งมั่นในการพัฒนาและยกระดับมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศในการดำเนินงาน

ผู้ใช้บริการ Colocation Service

ผู้ใช้บริการ Colocation Service มีความต้องการหลักในการได้รับบริการที่มีความมั่นคงปลอดภัยด้านสารสนเทศ ครอบคลุมถึงความเชื่อมั่นในระบบสารสนเทศที่นำฝาก รวมทั้งระบบเครือข่ายที่ใช้ในการเชื่อมต่อหรือเข้าถึงระบบดังกล่าว โดยผู้ใช้บริการประกอบด้วยหน่วยงานต่าง ๆ ภายในคณะแพทยศาสตร์ ซึ่งมีระบบงานหลากหลายประเภท เช่น ระบบ CCTV/Access Control, ระบบ PACS, ระบบ LIS, ระบบ Big Data, ML/AI และระบบ Tele Conference เป็นต้น

การจัดเก็บและตรวจสอบข้อมูล:

ข้อมูลรายละเอียดผู้ใช้บริการ Colocation Service (เช่น หน่วยงาน ระบบงานที่ใช้บริการ จำนวน HOST และพื้นที่ที่ใช้บริการ) สำหรับปี **พ.ศ. 2569** ได้รับการบันทึกและอัปเดตอย่างสม่ำเสมอในระบบ **Service Desk** ภายใต้ **Ticket ID: 303040** เพื่อให้ข้อมูลมีความเป็นปัจจุบัน และสามารถตรวจสอบย้อนกลับได้ตามกระบวนการบริหารจัดการของระบบ ISMS

โรงพยาบาลสงขลานครินทร์ และโรงพยาบาลสงขลานครินทร์เวชวิวัฒน์

เนื่องจากระบบ HIS (Hospital Information System) เป็นระบบสารสนเทศที่สำคัญภายใต้การดูแลของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ ซึ่งมีข้อมูลสุขภาพของผู้ใช้บริการโรงพยาบาล จึงมีความต้องการในการเก็บรักษาข้อมูลในระบบ HIS อย่างมั่นคงปลอดภัยและมีความพร้อมใช้สูง (High Availability) เนื่องจากเป็นระบบสารสนเทศสำคัญภายใต้บริการที่สำคัญของโรงพยาบาล ในการกำกับดูแลในฐานะโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII: Critical Information Infrastructure) ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์

นิสิตนักศึกษา คณะแพทยศาสตร์

ระบบ EDIS (Education Information System) เป็นระบบสารสนเทศสำคัญภายใต้การดูแลของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ ซึ่งเป็นระบบที่ให้บริการแก่นิสิตนักศึกษาของคณะแพทยศาสตร์ จำเป็นต้องมีการคุ้มครองข้อมูลในระบบอย่างปลอดภัย

ฝ่ายบุคคล คณะแพทยศาสตร์

ระบบ HRIS (Human Resource Information System) เป็นระบบสารสนเทศสำคัญภายใต้การดูแลของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ ซึ่งเป็นระบบที่ให้บริการข้อมูลที่เกี่ยวข้องกับการบริหารจัดการทรัพยากรบุคคลของ คณะแพทยศาสตร์ จำเป็นต้องมีการคุ้มครองข้อมูลในระบบอย่างปลอดภัย

หน่วยงานอื่น ๆที่เกี่ยวข้องกับการจัดการทั่วไปของคณะแพทยศาสตร์

ระบบ MIS (Management Information System) เป็นระบบสารสนเทศสำคัญภายใต้การดูแลของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ ซึ่งเป็นระบบที่ให้บริการการจัดการ อาทิ งานพัสดุ การเงิน บัญชี ของคณะแพทยศาสตร์ จำเป็นต้องมีการคุ้มครองข้อมูลในระบบอย่างปลอดภัยและมีความพร้อมในการใช้งานสูง

ผู้ให้บริการภายนอกและผู้รับจ้างช่วง

หน่วยงานภายนอกต้องปฏิบัติตามนโยบายและระเบียบของมหาวิทยาลัยและคณะแพทยศาสตร์เพื่อการส่งมอบสินค้าและบริการได้อย่างมีประสิทธิภาพ สามารถให้บริการได้ตามแผนงาน และได้รับข้อมูลข่าวสารที่จำเป็นต่อการประสานงานและให้บริการ

หน่วยงานกำกับดูแล

หน่วยงานรัฐในฐานะหน่วยงานกำกับดูแลและบังคับใช้กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและฝ่ายเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ ได้แก่

- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผ่านการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลและกฎหมายลำดับรองที่เกี่ยวข้อง
- สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ ผ่านการบังคับใช้ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายลำดับรองที่เกี่ยวข้อง
- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผ่านการบังคับใช้ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายลำดับรองที่เกี่ยวข้อง

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CIRT)

ในฐานะศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ในกลุ่ม Health Care ของประเทศไทยคาดหวังและต้องการให้หน่วยงาน (โรงพยาบาล) ภายใต้การกำกับรายงานและติดต่อประสานงานเพื่อแจ้งเหตุภัยคุกคามไซเบอร์

สรุป SWOT Analysis (ผู้มีส่วนได้ส่วนเสีย)

Strengths (จุดแข็ง):

- ผู้บริหารและบุคลากรมีความตระหนักด้านความมั่นคงปลอดภัย
- ระบบนโยบายและมาตรฐานความมั่นคงปลอดภัยที่มีอยู่แล้ว

Weaknesses (จุดอ่อน):

- ความเข้าใจที่แตกต่างกันระหว่างผู้มีส่วนได้ส่วนเสียบางกลุ่ม
- บุคลากรบางส่วนยังมีความรู้ด้านไซเบอร์และความมั่นคงปลอดภัยไม่เพียงพอ

Opportunities (โอกาส):

- การผลักดันของรัฐด้านกฎหมายไซเบอร์และความมั่นคงปลอดภัย
- การนำเทคโนโลยีและมาตรฐานใหม่ เช่น Zero Trust Security มาประยุกต์ใช้

Threats (อุปสรรค/ความเสี่ยง):

- ความคาดหวังที่สูงขึ้นของผู้ใช้บริการที่อาจทำให้เกิดแรงกดดัน
- การเปลี่ยนแปลงของกฎหมายที่รวดเร็ว
- ภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงและซับซ้อนมากขึ้น

การนำ SWOT ไปใช้ในการทบทวนประจำปี

ข้อมูล SWOT Analysis ของผู้มีส่วนได้ส่วนเสียนี้จะถูกนำไปใช้เป็นฐานข้อมูลประกอบการทบทวนระบบการจัดการความมั่นคงปลอดภัยสารสนเทศประจำปี เพื่อประเมินการตอบสนองต่อความคาดหวัง ความต้องการ และการบริหารความเสี่ยงที่เกี่ยวข้องกับผู้มีส่วนได้ส่วนเสียหลัก พร้อมทั้งปรับปรุงแผนการดำเนินงานให้เหมาะสมกับการเปลี่ยนแปลงที่เกิดขึ้น

กระบวนการที่สำคัญ

ภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ กระบวนการของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ ที่สำคัญ ได้แก่

กระบวนการบริหารจัดการเครือข่าย

กระบวนการบริหารจัดการเครือข่ายมีบทบาทสำคัญมากต่อประสิทธิภาพด้านความต่อเนื่องของระบบสารสนเทศ และความพร้อมใช้ (availability) ของสารสนเทศ ซึ่งเป็นการบริหารจัดการเครือข่ายและควบคุมการตั้งค่าของอุปกรณ์เครือข่ายให้ทำงานได้อย่างมีประสิทธิภาพ

ข้อมูลป้อนเข้า: มาตรการทางเครือข่ายและกิจกรรมการเฝ้าระวังทางเครือข่าย

ข้อมูลออก: รายงานอุบัติการณ์ (ถ้ามี)

สมรรถนะกระบวนการ: ผ่านตัวชี้วัดด้านความพร้อมของระบบสารสนเทศและเครือข่าย

กระบวนการบริหารจัดการทรัพย์สินสารสนเทศ

กระบวนการบริหารจัดการทรัพย์สินสารสนเทศโดยมุ่งเน้นไปที่ทรัพย์สินที่เกี่ยวข้องกับฝ่ายเทคโนโลยีสารสนเทศและระบบสารสนเทศหลักภายใต้การให้บริการของฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลป้อนเข้า: ทรัพย์สินครุภัณฑ์และข้อมูลสารสนเทศของระบบสารสนเทศที่สำคัญ

ข้อมูลออก: ทะเบียนทรัพย์สินสารสนเทศ

สมรรถนะกระบวนการ: ผ่านตัวชี้วัดการใช้ทรัพยากรอย่างคุ้มค่า

กระบวนการบริหารจัดการเหตุอุบัติการณ์และการรับเรื่อง

กระบวนการบริหารจัดการเหตุอุบัติการณ์และการรับเรื่องเป็นกลไกในการตอบโต้ แก้ไข ปัญหาหรืออุบัติการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศ

ข้อมูลป้อนเข้า: รายงานอุบัติการณ์และคำร้อง

ข้อมูลออก: บันทึกอุบัติการณ์และคำร้องในระบบ **Service Desk**

สมรรถนะกระบวนการ: ผ่านตัวชี้วัดเหตุละเมิดที่กระทบต่อความสอดคล้องด้านกฎหมาย

กระบวนการบริหารความมั่นคงปลอดภัยสารสนเทศ

กระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือกระบวนการที่มุ่งเน้นการตรวจสอบ เฝ้าระวัง และปรับแต่งค่ามาตรการด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดความพร้อม ความถูกต้อง และการรักษาความลับของสารสนเทศและระบบสารสนเทศ

ข้อมูลป้อนเข้า: มาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

ข้อมูลออก: รายงานทุกสัปดาห์ (**weekly report**)

สมรรถนะกระบวนการ: ผ่านตัวชี้วัดการจัดการช่องโหว่เชิงเทคนิคและความพร้อมของระบบสารสนเทศและเครือข่าย

กระบวนการบริหารโครงสร้างพื้นฐาน (facilities)

กระบวนการบริหารโครงสร้างพื้นฐาน คือกระบวนการที่มุ่งเน้นการตรวจสอบ เฝ้าระวัง และปรับแต่งค่ามาตรการกายภาพ สิ่งแวดล้อม และระบบโครงสร้างพื้นฐานอาทิ ระบบไฟฟ้า อุณหภูมิ ความชื้น เพื่อให้เกิดความพร้อมของโครงสร้างพื้นฐานที่สนับสนุนความต่อเนื่องของอุปกรณ์ภายในฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลป้อนเข้า: มาตรการเชิงกายภาพ

ข้อมูลออก: รายงานการตรวจสอบความพร้อมของโครงสร้างพื้นฐาน

สมรรถนะกระบวนการ: ผ่านตัวชี้วัดความพร้อมของระบบสารสนเทศและเครือข่าย

<u>กระบวนการที่จัดการโดยหน่วยงานภายนอก</u> (Outsourced Process)

กระบวนการที่จัดการโดยหน่วยงานภายนอกแต่มีอิทธิพลต่อประสิทธิภาพของระบบการจัดการ ได้แก่ 1) กระบวนการจัดการทรัพยากรบุคคล 2) กระบวนการจัดซื้อจัดจ้างและงานพัสดุ 3) กระบวนการจัดการของฝ่ายอาคารและสถานที่

ข้อมูลป้อนเข้า: การสื่อสารและขอความร่วมมือจากฝ่ายเทคโนโลยีสารสนเทศเพื่อการประสานงาน

ข้อมูลออก: ผลการประสานงานขอความร่วมมือ ได้แก่ 1) การจัดซื้อจัดจ้างตามระเบียบมหาวิทยาลัย 2) การจัดการทรัพยากรบุคคล 3) รายงานผลการบำรุงรักษาระบบงานของฝ่ายอาคารและสถานที่

สมรรถนะกระบวนการ: ไม่วัดผล (เนื่องจากเป็นผู้มีส่วนได้ส่วนเสียที่ไม่มีสัญญา)

<u>กระบวนการตรวจสอบภายใน</u>

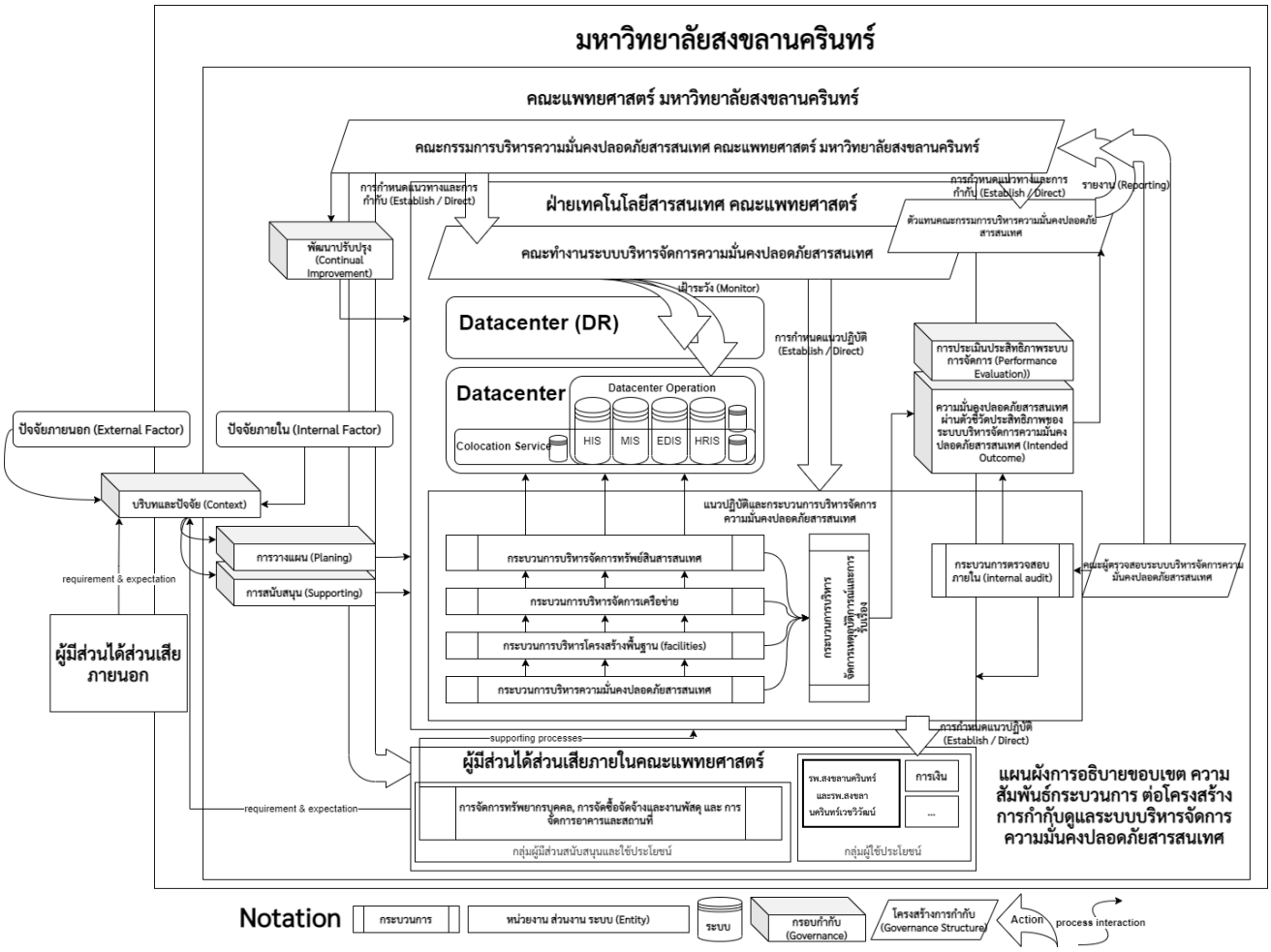
กระบวนการตรวจสอบภายในมุ่งเน้นการสร้างความมั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่ใช้มีความสอดคล้องกับมาตรฐานสากล ISO/IEC 27001:2022 หรือเกณฑ์การตรวจสอบอื่น ๆ ที่นำมาใช้

ข้อมูลป้อนเข้า: แผนการตรวจสอบและผลการดำเนินงานของกระบวนการภายใน

ข้อมูลออก: รายงานผลการตรวจสอบ

สมรรถนะกระบวนการ: ผ่านตัวชี้วัดความสอดคล้องด้านกฎหมาย

ผังอธิบายความสัมพันธ์ระหว่างกระบวนการ



๖. ผลจากการศึกษาปัจจัยภายในและภายนอก ความคาดหวัง และความต้องการของผู้มีส่วนได้ส่วนเสียให้พิจารณาสู่การกำหนดขอบเขตของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

๗. การกำหนดขอบเขตของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศต้องจัดให้เป็นลายลักษณ์อักษร และบ่งชี้ถึงขอบเขต (boundary) และส่วนประสานงาน (interface) กับหน่วยงานอื่น ๆ ที่อยู่นอกเหนือขอบเขตหรืออำนาจการกำกับดูแลของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์

๘. การเปลี่ยนแปลงหรือแก้ไขขอบเขตของระบบการจัดการ สำหรับกรณีที่มีหน่วยงานยังคงขอรับการรับรองและต่ออายุการรับรองกับหน่วยตรวจรับรองมาตรฐานสากล ISO/IEC 27001:2022 (CB: Certification Body) ต้องแจ้งอย่างเป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย 1 เดือน

ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสำหรับการจัดการและปฏิบัติงานศูนย์คอมพิวเตอร์ และบริการโคโลเคชั่น คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

"The Information Security Management System applied to Data center and DR Operation, Colocation service including supporting infrastructure managed by FACULTY OF MEDICINE, PRINCE OF SONGKLA UNIVERSITY"

-DC-

Floor 6, Chalerm Phra Baramee Building, Prince of Songkla University, 15 Karnjanavanich Rd., Hat Yai, Songkhla 90110

-DR-

Floor 4, Medical research and Technology Transfer Building, Prince of Songkla University, 15 Karnjanavanich Rd., Hat Yai, Songkhla 90110

*สิ่งที่อยู่นอกขอบเขต:

- กระบวนการพัฒนาและบำรุงรักษา software ภายใน
- การจัดการ Generator (อยู่ภายใต้การควบคุมดูแลโดยฝ่ายวิศวกรรมซ่อมบำรุง)
- การจัดการและบำรุงรักษาเครื่องคอมพิวเตอร์ผู้ใช้งานทั่วไป (Client Computer) รวมถึงอุปกรณ์ต่อพ่วงอื่น ๆ
- การบำรุงรักษาระบบสารสนเทศภายในศูนย์คอมพิวเตอร์ ได้แก่
  - ระบบ MIS/HIS
  - ระบบ Email
  - ระบบ Share Drive
  - ระบบ CCTV (นอกศูนย์คอมพิวเตอร์)
  - เป็นต้น

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๙. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ให้ยึดตาม นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ มหาวิทยาลัยสงขลานครินทร์ พ.ศ. 2567 และเพิ่มเติมตามที่ระบุในเอกสารฉบับนี้

๑๐. ให้คณะแพทยศาสตร์ออกนโยบายหรือแนวปฏิบัติเฉพาะเรื่องตราบเท่าที่ไม่ขัดหรือแย้งต่อนโยบายและแนวปฏิบัติในระดับมหาวิทยาลัย

๑๑. ต้องตรวจทานการแก้ไขและเปลี่ยนแปลงที่อาจเกิดขึ้นกับนโยบายและแนวปฏิบัติในระดับมหาวิทยาลัย เมื่อมีการแก้ไขหรือเปลี่ยนแปลง คณะแพทยศาสตร์ต้องตรวจทานความสอดคล้องและสื่อสารประชาสัมพันธ์เมื่อมีการเปลี่ยนแปลงที่สำคัญไม่ว่าจะเกิดขึ้นกับนโยบายและแนวปฏิบัติในระดับมหาวิทยาลัยหรือของคณะแพทยศาสตร์เองก็ตาม โดยการเปลี่ยนแปลงองค์ประกอบของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการผ่านแนวปฏิบัติควบคุมการเปลี่ยนแปลง

๑๒. เหตุละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต้องได้รับการรายงานและอนุมัติเป็นรายการไป เว้นแต่กรณีฉุกเฉินหรือความจำเป็นอันสำคัญยิ่งด้วยจรรยาบรรณหรือวิชาชีพทางการแพทย์ หรือเพื่อการช่วยเหลือชีวิต ให้แจ้งถึงความจำเป็นภายหลัง

๑๓. นโยบายด้านความมั่นคงปลอดภัยสารสนเทศต้องได้รับการสื่อสารภายในคณะแพทยศาสตร์ จัดให้มีการเผยแพร่อย่างเหมาะสม เมื่อเป็นไปได้จัดให้เป็นเอกสารแนบท้ายสัญญาบริการที่หน่วยงานภายนอกต้องปฏิบัติตามเพื่อให้การให้บริการแก่คณะแพทยศาสตร์มีความมั่นคงปลอดภัย

๑๔. การฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศถือเป็นความผิดทางวินัย

ภาวะผู้นำด้านความมั่นคงปลอดภัยสารสนเทศ

๑๕. คณะแพทยศาสตร์ให้ความสำคัญและมุ่งมั่นในการสร้างภาวะผู้นำด้านความมั่นคงปลอดภัยสารสนเทศ โดยให้มีการรายงานด้านความมั่นคงปลอดภัยสารสนเทศแก่ฝ่ายบริหารทั้งในระดับคณะแพทยศาสตร์และมหาวิทยาลัย

๑๖. คณะแพทยศาสตร์มุ่งมั่นการพัฒนามาตรการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อการคุ้มครองข้อมูลสำคัญ และการให้บริการเครือข่ายที่มีความน่าเชื่อถือและมีเสถียรภาพ

๑๗. คณะแพทยศาสตร์สื่อสารประชาสัมพันธ์อย่างต่อเนื่องและสร้างความตระหนักรู้ต่อเจ้าหน้าที่ทุกภาคส่วน ในการมีส่วนร่วมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

๑๘. คณะแพทยศาสตร์จัดให้มีตัวชี้วัดประสิทธิภาพของระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ การวัดประเมิน และ

รายงานผล เพื่อการพัฒนาปรับปรุงและยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

๑๙. คณะแพทยศาสตร์ต้องจัดให้มีโครงสร้างการกำกับด้านความมั่นคงปลอดภัยสารสนเทศและเจ้าหน้าที่ที่ได้รับมอบหมายจากคณะกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศหรือผู้บริหารระดับสูง ในการดำเนินกิจกรรมที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้เพื่อประโยชน์ในการมอบหมายภารกิจ หากเอกสารดังกล่าวเป็นส่วนหนึ่งหรือเป็นเอกสารแนบท้ายเอกสารฉบับนี้ ให้ถือเสมือนว่าเป็นการอนุมัติแต่งตั้งภายในคณะแพทยศาสตร์ หรืออาจพิจารณาประกาศตามระเบียบของมหาวิทยาลัย

๒๐. เพื่อให้การบริหารจัดการงานของโครงสร้างการกำกับด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างราบรื่น เจ้าหน้าที่สามารถมอบหมายอำนาจหน้าที่อื่น ๆ ที่สำคัญอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศตามลำดับสายบังคับบัญชาหรือตามโครงสร้างของคณะแพทยศาสตร์และมหาวิทยาลัย

โครงสร้างการกำกับด้านความมั่นคงปลอดภัยสารสนเทศ คณะแพทยศาสตร์ประจำปี 2569

คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ

ชื่อ	ตำแหน่ง
ผศ.นพ.กิตติพงศ์ เรียบร้อย	คณบดีคณะแพทยศาสตร์
ผศ.นพ.บุญชัย หวังศุภดิลก	รองคณบดีฝ่ายเวชสารสนเทศ
รศ.นพ.รังสรรค์ ภูรยานนทชัย	รองคณบดีฝ่ายโรงพยาบาลและผู้อำนวยการโรงพยาบาล
ผศ.พญ.นลินี โกวิทวนาวงษ์	รองคณบดีฝ่ายบริหาร
ผศ.ดร.นพ.ชนนท์ กองกมล	ผู้อำนวยการฝ่ายวิเคราะห์ข้อมูลและนวัตกรรมดิจิทัล
นายจรูญ แก้วมี	หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ตัวแทนคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ

นายจรูญ แก้วมี - หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ผู้ตรวจสอบภายในด้านความมั่นคงปลอดภัยสารสนเทศ

นายบัณฑิต พรหมพันธ์ - หัวหน้าหน่วยตรวจสอบภายใน

นางสาวพนิตนาถ เพ็งสุวรรณ - คณะผู้ตรวจสอบภายใน

นางสาวกัตติกาญจน์ คชรัตน์ - คณะผู้ตรวจสอบภายใน

คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ชื่อ	ตำแหน่ง
นายจรูญ แก้วมี	หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
นายโกเมน เรืองฤทธิ์	หัวหน้างานบริหารระบบเครือข่ายฐานข้อมูลและซ่อมบำรุง
น.ส.นันท์นภัส โดยประกอบ	หัวหน้างานพัฒนาระบบสารสนเทศ
นายไชยยันต์ ปาละมาณ	หัวหน้าหน่วยพัฒนาระบบสารสนเทศทางการบริหาร
นายณัฏฐพล นุ้ยแนบ	หัวหน้าหน่วยพัฒนาระบบสารสนเทศโรงพยาบาลด้านบริการและบริหาร
นายอภิชาต แซ่เอ้ง	หัวหน้าหน่วยพัฒนาระบบสารสนเทศโรงพยาบาลด้านรักษาพยาบาล
นายณรงค์วิทย์ บุญยังดำรง	หัวหน้าหน่วยพัฒนาระบบสารสนเทศโรงพยาบาลด้านวินิจฉัย
นายคณกรณ์ หอศิริธรรม	คณะทำงานฝ่ายวิเคราะห์ข้อมูลและนวัตกรรมดิจิทัล
นายเอกพงศ์ พรมอินทร์	คณะทำงานฝ่ายวิเคราะห์ข้อมูลและนวัตกรรมดิจิทัล
นายพงศ์กานต์ กาลสงค์	คณะทำงานเครือข่ายฐานข้อมูล
นายสานุนัย เทียนแพ	คณะทำงานเครือข่ายฐานข้อมูล
นายอัสมีน บาเหะ	คณะทำงานเครือข่ายฐานข้อมูล
นายนิติ โชติธรรมโม	คณะทำงานเครือข่ายฐานข้อมูล
นายศรัณย์ศักดิ์ แซ่ลิ่ม	คณะทำงานเครือข่ายฐานข้อมูล

การจัดการสารสนเทศในระบบการจัดการ

๒๑. เอกสารหรือสารสนเทศไม่ว่าจะอยู่ในรูปแบบของสื่อสิ่งพิมพ์หรือไฟล์ดิจิทัล จะต้องได้รับการคุ้มครองและควบคุมดังนี้:

๒๑.๑ อนุมัติเอกสารจากผู้ที่มีอำนาจอนุมัติก่อนที่จะประกาศใช้งาน

๒๑.๒ ตรวจทานและปรับปรุงเอกสาร เมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือตามรอบการตรวจทานที่กำหนดไว้อย่างเหมาะสม อย่างน้อย 1 ครั้งต่อปี

๒๑.๓ ถูกระบุการเปลี่ยนแปลงและสถานะการแก้ไขเอกสาร ควบคุมเวอร์ชั่น อย่างเหมาะสม

๒๑.๔ อ่านง่ายและทำความเข้าใจได้ง่าย

๒๑.๕ ถูกจำแนกประเภทและลำดับชั้นความลับได้อย่างถูกต้อง ถูกจัดเก็บอย่างเหมาะสม

๒๑.๖ ในกรณีที่อ้างอิงเอกสารภายนอก ตรวจทานแหล่งที่มาที่น่าเชื่อถือ หรือจัดเก็บเอกสารภายนอกที่อ้างอิงอย่างเหมาะสม ค้นหาได้

๒๑.๗ ถูกประกาศใช้งานหรือสื่อสารต่อผู้มีส่วนได้ส่วนเสียอย่างเหมาะสม

๒๒. กรณีการใช้ระบบสารสนเทศในการควบคุมและจัดเก็บเอกสารในลักษณะดิจิทัลไฟล์ ต้องมั่นใจว่าระบบสารสนเทศดังกล่าวมีฟังก์ชั่นการทำงานที่สอดคล้องต่อนโยบายและแนวปฏิบัติทั้งในระดับมหาวิทยาลัยและคณะแพทยศาสตร์

๒๓. กรณีที่เป็นการจัดเก็บเอกสารจำพวกบันทึก (record) ให้จัดเก็บตามระยะเวลาที่กำหนดหรือตามที่กฎหมายกำหนด

การจัดเก็บบันทึกทางคอมพิวเตอร์

ภายใต้การจัดการฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์

ประเภทบันทึก	ระยะเวลาจัดเก็บ
บันทึกการใช้งาน INTERNET	90 วัน
บันทึกการวิเคราะห์ TRAFFIC LOG	60 วัน
ภาพวงจรปิดภายในฝ่ายเทคโนโลยีสารสนเทศ	มากกว่า 30 วัน
บันทึกการเข้าออกประตูฝ่ายเทคโนโลยีสารสนเทศ	มากกว่า 60 วัน

*ทั้งนี้หากไม่ได้กำหนดไว้เป็นการเฉพาะให้จัดเก็บตามขีดความสามารถของระบบสารสนเทศอย่างเหมาะสม หรือตามระเบียบของมหาวิทยาลัย

๒๔. ระดับชั้นเอกสารในระบบการจัดการของคณะแพทยศาสตร์ประกอบด้วย 2 ระดับชั้น

๒๔.๑ ระดับชั้น 1: กระบวนการ นโยบาย แนวปฏิบัติ กรอบมาตรฐาน คู่มือการปฏิบัติงาน ผลการปฏิบัติงานที่สำคัญ อาทิ รายงานความเสี่ยง แผนการบริหารความเสี่ยง โดยมอบหมายให้ รองคณบดีฝ่ายเวชสารสนเทศ เป็นผู้อนุมัติ ตามผลการตรวจทานจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ และใช้ตัวย่อแทนเอกสารระดับชั้นที่ 1 ดังนี้

ตัวย่อ	***ความหมายของลักษณะเอกสาร***
PR	Practice: คือการแสดงหรือบันทึกถึงขีดความสามารถหน่วยงาน (Organization Capability) ที่อาจประกอบด้วยกระบวนการ นโยบาย กรอบมาตรฐาน และแนวปฏิบัติ เพื่อให้บรรลุวัตถุประสงค์หนึ่ง
PC	Policy: นโยบาย คณะแพทยศาสตร์
PD	Procedure: แนวปฏิบัติ คณะแพทยศาสตร์
SD	Support Document: เอกสารสนับสนุนต่าง ๆ ในระบบการจัดการ

๒๔.๒ ระดับชั้น 2: แบบฟอร์ม เอกสารแนบท้ายเอกสาร รายงานผลการดำเนินงาน ของ ระดับชั้น 1 ให้ถือว่าถูกอนุมัติเมื่อเอกสารในระดับชั้นที่ 1 ได้รับการอนุมัติ

๒๕. เอกสารต้องมีรหัสที่เป็นเอกลักษณ์ (ไม่ซ้ำ) กันในระบบการจัดการ โดยสามารถใช้ทั้งตัวเลขและอักษร แต่ควรพิจารณาใช้

ประโยชน์จากการสื่อความหมาย เพื่อสามารถบ่งชี้ได้โดยง่าย โดยประกอบ 2-4 อักขระ/ตัวเลข

๒๖. การตั้งชื่อเอกสารให้มีองค์ประกอบสำคัญ (ต้องมี) ดังนี้

[รหัสเอกสาร] – [ลำดับชั้นเอกสาร] _ {optional}

**{optional} คือส่วนของการตั้งชื่อเอกสารที่ผู้จัดทำสามารถเพิ่มเติมเพื่อสื่อความหมายหรือต้องการเน้นย้ำถึงผู้ใช้เอกสาร ตัวอย่างเช่น

ISMS-PR_ปรับปรุงล่าสุด

๒๗. ระดับชั้นความลับต้องไม่ขัดต่อที่กำหนดไว้ใน พ.ร.บ. ข้อมูลข่าวสารของราชการ

๒๘. การควบคุมเวอร์ชั่นของเอกสารให้ระบุไว้บนหน้าปกหรือส่วนของชื่อไฟล์ เพื่อให้มีความชัดเจน ในกรณีที่ใช้ระบบสารสนเทศในการควบคุมเอกสารต้องระบุถึงการเปลี่ยนแปลง วันและเวลาที่เกิดการแก้ไข และผู้ที่ดำเนินการแก้ไขได้ การกำหนดเวอร์ชั่นประกอบด้วย

[ปีที่เอกสารมีการทบทวนล่าสุด] - [approval date]

[ปีที่เอกสารมีการทบทวนล่าสุด] คือปีของการแก้ไขของเอกสารครั้งนั้น

[approval date] คือส่วนของวันที่มีการอนุมัติในปีนั้น ๆ ซึ่งจะเป็นภาษาไทยหรืออังกฤษก็ได้

2569-12October

๒๙. เอกสารต้องถูกควบคุมการเปลี่ยนแปลงไม่ว่าจะเป็นภาษาใด กรณีเป็นการแปลให้อ้างอิงต้นฉบับที่เป็นภาษาเดิมของเอกสาร และควบคุมการเปลี่ยนแปลงทั้งต้นฉบับและฉบับแปล กรณีที่เป็นเอกสารสำคัญและมีความละเอียดอ่อนหรืออาจส่งผลต่อความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างรุนแรงหากมีการใช้หรือสื่อสารผิดอันเป็นผลจากการแปล ต้องจัดให้มีการยืนยันผลการแปลด้วยหน่วยงานที่เชื่อถือได้

๓๐. การตั้งรหัสหรือเวอร์ชั่นเอกสารสามารถเป็นได้ทั้งภาษาไทยและอังกฤษ เลขอาราบิกหรือเลขไทย ย่อมให้ผลไม่ต่างกัน

๓๑. การควบคุมสิทธิการเข้าถึงเอกสารในระบบการจัดการกำหนดให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเท่านั้นที่มีสิทธิการแก้ไขเอกสาร และผู้อื่นมีสิทธิได้เพียงเรียกดู

๓๒. จัดให้มีบัญชีควบคุมเอกสารทั้งหมดในระบบการจัดการ

๓๓. บันทึกหรือระบบสารสนเทศที่ใช้ในการบันทึกสามารถนำมาพิจารณาใช้เพื่อการจัดทำการบันทึกเอกสาร ทดแทนการใช้กระดาษหรือแบบฟอร์มกระดาษ ประกอบด้วย

- ๓๓.๑ การบันทึกความเสี่ยงและแผนการจัดการความเสี่ยง
- ๓๓.๒ การบันทึกความไม่สอดคล้อง โอกาสการพัฒนาปรับปรุง และข้อสังเกต และการดำเนินการแก้ไข
- ๓๓.๓ การบันทึกอุบัติการณ์
- ๓๓.๔ การบันทึกการเปลี่ยนแปลง
- ๓๓.๕ การบันทึกประเด็นปัญหาคงค้าง
- ๓๓.๖ การบันทึกคำขอบริการ
- ๓๓.๗ การบันทึกตัวชี้วัดประสิทธิภาพระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ

๓๔. เอกสารภายนอกระบบการจัดการ ให้ควบคุมตามต้นฉบับที่ถูกนำส่งมายังหน่วยงาน หากไม่ได้มีการกำหนดชื่อไว้ ให้ผู้รับเอกสารกำหนดชื่อเอกสารและควบคุมไว้ เมื่อครบรอบการตรวจทานรายการเอกสารให้นำมาเพิ่มในบัญชีควบคุมเอกสารประจำปี

บัญชีควบคุมเอกสารประจำปี 2569

รายการ เอกสารภายในระบบการจัดการ

รหัสเอกสาร	ชื่อเอกสาร	เวอร์ชั่นล่าสุด
ISMS-PR	ขีดความสามารถด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	2569-17June
IS-PR	ขีดความสามารถด้านความมั่นคงปลอดภัยสารสนเทศ	2569-17June
ASST-SD	รายการทรัพย์สินสารสนเทศ	2569-17June
IAR-SD_06	รายงานผลตรวจสอบภายใน ครั้งที่ 6	2568-15August
MOM-SD_01	รายงานการประชุมฝ่ายบริหาร	2569-22May
BCP-SD	แผนการจัดการความต่อเนื่องทางธุรกิจ	2569-17June

รายการ เอกสารภายนอกระบบการจัดการ

- พระราชบัญญัติว่าด้วยการกระผิดเกี่ยวกับคอมพิวเตอร์
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
- พระราชบัญญัติข้อมูลข่าวสารของราชการ
- พระราชบัญญัติลิขสิทธิ์
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- การคุ้มครองข้อมูลส่วนบุคคลจากกล้องวงจรปิด มหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๖๕
- นโยบายคุ้มครองข้อมูลส่วนบุคคล คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๖๕
- นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ มหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๖๗
- นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) มหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๖๗
- คำสั่งคณะแพทยศาสตร์ ที่ ๙๐๐/๒๕๖๗ แต่งตั้งคณะกรรมการระบบ ISMS
- คำสั่งคณะแพทยศาสตร์ ที่ ๙๐๑/๒๕๖๗ แต่งตั้งคณะทำงานระบบ ISMS

การกำหนดวัตถุประสงค์และตัวชี้วัด

๓๕. ระบบการจัดการ มีวัตถุประสงค์เพื่อสร้างเสริมความปลอดภัยสารสนเทศภายใต้การกำกับของฝ่ายเทคโนโลยีสารสนเทศและมุ่งเน้นความพร้อมของระบบเครือข่ายและระบบสารสนเทศสำคัญของโรงพยาบาลสงขลานครินทร์ จึงต้องกำหนดตัวชี้วัดความสำเร็จของระบบการจัดการและมีการวัดผลตามรอบความถี่ที่เหมาะสม

๓๖. ผลการวัดประสิทธิภาพของระบบการจัดการต้องได้รับการสื่อสารและรายงานแก่คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง

๓๗. ตัวชี้วัดที่ไม่ผ่านค่าเป้าหมายต้องชี้แจงถึงปัญหาและอุปสรรคหรือข้อจำกัดที่ทำให้ผลการวัดประเมินไม่ผ่านค่าเป้าหมายที่ตั้งไว้

๓๘. ตัวแทนคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ มีบทบาทในการสนับสนุน รวบรวม และสรุปผลการวัดประเมินและรายงานผลตัวชี้วัดประสิทธิภาพของระบบการจัดการ

๓๙. ในการกำหนดวัตถุประสงค์และตัวชี้วัดประสิทธิภาพของระบบการจัดการให้พิจารณาครอบคลุมและเชื่อมโยงต่อผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ แนวโน้ม และการเปลี่ยนแปลงที่สำคัญของระบบการจัดการ ที่อาจส่งผลต่อประสิทธิภาพของระบบการจัดการ

๔๐. ตัวแทนคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศเป็นผู้ดำเนินการรวบรวมผลและนำเสนอแก่คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ

ตัวชี้วัดประสิทธิภาพและวัตถุประสงค์ของระบบการจัดการ ประจำปี 2569

ตัวชี้วัด	รายละเอียดและค่าเป้าหมาย
ความพร้อมของระบบสารสนเทศและเครือข่าย (Availability)	ร้อยละของความพร้อมของระบบเครือข่าย คิดเป็นนาที ต่อ ปี ดังนี้ ● ร้อยละ 99.98 คิดทั้งระบบเครือข่ายและบริการทั้งหมดภายใต้ฝ่ายเทคโนโลยีสารสนเทศ ● ร้อยละ 99.95 คิดต่อระบบ แหล่งข้อมูล: บันทึกอุบัติการณ์ ความถี่: รายปี
การใช้ทรัพยากรเทคโนโลยีสารสนเทศ (Resource Utilization)	ร้อยละของการใช้สิทธิ์การใช้โปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ได้รับการติดตั้งบนเครื่องเซ่า ● ต้องได้รับการติดตั้งระบบรักษาความปลอดภัยปลายทาง (ENDPOINT PROTECTION) ครบถ้วน 100% ทุกปี แหล่งข้อมูล: ระบบ ESET NOD32 ความถี่: รายปี
การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)	จำนวนความเสี่ยงในระดับสูงมากที่ขาดแผนการบริหารความเสี่ยงรองรับ (RISK TREATMENT) มีจำนวน 0 รายการต่อปี แหล่งข้อมูล: รายงานผลการประเมินความเสี่ยง ความถี่: รายปี
การจัดการช่องโหว่เชิงเทคนิค (Technical Vulnerability Management)	จำนวนช่องโหว่เชิงเทคนิคที่มีค่า CVE SCORE มากกว่า 9 มีจำนวน 0 รายการ หรือต้องได้รับการอนุมัติจากฝ่ายบริหารหากไม่ดำเนินการแก้ไขหรือมีข้อจำกัดในการแก้ไข แหล่งข้อมูล: ผลการสแกนช่องโหว่เชิงเทคนิค ความถี่: รายปี
ความไม่สอดคล้องต่อกฎหมาย	ผลการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศต้องไม่พบการรายงานความไม่สอดคล้องต่อกฎหมาย แหล่งข้อมูล: รายงานผลการตรวจสอบภายใน ความถี่: รายปี

กรอบการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและการจัดการ

๔๑. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศต้องใช้เกณฑ์ที่กำหนดไว้ในเอกสารฉบับนี้ โดยสามารถอ้างอิงหรือเทียบเคียงกับเกณฑ์ของมหาวิทยาลัยได้ตามความเหมาะสม

๔๒. ต้องจัดให้มีการประเมินความเสี่ยงอย่างน้อย 1 ครั้งต่อปี

๔๓. กำหนดให้ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ เป็นเจ้าของความเสี่ยง ภายใต้ฝ่ายเทคโนโลยีสารสนเทศ และอนุมัติผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยง

๔๔. กำหนดให้ ตัวแทนคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศเป็นผู้รายงานผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยง

๔๕. เกณฑ์การประเมินความเสี่ยงต้องครอบคลุมการละเมิดคุณสมบัติของสารสนเทศ อาทิ การหยุดชะงักของระบบที่เป็นผลหรือเกิดจากผลแห่งการละเมิดความพร้อมใช้ของสารสนเทศ (Availability) หรือ การผิดต่อข้อกำหนด กฎหมาย และระเบียบอันเกิดจากเหตุละเมิดความลับทางราชการ หรือ ข้อมูลส่วนบุคคล (Confidentiality) หรือการปลอมแปลงข้อมูล หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต (Integrity)

๔๖. ขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้เป็นไปตามมาตรฐานสากล ISO31000 อันประกอบด้วย

- ๔๖.๑ ขั้นตอนการบ่งชี้ความเสี่ยง
- ๔๖.๒ ขั้นตอนการวิเคราะห์ความเสี่ยงโดยการกำหนดภัยคุกคามหรือช่องโหว่ที่อาจก่อให้เกิดความเสี่ยงพร้อมโอกาสและผลกระทบที่จะเกิดขึ้น
- ๔๖.๓ ขั้นตอนการประเมินความเสี่ยง
- ๔๖.๔ ขั้นตอนการจัดการความเสี่ยงโดยการเลือกกลยุทธ์ ได้แก่ 1) การลดความเสี่ยง (ใช้มาตรการ) 2) การโอนย้ายความเสี่ยง 3) การหลีกเลี่ยงความเสี่ยง และ 4) การยอมรับความเสี่ยง (ตามเกณฑ์ที่กำหนด)

๔๗. ภัยคุกคามอาจทำให้เกิดเหตุการณ์ที่ไม่พึงประสงค์ซึ่งอาจส่งผลให้เกิดความเสียหายต่อทรัพย์สินของคณะแพทยศาสตร์ ภัยคุกคามที่อันตรายนี้อาจเกิดขึ้นจากการโจมตีสารสนเทศโดยผู้ไม่ประสงค์ดี ส่งผลให้เกิดการเปิดเผย การดัดแปลง การทุจริต การทำลาย ความพร้อมใช้งาน หรือการสูญเสียข้อมูลที่มีความสำคัญโดยไม่ได้รับอนุญาต ภัยคุกคามอาจมาจากเหตุการณ์โดยบังเอิญหรือโดยเจตนา ภัยคุกคามจะต้องใช้ประโยชน์จากช่องโหว่อย่างน้อยหนึ่งช่องโหว่ของระบบแอปพลิเคชันหรือบริการที่องค์กรใช้เพื่อให้เกิดอันตรายต่อทรัพย์สินได้สำเร็จ ภัยคุกคามอาจมาจากภายในองค์กรและภายนอกองค์กร

๔๘. จุดอ่อน (ช่องโหว่) ซึ่งอาจเป็นภัยคุกคามที่ก่อให้เกิดความเสียหายต่อทรัพย์สินและการควบคุมที่มีอยู่ ซึ่งปกป้องความเสียหายต่อทรัพย์สินตามสารสนเทศ สามารถดูได้จากแคตตาล็อกช่องโหว่หรือแหล่งสารสนเทศอื่นๆ เช่น รายงานเหตุการณ์เว็บไซต์รักษาความปลอดภัยที่หน่วยงานที่มีความเกี่ยวข้องได้ระบุไว้ เช่น ThaiCERT

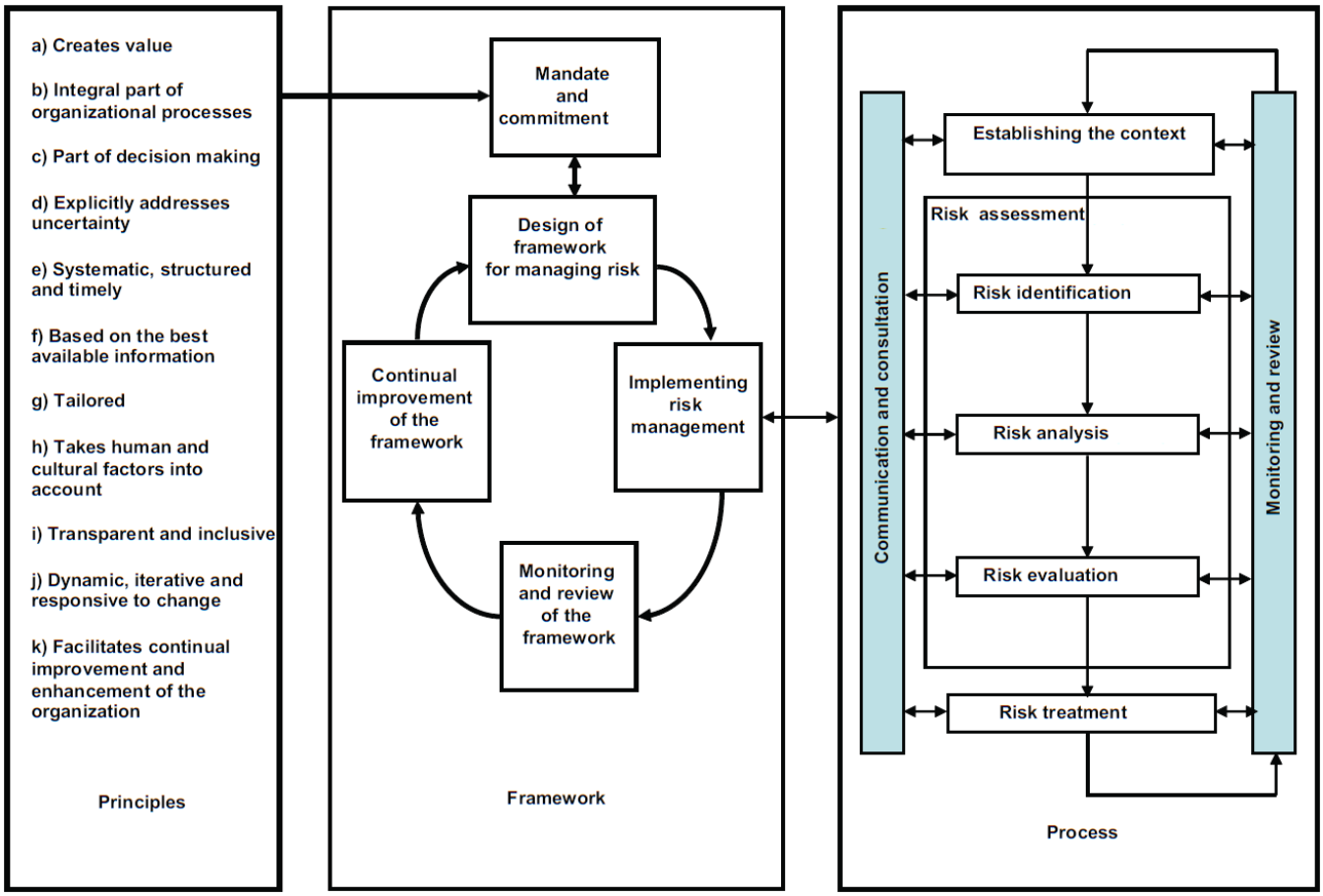
๔๙. กรอบการประเมินความเสี่ยงให้ยึดตามแนวทางของมหาวิทยาลัยเป็นสำคัญ

๕๐. ผลการประเมินความเสี่ยงต้องได้รับการอนุมัติจากเจ้าของความเสี่ยง และมีการจัดทำแผนการบริหารความเสี่ยงที่มุ่งเน้นการใช้มาตรการด้านความมั่นคงปลอดภัยสารสนเทศในการลดความเสี่ยง โดยแผนการบริหารความเสี่ยงต้องได้รับการอนุมัติเห็นชอบจากเจ้าของความเสี่ยงเช่นเดียวกัน

๕๑. การยอมรับความเสี่ยงเป็นแนวทางการจัดการความเสี่ยงที่ต้องนำรายงานคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศเสมอ

๕๒. เมื่อการดำเนินการตามแผนการจัดการความเสี่ยงแล้วเสร็จ ต้องประเมินระดับความเสี่ยงคงเหลือ และต้องเฝ้าระวังติดตาม

ผังการจัดเรียงหลักการ กรอบความคิด และกระบวนการของ
การจัดการความเสี่ยงใน ISO31000



ตารางเกณฑ์การประเมินความเสี่ยง ประจำปี 2569

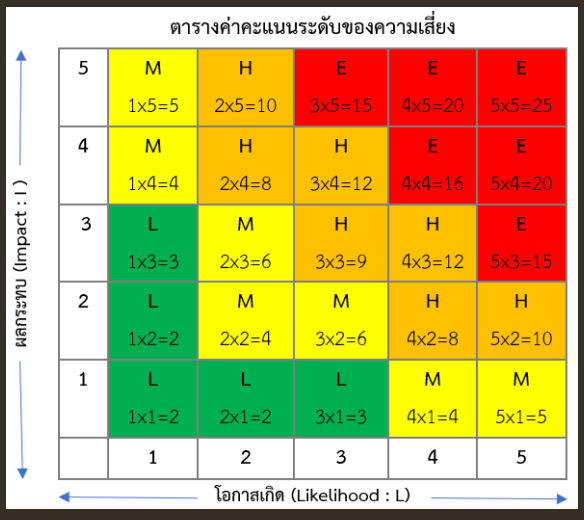
อ้างอิงตาม ตารางเกณฑ์ระดับโอกาสที่จะเกิดความเสี่ยง (LIKELIHOOD) และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้น (IMPACT) ประจำปีงบประมาณ พ.ศ. 2566 ของมหาวิทยาลัยสงขลานครินทร์

ระดับความเสี่ยง คือ ผลคูณของโอกาสการเกิดและผลกระทบ โดยจัดทำในรูปแบบ 5X5 MATRIX จำแนกความเสี่ยงออกเป็น 4 ระดับชั้น ได้แก่ L, M, H, และ E/VE/CRITICAL* ตามลำดับ
*การใช้คำในลักษณะดังต่อไปนี้ ให้ถือว่าเป็นระดับความเสี่ยงสูงมาก อาทิ VERY HIGH (VH), EXTREME (E), CRITICAL

การประเมินความเสี่ยงในระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย 2 ระดับ

- ระดับทรัพย์สินสารสนเทศ (ASSET RISK): เป็นความเสี่ยงที่เกิดจากช่องโหว่ของเทคโนโลยีของทรัพย์สินสารสนเทศ ผ่านกลไกการตรวจทานช่องโหว่ (VULNERABILITY ASSESSMENT) ซึ่งผลระดับความเสี่ยงจำแนกตามเกณฑ์มาตรฐานสากลของเครื่องมือ (CVE SCORING SYSTEM) โดยเกณฑ์ความเสี่ยงที่ยอมรับได้คือระดับ M ลงมา โดยกำหนดให้โอกาสและผลกระทบที่จะเกิดขึ้นสอดรับกับระดับความเสี่ยงดังนี้
  - ถ้า CVE SCORE = 9-10 ดังนั้น LIKELIHOOD = 5 / IMPACT = 4 ซึ่งเทียบเท่ากับระดับความเสี่ยงที่ E
  - ถ้า CVE SCORE = 7-8.9 ดังนั้น LIKELIHOOD = 4 / IMPACT = 3 ซึ่งเทียบเท่ากับระดับความเสี่ยงที่ H
  - ถ้า CVE SCORE = 4-6.9 ดังนั้น LIKELIHOOD = 3 / IMPACT = 2 (ซึ่งเป็นระดับความเสี่ยงของช่องโหว่ที่ยอมรับได้)

- ระดับการจัดการ (GOVERNANCE RISK): เป็นความเสี่ยงที่เกิดจากการประเมินบริบทของการจัดการด้านเทคโนโลยีสารสนเทศ ซึ่งอาจจะเชื่อมโยงไปยังทรัพย์สินสารสนเทศใดก็ได้ หรือไม่ระบุความเชื่อมโยงกับทรัพย์สินสารสนเทศ เพราะเป็นการกำกับที่ครอบคลุมทรัพย์สินสารสนเทศทุกรายการ โดยใช้เกณฑ์การประเมินความเสี่ยงของมหาวิทยาลัย



5	M 1x5=5	H 2x5=10	E 3x5=15	E 4x5=20	E 5x5=25
4	M 1x4=4	H 2x4=8	H 3x4=12	E 4x4=16	E 5x4=20
3	L 1x3=3	M 2x3=6	H 3x3=9	H 4x3=12	E 5x3=15
2	L 1x2=2	M 2x2=4	M 3x2=6	H 4x2=8	H 5x2=10
1	L 1x1=2	L 2x1=2	L 3x1=3	M 4x1=4	M 5x1=5
	1	2	3	4	5

โดยระดับความเสี่ยงถูกนำมาใช้เพื่อการกำหนดแนวทางการจัดการความเสี่ยง โดยพิจารณาถึงความจำเป็นในการจัดทำแผนรับมือ มาตรการควบคุม และการยอมรับความเสี่ยง

ระดับความเสี่ยง	ค่าช่วงคะแนน	สัญลักษณ์ระดับความเสี่ยง	มาตรการจัดการ
ระดับความเสี่ยงต่ำ (Low : L)	1-3	L	ระดับความเสี่ยงที่ยอมรับได้โดยไม่ต้องมีมาตรการควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ระดับความเสี่ยงปานกลาง (Medium : M)	4-7	M	ระดับความเสี่ยงที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ โดยต้องกำหนดและดำเนินมาตรการควบคุมให้แล้วเสร็จภายใน 1 รอบการประเมิน (ไม่เกิน 6 เดือน) และทบทวนผลในรอบการประเมินถัดไป
ระดับความเสี่ยงสูง (High : H)	8-14	H	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้โดยต้องมีการควบคุมและติดตามอย่างใกล้ชิด โดยต้องดำเนินมาตรการลดความเสี่ยงให้แล้วเสร็จภายใน 1 ไตรมาส (ไม่เกิน 3 เดือน) เพื่อให้ความเสี่ยงลดลงและป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับสูงมาก
ระดับความเสี่ยงสูงมาก (Extreme : E)	15-25	E	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ระดับที่ยอมรับได้ทันที (ต้องทำแผนการบริหารความเสี่ยง)

การยกระดับความเสี่ยงจากระดับปานกลาง (M) เป็นระดับสูง (H) ด้วยปัจจัยเวลา: ให้ยกระดับความเสี่ยงที่ประเมินอยู่ในระดับ M ขึ้นเป็นระดับ H เมื่อเข้าเงื่อนไขข้อใดข้อหนึ่ง ดังนี้ (1) เหตุการณ์ความเสี่ยงเกิดซ้ำในความถี่ที่สูงขึ้นจนทำให้คะแนนโอกาสการเกิด (LIKELIHOOD) เพิ่มขึ้น และคะแนนความเสี่ยงรวมเข้าสู่ช่วง 8-14 หรือ (2) ความเสี่ยงระดับ M ยังไม่ได้รับการแก้ไขให้ลดลงภายในกรอบเวลาที่กำหนด (1 รอบการประเมิน หรือไม่เกิน 6 เดือน) ทั้งนี้เพื่อป้องกันไม่ให้ความเสี่ยงที่คงค้างสะสมและลุกลามไปสู่ระดับที่ยอมรับไม่ได้

ทั้งนี้ฝ่ายเทคโนโลยีสารสนเทศต้องคำนึงถึงประเด็นความเสี่ยงที่เกี่ยวข้องอย่างน้อย ให้ครอบคลุม 2 ประเด็นความเสี่ยงได้แก่ เทคโนโลยี/ดิจิทัล และ ด้านความสอดคล้อง โดยการประเมินความเสี่ยงต้องครอบคลุมอย่างน้อย

- โครงสร้างองค์กร บทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT ASSET MANAGEMENT)
- การรักษาความมั่นคงปลอดภัยของข้อมูล (INFORMATION SECURITY)
- การควบคุมการเข้าถึง (ASSESS CONTROL)
- การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (PHYSICAL AND ENVIRONMENTAL SECURITY)
- การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (COMMUNICATIONS SECURITY)
- การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT OPERATIONS SECURITY)
- การจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศ (SYSTEM ACQUISITION AND DEVELOPMENT)
- การบริหารจัดการเหตุการณ์ผิดปกติ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT INCIDENT AND PROBLEM MANAGEMENT)
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT EMERGENCY PLAN)
- การบริหารจัดการผู้ให้บริการจากภายนอก (THIRD PARTY MANAGEMENT)

เกณฑ์ด้านโอกาสการเกิดขึ้นให้พิจารณาความน่าจะเป็นของการเกิดเหตุการณ์ด้านเทคโนโลยี / ดิจิทัล และความสอดคล้อง ที่บ่งชี้ความเสี่ยง

	ด้านเทคโนโลยี / ดิจิทัล		ด้านความสอดคล้อง	
คะแนน	คำอธิบาย	คำอธิบายต่อรอบประเมิน	คำอธิบาย	คำอธิบายต่อรอบประเมิน
5	ตั้งแต่ 3 ครั้ง ขึ้นไป ต่อเดือน	มากกว่า 18 ครั้ง ต่อ รอบประเมิน	ตั้งแต่ 5 ครั้งต่อปี	ตั้งแต่ 3 ครั้ง ต่อ รอบประเมิน
4	ไม่เกิน 3 ครั้งต่อเดือน	ไม่เกิน 18 ครั้ง ต่อ รอบประเมิน	ไม่เกิน 4 ครั้งต่อปี	ไม่เกิน 3 ครั้ง ต่อ รอบประเมิน
3	ไม่เกิน 3 ครั้งต่อ 6 เดือน	ไม่เกิน 3 ครั้ง ต่อ รอบประเมิน	ไม่เกิน 3 ครั้งต่อปี	ไม่เกิน 2 ครั้ง ต่อ รอบประเมิน
2	ไม่เกิน 2 ครั้งต่อปี	ไม่เกิน 1 ครั้ง ต่อ รอบประเมิน	โอกาสที่จะเกิด จำนวน 2 ครั้งต่อปี	ไม่เกิน 1 ครั้ง ต่อ รอบประเมิน
1	ไม่เกิน 1 ครั้งต่อ 2-5 ปี	ไม่เกิน 1 ครั้ง ทุกๆ 4 รอบประเมิน หรือต่ำกว่า	โอกาสที่จะเกิด น้อยกว่า หรือ 1 ครั้งต่อปี	ไม่เกิน 1 ครั้ง ต่อ 2 รอบประเมิน หรือต่ำกว่า

เกณฑ์การประเมินระดับผลกระทบจากค่าเฉลี่ยผลกระทบ 5 ด้านของประเด็นด้านเทคโนโลยี / ดิจิทัล และ 1 ด้านของประเด็นด้านความสอดคล้อง ดังนี้

- ผลกระทบด้านเทคโนโลยีสารสนเทศ (INFORMATION TECHNOLOGY IMPACT)
  – มีการปรับแก้เนื่องจากไม่เหมาะสมกับฝ่ายเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ที่ดูแลระบบสารสนเทศสำคัญ
- ผลกระทบด้านการดำเนินงาน (OPERATION IMPACT)
  – มีการปรับแก้เนื่องจากพิจารณาที่เจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ และให้รองรับความเสี่ยงที่กระทบต่อบุคลาผู้ปฏิบัติงาน
- ผลกระทบด้านภาพลักษณ์ (REPUTATION IMPACT)
- ผลกระทบด้านการเงิน (FINANCIAL IMPACT)
- ผลกระทบด้านบุคลากร (PERSONNEL IMPACT)
- ผลกระทบด้านกฎหมายและความสอดคล้อง (COMPLIANCE IMPACT)

การพิจารณาระดับผลกระทบของปัจจัยเสี่ยง หากความเสี่ยงนั้นมีผลกระทบเกิดขึ้นหลายด้าน ให้หาค่าเฉลี่ยระดับผลกระทบเทียบกับค่าช่วงคะแนนเฉลี่ย หากด้านใดด้านหนึ่งไม่ถูกนำมาพิจารณาให้นำออกจากตัวหารของค่าเฉลี่ย แต่อย่างน้อยต้องครอบคลุมผลกระทบด้านเทคโนโลยีสารสนเทศ

คะแนน	ด้านเทคโนโลยี / ดิจิทัล					ด้านความสอดคล้อง	การคำนวนค่าเฉลี่ยระดับผลกระทบ
	ผลกระทบด้านเทคโนโลยีสารสนเทศ (ปรับแก้)	ผลกระทบด้านการดำเนินงานของเจ้าหน้าที่ (ปรับแก้)	ผลกระทบด้านภาพลักษณ์	ผลกระทบด้านการเงิน	ผลกระทบด้านบุคลากร	ผลกระทบด้านกฎหมายและความสอดคล้อง	
5	กระทบต่อการหยุดชะงักทั้งหมดของระบบ HIS	เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้ทั้งหมด (กระทบเป็นวงกว้าง)	มีกิจกรรมของคนหมู่มาก และ/หรือ มีการเผยแพร่ข่าวในวงกว้างทั้งในหนังสือพิมพ์ วิทยุและโทรทัศน์ หรือสื่อสังคมออนไลน์ที่กว้าง กระทบต่อความมั่นคงและความเชื่อมั่นต่อ มหาวิทยาลัย	> 10 ล้านบาท	อันตรายถึงชีวิต/ สูญเสียอวัยวะ/ทุพพลภาพ	มีการละเมิดกฎระเบียบอย่างรุนแรง ซึ่งส่งผลกระทบชื่อเสียงองค์กร หรือโทษทางวินัย ไล่ออก /มีการดำเนินคดีทางอาญา ทางแพ่ง ทางวินัย /ผู้รับการประเมินไม่ผ่านประเมินและถูกออกจากงาน	มากกว่า 4.49
4	กระทบต่อการหยุดชะงักทั้งหมดของระบบภายใต้ Colocation Service หรือระบบอื่น ๆ ของคณะแพทยศาสตร์ หรือ กระทบต่อการหยุดชะงักบางส่วนของระบบ HIS	เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้บางส่วน (กระทบ 3-4 แผนก)	มีกิจกรรมของคนหมู่มาก และ/หรือ มีการเผยแพร่ข่าวในวงกว้างทั้งในหนังสือพิมพ์ วิทยุและโทรทัศน์ หรือสื่อสังคมออนไลน์ที่กว้าง ต้องมีการชี้แจงจากผู้บริหารระดับสูง	> 2.5 แสนบาท – 10 ล้านบาท	มีการบาดเจ็บสาหัสถึงขั้นพักงานไม่เกิน 1 เดือน	มีการละเมิดกฎระเบียบอย่างมาก ส่งผลกระทบต่อบุคคลหรือทรัพย์สิน และไม่สามารถแก้ไขได้ หรือโทษทางวินัย ปลดออก/มีการดำเนินคดีทางแพ่ง ทางวินัย/ผู้รับการประเมินไม่ผ่านประเมิน	3.50 - 4.49
3	กระทบต่อประสิทธิภาพและเสถียรภาพทั้งหมดระบบ HIS แต่ไม่หยุดชะงัก เช่น ความหน่วงช้า	เจ้าหน้าที่ทั้งหมดปฏิบัติงานได้ไม่เต็มประสิทธิภาพ (กระทบ 1-2 แผนก)	มีกิจกรรมของคนในวงจำกัด ตัวอย่าง น.ศ ในภาควิชาบางคน หรือจำนวนหนึ่ง และ/หรือ มีการเผยแพร่ข่าวทั้งในหนังสือพิมพ์ วิทยุและโทรทัศน์ หรือสื่อสังคมออนไลน์ในวงจำกัด	> 50,000 – 2.5 แสนบาท	มีการบาดเจ็บถึงขั้นพักงานไม่เกิน 7 วัน	มีการละเมิดกฎระเบียบอย่างมีนัยสำคัญส่งผลกระทบต่อบุคคลหรือทรัพย์สิน แต่สามารถแก้ไขได้ หรือโทษทางวินัย ลดค่าจ้าง/มีการดำเนินคดีทางวินัย	2.50 - 3.49
2	กระทบต่อประสิทธิภาพและเสถียรภาพของระบบทั้งหมดภายใต้ Colocation Service หรือระบบอื่น ๆ ของคณะแพทยศาสตร์ หรือกระทบต่อประสิทธิภาพและเสถียรภาพบางส่วนของระบบ HIS	เจ้าหน้าที่บางส่วนปฏิบัติงานได้ไม่เต็มประสิทธิภาพ (กระทบบางจุด)	มีการเผยแพร่ข่าวในวงจำกัด ไม่ออกสื่อ	> 10,000 – 50,000 บาท	มีการบาดเจ็บพักงานไม่เกิน 2 วัน	มีการละเมิดกฎระเบียบเล็กน้อยที่สามารถแก้ไขได้ หรือโทษทางวินัย ตัดค่าจ้าง	1.50 - 2.49
1	กระทบต่อประสิทธิภาพและเสถียรภาพของระบบบางส่วนภายใต้ Colocation Service หรือระบบอื่น ๆ ของคณะแพทยศาสตร์	เจ้าหน้าที่เป็นรายบุคคลไม่สามารถปฏิบัติงานได้หรือไม่เต็มประสิทธิภาพ (กระทบน้อยมาก)	ไม่มีการเผยแพร่ข่าว	ไม่เกิน 10,000บาท	บาดเจ็บเล็กน้อยไม่พักงาน	มีการละเมิดกฎระเบียบเล็กน้อยที่ไม่ส่งผลกระทบที่สำคัญ หรือโทษทางวินัยภาคทัณฑ์	ต่ำกว่า 1.50

ความเสี่ยงต้องถูกจัดลำดับความสำคัญในการบริหารจัดการ โดยใช้ระดับความเสี่ยงเป็นเกณฑ์สำคัญ ในกรณีที่ระดับความเสี่ยงเท่ากัน ให้มุ่งเน้นความเสี่ยงที่กระทบต่อชีวิต (Life safety) ของบุคคลเป็นสำคัญในลำดับต้น

ในกรณีที่มีการใช้สัญลักษณ์อักขระทดแทนตัวแทนให้พิจารณาดังนี้

VL = 1 / L = 2 / M = 3 / H = 4 / VH,E,CRITICAL = 5

การประเมินโอกาสการเกิดของเหตุการณ์ด้วยหลักความน่าจะเป็น

เพื่อให้การประเมินโอกาสการเกิดขึ้นของเหตุการณ์มีความสอดรับกำกับความน่าจะเป็นของการเกิดขึ้นเมื่อมีการเฝ้าระวังหรือประเมินความเสี่ยงในรอบถัด ๆ ที่เป็นผลหรือสามารถเทียบเคียงกับผลการประเมินครั้งที่ผ่านมา คณะแพทยศาสตร์พิจารณาจัดเก็บสถิติของการเกิดขึ้นของเหตุการณ์ความเสี่ยงและประเมินถึงค่าความน่าจะเป็นเมื่อเวลาผ่านไป ตัวอย่างเช่น การประเมินรอบที่ 1 ประจำปี 2566 เหตุการณ์น้ำท่วมถูกประเมินที่ระดับ 5 หมายถึงมีโอกาสมากกว่า 3 ครั้งต่อรอบประเมิน เมื่อข้อเท็จจริงปรากฏว่าเหตุการณ์ดังกล่าวเกิดขึ้นประมาณ 5 ครั้งต่อปี และเมื่อสิ้นสุดไตรมาสที่ 2 ของปี 2566 ปรากฏว่ามีน้ำท่วมเกิดขึ้นจริง 3 ครั้งในรอบการประเมินที่ 1 ดังนั้นในรอบการประเมินที่ 2 โอกาสการเกิดขึ้นจึงต้องพิจารณาที่ 2 ครั้งต่อปี (เพราะเกิดขึ้นไปแล้ว 3 ครั้ง) จึงมีโอกาสเกิดที่ระดับ 4

รายการมาตรการความมั่นคงปลอดภัยสารสนเทศ

คณะแพทยศาสตร์ต้องจัดให้มีรายการมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ โดยอ้างอิง มาตรฐานสากล ISO/IEC 27001:2022 และเพิ่มเติมตามมาตรฐาน CIS อย่างเหมาะสม

รายการมาตรการความมั่นคงปลอดภัยสารสนเทศ

เวอร์ชั่นปัจจุบันคือ 1.0 (เพื่อใช้ในการอ้างอิงการตรวจรับรองมาตรฐานสากล)

รายการมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability) คือรายการมาตรการอ้างอิง Annex-A ของมาตรฐานสากล ISO/IEC 27001:2022 มาประยุกต์ใช้ ความในที่ปรากฏในรายการมาตรการที่นำมาใช้ให้เสนอเป็นแนวปฏิบัติเพิ่มเติมจากที่กำหนดไว้ในมาตรฐาน นโยบาย แนวปฏิบัติที่กำหนดไว้เฉพาะ

- ✓ เมื่อปรากฏคำว่า “มาตรฐานระบบการจัดการ” หรือ “มาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ” ให้หมายถึงการอ้างอิงไปยังเอกสาร PSU-ISMS-PR และอาจครอบคลุมถึงมาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ

ในกรณีที่ปรากฏคำว่า MSS ในรายการมาตรการ (Column: CONTROLS) ให้มีนัยสำคัญครอบคลุม ดังนี้

- ✓ แทนที่ด้วยคำว่า ‘Information Security’ เพื่อหมายถึงมาตรการด้านความมั่นคงปลอดภัยสารสนเทศโดยเชื่อมโยงการเลือกใช้มาตรการตามที่กำหนดไว้ในมาตรฐาน ISO/IEC 27001:2022 หากมีการใช้ระบบการจัดการที่มากกว่า 1 ระบบการจัดการในอนาคต ให้ดำเนินการเพิ่มเติมคำแทนที่เพื่อหมายถึงระบบการจัดการอื่น ๆ ตามที่หน่วยงานนำมาใช้

ในกรณีที่มีการกำหนดมาตรการย่อย (Sub-Control) ให้พิจารณาใช้ ‘-X’ โดย X คือตัวเลขแสดงจำนวนมาตรการย่อย อาทิ 5.9-1 ซึ่งเป็นมาตรการย่อยที่เพิ่มมาจากมาตรการหลักที่อ้างอิงมาจาก มาตรการตามที่กำหนดไว้ในมาตรฐาน ISO/IEC 27001:2022

2013	CONTROLS	CHANGE IN 2022		CONTROLS	APPLICABLE (Y/N)	JUSTIFICATION FOR EXCLUSION	INCLUSION		IMPLEMENTATION DESCRIPTION/REFERENCE
							BL	RA	
A.5.1.1	Policies for information security	MERGE	5.1	Policies for MSS	Y		O		นโยบายแม่บทมาตรฐานระบบการจัดการที่ต้องได้รับการอนุมัติและกำหนดให้ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญที่ส่งผลกระทบต่อระบบจัดการความมั่นคงปลอดภัยสารสนเทศ
A.5.1.2	Review of the policies for information security	MERGE							
A.6.1.1	Information security roles and responsibilities	2013	5.2	MSS roles and responsibilities	Y		O		แต่งตั้งคณะกรรมการครอบคลุมมาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ
A.6.1.2	Segregation of duties	2013	5.3	Segregation of duties	Y		O		อำนาจตรวจสอบแยกออกจากอำนาจการดำเนินงาน
A.7.2.1	Management responsibilities	2013	5.4	Management responsibilities	Y		O		บทบาทและภาวะผู้นำปรากฏในมาตรฐานระบบการจัดการ
A.6.1.3	Contact with authorities	2013	5.5	Contact with authorities	Y		O		ระบุรายชื่อผู้ติดต่อหน่วยงานที่สำคัญ เช่น โรงพยาบาล, สถานีตำรวจ, ศูนย์ดับเพลิง, การไฟฟ้า, ผู้ให้บริการอินเตอร์เนต เป็นต้น
A.6.1.4	Contact with special interest groups	2013	5.6	Contact with special interest groups	Y		O		ระบุข้อมูลการติดต่อกับกลุ่มเฉพาะด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

2013	CONTROLS	CHANGE IN 2022		CONTROLS	APPLICABLE (Y/N)	JUSTIFICATION FOR EXCLUSION	INCLUSION		IMPLEMENTATION DESCRIPTION/REFERENCE
							BL	RA	
		NEW	5.7	Threat Intelligence	Y		O		หน่วยงานติดตามข่าวสารจากหน่วยงานด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง
A.6.1.5	Information security in project management	MERGE	5.8	MSS in project management	Y		O		โครงการด้านเทคโนโลยีสารสนเทศของหน่วยงาน กำหนดให้ต้องคำนึงถึงการรักษาความมั่นคงปลอดภัยสารสนเทศ อันเป็นส่วนหนึ่งในกระบวนการบริหารจัดการโครงการ และกำหนดให้มีการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อมีการจัดหาระบบสารสนเทศใหม่หรือพัฒนาต่อยอดจากระบบสารสนเทศเดิม
A.14.1.1	Information security requirements analysis and specification	MERGE							
A.8.1.1	Inventory of assets	MERGE	5.9	Inventory of information and other associated assets	Y		O		จัดทำบัญชีทรัพย์สินที่อยู่ภายใต้ขอบเขตของระบบการจัดการและมีรอบการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยมีส่วนปฏิบัติการผลิตภัณฑ์สื่อสารข้อมูลเป็นเจ้าของทรัพย์สิน
A.8.1.2	Ownership of assets	MERGE							
A.8.1.3	Acceptable use of assets	MERGE	5.10	Acceptable use of information and other associated assets	Y		O		กำหนดนโยบายสำหรับการใช้งานอุปกรณ์สารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลข้อมูลในขอบเขตของระบบการจัดการ อย่างเหมาะสม และ กำหนดนโยบายในการใช้งานทรัพย์สินประเภทต่าง ๆ ตามลำดับชั้นความลับของข้อมูลนั้น
A.8.2.3	Handling of assets	MERGE							
A.8.1.4	Return of assets	2013	5.11	Return of assets	N	เจ้าหน้าที่พนักงานไม่ได้รับเครื่องคอมพิวเตอร์หรือทรัพย์สินใด ๆ จึงไม่ได้มีการทำเรื่องคืนทรัพย์สินใด ๆ			
A.8.2.1	Classification of information	2013	5.12	Classification of information	Y		O		กำหนดการจัดลำดับชั้นความลับข้อมูลรวมถึงวิธีการใช้งานข้อมูลตามลำดับชั้นของข้อมูล
A.8.2.2	Labelling of information	2013	5.13	Labelling of information	Y		O		กำหนดการระบุชั้นความลับของข้อมูล
A.13.2.1	Information transfer policies and procedures	MERGE	5.14	Information transfer	Y		O		กำหนดวิธีการเผยแพร่ข้อมูลตามลำดับชั้นความลับของข้อมูล การจัดทำสัญญารักษาความลับ และ กำหนดการใช้งานและส่งข้อมูลผ่านอีเมลและการใช้งานอินเตอร์เน็ต สื่อสังคมออนไลน์ และ LINE
A.13.2.2	Agreements on information transfer	MERGE							
A.13.2.3	Electronic messaging	MERGE							
A.9.1.1	Access control policy	MERGE	5.15	Access control	Y		O		กำหนดการควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศในขอบเขตของระบบการจัดการให้เป็นไปอย่างเหมาะสมและสามารถเข้าถึงได้เฉพาะบุคคลที่มีสิทธิ์ในการเข้าถึงเท่านั้น และ กำหนดการควบคุมการเข้าถึงเครือข่ายของหน่วยงาน
A.9.1.2	Access to networks and network services	MERGE							
A.9.2.1	User registration and de-registration	2013	5.16	Identity management	Y		O		กำหนดกระบวนการในการลงทะเบียนใช้งานบัญชีผู้ใช้ รวมไปถึงกระบวนการปรับเปลี่ยน และการลบบัญชีผู้ใช้สำหรับพนักงานที่สิ้นสุดการทำงาน
A.9.2.4	Management of secret authentication information of users	MERGE	5.17	Authentication information	Y		O		กำหนดวิธีการและคุณภาพรหัสผ่าน กำหนดเกี่ยวกับการใช้งานรหัสผ่านอย่างปลอดภัย และจัดทำระบบการบริหารจัดการรหัสผ่านที่มั่นคงปลอดภัย รวมถึงกำหนดให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ
A.9.3.1	Use of secret authentication information	MERGE							
A.9.4.3	Password management system	MERGE							
A.9.2.2	User access provisioning	MERGE	5.18	Access rights	Y		O		การให้สิทธิ์สำหรับ account ต่าง ๆ จะให้สิทธ์เท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น กำหนดรอบการตรวจทานสิทธิ์และบัญชีผู้ใช้งาน อย่างน้อย ปีละ 1 ครั้ง และกำหนดกระบวนการยกเลิกและปรับเปลี่ยนสิทธิ์การเข้าถึงข้อมูล ระบบสารสนเทศและพื้นที่สำนักงานเมื่อพนักงานสิ้นสุดการทำงาน
A.9.2.5.	Review of user access rights	MERGE							
A.9.2.6	Removal or adjustment of access rights	MERGE							
A.15.1.1	Information security policy for supplier relationships	2013	5.19	MSS in supplier relationships	Y		O		กำหนดมีนโนบายในการบริหารจัดการผู้ให้บริการภายนอก ซึ่งกล่าวถึงการควบคุมบริหารจัดการผู้ให้บริการภายนอก และสิ่งที่ผู้ให้บริการภายนอกจำเป็นต้องรับทราบ และควบคุมตามระเบียบการจัดซื้อจัดจ้างของรัฐวิสาหกิจ และระเบียบองค์กร โดยมุ่งเน้นความมั่นคงปลอดภัยสารสนเทศ ความต่อเนื่องทางธุรกิจ และคุณภาพบริการ
A.15.1.2	Addressing security within supplier agreements	2013	5.20	Addressing MSS within supplier agreements	Y		O		จัดทำสัญญากับผู้ให้บริการภายนอกซึ่งครอบคลุมข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ
			5.20 -1	Service Level Agreement (SLA)	Y		O		กำหนดให้หน่วยงานผู้ให้บริการที่สำคัญต้องจัดให้มีสัญญาระดับบริการที่สอดรับการระดับสัญญาบริการที่หน่วยงานมีให้กับลูกค้าในรายที่ต่ำที่สุด

2013	CONTROLS	CHANGE IN 2022		CONTROLS	APPLICABLE (Y/N)	JUSTIFICATION FOR EXCLUSION	INCLUSION		IMPLEMENTATION DESCRIPTION/REFERENCE
							BL	RA	
A.15.1.3	Information and communication technology supply chain	2013	5.21	Managing MSS in the information and communication technology (ICT) supply chain	Y		O		กำหนดนโยบายให้ผู้ให้บริการภายนอกต้องควบคุมดูแลให้ผู้รับจ้าง (Sub-contractor) ปฏิบัติตามนโยบาย รวมถึงข้อปฏิบัติอื่น ๆที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ การบริหารความต่อเนื่องทางธุรกิจ และการจัดการบริการ อย่างเคร่งครัด
A.15.2.1	monitoring and review of supplier services	MERGE	5.22	Monitoring, review, and change management of supplier services	Y		O		กำหนดให้มีการติดตาม ประเมินผล รวมถึงตรวจสอบการให้บริการจากผู้ให้บริการภายนอก และกำหนดให้ผู้ให้บริการภายนอกต้องแจ้งให้หน่วยงานเมื่อมีการดำเนินการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อการให้บริการ
A.15.2.2	managing changes to supplier services	MERGE							
		NEW	5.23	Use of cloud computing service	N	ไม่มีใช้บริการ Cloud Service ในขอบเขต			
A.16.1.1	Responsibilities and procedures	2013	5.24	MSS incident management planning and preparation	Y		O		กำหนดหน้าที่และความรับผิดชอบ ขั้นตอนปฏิบัติในการแก้ไขปัญหาอุบัติการณ์ที่เกิดขึ้นในระบบการจัดการ อ้างอิงมาตรฐานระบบการจัดการ
A.16.1.4	Assessment and decision on information security events	2013	5.25	Assessment and decision on MSS events	Y		O		กำหนดการรับมือเหตุการณ์มีหน้าที่ระบุถึงระดับความรุนแรงและความเร่งด่วน เพื่อนำไปพิจารณาความสำคัญของเหตุการณ์และอุบัติการณ์
A.16.1.5	Response to information security incidents	2013	5.26	Response to MSS incidents	Y		O		กำหนดการรับมืออุบัติการณ์โดยมีหน้าที่ดำเนินการแก้ไขปัญหาตามการจัดลำดับความสำคัญ หาวิธีแก้ไขและรวบรวมหลักฐานเพื่อนำไปบันทึกในแบบฟอร์มบันทึกการจัดการอุบัติการณ์
A.16.1.6	Learning from information security incidents	2013	5.27	Learning from MSS incidents	Y		O		กำหนดการทบทวนอุบัติการณ์ที่เกิดขึ้น, สาเหตุของปัญหาและอุบัติการณ์, วิธีการแก้ไขและจัดทำองค์ความรู้ที่จำเป็นต่อการรับมืออุบัติการณ์ในอนาคตให้ได้อย่างรวดเร็วและมีประสิทธิภาพ
A.16.1.7	Collection of evidence	2013	5.28	Collection of evidence	Y		O		กำหนดแนวทางนิติวิทยาศาสตร์ในมาตรฐานระบบการจัดการ
A.17.1.1	Planning information security continuity	MERGE	5.29	Information security during disruption	Y		O		หน่วยงานมีการวางแผนความต่อเนื่องทางธุรกิจ และมาตรฐานระบบการจัดการความต่อเนื่องทางธุรกิจ โดยพิจารณาความมั่นคงปลอดภัยสารสนเทศเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่องทางธุรกิจ เตรียมพร้อมโดย แบ่งทีมงาน การติดต่อ รวมถึงระบบเพื่อให้สอดคล้องกับแผนความต่อเนื่องทางธุรกิจ และกำหนดขั้นตอนในการทดสอบแผนความต่อเนื่องทางธุรกิจ และมีการทดสอบแผนดังกล่าวอย่างน้อยปีละ 1 ครั้ง
A.17.1.2	Implementing information security continuity	MERGE							
A.17.1.3	Verify, review and evaluate information security continuity	MERGE							
A.18.1.1	Identification of applicable legislation and contractual requirements	MERGE	5.31	Legal, statutory, regulatory, and contractual requirements	Y		O		รวบรวมกฎหมายที่เกี่ยวข้องกับการดำเนินงาน รวมถึงระบุสิ่งที่หน่วยงานจัดทำเพื่อให้ดำเนินงานได้สอดคล้องกับกฎหมายดังกล่าวและปรับปรุงรายการกฎหมายให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง ในกรณีที่มีการส่งออกข้อมูลที่มีระเบียบบังคับหรือกฎหมายเฉพาะในการเข้ารหัสข้อมูลต้องวิเคราะห์กฎหมายและระเบียบดังกล่าวก่อนการจัดส่งข้อมูล เว้นแต่เป็นการปฏิบัติตามคำสั่งศาล
A.18.1.5	Regulation of cryptographic controls	MERGE							
			5.30	ICT readiness for business continuity	Y		O		หน่วยงานจัดทำระบบการจัดการความต่อเนื่องทางธุรกิจ และแผนความต่อเนื่องทางธุรกิจ
A.18.1.2	Intellectual property rights	2013	5.32	Intellectual property rights	Y		O		กำหนดนโยบายให้ใช้งานโปรแกรมที่มีลิขสิทธิ์และถูกกฎหมายเท่านั้น และกำหนดให้ พ.ร.บ. ลิขสิทธิ์เป็นหนึ่งในรายการกฎหมายที่ต้องมีการตรวจทานปรับปรุงให้เป็นปัจจุบันทุกปี
A.18.1.3	Protection of records	2013	5.33	Protection of records	Y		O		บันทึกที่ถูกจัดเก็บ ส่งต่อหรือทำลายจะปฏิบัติตามลำดับขั้นความลับของข้อมูลในบันทึก และตามที่ระยะเวลาที่กฎหมายกำหนด (ถ้ามี)
A.18.1.4	Privacy and protection of personally identifiable information	2013	5.34	Privacy and protection of personal identifiable information (PII)	Y		O		ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลในระดับองค์กร
A.18.2.1	Independent review of information security	2013	5.35	Independent review of MSS	Y		O		กำหนดให้มีการตรวจประเมินภายในเป็นประจำอย่างน้อยปีละ 1 ครั้ง โดยใช้ผู้ตรวจประเมินอิสระที่ไม่มีส่วนได้ส่วนเสียกับระบบการจัดการ
A.18.2.2	Compliance with security policies and standards	MERGE	5.36	Compliance with policies, rules, and standards for MSS	Y		O		กำหนดให้มีการตรวจประเมินภายในเป็นประจำอย่างน้อยปีละ 1 ครั้ง โดยใช้นโยบายและแนวปฏิบัติของหน่วยงานเป็นเกณฑ์การตรวจประเมิน โดยนโยบายและแนวปฏิบัติเหล่านั้น (รวมถึงมาตรฐานและขีดความสามารถ) ต้องสอดคล้องต่อมาตรฐานสากลที่หน่วยงานขอรับการรับรองด้วย
A.18.2.3	Technical compliance review	MERGE							
A.12.1.1	Documented operating procedures	2013	5.37	Documented operating procedures	Y		O		จัดทำเอกสารขั้นตอนการปฏิบัติงานต่าง ๆ ที่มีความสำคัญ ในกรณีที่เป็นระบบสารสนเทศที่สำคัญจัดให้มีการอ้างถึงแหล่งของคู่มือที่เป็นปัจจุบันหรือกำหนดไว้ให้เป็นเอกสารภายนอกที่สำคัญ
A.7.1.1	Screening	2013	6.1	Screening	Y		O		

2013	CONTROLS	CHANGE IN 2022		CONTROLS	APPLICABLE (Y/N)	JUSTIFICATION FOR EXCLUSION	INCLUSION		IMPLEMENTATION DESCRIPTION/REFERENCE
							BL	RA	
A.7.1.2	Terms and conditions of employment	2013	6.2	Terms and conditions of employment	Y		O		กระบวนการจัดจ้างและลงนามสัญญาจ้าง บุคลากรให้เป็นไปตามระเบียบรัฐ
A.7.2.2	Information security awareness, education, and training	2013	6.3	MSS awareness, education, and training	Y		O		สร้างความตระหนัก การให้ความรู้ และการอบรมในเรื่องที่เกี่ยวข้องกับระบบการจัดการ และมาตรฐานสากลให้แก่พนักงานอย่างสม่ำเสมอ จัดการให้ความรู้ ความเข้าใจในระบบการจัดการให้กับพนักงานที่เกี่ยวข้อง และจัดเก็บหลักฐานการอบรมในระบบสารสนเทศขององค์กร
A.7.2.3	Disciplinary process	2013	6.4	Disciplinary process	Y		O		กระบวนการและบทลงโทษทางวินัยให้เป็นไปตามระเบียบของรัฐวิสาหกิจ
A.7.3.1	Termination or change of employment responsibilities	2013	6.5	Responsibilities after termination or change of employment	Y		O		กำหนดนโยบายเพิ่มเติมจากในระดับองค์กรในการบริหารจัดการพนักงานที่สิ้นสุดการจ้างงาน หรือมีการเปลี่ยนแปลงการจ้างงาน
A.13.2.4	Confidentiality or nondisclosure agreements	2013	6.6	Confidentiality or non-disclosure agreements	Y		O		หน่วยงานจัดให้มีการลงนามสัญญาหรือข้อตกลงด้านการรักษาความลับกับผู้มีส่วนได้ส่วนเสีย
A.6.2.2	Teleworking	2013	6.7	Remote working	Y		O		กำหนดนโยบายการควบคุมการปฏิบัติงานผ่านเครือข่ายระยะไกลโดยการเข้าถึงระบบเครือผ่านระบบเครือข่ายระยะไกลสามารถทำได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น และผ่านอุปกรณ์ Firewall
A.16.1.2	Reporting information security events	MERGE	6.8	MSS event reporting	Y		O		หน่วยงานมีช่องทางการรายงานเหตุขัดข้องและจุดอ่อนและเหตุการณ์ของระบบการจัดการผ่านทางอีเมลหรือโทรศัพท์
A.16.1.3	Reporting information security weaknesses	MERGE							
A.11.1.1	Physical security perimeter	2013	7.1	Physical security perimeters	Y		O		กำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพ ประตู ผนัง เพดาน และพื้นของศูนย์ข้อมูล (Data Center) ถูกปิดกั้นด้วยวัสดุที่มีความมั่นคงแข็งแรง ยากต่อการถูกทุบทำลาย สามารถป้องกันการบุกรุกโดยผู้ที่ไม่ได้รับอนุญาตได้
A.11.1.2	Physical entry controls	MERGE	7.2	Physical entry	Y		O		ติดตั้งระบบ Door Access เพื่อใช้ในการควบคุมการเข้าพื้นที่สำนักงาน และศูนย์คอมพิวเตอร์ ติดตั้ง CCTV ตั้งแต่บริเวณทางเข้าสำนักงาน รวมถึงส่วนที่สำคัญภายในสำนักงาน จัดบริเวณที่ใช้สำหรับการรับ-ส่งทรัพย์สินสารสนเทศ กับบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต
A.11.1.6	Delivery and loading areas	MERGE							
A.11.1.3	Securing offices, rooms, and facilities	2013	7.3	Securing offices, rooms, and facilities	Y		O		ในกรณีที่ไม่พบระบบ Door Access ต้องจัดให้มีการล็อคด้วยกุญแจและควบคุมการเบิกแจกกุญแจเฉพาะบุคคลที่ได้รับอนุมัติอนุญาต
		NEW	7.4	Physical Security Monitoring	Y		O		หน่วยมีการเฝ้าระวังความปลอดภัยเชิงกายภาพผ่านห้องปฏิบัติงานของเจ้าหน้าที่
A.11.1.4	Protecting against external and environmental threats	2013	7.5	Protecting against physical and environmental threats	Y		O		ติดตั้งระบบดับเพลิงในพื้นที่สำนักงาน และศูนย์ข้อมูล เพื่อป้องกันอัคคีภัย ติดตั้งระบบปรับอากาศในพื้นที่สำนักงาน และศูนย์ข้อมูล เพื่อควบคุมอุณหภูมิ ความชื้น
A.11.1.5	Working in secure areas	2013	7.6	Working in secure areas	Y		O		กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศทางกายภาพในการเข้าใช้สถานที่หรือทำงานให้เหมาะสมกับบริบทของสถานที่และความสำคัญ
A.11.2.9	Clear desk and clear screen policy	2013	7.7	Clear desk and clear screen	Y		O		กำหนดให้ผู้ใช้งานต้องล็อคหน้าจอเครื่องคอมพิวเตอร์ทุกครั้งเมื่อไม่ได้ใช้งาน
A.11.2.1	Equipment siting and protection	2013	7.8	Equipment siting and protection	Y		O		มีการจัดวางอุปกรณ์ และมีการป้องกันทางกายภาพอย่างมั่นคงปลอดภัย
A.11.2.6	Security of equipment and assets off-premises	2013	7.9	Security of assets off-premises	Y		O		กำหนดให้มีการรักษาความมั่นคงปลอดภัยของอุปกรณ์ที่ใช้งานอยู่นอกองค์กร
A.8.3.1	Management of removable media	MERGE	7.10	Storage media	Y		O		กำหนดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศในการใช้งานสื่อบันทึกข้อมูลให้เหมาะสมตามลำดับชั้นของข้อมูลที่อยู่ในสื่อบันทึกข้อมูล กำหนดขั้นตอนการทำลายสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัย กำหนดนโยบายขนย้ายสื่อการบันทึกข้อมูลอย่างมั่นคงปลอดภัยตามลำดับชั้นความลับของข้อมูล
A.8.3.2	Disposal of media	MERGE							
A.8.3.3	Physical media transfer	MERGE							
A.11.2.2	Supporting utilities	2013	7.11	Supporting utilities	Y		O		มีระบบป้องกันการล้มเหลวของกระแสไฟฟ้า ดังนี้ Generator และมีระบบ UPS สำหรับจ่ายไฟอาคาร ระบบ Fire alarm และ smoke detector ทุก ๆ พื้นที่จะมีถังดับเพลิงแบบมือถือประจำอยู่ที่ห้องทำงาน ห้องควบคุมอุปกรณ์อาคาร
A.11.2.3	Cabling security	2013	7.12	Cabling security	Y		O		มีการเดินสายไฟฟ้า และสายสื่อสาร แยกรางกันอย่างชัดเจน โดยในการเดินสายจะเดินบนราง panel ด้านบนแบบได้

2013	CONTROLS	CHANGE IN 2022		CONTROLS	APPLICABLE (Y/N)	JUSTIFICATION FOR EXCLUSION	INCLUSION		IMPLEMENTATION DESCRIPTION/REFERENCE
							BL	RA	
									มาตรฐาน สำหรับสายสื่อสารจะใช้สายสัญญาณแบบสายสำเร็จที่ได้มาตรฐานเน้นประสิทธิภาพในการรับส่งข้อมูล
A.11.2.4	Equipment maintenance	2013	7.13	Equipment maintenance	Y		O		กำหนดให้มีการบำรุงรักษาทรัพย์สินสารสนเทศต่าง ๆ อย่างสม่ำเสมอ เพื่อให้ทรัพย์สินสารสนเทศเหล่านั้น สามารถทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความพร้อมใช้งาน
A.11.2.7	Secure disposal or reuse of equipment	2013	7.14	Secure disposal or re-use of equipment	Y		O		กำหนดให้มีนโยบายทำลายอุปกรณ์ตามระดับชั้นความลับ
A.6.2.1	Mobile device policy	2013	8.1	User end point devices	Y		O		กำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา เช่น laptop และ mobile phone และตั้งค่าให้ตั้งล็อคหน้าจอคอมพิวเตอร์ เมื่อไม่ได้ใช้งานระยะหนึ่ง
A.11.2.8	Unattended user equipment	2013							
A.9.2.3	Management of privileged access rights	2013	8.2	Privileged access rights	Y		O		กำหนดกระบวนการในการบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิ์สูง โดยเจ้าของระบบเป็นผู้กำหนดสิทธิในการเข้าถึงข้อมูล และใช้งานระบบในการประมวลผลของหน่วยงานให้น้อยที่สุดเท่าที่จำเป็นต่อการปฏิบัติงาน (Access Matrix)
A.9.4.1	Information access restriction	2013	8.3	Information access restriction	Y		O		ควบคุมการเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศ ให้เป็นไปอย่างมั่นคงปลอดภัย และสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
A.9.4.5	Access control to program source code	2013	8.4	Access to source code	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.9.4.2	Secure log-in procedures	2013	8.5	Secure authentication	Y		O		จัดให้มีขั้นตอนการเข้าระบบสารสนเทศอย่างมั่นคงปลอดภัย
A.12.1.3	Capacity management	2013	8.6	Capacity management	Y		O		มีการเฝ้าติดตาม Capacity ของระบบงานต่าง ๆ การเฝ้าระวังขีดความสามารถของบริการและองค์ประกอบของบริการที่เพียงพอ
A.12.2.1	Controls against malware	2013	8.7	Protection against malware	Y		O		ติดตั้งโปรแกรมป้องกันมัลแวร์ และอัพเดตฐานข้อมูลมัลแวร์อย่างสม่ำเสมอ สำหรับเครื่องแม่ข่ายที่ใช้ระบบปฏิบัติการ Windows
A.12.6.1	Management of technical vulnerabilities	MERGE	8.8	Management of technical vulnerabilities	Y		O	O	กำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ทางเทคนิคในระบบสารสนเทศต่าง ๆ สแกนหาช่องโหว่ทางเทคนิคและประเมินความเสี่ยงของช่องโหว่ทางเทคนิคเหล่านั้น รวมทั้งกำหนดมาตรการควบคุมรองรับเพื่อลดความเสี่ยงดังกล่าว และตั้งค่าบนเครื่องคอมพิวเตอร์ให้มีการอัพเดตแพตช์สำหรับ Window OS โดยอัตโนมัติ และกำหนดมาตรการตรวจสอบช่องโหว่ระบบเทคโนโลยีสารสนเทศโดยใช้เครื่องมือสแกน (vulnerability scan) อย่างน้อยปีละ 1 ครั้ง
A.18.2.3	Technical compliance review	MERGE							
		NEW	8.9	Configuration management	Y		O		กำหนดให้มีการตั้งค่าระบบสารสนเทศและอุปกรณ์อย่างปลอดภัย จัดให้มีการสำรองการตั้งค่า
		NEW	8.10	Information deletion	Y		O		ใช้วิธีการลบและทำลายสารสนเทศตามระดับชั้นความลับอย่างเหมาะสม ในกรณีเป็นการลงระบบปฏิบัติการจะใช้วิธีลง image file บนเครื่องคอมพิวเตอร์
		NEW	8.11	Data masking	Y		O		เมื่อจำเป็นต้องมีการส่งออกข้อมูลให้แก่บุคคลภายนอกที่พึงทราบถึงความสมบูรณ์ของข้อมูลอยู่แล้วสามารถลดรูปของข้อมูลหรือทดแทนด้วยสัญลักษณ์อื่นใด อาทิ 'X' เพื่อบดบังข้อมูล
		NEW	8.12	Data leakage prevention	Y		O		จัดให้มีการเฝ้าระวังการรั่วไหลของข้อมูล
A.12.3.1	Information backup	2013	8.13	Information backup	Y		O		กำหนดกระบวนการสำรองข้อมูลและทำการสำรองข้อมูล อย่างสม่ำเสมอ
A.17.2.1	Availability of information processing facilities	2013	8.14	Redundancy of information processing facilities	Y		O		จัดหาและติดตั้งอุปกรณ์ประมวลผลสารสนเทศสำรอง เพื่อบริหารจัดการอุปกรณ์ประมวลผลสารสนเทศให้มีระดับความพร้อมใช้งานที่สอดคล้องกับความต้องการทางธุรกิจขององค์กร
A.12.4.1	Event logging	MERGE	8.15	Logging	Y		O		มาตรการจัดเก็บ log ที่เกี่ยวข้องกับจราจรคอมพิวเตอร์ไว้เป็นระยะเวลาไม่น้อยกว่า 90 วัน และตรวจสอบเฝ้าระวัง log เพื่อตรวจจับเหตุการณ์ผิดปกติหรือกิจกรรมที่น่าสงสัยอย่างสม่ำเสมอ และป้องกันการเข้าถึง log จากผู้ที่ไม่ได้รับอนุญาต และจัดให้มี log ของการทำงานของผู้ดูแลระบบที่สำคัญ
A.12.4.2	Protection of log information	MERGE							
A.12.4.3	Administrator and operator logs	MERGE							
		NEW	8.16	Monitoring activities	Y		O		มีการเฝ้าระวังกิจกรรมที่เกี่ยวข้องกับการให้บริการ
A.12.4.4	Clock Synchronization	2013	8.17	Clock synchronization	Y		O		ตั้งค่าเวลาสำหรับเครื่องแม่ข่าย (Server) รวมถึงเครื่องคอมพิวเตอร์ของบุคลากรในขอบเขตให้เวลาตรงกันทั้งหมด (clock synchronization) โดยอ้างอิงจากแหล่งข้อมูลเวลาที่น่าเชื่อถือ
A.9.4.4	Use of privileged utility programs	2013	8.18	Use of privileged utility programs	Y		O		กำหนดนโยบายการใช้งานโปรแกรมอรรถประโยชน์ และการกำหนดรายการที่อนุญาตให้มีการใช้งานหรือติดตั้ง

2013	CONTROLS	CHANGE IN 2022		CONTROLS	APPLICABLE (Y/N)	JUSTIFICATION FOR EXCLUSION	INCLUSION		IMPLEMENTATION DESCRIPTION/REFERENCE
							BL	RA	
A.12.5.1	Installation of software on operational systems	MERGE	8.19	Installation of software on operational systems	Y		O		การควบคุมการติดตั้งซอฟต์แวร์ในระบบที่ให้บริการจริง เพื่อลดความเสี่ยงที่จะทำให้ระบบสารสนเทศให้บริการนั้นเกิดความเสียหาย เกิดการทำงานที่ผิดปกติ หรือไม่มีความพร้อมใช้งาน และกำหนดและจำกัดการติดตั้งซอฟต์แวร์ สำหรับอุปกรณ์สารสนเทศและอุปกรณ์เครือข่าย ของหน่วยงาน
A.12.6.2	Restrictions on soft-ware installation	MERGE							
A.13.1.1	Network controls	2013	8.20	Networks security	Y		O		กำหนดนโยบายในการบริหารจัดการระบบเครือข่าย
A.13.1.2	Security of network services	2013	8.21	Security of network services	Y		O		กำหนดนโยบายในการบริหารจัดการระบบเครือข่ายและแบ่งแยกเครือข่ายไร้สายสำหรับบุคคลภายนอกที่สำนักงาน โดยอนุญาตให้เข้าถึงเฉพาะอินเตอร์เน็ต ไม่สามารถเข้าถึงระบบภายในของหน่วยงานได้
A.13.1.3	Segregation in networks	2013	8.22	Segregation of networks	Y		O		แบ่งแยกเครือข่ายบน ระบบ Infrastructure, Network สำหรับ Internet Facing Zone และ Internal Zone
		NEW	8.23	Web filtering	Y		O		มีการเฝ้าระวังการใช้งาน Internet ของส่วนสำนักงาน
A.10.1.1	Policy on the use of cryptographic controls	MERGE	8.24	Use of cryptography	Y		O		กำหนดนโยบายและข้อกำหนดในการเข้ารหัสข้อมูล และกำหนดนโยบายในการบริหารจัดการกุญแจรหัส
A.10.1.2	Key management	MERGE							
A.14.2.1	Secure development policy	2013	8.25	Secure development life cycle	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.14.1.2	Securing application services on public networks	MERGE	8.26	Application security requirements	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.14.1.3	Protecting application services transactions	MERGE							
			8.26 -1	Application redundancy and resiliency requirements	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
			8.26 -2	Application's SLA	Y		O		กรณีเป็นการใช้ระบบสารสนเทศในรูปแบบ Subscription ที่ไม่เกิดสัญญาจ้างตามรูปแบบมาตรฐานที่พึงสามารถกำหนด Service Level Agreement ได้ กำหนดให้มีการตรวจสอบการรับประกันคุณภาพของระบบสารสนเทศดังกล่าวในมิติของความพร้อมของระบบ
A.14.2.5	Secure system engineering packages	2013	8.27	Secure system architecture and engineering principles	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
		NEW	8.28	Secure coding	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.14.2.8	System security testing	MERGE	8.29	Security testing in development and acceptance	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.14.2.9	System acceptance testing	MERGE							
A.14.2.7	Outsourced development	2013	8.30	Outsourced development	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.12.1.4	Separation of development, testing and operational environments	MERGE	8.31	Separation of development, test, and production environments	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.14.2.6	Secure development environment	MERGE							
A.12.1.2	Change management	MERGE	8.32	Change management	Y		O		กำหนดกระบวนการบริหารการเปลี่ยนแปลงเพื่อควบคุมแนวทางการปฏิบัติ ติดตามและแก้ไขในการดำเนินการเปลี่ยนแปลงระบบ และการเปลี่ยนแปลงที่เกิดขึ้นกับระบบการจัดการเช่นเดียวกัน ให้หมายรวมถึงการเปลี่ยนแปลงในระบบการจัดการ (Management System) ด้วย เพื่อให้สอดรับกับข้อกำหนดของระบบการจัดการ
A.14.2.2	System change control procedures	MERGE							
A.14.2.3	Technical review of applications after operating platform changes	MERGE							
A.14.2.4	Restrictions on changes to software packages	MERGE							
A.14.3.1	Protection of test data	2013	8.33	Test information	N	ไม่มีการพัฒนาระบบในขอบเขตการขอรับรอง			
A.12.7.1	Information systems audit controls	2013	8.34	Protection of information systems during audit testing	Y		O		กระบวนการตรวจประเมินภายในโดยต้องมีการแจ้งแผนการตรวจ รวมถึงขอบเขตในการตรวจก่อนเริ่มการตรวจ โดยครอบคลุมการตรวจสอบระบบและมาตรการที่ต้องมีในระหว่างการตรวจสอบ

สมรรถนะบุคลากร

๕๓. คณะแพทยศาสตร์สนับสนุนให้บุคลากรและเจ้าหน้าที่มีสมรรถนะด้านความมั่นคงปลอดภัยสารสนเทศ โดยส่งเสริมการอบรมสร้างเสริมความรู้ความเข้าใจด้านความมั่นคงปลอดภัยที่เหมาะสมกับ บทบาท ตำแหน่งหน้าที่

๕๔. เจ้าหน้าที่ของคณะแพทยศาสตร์ต้องจัดเก็บหลักฐานการอบรมหรือสร้างสมรรถนะ ประวัติการอบรม ในระบบของคณะแพทยศาสตร์และระบบส่วนกลางที่เกี่ยวข้อง

๕๕. ผู้ตรวจสอบภายในของระบบการจัดการ ต้องจบการศึกษาระดับปริญญาตรีด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง และได้รับการอบรมมาตรฐานและแนวทางการตรวจสอบ เป็นขั้นต่ำ

๕๖. จัดให้มีการบันทึกประวัติและหลักฐานการสร้างสมรรถนะ เมื่อเป็นไปได้ให้วิเคราะห์และวัดประเมินประสิทธิของการสร้างสมรรถนะ ทั้งในมิติของผลลัพธ์ที่เกิดขึ้นกับเจ้าหน้าที่และในมิติของวิธีการที่ใช้

ความตระหนักรู้

๕๗. เจ้าหน้าที่ของคณะแพทยศาสตร์ต้องได้รับการสร้างความตระหนักต่อเอกสารฉบับนี้ อย่างน้อยปีละ 1 ครั้ง เมื่อเป็นไปได้ให้พิจารณาถึงการสร้างความตระหนักในแนวโน้มภัยคุกคามที่เกิดขึ้นในสถานการณ์ปัจจุบัน หรือตามเหตุการณ์ที่เคยเกิดขึ้นกับคณะแพทยศาสตร์

๕๘. จัดให้มีการบันทึกประวัติและหลักฐานการสร้างความตระหนักรู้ เมื่อเป็นไปได้ให้วิเคราะห์และวัดประเมินประสิทธิของการสร้างความตระหนักรู้ทั้งในมิติของผลลัพธ์ที่เกิดขึ้นกับเจ้าหน้าที่และในมิติของวิธีการที่ใช้

๕๙. เจ้าหน้าที่ของคณะแพทยศาสตร์ควรทราบถึงการปฏิบัติที่ขัดต่อข้อกำหนดกฎหมาย นโยบาย และแนวปฏิบัติ รวมถึงบทบาทหน้าที่ในการสนับสนุนและพัฒนาปรับปรุงระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ

ทรัพยากร

๖๐. กำหนดทรัพยากรบุคคลที่เพียงพอต่อการปฏิบัติงานภายใต้ฝ่ายเทคโนโลยีสารสนเทศ

๖๑. ทรัพยากรเทคโนโลยีที่เพียงพอต่อการคุ้มครองความมั่นคงปลอดภัยสารสนเทศขั้นพื้นฐานของคณะแพทยศาสตร์

- ๖๑.๑ ระบบป้องกันภัยคุกคามทางเครือข่าย
- ๖๑.๒ ระบบป้องกันภัยคุกคามทางกายภาพ
- ๖๑.๓ ระบบป้องกันภัยคุกคามทางสิ่งแวดล้อม
- ๖๑.๔ ระบบสำรองกระแสไฟฟ้า
- ๖๑.๕ ระบบสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูล
- ๖๑.๖ ระบบป้องกันมัลแวร์
- ๖๑.๗ ระบบการควบคุมการเข้าถึงระบบสารสนเทศ
- ๖๑.๘ ระบบการบันทึกอุบัติการณ์
- ๖๑.๙ ระบบการสื่อสารขั้นพื้นฐาน (โทรศัพท์)

การสื่อสารและประชาสัมพันธ์

๖๒. คณะแพทยศาสตร์สนับสนุนการสื่อสารประชาสัมพันธ์ในหลากหลายช่องทางในแต่ละกลุ่มเป้าหมายที่แตกต่างกัน

๖๓. กำหนดให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้ตรวจทานแผนและเนื้อหาที่มีการสื่อสารประชาสัมพันธ์ภายใต้ระบบการจัดการไม่ว่าการสื่อสารดังกล่าวจะถูกมอบหมายให้เจ้าหน้าที่คนใดก็ตาม

๖๔. จัดให้มีการสื่อสารไปยังหน่วยงานภายนอกที่เกี่ยวข้อง อาทิ ผู้รับจ้างภายนอก หรือบุคคลที่ต้องเข้าพื้นที่ศูนย์คอมพิวเตอร์

แผนการสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ ประจำปี 2569

ช่องทาง	รายละเอียด
ปิดประกาศทั้งสื่อสิ่งพิมพ์และอิเล็กทรอนิกส์ (เว็บไซต์)	มุ่งเน้นการสื่อสารภัยคุกคามในมุมของผู้ใช้งานระบบและสร้างความตระหนักรู้ภัยคุกคามที่เป็นแนวโน้มทางสังคม อาทิ CALL CENTER, RANSOMEWARE กลุ่มเป้าหมาย: บุคคลทั่วไป ผู้ใช้งาน ความถี่: ปิดประกาศ 6 เดือน
ส่ง EMAIL เพื่อแจ้งหรือทำหนังสือเวียน	มุ่งเน้นการสื่อสารถึงการเปลี่ยนแปลงแก้ไขในระบบการจัดการที่มีนัยสำคัญต่อหน่วยงานอื่น ๆ ภายในมหาวิทยาลัยและคณะแพทยศาสตร์ อาทิ การได้รับการรับรองมาตรฐานสากล กลุ่มเป้าหมาย: หน่วยงานภายใน ความถี่: ปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
ส่งหนังสือราชการ	มุ่งเน้นการสื่อสารถึงหน่วยงานกำกับดูแล หน่วยงานราชการ หรือหน่วยงานหรือบุคคลภายนอกที่ร้องขอข้อมูลราชการของคณะแพทยศาสตร์ กลุ่มเป้าหมาย: ผู้ร้องขอข้อมูลข่าวสารราชการ ความถี่: เมื่อมีการร้องขอ
การเปลี่ยนแปลงที่สำคัญและส่งกระทบต่อระบบ (MAJOR CHANGE	มุ่งเน้นการสื่อสารเพื่อรับทราบและเตรียมความพร้อมในการเปลี่ยนแปลงที่สำคัญและอาจมีผลกระทบต่อผู้ใช้งานระบบสารสนเทศหรือบริการของคณะแพทยศาสตร์ที่สำคัญ กลุ่มเป้าหมาย: ผู้ใช้งานระบบสารสนเทศ ความถี่: เมื่อมีการเปลี่ยนแปลงที่สำคัญ

การจัดการระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ

๖๕. ระบบการจัดการต้องดำเนินอย่างต่อเนื่องเป็นรอบในทุก ๆ ปี โดยคณะแพทยศาสตร์ต้องจัดให้มีแผนงานที่กำหนดช่วงเวลาของการดำเนินกิจกรรมสำคัญในระบบการจัดการ

๖๖. การจัดทำแผนการดำเนินงานระบบการจัดการ ต้องพิจารณาให้เกิดการบูรณาการร่วมกับแผนการดำเนินงานของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์

๖๗. ผลการดำเนินกิจกรรมในระบบการจัดการต้องได้รับการบันทึกอย่างเป็นลายลักษณ์อักษร อย่างน้อย 1) ขอบเขตของระบบการจัดการ 2) รายงานผลการประเมินความเสี่ยง 3) รายงานผลการบริหารความเสี่ยง

๖๘. เมื่อมีการเปลี่ยนแปลงที่สำคัญในระบบการจัดการ ต้องเข้าที่ประชุมคณะกรรมการ ตามกระบวนการเปลี่ยนแปลง (change management) เพื่อให้ที่ประชุมพิจารณาถึงการเปลี่ยนแปลงที่เกิดขึ้นและอนุมัติ

แผนการดำเนินงานระบบการจัดการ ประจำปี 2569

กิจกรรม (ตามปีงบประมาณ)	ช่วงเวลาดำเนินงาน
ทบทวนและวิเคราะห์บริบทหน่วยงาน	Q1
ประเมินความเสี่ยงรอบที่ 1	Q1
ทบทวนและกำหนดตัวชี้วัด	Q1
สร้างความตระหนักรู้	Q1
จัดทำแผนการจัดการความเสี่ยง	Q2
ดำเนินการจัดทำมาตรการ	Q2
ประเมินความเสี่ยงคงเหลือรอบที่ 1 และประเมินความเสี่ยงรอบที่ 2	Q3
จัดทำแผนการจัดการความเสี่ยง	Q3
ดำเนินการจัดทำมาตรการ	Q3
วัดวิเคราะห์ผลประสิทธิภาพระบบการจัดการ	Q4
ตรวจสอบภายในระบบการจัดการ	Q4
ดำเนินการแก้ไขความไม่สอดคล้อง	Q4
รายงานฝ่ายบริหาร	Q4
ตรวจติดตาม / รับรองจาก CB (Certify Body)	Q4

การวัดประเมิน วิเคราะห์ ตัวชี้วัดประสิทธิภาพ

๖๙. ตัวชี้วัดที่ถูกกำหนดไว้ใน รายการตัวชี้วัด ต้องได้รับการประเมินและวัดผล และรายงาน

๗๐. ผลการวัดประเมิน วิเคราะห์ ตัวชี้วัดประสิทธิภาพต้องสื่อสารให้ผู้มีส่วนได้ส่วนเสียกับตัวชี้วัดในแต่ละรายการ

๗๑. ผลการวัดประเมินต้องเปรียบเทียบได้ (comparable) หมายถึงควรวัดประเมินด้วยวิธีปริมาณที่น่าเชื่อถือและสามารถเทียบเคียงกับผลการวัดประเมินที่ผ่านมา

๗๒. ผู้รับผิดชอบต่อการวัดและวิเคราะห์ผลในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือ คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

การตรวจสอบภายใน

๗๓. ระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตรวจสอบตามข้อกำหนดของมาตรฐานสากล ISO/IEC 27001:2022

๗๔. การจัดทำโปรแกรมการตรวจสอบ (audit program) ต้องสอดรับกับปัญหา ปัจจัย ความเสี่ยง และผลการดำเนินงานที่ผ่านมาของระบบบริการจัดการความมั่นคงปลอดภัยสารสนเทศ

๗๕. ภายใต้โปรแกรมการตรวจสอบต้องประกอบด้วยแผนการตรวจสอบภายในอย่างน้อย 1 ครั้งต่อปี

๗๖. ผู้ตรวจสอบภายในต้องมีคุณสมบัติอย่างเหมาะสม

๗๗. เกณฑ์การตรวจสอบสามารถมีมากกว่า 1 เกณฑ์ต่อการตรวจสอบได้ แต่อย่างน้อยต้องประกอบด้วย เกณฑ์ตามข้อกำหนดของมาตรฐานสากล ISO/IEC 27001:2022

๗๘. ผลการตรวจสอบ (finding) ประกอบไปด้วย 1) ความไม่สอดคล้อง 2) โอกาสในการพัฒนาปรับปรุง และ 3) ข้อสังเกต

๗๙. ขอบเขตการตรวจสอบต้องครอบคลุมการปฏิบัติงานของฝ่ายเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

๘๐. กระดาษทำการผู้ตรวจสอบหรือรายการตรวจสอบ (audit checklist) จะมีหรือไม่ขึ้นอยู่กับผู้ตรวจสอบ เว้นแต่มาตรฐานที่ใช้ในการอ้างอิงการตรวจสอบกำหนดให้ผู้ตรวจสอบต้องมีการจัดทำกระดาษทำการหรือรายการตรวจสอบไว้เป็นสำคัญ

๘๑. รายงานผลการตรวจสอบต้องได้รับการสื่อสารและผู้ที่เกี่ยวข้องในความไม่สอดคล้องต้องดำเนินการแก้ไขความไม่สอดคล้องโดยพิจารณามาตรฐานระยะเวลา ดังนี้

๘๑.๑ ความไม่สอดคล้อง ต้องได้รับการแก้ไข (correction) ในระยะเวลา 30 วันทำการ เว้นแต่มีการแสดงถึงเหตุผลเชิงประจักษ์ถึงข้อจำกัดในการแก้ไข และต้องมีการแก้ไขต่อสาเหตุที่แท้จริง (root cause/corrective action) ภายในระยะเวลา 60 วันทำการ เว้นแต่มีการแสดงถึงเหตุผลเชิงประจักษ์ถึงข้อจำกัดในการแก้ไข

๘๒. รายงานผลการตรวจสอบต้องได้รายงานถึงคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

การตรวจสอบจากฝ่ายบริหาร

๘๓. กำหนดให้คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศต้องประชุมเพื่อติดตามการปฏิบัติงานของคณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยมีวาระการประชุม อย่างน้อยประกอบด้วย

๘๓.๑ ผลการประชุมที่ผ่านมา การติดตามเรื่องคงค้างที่ได้มอบหมายไว้

๘๓.๒ ผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและผลการจัดการ

๘๓.๓ ผลการตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๘๓.๔ ปัญหาและอุปสรรคในการดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๘๓.๕ การเปลี่ยนแปลงทางบริบท ปัจจัยภายใน ปัจจัยภายนอก ความคาดหวังและความต้องการของผู้มีส่วนได้ส่วนเสีย และการเปลี่ยนแปลงที่สำคัญของระบบบริหารจัดการความมั่นคงปลอดภัยสาราสนเทศ

๘๓.๖ ผลตอบรับหรือการแสดงความคิดเห็นจากผู้มีส่วนได้ส่วนเสียของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๘๓.๗ ตัวชี้วัดประสิทธิภาพและความสำเร็จตามเป้าหมายของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๘๓.๘ โอกาสในการพัฒนาปรับปรุง

๘๔. ทั้งนี้คณะกรรมการบริหารฯ ควรพิจารณามอบข้อเสนอแนะหรือโอกาสในการพัฒนาปรับปรุงพร้อมตัดสินใจในประเด็นสำคัญที่เกี่ยวข้องกับประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๘๕. รายงานประชุมต้องจัดทำขึ้นอย่างเป็นลายลักษณ์อักษร และสื่อสารประชาสัมพันธ์ถึงผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องตามความเหมาะสมและความจำเป็น

๘๖. คณะกรรมการบริหารฯ อาจมอบหมายตัวแทนให้เข้าร่วมประชุม และการประชุมจะดำเนินการได้เมื่อองค์ประชุมครบถ้วนไม่น้อยกว่าสองในสามขององค์ประชุม

๘๗. คณะกรรมการบริหารฯ อาจเรียนเชิญผู้เชี่ยวชาญหรือบุคลากรจากหน่วยงานภายนอกเข้าร่วมประชุมเพื่อรับฟังและให้ข้อคิดเห็นเกี่ยวกับวาระการประชุมใด ๆ ก็ได้

การแก้ไขความไม่สอดคล้อง

๘๘. เมื่อมีความไม่สอดคล้องหรือตรวจพบปัญหาหรือข้อบกพร่องใด ๆ ทั้งในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรือการใช้มาตรการด้านความมั่นคงปลอดภัยสารสนเทศ เจ้าหน้าที่สามารถดำเนินการแก้ไขความไม่สอดคล้องหรือแจ้งแก่คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อดำเนินการแก้ไข

๘๙. การแก้ไขความไม่สอดคล้องต้องถูกบันทึกอย่างเป็นลายลักอักษร โดยประกอบไปด้วย

- ๘๙.๑ ผู้แจ้งปัญหาหรือประเด็น ในกรณีความไม่สอดคล้องเกิดจากผลการตรวจสอบภายใน ให้หมายถึงหัวหน้าคณะผู้ตรวจสอบภายใน
- ๘๙.๒ ปัญหาหรือความไม่สอดคล้องที่พบ กรณีที่เป็นความไม่สอดคล้องจากผลการตรวจสอบภายใน ต้องอ้างอิงถึงข้อกำหนดตามเกณฑ์การตรวจสอบ
- ๘๙.๓ สาเหตุหรือต้นเหตุแห่งปัญหาหรือประเด็นความไม่สอดคล้อง
- ๘๙.๔ การแก้ไขเฉพาะหน้า (correction) และการแก้ไขที่สาเหตุ (corrective action)
- ๘๙.๕ ผู้ที่ได้รับมอบหมายให้ดำเนินการแก้ไข

๙๐. การแก้ไขใด ๆ ต้องควรพิจารณาระบุกำหนดการแล้วเสร็จให้สอดคล้องกับความเสี่ยงหรือความเร่งด่วนของปัญหา

๙๑. กรณีที่ประเด็นปัญหาไม่สามารถดำเนินการแก้ไขได้ทันที ให้พิจารณาจัดเป็นประเด็นปัญหา (problem/known error) ที่ต้องได้รับการสื่อสารถึงผู้มีส่วนได้ส่วนเสียถึงข้อจำกัดหรือสาเหตุที่ไม่สามารถดำเนินการแก้ไขได้ และให้ประชาสัมพันธ์ในกลุ่มบุคคลที่เกี่ยวข้องและพึงรับทราบเพื่อให้เกิดความตระหนักรู้

การพัฒนาปรับปรุงอย่างต่อเนื่อง

๙๒. กำหนดให้มีแผนการพัฒนาปรับปรุงที่ผ่านการนำเสนอถึงฝ่ายบริหารขององค์กรหรือคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ ในกรณีที่แผนงานดังกล่าวต้องมีการจัดสรรงบประมาณการลงทุนที่เกี่ยวข้องกับการพัฒนาปรับปรุงอย่างต่อเนื่องของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สามารถพิจารณาให้คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศพิจารณาก่อนจะนำส่งไปยังหน่วยงานในระดับคณะแพทยศาสตร์หรือมหาวิทยาลัยในการพิจารณากลั่นกรองตามลำดับขั้น

๙๓. ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตรวจจากหน่วยงานภายนอกหรือหน่วยงานตรวจรับรองมาตรฐาน (certify body) อย่างน้อย 1 ครั้งต่อปี

แนวปฏิบัติเชิงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ประจำปี 2569

๙๔. แนวปฏิบัตินี้จัดทำเพื่อสร้างความชัดเจนในนโยบายด้านความมั่นคงปลอดภัยของฝ่ายเทคโนโลยีสารสนเทศที่สอดรับกับนโยบายในระดับมหาวิทยาลัย

๙๕. ถ้าไม่ได้กำหนดไว้เป็นการเฉพาะในการดำเนินกิจกรรมใดตามแนวปฏิบัติ ให้ถือว่าเป็นหน้าที่ของผู้ดูแลระบบที่ได้รับมอบหมาย หากไม่มีการกำหนดไว้ให้หมายถึงคณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเป็นผู้รับผิดชอบ แต่ให้ยกเว้นถึงบทบาทที่เกี่ยวข้องกับการตรวจสอบ และความในส่วนที่ 0 แนวปฏิบัติที่ดีของผู้ใช้งานทั่วไป

๙๖. แนวปฏิบัติที่เกี่ยวข้องกับการตรวจสอบ หากไม่ได้กำหนดผู้รับผิดชอบไว้เฉพาะให้หมายถึงคณะผู้ตรวจสอบภายในเป็นผู้รับผิดชอบ

ส่วนที่ 0: แนวปฏิบัติที่ดีของผู้ใช้งานทั่วไป

๙๗. ผู้ดูแลระบบ (administrator) ต้องมีแนวปฏิบัติที่ไม่ต่ำกว่าที่บังคับใช้กับผู้ใช้งานทั่วไป

๙๘. การควบคุมการเข้าถึงระบบคอมพิวเตอร์ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๙๘.๑ ผู้ใช้บริการต้องปฏิบัติตามกฎหมายและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่บังคับใช้ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ปัจจุบันใช้ฉบับแก้ไขเพิ่มเติม พ.ศ. 2560), ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), ระเบียบและประกาศของมหาวิทยาลัยสงขลานครินทร์ และคู่มือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ของคณะแพทยศาสตร์

ทั้งนี้ หน่วยงานอาจอ้างอิงมาตรฐานการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล (HAIT/HAIT Plus) ของสถาบันรับรองคุณภาพสถานพยาบาล (สรพ.) ร่วมกับสมาคมเวชสารสนเทศไทย (TMI) เป็นแนวทางเสริมในบริบทคุณภาพโรงพยาบาลตามความเหมาะสม

กรณีเกิดความขัดแย้งหรือความไม่สอดคล้องระหว่างเอกสาร ให้ถือปฏิบัติตามเอกสารที่มีข้อกำหนดเข้มงวดกว่า หรือเป็นปัจจุบันที่สุดเป็นสำคัญ เว้นแต่จะมีประกาศเป็นลายลักษณ์อักษรจากผู้มีอำนาจให้ปฏิบัติเป็นอย่างอื่นเท่านั้นผู้ใช้บริการต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้บริการและรหัสผ่านของตน ในการเข้า ใช้งาน ระบบคอมพิวเตอร์ของหน่วยงานร่วมกัน

๙๘.๒ ผู้ใช้บริการตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้อง ใส่รหัสผ่านการใช้งานบัญชี

๙๙. ผู้ใช้บริการต้องเก็บรักษารหัสผ่าน โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่ เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบ และไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบ คอมพิวเตอร์โดยไม่ป้องกันการเข้าถึง ผู้ใช้บริการจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการของตนเองและทำการลง บันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๑๐๐. ผู้ใช้บริการควรกำหนดรหัสผ่าน ดังนี้

๑๐๐.๑ รหัสผ่าน ควรมีความยาวไม่น้อยกว่า 6 ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษร ที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ตัวอักขระพิเศษและสัญลักษณ์ต่าง ๆด้วย

๑๐๐.๒ ไม่ควรกำหนดรหัสผ่าน จากชื่อ หรือชื่อสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือหมายเลขโทรศัพท์

๑๐๐.๓ ควรทำการเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานอย่างน้อยทุก 6 เดือน หรือเปลี่ยนรหัสผ่าน ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

ส่วนที่ 0.1: การใช้เครื่องคอมพิวเตอร์ส่วนบุคคล

๑๐๑. เครื่องคอมพิวเตอร์ที่คณะแพทยศาสตร์ อนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของคณะแพทยศาสตร์ ดังนั้นผู้ใช้จึง ควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของคณะแพทยศาสตร์

๑๐๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของคณะแพทยศาสตร์ เป็นโปรแกรมที่คณะแพทยศาสตร์ได้ซื้อ ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบน เครื่องคอมพิวเตอร์ส่วนตัว แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๐๓. ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๑๐๔. ไม่ควรเก็บข้อมูลสำคัญของคณะแพทยศาสตร์ไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้งานอยู่

๑๐๕. ผู้ใช้งานควรบันทึกข้อมูลต่าง ๆ ไว้ที่ Drive อื่น ๆ ยกเว้น Drive C และหน้า Desktop

๑๐๖. ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของคณะแพทยศาสตร์

๑๐๗. ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยควรปฏิบัติดังนี้

๑๐๗.๑ ไม่ควรนำอาหารหรือเครื่องดื่มวางใกล้บริเวณเครื่องคอมพิวเตอร์

๑๐๗.๒ ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk

๑๐๘. ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๑๐๙. ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver)โดยตั้งเวลาประมาณ 10 นาทีเพื่อให้ ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๑๑๐. ผู้ใช้ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตนในการเข้า ใช้เครื่องคอมพิวเตอร์ร่วมกัน

๑๑๑. ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อค หน้าจอด้วยโปรแกรม Screen Saver

ส่วนที่ 0.2: แนวทางการป้องกันโปรแกรมไม่พึงประสงค์ (Malware)

๑๑๒. ผู้ใช้มีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability)ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๑๑๓. ผู้ใช้มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus)ให้กับเครื่องคอมพิวเตอร์

๑๑๔. ผู้ใช้ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่น ๆ ก่อนนำ มาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๑๑๕. ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๑๑๖. ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ 0.3: การใช้ทรัพย์สินขององค์กร

๑๑๗. เครื่องคอมพิวเตอร์แบบพกพาที่คณะแพทยศาสตร์อนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของคณะแพทยศาสตร์ ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของคณะแพทยศาสตร์

๑๑๘. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของคณะแพทยศาสตร์ เป็นโปรแกรมที่ คณะแพทยศาสตร์ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไป ติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๑๙. การตั้งชื่อเครื่องคอมพิวเตอร์ (computer name)แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่กลุ่มงาน เทคโนโลยีสารสนเทศเท่านั้น

๑๒๐. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มงาน เทคโนโลยีสารสนเทศเท่านั้น

๑๒๑. ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมี ประสิทธิภาพ

๑๒๒. ไม่ดัดแปลงแก้ไข ส่วนประกอบต่าง ๆของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๑๒๓. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์ แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๑๒๔. ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจ จากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

๑๒๕. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิด เครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๒๖. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำ ให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๒๗. ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

๑๒๘. การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้าย เครื่องโดยการดึงหน้าจอภาพขึ้น

๑๒๙. ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

๑๓๐. ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ เครื่องดื่มต่าง ๆ เป็นต้น

๑๓๑. ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

๑๓๒. ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๑๓๓. ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

๑๓๔. การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้าม เช็ดแบบหมุนวน เพราะจะทำให้หน้าจอข่วนได้

๑๓๕. ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่อง ทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๓๖. ผู้ใช้ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๑๓๗. ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

ส่วนที่ 0.4: การใช้งานเครื่องคอมพิวเตอร์ลูกข่ายระบบสารสนเทศโรงพยาบาล

๑๓๘. เครื่องคอมพิวเตอร์ลูกข่ายฯ ที่ให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของคณะแพทยศาสตร์ ดังนั้นผู้ใช้จึง ควรใช้งานเครื่องคอมพิวเตอร์ลูกข่ายฯ อย่างมีประสิทธิภาพเพื่องานของโรงพยาบาลสงขลานครินทร์ คณะแพทยศาสตร์

๑๓๙. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ลูกข่ายฯ เป็นโปรแกรมที่คณะแพทยศาสตร์ได้ซื้อ ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบน เครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๔๐. ห้ามผู้ใช้งานทำการแก้ไข ปรับเปลี่ยน ทั้งอุปกรณ์บนเครื่องลูกข่าย รวมถึงระบบปฏิบัติการ และการตั้งค่าต่าง ๆ ของเครื่องลูกข่าย

๑๔๑. ห้ามการใช้งานสื่อบันทึกพกพาต่าง ๆ กับเครื่องลูกข่ายโรงพยาบาลสงขลานครินทร์

๑๔๒. ห้ามผู้ใช้งานนำอุปกรณ์ต่อพ่วงอื่น ๆ มาใช้กับเครื่องลูกข่ายฯ โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ

๑๔๓. ไม่ควรเก็บข้อมูลใด ๆ ไว้บนเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งานอยู่

๑๔๔. ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังโปรแกรมอื่น ๆ โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ

๑๔๕. ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ลูกข่ายโดยควรปฏิบัติดังนี้

๑๔๖. ไม่ควรนำอาหารหรือเครื่องดื่มวางใกล้บริเวณเครื่องคอมพิวเตอร์

๑๔๗. ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk

๑๔๘. ตั้งค่า Screen Saver เพื่อป้องกันการเข้าถึงเมื่อไม่อยู่ที่ตัวเครื่อง เกิน 10 นาที ขึ้นไป เว้นแต่ไม่สามารถดำเนินการได้ตามเหตุผลทางการแพทย์

ส่วนที่ 0.5: การใช้งาน Internet ขององค์กร

๑๔๙. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่อ อินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการ อุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

๑๕๐. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning)โดย โปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๑๕๑. ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของคณะแพทยศาสตร์เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการ เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อ ชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๑๕๒. ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของ เครือข่ายและความปลอดภัยทางข้อมูลของคณะแพทยศาสตร์

๑๕๓. ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือ ข้อมูลที่ละเมิดสิทธิ์

ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับคณะแพทยศาสตร์

๑๕๔. ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของคณะแพทยศาสตร์ ที่ยังไม่ได้ประกาศอย่างเป็น ทางการผ่านอินเทอร์เน็ต

๑๕๕. ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับ ความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๑๕๖. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและซึ่งต้องเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๕๗. ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้งาน

๑๕๘. ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขายต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๑๕๙. การใช้งานเว็บบอร์ด (Web Board)ของคณะแพทยศาสตร์ ผู้ใช้ต้องใช้ข้อความที่สุภาพ และต้องไม่ เปิดเผยข้อมูลที่สำคัญและเป็นความลับของคณะแพทยศาสตร์

๑๖๐. ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียง ของคณะแพทยศาสตร์ หรือเป็นการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

๑๖๑. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ส่วนที่ 0.6: การใช้งานจดหมายอิเล็กทรอนิกส์(E-mail) ขององค์กร

๑๖๒. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของคณะแพทยศาสตร์ให้เหมาะสมกับ การเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้า ใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

๑๖๓. ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของคณะแพทยศาสตร์

๑๖๔. สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password)ในการผ่านเข้าระบบจดหมาย อิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดย ทันที

๑๖๕. การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “การบริหาร จัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๑๖๖. รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดง ออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

๑๖๗. ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง

๑๖๘. ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการ Logout ออกจากหน้าจอตัดการ ใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้เช่น 10 นาที เมื่อต้องการเข้าใช้ งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๑๖๙. ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบ จดหมายอิเล็กทรอนิกส์

๑๗๐. ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน

๑๗๑. ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อคณะแพทยศาสตร์หรือ ละเมิดลิขสิทธิ์สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ ผ่านระบบเครือข่ายของคณะแพทยศาสตร์

๑๗๒. ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมาย

อิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑๗๓. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของคณะแพทยศาสตร์ เพื่อการทำงานของคณะแพทยศาสตร์เท่านั้น

๑๗๔. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๑๗๕. ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการ ตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

๑๗๖. ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์ ข้อความ ที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๗๗. ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้ เสียชื่อเสียงของคณะแพทยศาสตร์ ทำให้เกิดความแตกแยกระหว่างคณะแพทยศาสตร์ผ่านทางจดหมาย อิเล็กทรอนิกส์

๑๗๘. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมาย อิเล็กทรอนิกส์

๑๗๙. ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและ จดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๘๐. ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบ จดหมายอิเล็กทรอนิกส์

๑๘๑. ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่อง คอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ส่วนที่ 1: การรักษาความมั่นคงปลอดภัยด้านกายภาพและสิ่งแวดล้อม

๑๘๒. ภายในคณะแพทยศาสตร์ จำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่าง เหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๑๘๓. ตรวจดูแลความสะอาด ความเรียบร้อย ในพื้นที่ฝ่ายเทคโนโลยีสารสนเทศ ตลอดจนสำนักงาน ไม่จัดเก็บเอกสารสำคัญไว้บนโต๊ะทำงานของเจ้าหน้าที่หรือในสถานที่ที่สามารถเข้าถึงได้โดยง่ายและปราศจากมาตรการป้องกัน

๑๘๔. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการ กำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงาน ของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่าย ไร้สาย (Wireless LAN coverage area) เป็นต้น โดยสามารถใช้สัญลักษณ์สีดังนี้

๑๘๔.๑ สีแดง: หมายถึงบริเวณเขตจำกัดสูงสุด ต้องใช้การยืนยันตัวตนด้วย Biometric หรือ PIN คู่กับบัตรพนักงานเท่านั้น หน่วยงานภายนอกที่ทำงานในเขตพื้นที่สีแดงต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศอยู่ด้วยตลอดเวลา มาตรการความปลอดภัยที่ใช้ในเขตพื้นที่นี้ต้องอยู่ภายใต้การกำกับดูแลของฝ่ายเทคโนโลยีสารสนเทศ

๑๘๔.๒ สีเหลือง: หมายถึงบริเวณสำนักงานเฉพาะผู้มีบัตรพนักงานหรือหน่วยงานภายนอกที่มีผู้พาเข้าพื้นที่เท่านั้น

๑๘๔.๓ สีเขียว: หมายถึงเขตทั่วไปบุคลลาภายนอกสามารถผ่านเข้าออกได้ โดยใช้มาตรการของฝ่ายอาคารสถานที่ในการกำกับดูแล

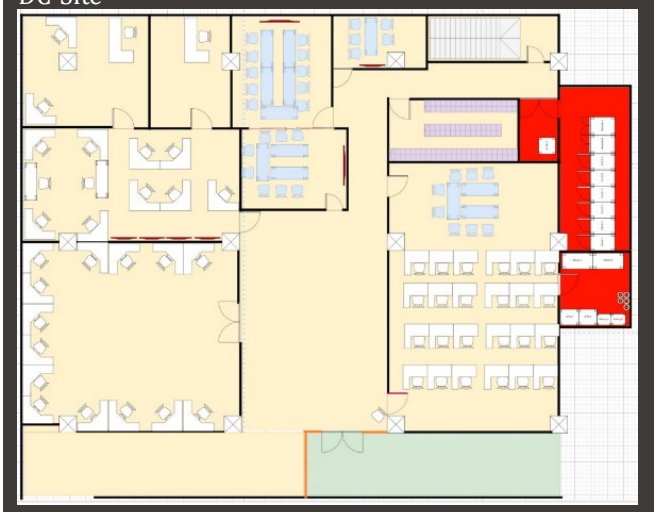
QR Code เพื่อขอเข้าพื้นที่ฝ่ายเทคโนโลยีสารสนเทศ

DC

DR

ผังพื้นที่ฝ่ายเทคโนโลยีสารสนเทศและการกำหนดบริเวณ

DC-Site



DR-Site

๑๘๕. กำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยี สารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน

๑๘๖. จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” ในส่วนที่สำคัญ ได้แก่ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์เป็นต้น เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑๘๗. ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออก ดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่” หรืออยู่ในรูปแบบอิเล็กทรอนิกส์ก็ได้

๑๘๘. หากมีบุคคลอื่นที่ไม่ใช่ผู้ใช้ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้าหน่วยงานเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่ องค์กรออกให้โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการเข้าออกไว้เป็นหลักฐานทั้งใน กรณี ที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๑๘๙. ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลา ที่อยู่ในคณะแพทยศาสตร์

๑๙๐. จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ เป็นประจำทุกสัปดาห์ และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศ และการสื่อสารอย่างน้อยปีละ 1 ครั้ง

๑๙๑. ระบบบันทึกภาพวงจรปิดต้องได้รับการติดตั้งในตำแหน่งทางเข้าออกสำคัญและภายในฝ่ายเทคโนโลยีสารสนเทศ ติดตั้งระบบตรวจสอบควันไฟ ระบบดับเพลิงอัตโนมัติ และตัวตรวจจับการรั่วไหลของน้ำ

๑๙๒. ห้ามมิให้นำอาวุธอันตราย วัตถุไวไฟที่จะสามารถเกิดการระเบิดหรือก่อให้เกิดประกายไฟ เข้าฝ่ายเทคโนโลยีสารสนเทศโดยเด็ดขาด

๑๙๓. จัดเก็บอุปกรณ์และวัตถุไวไฟให้เป็นระเบียบ ไม่วางสิ่งกีดขวางทางเข้าออกฉุกเฉิน

๑๙๔. ควบคุมความชื้นและอุณหภูมิที่เหมาะสมภายในฝ่ายเทคโนโลยีสารสนเทศ โดยเฉพาะอย่างยิ่งบริเวณตู้ rack ที่จัดเก็บอุปกรณ์สำคัญ โดยกำหนดค่ามาตรฐานอย่างเหมาะสม

๑๙๕. บริเวณสำนักงานจัดเก็บเอกสารสำคัญในตู้ล็อคได้ ไม่จัดวางเอกสารสำคัญทิ้งไว้บนโต๊ะทำงาน และตั้งค่ามาตรฐานของเวลา screen saver/lock

๑๙๖. จัดวางอุปกรณ์อย่างเหมาะสมโดยเฉพาะอุปกรณ์ที่ต้องใช้ในกรณีฉุกเฉิน เช่น ถังดับเพลิง ไฟฉุกเฉิน

๑๙๗. เมื่อเกิดอุบัติเหตุในสถานที่ทำงาน ต้องมีการจัดบันทึกเหตุอุบัติเหตุดังกล่าวและเก็บรวบรวมหลักฐานหรือเอกสารที่จำเป็น เพื่อแสดงถึงความปลอดภัยในสถานประกอบการ

๑๙๘. การใช้งานอุปกรณ์นอกสถานที่ต้องคำนึงถึงความมั่นคงปลอดภัยและเมื่อเกิดการสูญหายต้องเร่งดำเนินการแจ้งแก่เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ และดำเนินการตามขั้นตอนทางกฎหมายที่สำคัญ อาทิ การแจ้งความ

๑๙๙. ไม่อนุญาตให้ใช้สื่อบันทึกข้อมูลส่วนตนในอุปกรณ์และเครื่องคอมพิวเตอร์ที่มีการเชื่อมต่อโดยตรงเข้ากับเครือข่ายของฝ่ายเทคโนโลยีสารสนเทศ เว้นแต่ได้รับอนุญาต ให้หมายรวมถึงอุปกรณ์เคลื่อนที่ทุกชนิดที่สามารถใช้งานเป็นสื่อบันทึกข้อมูลได้ อาทิ โทรศัพท์สมาร์ทโฟน

๒๐๐. เอกสารการตรวจสอบระบบสาธารณูปโภคจากผู้มีส่วนได้ส่วนเสียเช่น ฝ่ายอาคารสถานที่ ต้องรายงานถึงฝ่ายเทคโนโลยีสารสนเทศ รวมถึงการรายงานปัญหาหรือเหตุขัดข้องที่จะส่งผลกระทบต่อฝ่ายเทคโนโลยีสารสนเทศด้วย

๒๐๑. สายไฟฟ้า สายสัญญาณ ต้องจัดวางและเดินสายอย่างปลอดภัยเมื่อเป็นไปได้ให้แยกสายไฟฟ้าและสายสัญญาณเพื่อป้องกันการรบกวนจากสนามแม่เหล็กไฟฟ้า และจัดให้มีการทำแผนผังสายสัญญาณและการติดป้ายแสดงเส้นทางการเดินสายสัญญาณที่สำคัญ เลือกใช้ประเภทและชนิดของสายสัญญาณที่เหมาะสมต่อระยะทางและการใช้งาน สายสัญญาณอุปกรณ์ฉุกเฉินด้านความปลอดภัยต้องพิจารณาป้องกันเป็นพิเศษ

๒๐๒. อุปกรณ์ฉุกเฉินและความปลอดภัยต้องปิดป้ายแสดงผลการบำรุงรักษาและเวลาล่าสุด

๒๐๓. อุปกรณ์เทคโนโลยีสารสนเทศสำคัญต้องจัดเก็บรายงานผลการบำรุงรักษา ไม่ว่าจะดำเนินการโดยหน่วยงานภายในหรือผู้ให้บริการภายนอกก็ตาม เมื่อพบว่ามีปัญหาหรือจุดอ่อน ต้องจัดให้มีการเฝ้าระวังหรือดำเนินการแก้ไข

๒๐๔. การทำลายอุปกรณ์และสื่อบันทึกข้อมูลต้องใช้วิธีที่ปลอดภัยเหมาะสม อาทิ การใช้เครื่องทำลาย และการนำอุปกรณ์หรือเครื่องคอมพิวเตอร์กลับมาใช้ใหม่ต้องดำเนินการลบข้อมูลสารสนเทศด้วยวิธีที่ปลอดภัย (secure erase)

๒๐๕. ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอก พื้นที่ของคณะแพทยศาสตร์ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บ อยู่ในสื่อบันทึกก่อน เป็นต้น

๒๐๖. การเฝ้าระวังความปลอดภัยเชิงกายอย่างต่อเนื่อง เมื่อเป็นไปได้ให้มีการใช้มาตรการด้านความปลอดภัยเชิงกายภาพที่สามารถแจ้งเตือนหรือเฝ้าระวังได้อย่างต่อเนื่อง

ส่วนที่ 2: การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ เครื่องแม่ข่าย และระบบเครือข่าย

ส่วนที่ 2.1: ข้อกำหนดทั่วไปในการควบคุมการเข้าถึง

๒๐๗. กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึง

อย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้อง ได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒๐๘. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและ ระบบข้อมูลได้

๒๐๙. จัดให้มีการระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการ สื่อสารของคณะแพทยศาสตร์ และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

๒๑๐. จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

ส่วนที่ 2.2: การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒๑๑. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้ใน การขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารการกำหนดสิทธิ์ในการเข้าสู่ระบบและ ต้องมีการจัดเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน

๒๑๒. เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการ ใช้งานเกินอำนาจหน้าที่ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๒๑๓. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการ ใช้งานระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 2.3: การบริหารจัดการการเข้าถึงของผู้ใช้

๒๑๔. การลงทะเบียนเจ้าหน้าที่ใหม่ของศูนย์ปฏิบัติการเครือข่ายควรกำหนดให้มีขั้นตอนอย่างเป็นทางการ เพื่อให้มีสิทธิในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนการปฏิบัติสำหรับการยกเลิกการใช้งาน เช่นเมื่อลาออก หรือเปลี่ยนตำแหน่งงานภายในคณะแพทยศาสตร์

๒๑๕. กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒๑๖. ผู้ใช้ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลาย ลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

๒๑๗. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๒๑๗.๑ ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่ รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้

๒๑๗.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน มีแนวทางปฏิบัติตามที่กำหนดไว้

๒๑๗.๓ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

- ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ
- ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะ กรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

๒๑๘. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๒๑๘.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติใน การควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการ เข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๒๑๘.๒ เจ้าของข้อมูลจะต้องมีการตรวจทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๒๑๘.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและ การเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๒๑๘.๔ ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

ส่วนที่ 2.4: การบริหารจัดการการเข้าถึงระบบเครือข่ายและเครือข่ายไร้สาย

๒๑๙. ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ ได้รับอนุญาตเท่านั้น

๒๒๐. ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของคณะแพทยศาสตร์ จะต้องได้รับการพิจารณาอนุญาตจาก หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

๒๒๑. ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การ เข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒๒๒. ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๒๒๓. ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุม ไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่ง สัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒๒๔. ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไป ภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของ สัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

๒๒๕. ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มา จากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

๒๒๖. ผู้ดูแลระบบ ควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีคาดเดาหรือเจาะรหัสได้โดยง่าย

๒๒๗. ผู้ดูแลระบบจำเป็นต้องกำหนดค่าการเข้ารหัสในระดับ WPA2 หรือที่สูงกว่า สำหรับการสื่อสารระหว่าง Wireless LAN Client และ Access Point เพื่อเพิ่มความยากในการดักจับหรือการโจมตีข้อมูลในเครือข่ายไร้สาย

๒๒๘. ผู้ดูแลระบบจำเป็นต้องประยุกต์ใช้วิธีการควบคุมที่อาศัยการตรวจสอบทั้ง MAC Address และข้อมูลประจำตัวผู้ใช้ ซึ่งประกอบด้วยชื่อผู้ใช้และรหัสผ่าน ในการกำหนดสิทธิ์การเข้าถึงเครือข่ายไร้สาย การเข้าถึงจะถูกอนุญาตเฉพาะสำหรับอุปกรณ์ที่มี MAC Address และข้อมูลประจำตัวผู้ใช้ที่ได้รับการอนุมัติแล้วเท่านั้น

๒๒๙. ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในคณะแพทยศาสตร์

๒๓๐. ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย อย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ 2.5: การควบคุมการเข้าถึงระยะไกล

๒๓๑. การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของคณะแพทยศาสตร์ ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของคณะแพทยศาสตร์ การควบคุมบุคคลที่เข้าสู่ระบบของคณะแพทยศาสตร์จากระยะไกลต้องมีการกำหนดมาตรการการรักษา ความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๒๓๒. วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุมัติจาก หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้อง ปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๒๓๓. ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นใน การดำเนินงานกับคณะแพทยศาสตร์อย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๒๓๔. ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบต้องได้รับการอนุมัติอย่างถูกต้องและ เหมาะสมแล้วเท่านั้น

๒๓๕. การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควร เปิดสิทธิ์ที่อนุญาตให้ใช้ทิ้งเอาไว้โดยไม่จำเป็น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๒๓๖. ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบของคณะแพทยศาสตร์ สำหรับ ในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

๒๓๖.๑ การแสดงตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

๒๓๖.๒ การพิสูจน์ยืนยันตัวตน (Authentication): ขั้นตอนนี้เป็นการตรวจสอบหลักฐานที่สามารถยืนยันว่าผู้ที่เข้าใช้งานเป็นตนเอง หรือ "ผู้ใช้ตัวจริง" ซึ่งอาจจะเป็นการใช้รหัสผ่าน (Password), การใช้สมาร์ทการ์ด, หรือการใช้ USB Token ที่มีความสามารถในการใช้ PKI (Public Key Infrastructure) เป็นต้น นอกจากนี้ยังควรมีการใช้งาน Multi-Factor Authentication (MFA) หรือการยืนยันตัวตนแบบหลายขั้นตอน เพื่อเพิ่มความปลอดภัยในการเข้าถึงระบบ

๒๓๗. การเข้าสู่ระบบสารสนเทศของคณะแพทยศาสตร์นั้นจะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ ตัวตนอย่างน้อย 1 วิธี

๒๓๘. การเข้าสู่ระบบสารสนเทศของคณะแพทยศาสตร์จากอินเทอร์เน็ต ควรมีการตรวจสอบผู้ใช้งานด้วย

๒๓๙. การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ส่วนที่ 2.6: การควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานภายนอก

๒๔๐. หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบ เทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และ กำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสารได้

๒๔๑. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๒๔๒. บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ คณะแพทยศาสตร์จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้ากลุ่มงาน เทคโนโลยีสารสนเทศ

๒๔๓. จัดทำเอกสารแบบฟอร์ม หรือดำเนินการจัดส่งคำขอบริการ (Service Request) ผ่านระบบ Service Desk สำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

๒๔๓.๑ เหตุผลในการขอใช้

๒๔๓.๒ ระยะเวลาในการใช้

๒๔๓.๓ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๒๔๓.๔ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๒๔๔. เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้อง กำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น

๒๔๕. สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของ คณะแพทยศาสตร์ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง 4 ด้าน คือ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) และความปลอดภัย (Safety)

๒๔๖. ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุม

หรือตรวจสอบการ ให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ 3: ความมั่นคงปลอดภัยทางเครือข่าย

๒๔๗. จัดทำแผนผังระบบเครือข่าย (Network Diagram) ประกอบด้วยรายละเอียดเกี่ยวกับ ขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกโดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย การ แบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ การกำหนดเส้นทางบนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒๔๘. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและ การสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒๔๙. กำหนด หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameterต่าง ๆ อย่างน้อยเดือนละ 1 ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้ง บุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๒๕๐. ระบบเครือข่ายทั้งหมดของคณะแพทยศาสตร์ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก คณะแพทยศาสตร์ ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำPacket filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

๒๕๑. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS)เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งาน ระบบเครือข่ายของคณะแพทยศาสตร์ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุก รุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดย บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๒๕๒. การเข้าสู่ระบบงานเครือข่ายภายในคณะแพทยศาสตร์โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication)เพื่อตรวจสอบความถูกต้อง

๒๕๓. IP address ภายในของระบบงานเครือข่ายภายในของคณะแพทยศาสตร์ จำเป็นต้องมีการป้องกันมิให้ หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการ สื่อสารได้โดยง่าย

๒๕๔. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแล ระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒๕๕. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ห้องศูนย์ปฏิบัติการ เครือข่ายเท่านั้น

๒๕๖. ระบบเครือข่ายไร้สายต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือไร้สายอย่างสม่ำเสมอ

๒๕๗. กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้อง เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่คณะแพทยศาสตร์จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS/IDS เป็นต้น ห้ามทำการเชื่อมต่อระบบคอมพิวเตอร์ของคณะแพทยศาสตร์ ผ่านช่องทางอื่น เช่น Mobile Hotspot จากโทรศัพท์มือถือ หรืออุปกรณ์ Pocket Wi-Fi ส่วนตัว ยกเว้น ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษร หรือผ่านระบบอนุมัติอิเล็กทรอนิกส์ที่เชื่อถือได้

๒๕๘. กำหนดให้มีแหล่งข้อมูลที่น่าเชื่อถือในการรับข่าวสารด้านภัยคุกคามเชิงรุก (Threat Intelligence) เพื่อใช้ในการติดตามและรับมือต่อภัยคุกคามไซเบอร์ที่เกี่ยวข้องในบริบทของระบบสารสนเทศ เครื่องแม่ข่าย และระบบเครือข่ายที่สำคัญ

ส่วนที่ 4: ความมั่นคงปลอดภัยเครื่องแม่ข่าย

๒๕๙. ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server)ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๒๖๐. ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

๒๖๑. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิด ให้ตรงกับเวลาอ้างอิง

มาตรฐานระดับชาติได้แก่ สถาบันมาตรวิทยาแห่งชาติ, กรมอุทกศาสตร์ กองทัพเรือ, ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย

๒๖๒. ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกัน เพิ่มเติมด้วย

๒๖๓. ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๒๖๔. ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไข หรือบำรุงรักษา

๒๖๕. การติดตั้ง และการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์ปฏิบัติการ เครือข่ายเท่านั้น

ส่วนที่ 5: การจัดเก็บบันทึกของระบบสารสนเทศและเครือข่าย

๒๖๖. ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการ ปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน

๒๖๗. ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๒๖๘. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้ เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ 6: การสำรองข้อมูลสารสนเทศ

๒๖๙. กำหนดเจ้าหน้าที่รับผิดชอบดำเนินการสำรองข้อมูล โดยจัดทำเป็นลายลักษณ์อักษร และให้เจ้าหน้าที่ลงนามรับทราบ

๒๗๐. กำหนดขั้นตอนปฏิบัติและดำเนินการสำรองข้อมูล และการกู้คืนข้อมูล ที่เหมาะสม และ รองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ปัจจุบันใช้ฉบับแก้ไขเพิ่มเติม พ.ศ. 2560) เพื่อให้ระบบอยู่ ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒๗๑. ทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผน เพื่อเตรียมความพร้อมในกรณีฉุกเฉินตามระยะเวลาที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

๒๗๒. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๒๗๓. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจนข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒๗๔. จัดการกับอุปกรณ์สำหรับสำรองข้อมูลให้ปลอดภัยต่อการเข้าถึงโดยไม่ได้รับอนุญาต และสะดวกต่อการนำมาใช้กู้คืนข้อมูล ในกรณีฉุกเฉินเมื่อข้อมูลที่จัดทำไว้เกิดการเสียหาย

ตารางการสำรองข้อมูลสารสนเทศบนระบบงานสำคัญ

ระบบ	ค่า RPO (Recovery Point Objective)	รอบการ Backup (Offline)
HIS	0	1 (Days)
Switch – IMC	7 (Day)	7 (Days)
Load Balance Configuration	7 (Day)	7 (Days)
SMS Gateway	7 (Day)	7 (Days)
FortiGate Firewall	7 (Day)	7 (Days)
Wireless Controller	7 (Day)	7 (Days)

*RPO คือ ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายได้ ถ้ากำหนด RPO 4 ชั่วโมง ต้องทำ Job Backup สำรองข้อมูลไว้ทุก 4 ชั่วโมง หรือน้อยกว่านั้น

ส่วนที่ 7: ความสอดคล้องต่อกฎหมาย

๒๗๕. ระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องสอดคล้องกับกฎหมายที่เกี่ยวข้อง หรือกฎหมายที่มีอิทธิพลต่อประสิทธิภาพของระบบการบริการจัดการความมั่นคง

ปลอดภัยสารสนเทศ นอกจากนี้ระบบการจัดการยังอ้างอิงแนวทาง HA IT Plus (สรพ.) ซึ่งเป็นกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐ และสอดคล้องกับมาตรฐาน HA ฉบับที่ 5/6 ในหมวด IT (คาดว่าจะบังคับใช้ ต.ค. 2569)

๒๗๖. เมื่อมีประเด็นหรือความไม่มั่นใจที่เกี่ยวข้องกับความสอดคล้องของกฎหมายต้อง ให้ผู้ที่เกี่ยวข้องดำเนินการส่งเรื่องถึงนิติกรของคณะแพทยศาสตร์เพื่อการตรวจทานและหาข้อสรุป หรือแนวทางปฏิบัติเพื่อให้เกิดความสอดคล้อง

รายการข้อกำหนดกฎหมายที่เกี่ยวข้อง

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และประกาศที่เกี่ยวข้อง

มาตรา	ฐานความผิด
มาตรา 5	เข้าถึงคอมพิวเตอร์โดยมิชอบ
มาตรา 6	เปิดเผยรหัสเข้าถึงคอมพิวเตอร์บุคคลอื่น
มาตรา 7	เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา 8	ดักเก็บข้อมูลการใช้งานคอมพิวเตอร์
มาตรา 9	แก้ไข/ทำลายข้อมูลคอมพิวเตอร์บุคคลอื่น
มาตรา 10	ขัดขวางการใช้งานคอมพิวเตอร์บุคคลอื่น
มาตรา 11	ส่งสแปมเมล์ไปยังบุคคลอื่น
มาตรา 12	12.1 ทำความผิดตามมาตรา 5 6 7 8 และ 11 ส่งผลต่อความมั่นคง
	12.2 ทำความผิดตามมาตรา 5 6 7 8 และ 11 ส่งผลต่อความมั่นคงและข้อมูลเสียหาย
	12.3 ทำความผิดตามมาตรา 9 หรือ 10 ส่งผลต่อความมั่นคง
	12.4 ทำความผิดตามข้อ 12.1 หรือ 12.3 แล้วมีผู้เสียชีวิต
มาตรา 12/1	12/1.1 ทำความผิดตามมาตรา 9 และ 10 ส่งผลให้เกิดอันตรายต่อบุคคลหรือทรัพย์สิน
	12/1.2 ทำความผิดตามมาตรา 9 และ 10 ส่งผลให้มีผู้เสียชีวิต
มาตรา 13	13. เผยแพร่ชุดคำสั่ง ที่สามารถนำไปใช้กระทำความผิดตามมาตรา 5 - 11
	13.2 เผยแพร่ชุดคำสั่ง ที่สามารถนำไปใช้กระทำความผิดตามมาตรา 12.1 หรือ 123
	13.3 เผยแพร่ชุดคำสั่ง ที่สามารถนำไปใช้กระทำความผิดตามมาตรา 5 - 11 และถูกนำไปใช้ก่อความผิดตามมาตรา 12
	13.4 เผยแพร่ชุดคำสั่ง ที่สามารถนำไปใช้กระทำความผิดตามมาตรา 12.1 หรือ 123 และถูกนำไปใช้ก่อความผิดตามมาตรา 12
มาตรา 14	14.1 เผยแพร่ข้อมูลเท็จประชาชนเสียหาย ที่ไม่ใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา
	14.2 เผยแพร่ข้อมูลเท็จประเทศเสียหาย หรือมีผลต่อความมั่นคง
	14.3 แพร่ข้อมูลเท็จ ตามความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
	14.4 เผยแพร่ข้อมูลลามกอนาจาร
	14.5 เผยแพร่ส่งต่อข้อมูลตามข้อ 14.1 - 14.4
	14.6 เผยแพร่ข้อมูลเท็จบุคคลเสียหาย ที่ไม่ใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา
มาตรา 15	สนับสนุนให้เกิดความผิดตาม มาตรา 14
มาตรา 16	16.1 นำเข้าภาพโปละเมิดบุคคลอื่น
	16.2 นำเข้าภาพผู้ที่เสียชีวิต โปละเมิดบุคคลรอบข้างผู้เสียชีวิต
มาตรา 16/1	16/1.1 ทำความผิดตามมาตรา 14 หรือ 16
	16/1 2 ไม่ทำลายข้อมูลการทำความผิดตามมาตรา 14 หรือ 16
มาตรา 26	ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

พ.ร.บ. ลิขสิทธิ์

มาตรา 31 ผู้ใดรู้อยู่แล้วหรือมีเหตุอันควรรู้ว่างานใดได้ทำขึ้นโดยละเมิดลิขสิทธิ์ของผู้อื่น กระทำอย่างใดอย่างหนึ่งแก่งานนั้นเพื่อหากำไร ให้ถือว่าผู้นั้นกระทำการละเมิดลิขสิทธิ์ ถ้าได้กระทำดังต่อไปนี้ 1) ขาย มีไว้เพื่อขาย เสนอขาย ให้เช่า เสนอให้เช่า ให้เช่าซื้อ หรือเสนอให้เช่าซื้อ 2) เผยแพร่ต่อสาธารณชน 3) แจกจ่ายในลักษณะที่อาจก่อให้เกิดความเสียหายแก่เจ้าของลิขสิทธิ์ 4) นำหรือสั่งเข้ามาในราชอาณาจักร

กฎกระทรวง กำหนดประเภทและระบบความปลอดภัยของอาคารที่ใช้เพื่อประกอบกิจการเป็นสถานบริการ (เฉพาะส่วนที่สำคัญและเกี่ยวข้องกับความปลอดภัยเชิงกายภาพและสิ่งแวดล้อม)

สถานบริการ ในที่นี้ให้มีความหมายครอบคลุมสำนักงานของคณะแพทยศาสตร์ มหาวิทยาลัยสงขลานครินทร์

ข้อ ๘ สถานบริการต้องจัดให้มีการติดตั้งแบบแปลนแผนผังของอาคารซึ่งแสดงตำแหน่งที่ติดตั้งอุปกรณ์ดับเพลิงต่าง ๆ ทางหนีไฟ ทางออก และประตูทางออก โดยแบบแปลนแผนผังดังกล่าวให้ติดไว้ในตำแหน่งที่ชัดเจนอย่างน้อยบริเวณโถงบันไดหรือโถงลิฟต์ทุกแห่งทุกชั้น และบริเวณทางเข้าออกหลักของสถานบริการ

ข้อ ๒๐ สถานบริการหรืออาคารที่ตั้งสถานบริการต้องมีระบบจ่ายพลังงานไฟฟ้าสำรองสำหรับเครื่องหมายแสดงทางฉุกเฉิน ทางเดิน บันได บันไดหนีไฟ ระบบสัญญาณเตือนเพลิงไหม้และไฟส่องสว่างสำหรับทางเดิน ห้องโถง บันได บันไดหนีไฟ และแยกเป็นอิสระจากระบบไฟฟ้าปกติครอบคลุมพื้นที่สถานบริการถึงบันไดหนีไฟ และสามารถทำงานได้โดยอัตโนมัติไม่น้อยกว่าหนึ่งชั่วโมงเมื่อระบบจ่ายพลังงานไฟฟ้าปกติหยุดทำงาน เว้นแต่สถานบริการประเภท ฉ อย่างน้อยต้องจัดให้มีระบบจ่ายพลังงานไฟฟ้าสำรองสำหรับไฟส่องสว่างที่สามารถมองเห็นทางเดินได้ และระบบสัญญาณเตือนเพลิงไหม้ที่แยกเป็นอิสระจากระบบไฟฟ้าปกติครอบคลุมพื้นที่สถานบริการ และสามารถทำงานได้โดยอัตโนมัติไม่น้อยกว่าหนึ่งชั่วโมง เมื่อระบบจ่ายพลังงานไฟฟ้าปกติหยุดทำงาน

ข้อ ๒๒ การเดินสายระบบไฟฟ้า ระบบเสียง และระบบสัญญาณต่าง ๆ ให้เดินในรางหรือท่อร้อยสายไฟซึ่งทำด้วยโลหะ

ข้อ ๒๕ สถานบริการต้องมีระบบสัญญาณเตือนเพลิงไหม้ซึ่งประกอบด้วย

(๑) อุปกรณ์ส่งสัญญาณเพื่อให้หนีไฟที่สามารถส่งสัญญาณเสียงและแสงให้คนที่อยู่ในอาคารได้ยินหรือทราบอย่างทั่วถึง

(๒) อุปกรณ์ตรวจจับอัตโนมัติและอุปกรณ์แจ้งเหตุที่มีทั้งระบบแจ้งเหตุอัตโนมัติและระบบแจ้งเหตุที่ใช้มือเพื่อให้อุปกรณ์ตาม (๑) ทำงาน เว้นแต่สถานบริการประเภท ก และประเภท ฉ ที่อย่างน้อยต้องติดตั้งอุปกรณ์แจ้งเหตุที่ใช้มือ
ในการออกแบบและติดตั้งระบบสัญญาณเตือนภัยในวรรคหนึ่งให้เป็นไปตามมาตรฐานว่าด้วยระบบแจ้งเหตุเพลิงไหม้ของกรมโยธาธิการและผังเมือง หรือมาตรฐานอื่นที่คณะกรรมการควบคุมอาคารให้การรับรอง

ในกรณีที่เป็นสถานบริการประเภท ง หรือประเภท จ ซึ่งตั้งอยู่ในอาคารขนาดใหญ่อาคารสูงหรืออาคารขนาดใหญ่พิเศษ ระบบสัญญาณเตือนเพลิงไหม้ของสถานบริการจะต้องต่อเชื่อมเข้ากับระบบสัญญาณเตือนเพลิงไหม้ของอาคารดังกล่าวด้วย

ข้อ ๒๖ สถานบริการต้องติดตั้งเครื่องดับเพลิงแบบมือถือหรือเครื่องดับเพลิงยกหิ้วตามมาตรฐานผลิตภัณฑ์อุตสาหกรรม โดยให้มี ๑ เครื่องต่อพื้นที่สถานบริการไม่เกิน ๒๐๐ ตารางเมตรแต่ไม่น้อยกว่าชั้นละ ๒ เครื่อง โดยการติดตั้งให้กระจายครอบคลุมทั้งพื้นที่สถานบริการ สำหรับประเภท ขนาด และสมรรถนะของเครื่องดับเพลิงดังกล่าวให้เป็นไปตามมาตรฐานว่าด้วยเครื่องดับเพลิงแบบมือถือหรือเครื่องดับเพลิงยกหิ้วของกรมโยธาธิการและผังเมือง หรือมาตรฐานอื่นที่คณะกรรมการควบคุมอาคารให้การรับรอง

การติดตั้งเครื่องดับเพลิงต้องติดตั้งให้ส่วนบนสุดของตัวเครื่องสูงจากระดับพื้นอาคารไม่เกิน๑.๕๐ เมตร โดยส่วนล่างสุดของทุกเครื่องต้องสูงไม่น้อยกว่า ๐.๑๐ เมตร ในที่ที่สามารถมองเห็นได้ชัดเจนหรือใช้ป้ายเครื่องหมายแสดงที่ตั้งของเครื่องดับเพลิงที่มองเห็นได้ชัดเจน รวมถึงสามารถอ่านคำแนะนำการใช้ได้ และสามารถเข้าใช้สอยได้โดยสะดวก

ข้อ ๓๐ ทางออกหรือประตูทางออกจากสถานบริการ ไปสู่ทางหนีไฟหรือออกสู่ภายนอกอาคารจะต้องมีลักษณะ ดังต่อไปนี้

(๑) เหนือทางออกหรือประตูทางออกต้องมีป้ายบอกทางหนีไฟด้วยตัวอักษรหรือสัญลักษณ์แสดงทางหนีไฟที่สามารถมองเห็นได้ชัดเจนตลอดเวลาโดยรายละเอียดของตัวอักษรหรือสัญลักษณ์ดังกล่าวให้เป็นไปตามมาตรฐานว่าด้วยป้ายบอกทางหนีไฟของกรมโยธาธิการและผังเมืองหรือมาตรฐานอื่นที่คณะกรรมการควบคุมอาคารให้การรับรอง

(๒) ความกว้างสุทธิของช่องทางออกหรือช่องประตูทางออกต้องไม่น้อยกว่า ๐.๘๔ เมตร สูงสุทธิไม่น้อยกว่า ๑.๙๗ เมตร และขนาดความกว้างของทางออกและประตูทางออกทุกแห่งรวมกันจะต้องไม่น้อยกว่าผลคูณระหว่างจำนวนคนตามที่คำนวณจากตารางที่ ๒ และตัวคูณความกว้างต่ำสุดตามที่ระบุในตารางที่ ๖

(๓) ทางออกหรือประตูทางออกต้องไม่มีธรณีประตูหรือขอบกั้นที่สูงเกินกว่า ๑๓ มิลลิเมตรทั้งนี้ พื้นบริเวณหน้าทางออกจากสถานบริการหากจะมีระดับพื้นด้านนอกและด้านในอยู่ต่างระดับกันให้ระดับพื้นด้านนอกอยู่ต่ำกว่าพื้นด้านในได้ไม่เกิน ๒๕ มิลลิเมตร

กรณีธรณีประตูหรือขอบกั้นสูงเกินกว่า ๖ มิลลิเมตร ให้ปรับขอบธรณีประตูหรือขอบกั้นให้มีความลาดเอียงแนวดิ่งต่อแนวราบไม่เกิน ๑ ต่อ ๒

(๔) ประตูทางออกต้องสามารถเปิดออกได้โดยสะดวกตลอดเวลาที่มีคนอยู่ข้างในและต้องเปิดออกในทิศทางการหนีไฟ รวมทั้งเมื่อเปิดออกแล้วจะต้องไม่กีดขวางทางเดินหรือบันไดหรือชานพักบันได

(๕) กรณีเป็นประตูทางออก เมื่อเปิดออกสู่บันไดหนีไฟโดยตรงจะต้องมีชานพักขนาดความกว้างสุทธิด้านละไม่น้อยกว่า ๑.๕๐ เมตร

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (เฉพาะส่วนที่เกี่ยวข้องกับหน่วยงานของรัฐ)

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษา ความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้
(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง
(๒) แผนการรับมือภัยคุกคามทางไซเบอร์เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่อาจดำเนินการหรือปฏิบัติตามวรรคหนึ่งได้ สำนักงานอาจให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้

มาตรา ๔๖ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน ในกรณีที่มีการเปลี่ยนแปลงเจ้าหน้าที่ตามวรรคหนึ่ง ให้หน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งให้สำนักงานทราบโดยเร็ว

ข้อบังคับมหาวิทยาลัยสงขลานครินทร์ ว่าด้วยการบริหารงานบุคคลพนักงานมหาวิทยาลัย พ.ศ. ๒๕๖๗

หมวด ๘ การพัฒนาพนักงานมหาวิทยาลัย (ทุกข้อ)
หมวด ๑๐ การออกจากงาน (ทุกข้อ)
หมวด ๑๓ วินัย จรรยาบรรณ การดำเนินการทางวินัยและจรรยาบรรณ (ทุกข้อ)

ข้อบังคับมหาวิทยาลัย สงขลานครินทร์ ว่าด้วยการบริหารงานบุคคลพนักงานเงินรายได้มหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๖๒
(จะเหมือนกับข้อบังคับมหาวิทยาลัยสงขลานครินทร์ ว่าด้วยการบริหารงานบุคคลพนักงานมหาวิทยาลัย พ.ศ. ๒๕๖๗)

ระเบียบการรักษาความลับของทางราชการ
หมวด ๒ การกำหนดชั้นความลับ ส่วนที่ 2 การแสดงชั้นความลับ
หมวด ๓ การปรับชั้นความลับ
หมวด ๔ การดำเนินการ
ส่วนที่ ๑ การจัดทำ
ส่วนที่ ๒ การทำสำเนาและการแปล
ส่วนที่ ๓ การโอน
ส่วนที่ ๔ การส่งและการรับ
ส่วนที่ ๕ การเก็บรักษา
ส่วนที ๖ การยืม
ส่วนที่ ๗ การทำลาย
ส่วนที่ ๑๐ การเปิดเผย

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
มาตรา ๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติ แห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้
มาตรา ๒๒ การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้ วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล
มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้ง ให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว
(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึง วัตถุประสงค์ตามที่ มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของ ข้อมูลส่วนบุคคล
(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติ ตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณี ที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐาน ของการเก็บรวบรวม
(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณี ที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย
(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง
มาตรา ๒๕ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง
มาตรา ๒๖ ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลชั้นความอ่อนไหว (Sensitive Data) โดยไม่ได้รับความยินยอมชัดแจ้ง ซึ่งครอบคลุมถึงข้อมูลสุขภาพ ประวัติการบำบัด โปรไฟล์ทางชีวภาพและชั้นความลับ ซึ่งเป็นกรณีที่คณะแพทยศาสตร์จัดเก็บสำหรับผู้ป่วยทุกรายในระบบ HIS
มาตรา ๒๗ ห้ามเปิดเผยข้อมูลชั้นความอ่อนไหวโดยไม่ได้รับความยินยอมชัดแจ้ง เว้นแต่มีเหตุผลที่กฎหมายบัญญัติให้กระทำได้ (เช่น การรักษาพยาบาล) — คณะแพทยศาสตร์ต้องบันทึกฐานทางกฎหมายในการประมวลผลข้อมูลสุขภาพทุกครั้ง

**การประมวลผลข้อมูลส่วนบุคคลผ่านการบันทึกการเข้าออกพื้นที่ และภาพวงจรปิด เป็นฐานการประมวลผลตามสิทธิอันชอบธรรม ของผู้ควบคุมข้อมูลส่วนบุคคล
มาตรา ๓๗ ผู้ประมวลผลข้อมูล (Data Processor) ที่ได้รับมอบหมายจากคณะแพทยศาสตร์ให้ประมวลผลข้อมูลส่วนบุคคล (เช่น Vendor หรือผู้รับจ้างภายนอกที่เข้าถึงข้อมูลใน HIS) ต้อง

ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้น และต้องยืนยันมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอ

มาตรา ๔๐ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมงนับจากทราบเหตุ ซึ่งคณะแพทยศาสตร์ต้องกำหนดแผน Incident Response เพื่อรองรับข้อกำหนดนี้

มาตรา ๔๑ ผู้ควบคุมข้อมูลต้องแจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้าเมื่อเกิดเหตุละเมิด หากเหตุดังกล่าวอาจก่อให้เกิดความเสียหายแก่สิทธิและเสรีภาพของบุคคล

มาตรา ๔๒ กำหนดให้หน่วยงานของรัฐแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO — Data Protection Officer) ผู้มีหน้าที่ให้คำปรึกษา ตรวจสอบ และติดตามการปฏิบัติตาม PDPA ภายในหน่วยงาน — คณะแพทยศาสตร์ในฐานะหน่วยงานของรัฐต้องมีผู้ให้บริการ DPO ที่แต่งตั้งอย่างเป็นทางการ ไม่ใช่การดำเนินการแบบไม่เป็นทางการหรือปราศจากหลักฐานการแต่งตั้ง

ส่วนที่ ๘: ความปลอดภัยด้านข้อมูลและการเข้ารหัส

๒๗๗. การจัดส่งข้อมูลที่มีชั้นความลับ ให้แก่หน่วยงานภายนอก หากปราศจาก NDA ต้องพิจารณาถึงมาตรการเข้ารหัสข้อมูลอย่างเหมาะสม รวมถึงการใช้ Password Protection ข้อมูลก่อนการจัดส่ง ทั้งนี้ให้อยู่บนพื้นฐานของความสามารถในการปฏิบัติได้ และการเอื้ออำนวยต่อการใช้ข้อมูลประกอบ รวมถึงบริบทอื่น ๆ

๒๗๘. เมื่อต้องแสดงหรือจำเป็นต้องแสดงข้อมูลส่วนบุคคล เพื่อยืนยันตัวตนแก่เจ้าของข้อมูลส่วนบุคคลหรือผู้ทราบอยู่แล้วถึงข้อมูลนั้น ให้พิจารณาใช้เทคนิคการทำ Data Masking โดยการใช้สัญลักษณ์ปกปิดบางส่วนของข้อมูล ตัวอย่างเช่น

๒๗๘.๑ เลขบัตรประชาชน เปิดเผยแค่ 4 ตัวท้าย

๒๗๘.๒ เบอร์โทรศัพท์ ปกปิด 4 ตัวท้าย

๒๗๘.๓ บัตรเครดิต เปิดเผยแค่ 4 ตัวท้าย

๒๗๙. ในการเข้ารหัสข้อมูล ต้องจัดการไฟล์คีย์ (Key File) ที่ใช้ในการเข้ารหัสข้อมูลอย่างเหมาะสม และกำหนดรอบการเปลี่ยนแปลงเมื่อไม่กระทบต่อระบบสารสนเทศหลัก อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ส่วนที่ ๙: การใช้งาน Cloud Service

๒๘๐. กำหนดกลยุทธ์ที่ชัดเจนในการใช้งานระบบ Cloud Computing เช่น เหตุผลและความจำเป็นทางธุรกิจ ประโยชน์ การดำเนินการตามกฎหมายและข้อบังคับทั้งภายในและภายนอกประเทศ ความเสี่ยงและการบริหารความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์

๒๘๑. ต้องกำหนด ประเภทงานที่จะใช้บริการ ผู้ดูแลระบบ ประเภทข้อมูลที่จะถูกจัดเก็บ ระยะเวลาการใช้บริการ แนวทางการยกเลิกการใช้บริการ ที่ครอบคลุมการจัดการข้อมูลของหน่วยงานที่อยู่บน Cloud Service เมื่อมีการยกเลิกการใช้งาน

๒๘๒. จัดให้ประเมิน ติดตาม และเฝ้าระวังสมรรถนะของผู้ให้บริการ Cloud Service ตามระเบียบของภาครัฐ เมื่อเป็นไปได้ให้พิจารณาการเข้าตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ (กรณีผู้ให้บริการในประเทศ)

๒๘๒.๑ ควรพิจารณาคัดเลือกผู้ให้บริการที่ผ่านการรับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ อาทิ ISO/IEC 27001:2022 CloudStar PCI/DSS เป็นต้น

๒๘๒.๒ พิจารณาระดับสัญญาบริการ (SLA) ของผู้ให้บริการว่าเป็นที่ยอมรับได้ต่อความเสี่ยงของข้อมูลและระบบสารสนเทศที่ใช้งาน Cloud Service

๒๘๒.๓ เมื่อมีการยกเลิกใช้งานต้องมีกลไกในการตรวจสอบว่าข้อมูลของหน่วยงานได้รับการทำลายจาก Cloud Service เรียบร้อยแล้วก่อนการยกเลิกสัญญาหรือหมดอายุสัญญาบริการ

๒๘๓. ในกรณีที่การใช้งาน Cloud Service เป็นระดับผู้ปฏิบัติงานและพนักงาน ต้องสื่อสารถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลบน Cloud Service และวิธีการใช้งานอย่างปลอดภัย อาทิ การแชร์ไฟล์ การกำหนดสิทธิการเข้าถึง Folder

๒๘๔. กำหนดให้มีการเฝ้าระวังการใช้ทรัพยากรของ Cloud Service เพื่อการวางแผนจัดสรรทรัพยากรของ Cloud Service ให้อย่างเหมาะสม

ส่วนที่ 10: การควบคุมการตั้งค่า Configuration

๒๘๕. อุปกรณ์เครือข่ายที่สำคัญ (Critical) ต้องจัดให้มีการสำรองค่า configuration ไว้ ทุกครั้งที่มีการเปลี่ยนแปลงการตั้งค่า

๒๘๖. การตั้งค่าของอุปกรณ์เครือข่ายต้องมีความมั่นคงปลอดภัย โดยพิจารณาร่วมกับการเข้ารหัสและเทคโนโลยีการสื่อสารที่จำเป็น

๒๘๗. ทุกการตั้งค่าที่เป็น default ที่ติดมากับอุปกรณ์ต้องได้รับการตรวจทาน และไม่แนะนำให้ใช้การตั้งค่าเหล่านั้นหากไม่จำเป็น ประกอบการพิจารณาความเสี่ยง

ส่วนที่ 11: การใช้ตัวกรองเว็บไซต์ (Web Filtering)

๒๘๘. ตัวกรองที่ต้องควบคุมในระดับการตัดการเชื่อมต่อ (block) ได้แก่

๒๘๘.๑ เกี่ยวกับเนื้อหาอนาจาร

๒๘๘.๒ เกี่ยวกับการเจาะระบบและภัยคุกคาม

๒๘๘.๓ เกี่ยวกับการค้ายาเสพติด

๒๘๙. ตัวกรองอื่น ๆ ที่กำหนดมาโดยระบบป้องกัน ให้ดำเนินการตั้งค่าด้วยระวังเฝ้าระวัง (Monitoring)

๒๙๐. ปรับปรุงแหล่งอ้างอิงตัวกรอง (reference source) ตามความเหมาะสม หรือตามแหล่งอ้างอิงที่น่าเชื่อถือ

ส่วนที่ 12: การขอใช้บริการ Colocation

๒๙๑. หน่วยงานภายในคณะแพทยศาสตร์ที่มีความประสงค์ต้องการใช้บริการ Colocation (ครั้งแรก) ต้องทำเป็นหนังสือขอใช้บริการส่งถึงรองคณบดีฝ่ายเทคโนโลยีสารสนเทศ โดยระบุ ชนิดของอุปกรณ์ที่ต้องใช้บริการ ขนาดและน้ำหนัก รวมถึงปริมาณการใช้พลังงานไฟฟ้า

๒๙๒. เมื่อหน่วยงานมีความต้องการเข้าใช้พื้นที่หรือติดตั้งอุปกรณ์เพิ่มเติม ให้ดำเนินการจัดส่งคำขอบริการ (Service Request) ผ่านระบบ Service Desk โดยระบุ

๒๙๒.๑ กรณีเข้าบำรุงรักษา: อุปกรณ์ที่ต้องการเข้าถึง ระยะเวลาหรือช่วงเวลา และสาเหตุของการขอเข้าพื้นที่

๒๙๒.๒ กรณีเข้าติดตั้งเพิ่มเติม: ชนิดของอุปกรณ์ที่ต้องใช้บริการ ขนาดและน้ำหนัก รวมถึงปริมาณการใช้พลังงานไฟฟ้า

๒๙๒.๓ กรณีเพิกถอน: อุปกรณ์ที่ต้องการเพิกถอน ระยะเวลาหรือช่วงเวลา โดยต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศติดตามตลอดเวลาการดำเนินการ

๒๙๓. กรณีมีเหตุเสียที่เกี่ยวข้องกับเครื่องหรืออุปกรณ์ในบริการ Colocation ให้ดำเนินการตามกระบวนการรับมืออุบัติการณ์ (Incident) หรือติดต่อเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

๒๙๔. กรณีที่การดำเนินการใด ๆ ดำเนินการโดยบุคลากรหรือองค์กรภายนอก ต้องระบุชื่อองค์กร หรือผู้รับผิดชอบในการดำเนินการทุกครั้ง

ส่วนที่ 13: การคุ้มครองข้อมูลส่วนบุคคลและการแจ้งเหตุละเมิด

๒๙๕. แนวปฏิบัตินี้กำหนดข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐาน ISO/IEC 27001:2022 Annex A.5.21, A.5.24–A.5.26 ครอบคลุมบุคลากร ระบบสารสนเทศ และหน่วยงานภายนอกที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของคณะแพทยศาสตร์

๒๙๖. หน่วยงานภายนอกที่ประมวลผลข้อมูลส่วนบุคคลในนามของคณะแพทยศาสตร์ (Data Processor) ต้องลงทะเบียนใน DP Register ก่อนเริ่มดำเนินการ และทบทวนทุกปี

๒๙๗. Data Processor ทุกรายต้องลงนามใน Data Processing Agreement (DPA) ที่ระบุขอบเขตการประมวลผล มาตรการความปลอดภัย ข้อกำหนด Sub-processor และสิทธิ์ตรวจสอบของคณะแพทยศาสตร์

๒๙๘. Data Processor ต้องแจ้งคณะแพทยศาสตร์ภายใน 24 ชั่วโมงเมื่อทราบว่าเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เพื่อให้คณะแพทยศาสตร์สามารถแจ้ง PDPC ได้ทันภายใน 72 ชั่วโมง

๒๙๙. เมื่อตรวจพบหรือได้รับแจ้งว่าอาจเกิดการละเมิดข้อมูลส่วนบุคคล ให้บันทึกทันทีใน Service Desk และระบุเวลาที่ทราบเรื่อง (T_0) ซึ่งเป็นจุดเริ่มต้นนับกรอบเวลา 72 ชั่วโมง

๓๐๐. ภายใน 4 ชั่วโมงนับจาก T_0 ให้ประเมินความเสี่ยงของเหตุการณ์และแจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เป็นลายลักษณ์อักษรทันที พร้อมระบุลักษณะเหตุการณ์ ประเภทและจำนวนข้อมูลที่อาจได้รับผลกระทบ

๓๐๑. หากผลการประเมินพบว่าเหตุการณ์มีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล ให้แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ภายใน 72 ชั่วโมงนับจาก T_0 ตามมาตรา 37 แห่ง พ.ร.บ. PDPA

๓๐๒. การแจ้ง PDPC ต้องระบุ: ลักษณะของการละเมิด จำนวนและประเภทของเจ้าของข้อมูลที่ได้รับผลกระทบ ผลที่อาจเกิดขึ้น และมาตรการที่ดำเนินการแล้วและที่วางแผนไว้ หากแจ้งช้ากว่า 72 ชั่วโมงต้องระบุเหตุผลที่ชัดเจนด้วย

๓๐๓. ในกรณีที่เหตุการณ์ก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพ ให้แจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า พร้อมคำแนะนำแนวทางลดความเสียหาย ยกเว้นกรณีที่ข้อมูลได้รับการเข้ารหัสอย่างเหมาะสมหรือความเสี่ยงได้รับการบรรเทาแล้ว

ช่วงเวลา	กิจกรรม	ผู้รับผิดชอบ
T_0 + 0–4 ชม.	บันทึก Service Desk + ประเมินความเสี่ยง + แจ้ง DPO	Security Officer + IT Head
T_0 + 24 ชม.	เตรียมเอกสารแจ้ง PDPC + ร่างแจ้งเจ้าของข้อมูล (ถ้าจำเป็น)	IT Head + DPO
T_0 + 72 ชม.	แจ้ง PDPC (Deadline) — หากช้าต้องระบุเหตุผลชัดเจน	DPO + คณะแพทยศาสตร์
T_0 + 14 วัน	Root Cause Analysis + ปรับปรุง Control + รายงานคณะกรรมการ	ISMS Team

๓๐๔. ต้องบันทึก Breach Log ทุกกรณีไม่ว่าจะแจ้ง PDPC หรือไม่ โดยระบุ: ข้อเท็จจริง วันเวลาที่แจ้ง DPO วันเวลาที่แจ้ง PDPC และมาตรการแก้ไข จัดเก็บไว้อย่างน้อย 3 ปี โดยใช้แบบฟอร์ม PDPA-Breach-Log-SD

๓๐๕. ให้จัดซ้อมรับมือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Tabletop Exercise) อย่างน้อยปีละ 1 ครั้ง โดยบันทึก Attendance List และ After-Action Report เป็นหลักฐานสำหรับการตรวจสอบจาก CB Auditor

๓๐๖. ผลการซ้อมที่พบช่องว่างให้บันทึกเป็น Corrective Action ใน Service Desk และรายงานต่อคณะกรรมการบริหาร ISMS ในการประชุมครั้งถัดไป