



ระเบียบสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา
ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา
พ.ศ. ๒๕๖๕

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ จึงวางระเบียบ ไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา พ.ศ. ๒๕๖๕”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันนี้เป็นต้นไป

ข้อ ๓ บรรดาระเบียบและคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับระเบียบนี้ให้ระเบียบนี้แทน โดยยึดถือให้อยู่ภายใต้ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงานข้าราชการ พนักงานกระทรวง และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

ข้อ ๕ คำนิยามในระเบียบนี้

๕.๑ ระบบสารสนเทศ (Information System) หมายถึง ระบบข้อมูลของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบสื่อสาร มาช่วยในการสร้างสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาและสามารถนำสารสนเทศมาใช้ในการวางแผน การบริหาร การพัฒนา ควบคุม รวมทั้งแนวทางหรือระเบียบปฏิบัติในการใช้อุปกรณ์เหล่านี้ ซึ่งมีองค์ประกอบดังนี้

๕.๑.๑ ระบบคอมพิวเตอร์ (Computer System) หมายถึง ระบบที่ประกอบด้วย ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (People ware)

๕.๑.๒ เครือข่ายคอมพิวเตอร์ (Computer Network) หมายถึง การติดต่อสื่อสาร หรือการรับ-ส่งข้อมูลระหว่างระบบสารสนเทศภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา และหน่วยงานอื่นๆ ที่เกี่ยวข้องกัสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๕.๑.๓ สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากการสกัดข้อมูลให้มีความหมายโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความ หรือ ภาพกราฟฟิกที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจ และอื่นๆ

๕.๒ จดหมายอิเล็กทรอนิกส์ (Electronic Mail: E-mail) หมายถึง การรับส่งข้อมูลผ่านอินเทอร์เน็ตหรืออินทราเน็ต โดยชื่อที่ใช้ในการรับส่งจดหมายอิเล็กทรอนิกส์ จะมีรูปแบบซึ่งประกอบไปด้วย ๒ ส่วน คือ ชื่อผู้ใช้ และชื่อโดเมน เช่น somdet_chaopraya@mail.somdet.go.th เป็นต้น

๕.๓ ผู้ใช้งาน (User) หมายถึง ข้าราชการ พนักงานราชการ พนักงานกระทรวง และ ลูกจ้างของสถาบันจิตเวชศาสตร์สมเด็จพระยาที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระยา รวมถึงบุคคลภายนอกที่หน่วยงานอนุญาตให้เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระยา

๕.๔ ผู้ดูแลระบบ (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลระบบสารสนเทศของหน่วยงานนั้นๆ

๕.๕ ผู้ดูแลเครือข่าย (Network Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลเครือข่ายสารสนเทศของหน่วยงานนั้นๆ

๕.๖ ผู้ดูแลฐานข้อมูล (Database Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ดูแลฐานข้อมูล

๕.๗ ผู้บังคับบัญชา หมายถึง หัวหน้าหน่วยงานของผู้ปฏิบัติหน้าที่ในระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระยา

๕.๘ ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า ความมั่นคงและความปลอดภัยในบริบทของ การรักษาความลับ ความเชื่อถือได้ และความพร้อมใช้งานของข้อมูล สำหรับระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระยา

๕.๙ ทรัพย์สินสารสนเทศ หมายความว่า

๕.๙.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๕.๙.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใดที่มีใช้ในระบบ

๕.๙.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์และข้อมูลคอมพิวเตอร์

๕.๑๐ ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) หมายความว่า การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้เปิดเผยขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๕.๑๑ ความมั่นคงปลอดภัยด้านกายภาพ (Physical Security) หมายความว่า การจัดทำมีนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใดๆ เพื่อนำมาใช้ป้องกัน ทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติอุบัติภัย หรือภัยทางกายภาพอื่น

๕.๑๒ เหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของสถาบันจิตเวชศาสตร์สมเด็จพระยา หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรืออาจสร้างความเสียหายได้ในที่สุดซึ่งอาจส่งผลให้

๕.๑๒.๑ เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ เช่น ระบบสารสนเทศของหน่วยเกิดการหยุดชะงัก เป็นต้น

๕.๑๒.๒ เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของสถาบันจิตเวชศาสตร์สมเด็จพระยา

๕.๑๒.๓ เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กำหนดไว้

๕.๑๒.๔ เกิดภาพลักษณ์ที่ไม่ดีต่อสถาบันจิตเวชศาสตร์สมเด็จพระยาหรือทำให้สูญเสียชื่อเสียง เช่น การไปโพสต์ข้อความพาดพิงถึงสถาบันจิตเวชศาสตร์สมเด็จพระยาในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของสถาบันจิตเวชศาสตร์สมเด็จพระยา เป็นต้น

๕.๑๒.๕ ตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัย ได้แก่ โปรแกรมไม่พึงประสงค์ การพบจุดอ่อนในซอฟต์แวร์ ระบบงาน หรือฮาร์ดแวร์ที่ใช้งาน การแจ้งเตือนของระบบป้องกันการบุกรุก ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลง หรือสูญหาย เว็บไซต์ที่ถูกเปลี่ยนแปลงการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต การใช้ทรัพยากรของหน่วยงานผิดวัตถุประสงค์ เช่น การใช้เครือข่ายของหน่วยงานเพื่อกระทำการที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อกระทำการที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา เพื่อทำการส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ เป็นต้น ระบบถูกโจมตีจนไม่สามารถให้บริการได้ ระบบ อุปกรณ์ ฮาร์ดแวร์ หรือทรัพย์สินในระบบสารสนเทศอื่นๆ ถูกขโมย การแอบติดตั้งซอฟต์แวร์เพื่อดักขโมยข้อมูลหรือดักดูข้อมูลในเครือข่ายของสถาบันจิตเวชศาสตร์สมเด็จพระยา การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่นๆ ที่เป็นการละเมิดระเบียบฉบับนี้

๕.๑๒.๖ ตัวอย่างของเหตุการณ์ที่เป็นจุดอ่อน ได้แก่ ประตุนันท์คอมพิวเตอร์ไม่สามารถปิดให้สนิทได้ ระบบสารสนเทศของหน่วยมีช่องทางอื่นในการเข้าสู่ระบบได้โดยไม่ผ่านการพิสูจน์ตัวตนตามปกติ เจ้าหน้าที่รักษาความปลอดภัยของหน่วยไม่เข้มงวดหรือละเลยการปฏิบัติหน้าที่ บุคคลภายนอกสามารถเดินตามเจ้าหน้าที่เข้าห้องระบบสารสนเทศของหน่วยโดยไม่มีการแลกบัตรผ่าน บุคคลภายนอกไม่ได้ล็อกก่อนเข้าศูนย์คอมพิวเตอร์ของหน่วย เจ้าหน้าที่ไม่มีการระบุตัวตนก่อนที่จะเข้าถึงห้องระบบสารสนเทศของหน่วยนั้น

๕.๑๒.๗ เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ที่เป็นจุดอ่อน จำเป็นต้องได้รับรายงานจากผู้ใช้งานเพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสมได้ผลและทันกาล

๕.๑๓ ทรัพย์สินทางปัญญา หมายถึง ผลงานอันเกิดจากความคิดสร้างสรรค์ของมนุษย์ ทรัพย์สินทางปัญญาเป็นทรัพย์สินอีกชนิดหนึ่งที่นอกเหนือจากสังหาริมทรัพย์นั้นคือทรัพย์สินที่สามารถเคลื่อนย้ายได้ เช่น นาฬิกา รถยนต์ โต๊ะ เป็นต้น และอสังหาริมทรัพย์ คือทรัพย์สินที่ไม่สามารถเคลื่อนย้ายได้ เช่น บ้าน ที่ดิน เป็นต้น ซึ่งทรัพย์สินทางปัญญา ได้แก่

๕.๑๓.๑ ลิขสิทธิ์ (Copyright)

๕.๑๓.๓ สิทธิบัตร (Patent)

๕.๑๓.๓ เครื่องหมายการค้า (Trademark)

๕.๑๓.๔ แบบผังภูมิของวงจรรวม (Layout - Designs of Integrated Circuit)

๕.๑๓.๕ ความลับทางการค้า (Trade Secrets)

๕.๑๓.๖ สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication)

๕.๑๔ สิทธิพจน์ หมายถึง สิ่งของที่จำเป็นทั้งหมดสำหรับสถาบันจิตเวชศาสตร์ สมเด็จพระเจ้าพระยาทั้งที่มีไว้เพื่อการดำรงอยู่ และการปฏิบัติของหน่วยภายในสถาบันจิตเวชศาสตร์ สมเด็จพระเจ้าพระยา ทั้งให้เป็นไปตามสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยาว่าด้วยความรับผิดชอบ ในสิ่งอุปกรณ์ พ.ศ. ๒๕๓๕ ตามคำจำกัดความ ข้อ ๔ ว่าด้วยสิ่งอุปกรณ์ของสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา

๕.๑๕ สิทธิของผู้ใช้งาน (User Access Right) หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา หรือ เพื่อ การเข้าถึงเข้าใช้สารสนเทศ และทรัพย์สินสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา

๕.๑๖ การเข้าถึง (Access) หมายถึง ความสามารถในการเข้าไป อันอาจทำให้ สามารถจะอ่านทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใดๆ หรือได้อ่าน ทำ สร้าง แก้ไข ปรับปรุงเปลี่ยนแปลง ล่วงรู้ด้วยประการใดๆ สำหรับข้อมูลคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ สารสนเทศ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์และวิธีการทางกายภาพ

๕.๑๗ การควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบ สารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๕.๑๘ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบของสถาบันจิตเวชศาสตร์ สมเด็จพระเจ้าพระยา สูญเสีย การปฏิบัติงาน รวมถึงการให้บริการต่างๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูก บุกรุกหรือโจมตีทางช่องทาง และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่างๆ

๕.๑๙ ภัยคุกคาม (threats) หมายถึง เหตุการณ์ต่างๆ ที่เป็นไปได้หรือเหตุการณ์ที่ไม่ พึงประสงค์ ซึ่งอาจส่งผลกระทบต่อหรือสร้างความเสียหายต่อระบบสารสนเทศของสถาบันจิตเวชศาสตร์ สมเด็จพระเจ้าพระยา

๕.๒๐ ช่องโหว่ (vulnerabilities) หมายถึง จุดอ่อนของทรัพย์สินหรือมาตรการที่เป็น ช่องทางเกิดปัจจัยเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อทรัพย์สินหรือต่อระบบสารสนเทศของสถาบัน จิตเวชศาสตร์สมเด็จพระเจ้าพระยา

ข้อ ๖ ผู้อำนวยการ สถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา ในฐานะผู้บริหารระดับสูงสุดของ สถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบระบบสารสนเทศ ในภาพรวม ของสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา รวมถึงการละเมิดมาตรการต่างๆ อันทำให้เกิดความเสียหายของระบบสารสนเทศที่เกิดขึ้นตามระเบียบนี้

ข้อ ๗ ให้หัวหน้ากลุ่มงานยุทธศาสตร์และเทคโนโลยีสารสนเทศ เป็นผู้รักษาการให้เป็นไปตาม ระเบียบนี้ และให้กำหนดการทบทวนระเบียบนี้ให้มีความทันสมัยอย่างต่อเนื่อง โดยมีวงรอบปีงบประมาณละ ๑ ครั้ง

หมวด ๑ กล่าวทั่วไป

ข้อ ๘ ความมุ่งหมายของระเบียบนี้

๘.๑ เพื่อให้เกิดความเชื่อมั่นและมีระบบการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาดำเนินงานไปได้อย่างมีประสิทธิภาพและประสิทธิผล

๘.๒ เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บังคับบัญชาของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๘.๓ เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ยกกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศไปสู่สากล

๘.๔ เพื่อเป็นมาตรการในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาสำหรับการพิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการรั่วไหล หรือรู้ไปถึง หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่ ป้องกันการจารกรรม ทั้งจาก บุคคลภายในและภายนอกส่วนราชการ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่เครื่องคอมพิวเตอร์ อุปกรณ์สารสนเทศ เครื่องใช้สำนักงาน อาคาร สถานที่ และเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ เป็นต้น

ข้อ ๙ หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของส่วนราชการ และแต่งตั้งผู้รับผิดชอบระบบสารสนเทศของส่วนราชการเพิ่มเติมได้โดยให้สอดคล้องและไม่ขัดแย้งกับระเบียบนี้

ข้อ ๑๐ เหตุผลในการประกาศใช้ระเบียบนี้ คือ วางนโยบายและแนวปฏิบัติของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เกี่ยวกับระบบคอมพิวเตอร์ ระบบสื่อสารสารสนเทศ ระบบเครือข่ายสารสนเทศ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ พนักงาน ข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการ เกี่ยวกับระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

ข้อ ๑๑ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พรบ.ข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่ได้ ประกาศใช้ทดแทน

หมวด ๒

การจัดทำโครงการและการจัดหาระบบงาน คอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ (Application, Computer and Device Project Development and Acquisition)

ข้อ ๑๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องควบคุมการจัดหาระบบงาน คอมพิวเตอร์ และอุปกรณ์เครือข่ายและคอมพิวเตอร์ดังนี้

๑๒.๑ ต้องเป็นผู้ให้ความเห็นชอบในการจัดทำโครงการด้านระบบสารสนเทศของหน่วยงานภายในต่างๆ ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาเพื่อให้ความเหมาะสมและเกิดประโยชน์สูงสุดแก่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๑๒.๒ ต้องเป็นผู้ให้ความเห็นชอบสำหรับการจัดหาระบบงาน คอมพิวเตอร์ อุปกรณ์เครือข่าย หรืออุปกรณ์คอมพิวเตอร์ของหน่วยงานภายในของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๑๒.๓ ไม่อนุญาตให้หน่วยงานภายในต่างๆ ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ดำเนินการด้วยตนเอง โดยไม่ผ่านความเห็นชอบจากหน่วยรับผิดชอบตามสายงานหรือหน่วยงานที่ได้รับมอบหมายจากผู้บังคับบัญชา

หมวด ๓

การควบคุมการเข้าถึงหรือการใช้งานระบบสารสนเทศ (Access Control)

ข้อ ๑๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดการควบคุม การเข้าถึงระบบสารสนเทศของหน่วยงาน โดยกำหนดเป็นมาตรการทั้ง ๔ ด้าน ดังนี้

๑๓.๑ ด้านการเข้าถึงระบบสารสนเทศทั่วไป

๑๓.๑.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบข้อมูลและ/หรือผู้รับผิดชอบระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๑๓.๑.๒ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นบันทึกและกรอกแบบเอกสารที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยากำหนด เพื่อขอสิทธิในการเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้บังคับบัญชาหรือผู้รับมอบอำนาจจากผู้บังคับบัญชาเพื่อการจัดเก็บไว้เป็นหลักฐาน

๑๓.๑.๓ ผู้รับผิดชอบข้อมูลและผู้รับผิดชอบระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๑๓.๒ ด้านการเข้าถึงระบบเครือข่ายสารสนเทศ

๑๓.๒.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้รับผิดชอบระบบเครือข่ายของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาตามสิทธิและความจำเป็นในการเข้าถึงเครือข่ายก่อนที่จะเข้าใช้งาน

๑๓.๒.๒ ผู้ดูแลเครือข่ายสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยามีหน้าที่ตรวจสอบ อนุมัติและกำหนดการอนุญาตในการผ่านเข้าสู่เครือข่ายสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ตามสิทธิและความจำเป็นในการปฏิบัติงานเท่านั้น

๑๓.๒.๓ ผู้ดูแลเครือข่ายสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา จะต้องจัดให้มีการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนการเฝ้าระวังการใช้งานไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิการใช้งาน ล่วงละเมิดสิทธิของผู้ใช้งานอื่นๆ อีกด้วย

๑๓.๓ ด้านการเข้าถึงระบบปฏิบัติการ

๑๓.๓.๑ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบระบบปฏิบัติการ ซึ่งเป็นทรัพย์สินของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาจึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะ ระบบปฏิบัติการที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาจัดหามาอย่างถูกต้องตามกฎหมายเท่านั้น

๑๓.๓.๒ ผู้รับผิดชอบระบบปฏิบัติการ มีหน้าที่ตรวจสอบสิทธิอนุญาตให้เข้าใช้งานระบบปฏิบัติการของผู้ใช้ และควบคุมการใช้งานให้เป็นไปตามสิทธิและตามความจำเป็นในการใช้งาน รวมถึงการบันทึกการใช้งานของผู้ใช้ ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิการใช้งาน รวมถึงล่วงละเมิดสิทธิของผู้ใช้งานอื่นๆ อีกด้วย

๑๓.๔ ด้านการเข้าถึงโปรแกรมประยุกต์ (Application)

๑๓.๔.๑ ผู้ใช้งานต้องได้รับอนุญาตจากผู้รับผิดชอบโปรแกรมประยุกต์ซึ่งเป็นทรัพย์สินของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาจึงจะสามารถเข้าถึงการใช้งานได้ และผู้ใช้งานต้องใช้งานเฉพาะโปรแกรมประยุกต์ที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาจัดหามาอย่างถูกต้องตามกฎหมายเท่านั้น

๑๓.๔.๒ ผู้รับผิดชอบโปรแกรมประยุกต์ มีหน้าที่ตรวจสอบสิทธิอนุญาตให้เข้าใช้งานโปรแกรมประยุกต์ของผู้ใช้ และควบคุมการใช้งานให้เป็นไปตามสิทธิและตามความจำเป็นในการใช้งาน รวมถึงการบันทึกการใช้งานของผู้ใช้ ตลอดจนการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย ล่วงละเมิดสิทธิการใช้งาน รวมถึงล่วงละเมิดสิทธิของผู้ใช้งานอื่นๆ อีกด้วย

ข้อ ๑๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดการบริหาร จัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ดังนี้

๑๔.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ที่ปฏิบัติงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เป็นต้น

๑๔.๑.๑ ขั้นตอนการลงทะเบียนเจ้าหน้าที่ (user registration)

๑๔.๔.๑.๑ หน่วยต้นสังกัดของเจ้าหน้าที่ใหม่ แจ้งข้อมูลการขอลงทะเบียนเจ้าหน้าที่ใหม่เป็นลายลักษณ์อักษรตามสายการบังคับบัญชา ให้ผู้รับผิดชอบระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๑๔.๔.๑.๒ ผู้รับผิดชอบระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา พิจารณาข้อมูลการลงทะเบียนของเจ้าหน้าที่ใหม่ โดยตรวจสอบให้ถูกต้องว่าเป็นเจ้าหน้าที่ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา อย่างแท้จริง และได้รับสิทธิในการใช้งานตามคำร้องขอลงทะเบียนอย่างถูกต้อง

๑๔.๔.๑.๓ ผู้รับผิดชอบระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา พิจารณานุมัติให้ลงทะเบียนเจ้าหน้าที่ใหม่ และแจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชา และเจ้าหน้าที่ใหม่ทราบต่อไป

๑๔.๑.๒ ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน

๑๔.๑.๒.๑ หน่วยต้นสังกัดของเจ้าหน้าที่ แจ้งข้อมูลการขอยกเลิก สิทธิการใช้งานเป็นลายลักษณ์อักษรตามสายการบังคับบัญชา ให้ผู้รับผิดชอบระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๑๔.๑.๒.๒ ผู้รับผิดชอบ ระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา พิจารณาข้อมูลการขอยกเลิกสิทธิการใช้งานของเจ้าหน้าที่ โดยตรวจสอบให้ถูกต้องว่าเป็นเจ้าหน้าที่ของ สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาอย่างแท้จริง และได้รับการยกเลิกสิทธิในการใช้งานตามคำร้องอย่างถูกต้อง

๑๔.๑.๒.๓ ผู้รับผิดชอบ ระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา พิจารณานุมัติให้ยกเลิกสิทธิการใช้งานของเจ้าหน้าที่ และแจ้งผลการอนุมัติตามสายการบังคับบัญชาให้ผู้บังคับบัญชาและเจ้าหน้าที่นั้นทราบต่อไป

๑๔.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑๔.๓ กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน และถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของผู้ใช้งานต่อไป

๑๔.๔ จำกัดการใช้งานบัญชีชื่อผู้ใช้งานแบบกลุ่มซึ่งมีการใช้งานร่วมกัน กล่าวคือ อนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้น และผู้ใช้งานบัญชีแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน

๑๔.๕ ไม่อนุญาตให้ผู้ร้องขอใช้ระบบสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

๑๔.๖ จัดเก็บข้อมูลการลงทะเบียนของผู้ที่ร้องขอเข้าใช้ระบบสารสนเทศ เพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบในภายหลัง

๑๔.๗ ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

๑๔.๗.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบสารสนเทศแยกตามหน่วยงานภายในของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๑๔.๗.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาที่รับผิดชอบระบบสารสนเทศของหน่วยเพื่อดำเนินการทบทวนว่ามีรายชื่อที่ออกสิทธิเข้าถึงระบบสารสนเทศไปแล้วหรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๑๔.๗.๓ ผู้บังคับบัญชาของหน่วยแจ้งหรืออนุมัติรายชื่อของผู้มีสิทธิในระบบสารสนเทศที่ได้รับการแก้ไขให้ถูกต้องแล้ว

๑๔.๗.๔ ผู้ดูแลระบบสารสนเทศของหน่วยดำเนินการแก้ไขข้อมูลผู้มีสิทธิให้ถูกต้องตามที่ได้รับแจ้งหรือได้รับการอนุมัติ

ข้อ ๑๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่ดังนี้

๑๕.๑ ผู้ดูแลระบบที่รับผิดชอบระบบนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติโดยต้องกำหนดไว้เป็นลายลักษณ์อักษรอย่างชัดเจน เช่น กำหนดเป็นเอกสารการบริหารจัดการสิทธิ การใช้งานระบบและรหัสผ่าน เป็นต้น

๑๕.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม เอกสารหรือตามระเบียบที่ทางสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยากำหนดขึ้น

๑๕.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณาควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา

๑๕.๓.๑ ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๑๕.๓.๒ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๑๕.๓.๓ มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๖๐ วัน เป็นต้น

ข้อ ๑๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องจัดวิธีการบริหารจัดการ การเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๖.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑๖.๒ ผู้ดูแลฐานข้อมูลหรือเจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๖.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทขึ้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๑๖.๔ การรับส่งข้อมูลสำคัญ ผ่านเครือข่ายสาธารณะผู้ใช้งานควรได้รับ การเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

๑๖.๕ มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสารหรือตามระเบียบที่ทางสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา กำหนดขึ้น

๑๖.๖ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ ออกนอกพื้นที่ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๑๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดการควบคุม การเข้าใช้งานระบบจากภายนอก หน่วยงานที่มีระบบสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งเอาไว้ภายในหน่วยของตนเอง เพื่อดูแลรักษาความปลอดภัยของระบบภายในจากการเข้าถึงระบบจากภายนอกโดยมีแนวทางปฏิบัติ ดังนี้

๑๗.๑ การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาการควบคุมบุคคลที่เข้าสู่ระบบของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา จากระยะไกลจึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๑๗.๒ วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๑๗.๓ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดง หลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาอย่างเพียงพอและต้องได้รับอนุมัติจากผู้บังคับบัญชา

๑๗.๔ มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับการอนุมัติ อย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๑๗.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ข้อ ๑๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกดังนี้ ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องผ่านการพิสูจน์ตัวตนจากระบบของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา โดยมีแนวทางปฏิบัติดังนี้

- ๑๘.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)
- ๑๘.๒ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่าน (Password)
- ๑๘.๓ การเข้าสู่ระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา จากอินเทอร์เน็ตนั้นจะมีการตรวจสอบผู้ใช้งานด้วย
- ๑๘.๔ การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัย จะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

หมวด ๔

การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน

ข้อ ๑๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดวิธีการบริหารจัดการรหัสผ่าน (User Password Management) และการใช้งานรหัสผ่าน (Password Use) ของเจ้าหน้าที่ให้มีความมั่นคงปลอดภัย และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) โดยมีแนวทางปฏิบัติ ดังนี้

- ๑๙.๑ วิธีการบริหารจัดการรหัสผ่าน
 - ๑๙.๑.๑ ต้องเก็บรักษารหัสผ่านที่ได้รับให้เป็นความลับ
 - ๑๙.๑.๒ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
 - ๑๙.๑.๓ ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุล ของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในงานธุรการ
 - ๑๙.๑.๔ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
 - ๑๙.๑.๕ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)
 - ๑๙.๑.๖ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
 - ๑๙.๑.๗ เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
 - ๑๙.๑.๘ การกำหนดรหัสผ่านเริ่มต้นให้กับเจ้าหน้าที่ให้ยากต่อการเดา และกำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกันอีกด้วย
 - ๑๙.๑.๙ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๑๙.๑.๑๐ เมื่อเจ้าหน้าที่ของหน่วยงานลาออก หรือเปลี่ยนแปลงหน้าที่ ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้หน่วยแจ้งผู้รับผิดชอบระบบสารสนเทศทันที เพื่อเปลี่ยนสิทธิ หรือถอดถอนสิทธิของผู้ที่ลาออกออกจากระบบทันทีที่ได้รับแจ้ง

๑๙.๑.๑๑ การส่งมอบรหัสผ่านให้กับเจ้าหน้าที่ต้องเป็นไปอย่างปลอดภัย โดย ใส่ซองปิดผนึก และประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และ แนบเอกสารการได้รับอนุญาตจาก ผู้บังคับบัญชา รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๑๙.๒ การใช้งานรหัสผ่าน

๑๙.๒.๑ ผู้ใช้งานต้องใช้งานรหัสผ่านของตนเองหรือตามที่ได้รับอนุมัติเท่านั้น

๑๙.๒.๒ ผู้ใช้งานรหัสผ่านต้องปฏิบัติให้เป็นไปตามวิธีการบริหารจัดการ รหัสผ่านอย่างเคร่งครัด

๑๙.๒.๓ กรณีต้องการยกเลิกหรือเปลี่ยนแปลงรหัสผ่านให้แจ้งเป็นลายลักษณ์อักษรตามสายการบังคับบัญชาให้ผู้รับผิดชอบดำเนินการต่อไป

๑๙.๒.๔ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่าน

๑๙.๒.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วัน หรือทุกครั้ง ที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๑๙.๒.๖ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของ ผู้ใช้งาน (Username) ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๑๙.๒.๗ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สิน หรือ ระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระยาและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนลื้อค้คีดีหรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

๑๙.๒.๗.๑ คอมพิวเตอร์โน้ตบุ๊ก (Notebook) ต้องทำการ พิสูจน์ตัวตนในการเข้าใช้งานเครือข่ายคอมพิวเตอร์โดยระบุ Mac Address ให้กับผู้ดูแลระบบและได้รับการ Fix IP-Address จากผู้ดูแลระบบก่อนเข้าใช้งานทุกครั้ง

๑๙.๒.๗.๒ คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึง ระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๑๙.๒.๗.๓ การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่าย จะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๑๙.๒.๗.๔ การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการ พิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๑๙.๒.๗.๕ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่อง คอมพิวเตอร์ทุกเครื่องต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานทุกครั้ง

๑๙.๒.๗.๖ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลา พักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๕ นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

๑๙.๓ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๑๙.๓.๑ ผู้ดูแลระบบ (System Administrator) เป็นผู้รับผิดชอบในการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๑๙.๓.๒ วงรอบการทบทวนสิทธิการเข้าถึงของผู้ใช้งานให้ทบทวน ทุกๆ ๑ ปี หรือเมื่อเกิดการเปลี่ยนแปลงสิทธิของผู้ใช้ ได้แก่ การลาออก การย้ายหน่วย เป็นต้น อีกทั้งการ ทบทวนสิทธิต้องพิจารณาถึงพฤติกรรมการทำงานของผู้ใช้ รวมทั้งถ้ามีการเปลี่ยนแปลงของระบบงานใหม่ จะต้องมีการทบทวนสิทธิการเข้าถึงผู้ใช้งานทุกครั้งอีกด้วย

๑๙.๓.๓ การทบทวนสิทธิผู้ดูแลระบบ จะต้องแจ้งรายงานการทบทวนสิทธิเป็นลายลักษณ์อักษรให้ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาอนุมัติให้ดำเนินการต่อไป

หมวด ๕

**การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)**

ข้อ ๒๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องจัดการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Physical Security)

๒๐.๑ กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

๒๐.๒ พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในโดยเฉพาะศูนย์สารสนเทศกลาง (Data Center) ให้ติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

๒๐.๓ มีระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

๒๐.๔ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบยังใช้งานได้ตามปกติ

๒๐.๕ บุคลากรของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาควรปิดประตูและหน้าต่างให้ล็อกอยู่เสมอ

๒๐.๖ ถ้าตรวจพบอุปกรณ์สารสนเทศที่ถูกละทิ้งโดยไม่มีผู้ใช้อยู่ในบริเวณใกล้เคียงให้รีบแจ้งผู้รับผิดชอบดำเนินการเก็บอุปกรณ์ดังกล่าวในสถานที่ปลอดภัย เพื่อป้องกันการโจรกรรมหรือลักลอบขโมยข้อมูลจากผู้ไม่ประสงค์ดีต่อไป

ข้อ ๒๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องจัดการควบคุม การเข้า-ออก (Physical Entry Controls) ดังนี้

๒๑.๑ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

๒๑.๒ ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒๑.๓ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๒๑.๔ สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๒๑.๕ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๒๑.๖ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๒๑.๗ มีการพิสูจน์ตัวตน เช่น การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะในศูนย์ สารสนเทศกลาง (Data Center)

๒๑.๘ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะศูนย์สารสนเทศกลาง (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๒๑.๙ บุคคลภายนอก เช่น เจ้าหน้าที่บริษัท นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่นๆ ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๒๑.๑๐ ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๒๑.๑๑ ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก ในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๒๑.๑๒ จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

ข้อ ๒๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบสิ่งอุปกรณ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas) ดังนี้

๒๒.๑ จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายสิ่งอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒๒.๒ จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๒๒.๓ จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในระบบสารสนเทศของหน่วย

๒๒.๔ ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้น ไปยังพื้นที่ที่มีการใช้งาน

๒๒.๕ ตรวจสอบและลงทะเบียนหรือขึ้นบัญชีคุมสิ่งอุปกรณ์ที่ส่งมอบโดยผู้ถูกจ้าง ผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการสิ่งอุปกรณ์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

ข้อ ๒๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการจัดวางและการป้องกันอุปกรณ์ (Equipment Sitting and Protection) ดังนี้

๒๓.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในห้องศูนย์สารสนเทศกลาง (Data Center) ให้น้อยที่สุด

๒๓.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่ความมั่นคงปลอดภัย

๒๓.๓ ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในศูนย์สารสนเทศกลาง (Data Center)

๒๓.๔ ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิความชื้น ให้อยู่ในระดับปกติหรือไม่

ข้อ ๒๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดระบบ และอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ดังนี้

๒๔.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

๒๔.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS)

๒๔.๑.๒ เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

๒๔.๑.๓ ระบบระบายอากาศ

๒๔.๑.๔ ระบบปรับอากาศ และควบคุมความชื้น

๒๔.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านี้้อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๒๔.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีจากระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๒๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนด และควบคุมการเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security) ดังนี้

๒๕.๑ เครือข่ายของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหายและป้องกันสัตว์ต่างๆ กัดสาย เช่น หนู เป็นต้น

๒๕.๒ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๒๕.๓ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๒๕.๔ จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๒๕.๕ ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิทเพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ ๒๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการบำรุงรักษาอุปกรณ์(Equipment Maintenance) ดังนี้

๒๖.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

๒๖.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามจากผู้ผลิตแนะนำ

๒๖.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๒๖.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๒๖.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วย

๒๖.๖ ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒๖.๗ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๒๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องควบคุมและกำหนดขั้นตอนการนำสิ่งอุปกรณ์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาออกนอกหน่วยงาน (Removal of Property) ดังนี้

๒๗.๑ ให้มีการขออนุญาตก่อนนำสิ่งอุปกรณ์หรือทรัพย์สินออกนอกหน่วย

๒๗.๒ บันทึกข้อมูลการนำสิ่งอุปกรณ์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาออกนอกหน่วย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๒๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดการป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of equipment off-premises)

๒๘.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำสิ่งอุปกรณ์หรือทรัพย์สินของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาออกไปใช้งานนอก

๒๘.๒ ไม่ทิ้งสิ่งอุปกรณ์หรือทรัพย์สินของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาไว้โดยทิ้งในที่สาธารณะ

๒๘.๓ ให้เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๒๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องควบคุมการจำหน่ายสิ่งอุปกรณ์หรือการนำสิ่งอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment) ดังนี้

๒๙.๑ ให้ทำลายข้อมูลสำคัญในสิ่งอุปกรณ์ก่อนที่จะดำเนินการจำหน่ายสิ่งอุปกรณ์ดังกล่าว และดูแลแนวทางปฏิบัติในการทำลายสื่อบันทึกข้อมูลในหมวด ๘

๒๙.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลสำคัญนั้นได้

หมวด ๖

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communications and Operations Management)

ข้อ ๓๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures) ดังนี้

๓๐.๑ จัดทำขั้นตอนปฏิบัติงานอย่างเป็นลายลักษณ์อักษรสำหรับภารกิจการปฏิบัติงานกับระบบเทคโนโลยีสารสนเทศดังต่อไปนี้

๓๐.๑.๑ การปฏิบัติงานในห้องเครื่องคอมพิวเตอร์ที่ให้บริการหรือศูนย์สารสนเทศกลาง (Data Center)

๓๐.๑.๒ การเปิดและปิดระบบงาน เช่น การเปิด - ปิดเครื่อง เปิด - ปิดระบบงาน เปิด - ปิด ระบบให้บริการ เป็นต้น

๓๐.๑.๓ การสำรองข้อมูล

๓๐.๑.๔ การบำรุงรักษาอุปกรณ์

๓๐.๑.๕ การจัดการกับสื่อบันทึกข้อมูล เช่น การทำป้ายชื่อป้องกัน การลบทิ้ง การป้องกันการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง เป็นต้น

๓๐.๑.๖ การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้น

๓๐.๑.๗ การประมวลผลข้อมูล เช่น ขั้นตอนในการนำข้อมูลเข้าระบบงานประมวลผล และแสดงผล เป็นต้น

๓๐.๑.๘ การใช้งานโปรแกรมมอรรถประโยชน์ต่างๆ (Utilities)

๓๐.๑.๙ การรายงานและการจัดการกับปัญหาที่เกิดขึ้น

๓๐.๑.๑๐ การจัดการกับการทำงานล้มเหลวและความผิดพลาดของระบบคอมพิวเตอร์ ระบบงาน และระบบเครือข่าย

๓๐.๑.๑๑ การกู้คืนระบบงานและระบบเครือข่าย

๓๐.๒ กำหนดผู้รับผิดชอบและผู้มีอำนาจในการควบคุมการดำเนินการในการจัดทำเอกสาร ขั้นตอนการปฏิบัติข้างต้น และให้มีการปรับปรุงเอกสารอย่างสม่ำเสมอ

ข้อ ๓๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบเทคโนโลยีสารสนเทศดังนี้

๓๑.๑ กำหนดขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงต่อระบบ เทคโนโลยีสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เช่น ซอฟต์แวร์ ฮาร์ดแวร์ของระบบงาน ซอฟต์แวร์ระบบปฏิบัติการ เป็นต้น ควรมีขั้นตอนการดำเนินการดังต่อไปนี้

๓๑.๑.๑ ระบุและบันทึกที่ระดับผลกระทบและความเร่งด่วนของการเปลี่ยนแปลงที่ขออนุมัติ เช่น มากหรือน้อย เป็นต้น

๓๑.๑.๒ บันทึกรายละเอียดการดำเนินการที่เกี่ยวข้องเพื่อใช้เป็นหลักฐาน

๓๑.๑.๓ กำหนดให้มีการวางแผนการดำเนินการ

๓๑.๑.๔ กำหนดให้มีการทดสอบตามความจำเป็น

๓๑.๑.๕ กำหนดให้มีการแจ้งผู้ที่เกี่ยวข้องทั้งหมด

๓๑.๑.๖ กำหนดให้มีการวางแผนหรือขั้นตอนปฏิบัติสำหรับการ ถอยหลังกลับสำหรับกรณีที่ทำแล้วไม่สำเร็จ

๓๑.๑.๗ กำหนดผู้มีอำนาจในการอนุมัติให้ดำเนินการในการปรับปรุง หรือแก้ไขขั้นตอนปฏิบัติดังกล่าว

ข้อ ๓๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties) ดังนี้

๓๒.๑ กำหนดให้การปฏิบัติงานที่มีความสำคัญแยกหน้าที่ความรับผิดชอบออกจากกัน และมีผู้ปฏิบัติงานมากกว่าหนึ่งคน

๓๒.๒ ป้องกันไม่ให้งานที่มีความสำคัญสามารถดำเนินการได้ตั้งแต่ต้นจนจบได้ด้วยบุคคลเพียงคนเดียว

๓๒.๓ ให้ผู้บังคับบัญชามีการสอดส่องดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย

๓๒.๔ ให้มีการจัดเก็บหลักฐานที่สามารถใช้ตรวจสอบได้ในภายหลังสำหรับงานที่มีความเสี่ยง

ข้อ ๓๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดการแยกระบบสำหรับการพัฒนาการทดสอบ และการให้บริการออกจากกัน (Separation of Development, Test and Operational Facilities) ดังนี้

๓๓.๑ ให้พิจารณาการแยกเครื่องคอมพิวเตอร์ของระบบงานและมาตรการ เพื่อใช้ในการแยกเครื่องคอมพิวเตอร์สำหรับการพัฒนาการทดสอบและการให้บริการออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงานที่มีต่อกัน

๓๓.๒ กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องคอมพิวเตอร์ที่ใช้สำหรับการพัฒนาไปสู่เครื่องที่ใช้สำหรับการให้บริการ

๓๓.๓ ให้มีการป้องกันการเข้าถึงโปรแกรมมัลแวร์ เช่น ซอฟต์แวร์ทูล และยูทิลิตี้ เป็นต้น ที่ใช้สำหรับการพัฒนาระบบงานโดยไม่ได้รับอนุญาตในการเข้าถึงโปรแกรมฯ ดังกล่าว บนเครื่องคอมพิวเตอร์สำหรับการพัฒนา

๓๓.๔ กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกันสำหรับระบบงานที่ใช้ในการพัฒนาทดสอบและให้บริการจริง

ข้อ ๓๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดให้มีการตรวจสอบและติดตามการใช้ทรัพยากรของระบบและเครือข่ายคอมพิวเตอร์ ดังนี้

๓๔.๑ จัดทำแผนการตรวจสอบและติดตามทรัพยากรของระบบสารสนเทศ ดังนี้

๓๔.๑.๑ กำหนดประเภทของข้อมูลที่ใช้ในการตรวจสอบและติดตามการใช้ทรัพยากรของระบบ เช่น ร้อยละของการใช้ซีพียู ร้อยละของการใช้หน่วยความจำ ร้อยละของการใช้พื้นที่ฮาร์ดดิสก์ และร้อยละของปริมาณการใช้เครือข่าย เป็นต้น

๓๔.๑.๒ กำหนดค่าปริมาณการใช้ทรัพยากรสูงสุดบนระบบที่ยอมรับได้ค่าต่างๆเหล่านี้ใช้สำหรับเป็นจุดในการแจ้งเตือนว่าระบบสารสนเทศได้มีการใช้ทรัพยากรมาจนถึงค่าสูงสุดที่ยอมรับได้แล้วหรือไม่ เช่น กำหนดไว้ที่ร้อยละ ๘๐ ของการใช้ซีพียู เป็นต้น

๓๔.๑.๓ กำหนดความถี่ในการเข้าตรวจสอบปริมาณการใช้ทรัพยากรของระบบสารสนเทศสำหรับระบบที่มีความสำคัญจากมากไปน้อยให้กำหนดแผนการตรวจสอบและติดตามทรัพยากรของระบบด้วยความถี่ในการตรวจสอบจากสูงไปต่ำ เช่น ระบบที่มีความสำคัญมากควรมีความถี่ในการตรวจสอบสูงกว่าระบบที่มีความสำคัญปานกลางและน้อย เป็นต้น

๓๔.๒ ติดตามและตรวจสอบทรัพยากรของระบบตามแผนการตรวจสอบและติดตามทรัพยากรของระบบฯ ที่ได้กำหนดไว้เพื่อดูว่ายังมีทรัพยากรเพียงพอต่อการให้บริการหรือไม่

๓๔.๓ รายงานข้อมูลผลการติดตามการใช้ทรัพยากรของระบบสารสนเทศ เช่น สถิติปริมาณการใช้ซีพียู หน่วยความจำฮาร์ดดิสก์ และปริมาณเครือข่ายคอมพิวเตอร์ ให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

๓๔.๔ ประเมินความต้องการทรัพยากรของระบบสารสนเทศที่ต้องการเพิ่มเติม เพื่อนำไปใช้ในการวางแผนปรับปรุงประสิทธิภาพและขีดความสามารถของระบบต่อไป

หมวด ๗

การป้องกันชุดคำสั่งไม่พึงประสงค์ (Protection Against Malicious Code)

ข้อ ๓๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ดังนี้

๓๕.๑ ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอกรวมทั้งการใช้แฟ้มข้อมูล (File) อื่นที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาไม่อนุญาตให้ใช้งาน

๓๕.๒ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๓๕.๓ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันชุดคำสั่งไม่พึงประสงค์ให้กับระบบเทคโนโลยีสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา และอัปเดตซอฟต์แวร์ป้องกันชุดคำสั่งไม่พึงประสงค์เป็นประจำสม่ำเสมอ

๓๕.๔ ให้ผู้ดูแลระบบดำเนินการตรวจสอบชุดคำสั่งไม่พึงประสงค์ในเครื่องคอมพิวเตอร์ ที่ให้บริการและอุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ในบริเวณจุดทางเข้า-ออกเครือข่ายอย่างสม่ำเสมอเพื่อ ดักจับชุดคำสั่งไม่พึงประสงค์ที่จะเข้าสู่ระบบ

๓๕.๕ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับชุดคำสั่งไม่พึงประสงค์ได้แก่การรายงานการเกิดขึ้นของชุดคำสั่งไม่พึงประสงค์ การวิเคราะห์ การจัดการ การกู้คืนระบบ จากความเสียหายที่ตรวจพบ เป็นต้น

๓๕.๖ มีการติดตามข้อมูลข่าวสารเกี่ยวกับชุดคำสั่งไม่พึงประสงค์อย่างสม่ำเสมอ

๓๕.๗ ให้มีการสร้างความตระหนักเกี่ยวกับชุดคำสั่งไม่พึงประสงค์เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุชุดคำสั่งไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร รวมทั้งให้หน่วยมีการจัดการฝึกอบรมสร้างความตระหนักอย่างน้อยปีละ ๑ ครั้ง

หมวด ๘

การจัดการเข้าถึงข้อมูลสารสนเทศและโปรแกรมประยุกต์

ข้อ ๓๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการจัดการกับข้อมูลในแต่ละชั้นความลับ ดังนี้

๓๖.๑ กำหนดระดับชั้นความลับของข้อมูลซึ่งอย่างน้อยประกอบด้วย ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายใน และข้อมูลลับ

๓๖.๒ กำหนดแนวทางในการจัดหมวดหมู่ข้อมูลเป็นชั้นความลับที่เหมาะสมซึ่งควร พิจารณาจัดหมวดหมู่จาก

๓๖.๒.๑ แหล่งที่มาของข้อมูล เช่น หากข้อมูลนั้นมาจากภายนอก และเป็น ข้อมูลลับ ชั้นความลับก็จะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับก็จะเป็น ประเภทเปิดเผยได้ เป็นต้น

๓๖.๒.๒ วิธีการนำไปใช้ประโยชน์ เช่น หากข้อมูลนั้นสามารถนำไปใช้ ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบต่อด้านระบบงบประมาณของหน่วย ดังนั้นข้อมูลนี้จะ อยู่ในประเภทลับ เป็นต้น

๓๖.๒.๓ จำนวนบุคคลที่ควรรับทราบ เช่น หากข้อมูลนั้นสามารถเปิดเผย ต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

๓๖.๒.๔ ผลกระทบหากมีการเปิดเผย เช่น หากข้อมูลนั้นถูกเปิดเผยจะมี ผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการงบประมาณ ด้านการไม่ปฏิบัติตามกฎระเบียบข้อบังคับ ที่หน่วยกำหนดต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้นข้อมูลจะสามารถจัดอยู่ใน ประเภทใช้ภายในเท่านั้น หรือประเภทชั้นความลับ เป็นต้น

๓๖.๓ กำหนดขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับ ชั้นตอนๆ ควรประกอบด้วย การควบคุมการประมวลผล การควบคุมการเข้าถึง การจัดเก็บ การจัดการกับสื่อ บันทึก ข้อมูล การทำป้าย ปังซี และการสื่อสารข้อมูลอย่างมั่นคงปลอดภัย

๓๖.๔ กำหนดให้มีการจำกัดการเข้าถึงข้อมูลสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓๖.๕ กำหนดมาตรการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลสำคัญที่ยังคงค้างอยู่บนสื่อบันทึกข้อมูลนั้น โดยอาจปฏิบัติตามแนวทางดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การตัดด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้การตัดด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการฟอร์แมตเป็นจำนวนหลายรอบ)

๓๖.๖ กำหนดมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้อง และสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

๓๖.๗ กำหนดมาตรการป้องกันข้อมูลสำคัญที่มีการส่งพิมพ์ออกมาทางเครื่องพิมพ์เพื่อป้องกันการเข้าถึงโดยผู้อื่น

๓๖.๘ จัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๓๖.๙ มาตรการในการนำวิธีการเข้ารหัสมาใช้กับข้อมูลชั้นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และระเบียบสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ว่าด้วยการรักษาความปลอดภัยทางการอักษรลับ พ.ศ. ๒๕๑๕

ข้อ ๓๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดการสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System Documentation) ดังนี้

๓๗.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๓๗.๒ ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๓๗.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น เพื่อป้องกันการเข้าถึงหรือ เปลี่ยนแปลงแก้ไขเอกสารนั้น

ข้อ ๓๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดนโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures) ดังนี้

๓๘.๑ จัดทำนโยบายหรือแนวทางการใช้อย่างเหมาะสมสำหรับการใช้งานระบบ หรือ อุปกรณ์ที่ใช้ในการสื่อสารข้อมูลระหว่างสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาเช่น ห้ามใช้เพื่อก่อความรำคาญ แก่ผู้อื่น ทำให้ผู้อื่น สูญเสียชื่อเสียง ปลอดภัยเป็นบุคคลอื่น เป็นต้น

๓๘.๒ มีวิธีการทางเทคนิคป้องกันข้อมูลสำคัญจากการถูกเข้าถึง ถูกเปลี่ยนแปลง แก้ไข ถูกสวมรอยโดยผู้อื่น ถูกเปิดเผยความลับ โดยไม่ได้รับอนุญาต

๓๘.๓ จัดทำแนวทางสำหรับการจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับ ข้อมูลหรือเอกสารโต้ตอบ และแนวทางตรวจสอบคล้อยกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่ หน่วยต้องปฏิบัติตาม

ข้อ ๓๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements) โดยมีแนวทางข้อตกลงสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายในกับหน่วยงานภายนอกดังต่อไปนี้

๓๙.๑ กำหนดนโยบายขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึก ข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๓๙.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการ แลกเปลี่ยนข้อมูล เช่น วิธีการส่ง วิธีการรับ เป็นต้น

๓๙.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๓๙.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับ ข้อมูลเพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบ

๓๙.๕ กำหนดความรับผิดชอบสำหรับกรณีข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหาย หรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น

๓๙.๖ กำหนดสิทธิการเข้าถึงข้อมูล

๓๙.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๓๙.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ข้อ ๔๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดระบบสารสนเทศทางตามภารกิจที่ได้รับมอบที่มีการเชื่อมโยงถึงกัน พิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบ เทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างหน่วยงานภายใน สถาบันจิตเวชศาสตร์ สมเด็จเจ้าพระยาหรือหน่วยงานอื่นๆ ที่จะมาขอเชื่อมโยงกับสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เป็นต้นดังนี้

๔๐.๑ กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

๔๐.๒ พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๔๐.๓ พิจารณาว่ามีกำลังพลใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

๔๐.๔ พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

๔๐.๕ ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลที่กำหนดชั้นความลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ข้อ ๔๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการหมดเวลาหรือหมดอายุการใช้งานระบบสารสนเทศ (Session Time-out) ดังนี้

๔๑.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานอุปกรณ์เครือข่าย เป็นต้น มีการตัดการติดต่อและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการ ใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๔๑.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดการติดต่อและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานที่มีข้อมูลสำคัญ ระบบงานที่กำหนดชั้นความลับ เป็นต้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔๑.๓ แนวทางปฏิบัติดังนี้

๔๑.๓.๑ เมื่อผู้ใช้งานไม่ได้ใช้งานหรือว่างเว้นจากการใช้งานในระยะเวลา ๕ นาทีหรือตามที่ผู้รับผิดชอบกำหนดให้มีการตัดการเชื่อมต่อการใช้งานออกจากระบบสารสนเทศ โดยอัตโนมัติ

๔๑.๓.๒ ถ้ามีความพยายามเข้าสู่ระบบใหม่ ให้ยืนยันการใช้งานโดยใส่ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หรือวิธีการที่ปลอดภัยในการยืนยันตัวบุคคลในทุกๆ ครั้ง

ข้อ ๔๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time) ดังนี้

๔๒.๑ กำหนดให้ระบบสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น

๔๒.๒ กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกหน่วย) ระบบงานที่กำหนดชั้นความลับ เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อเพื่อป้องกันบุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึงข้อมูลได้โดยง่าย

๔๒.๓ แนวทางปฏิบัติดังนี้

๔๒.๓.๑ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา กำหนดให้ใช้งานได้ ๒ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หรือตามที่ผู้บังคับบัญชาเห็นสมควร

๔๒.๓.๒ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น

๔๒.๓.๓ การเชื่อมต่อเข้าสู่ระบบสารสนเทศของสถาบันจิตเวชศาสตร์ สมเด็จพระเจ้าพระยาถ้ากระทำในช่วงนอกเวลาทำงานตามปกติ ต้องได้รับอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ ๔๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา ต้องกำหนดคุณสมบัติของการล็อกอิน (Login) ที่มีความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ สำหรับเครื่องคอมพิวเตอร์ให้บริการหรืออุปกรณ์เครือข่ายคอมพิวเตอร์ที่หน่วยรับผิดชอบ ดังนี้

๔๓.๑ ไม่มีหรือไม่แสดงฟังก์ชัน (Function) ให้การช่วยเหลือในระหว่างที่ทำการล็อกอิน (Login)

๔๓.๒ บันทึกความพยายามในการล็อกอินทั้งที่สำเร็จและไม่สำเร็จและแสดงประวัติการล็อกอิน ๓ ครั้งล่าสุด

๔๓.๓ ตัดการเชื่อมต่อหลังจากที่ทำการล็อกอินไม่สำเร็จเกินกว่า ๓ ครั้ง

๔๓.๔ เมื่อมีการใส่ข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้องให้แสดง ข้อความรวมๆ เช่น “ข้อมูลการล็อกอิน ไม่ถูกต้อง”

๔๓.๕ ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยาการใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงาน หากมีการตรวจพบ อาจมีการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม สถาบันจิตเวชศาสตร์ สมเด็จพระเจ้าพระยามีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว”

๔๓.๖ ไม่แสดงรายละเอียดของระบบใดๆ จนกว่าจะล็อกอินสำเร็จ

ข้อ ๔๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยา ต้องกำหนดการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging) ของระบบงานภายในสถาบันจิตเวชศาสตร์สมเด็จพระเจ้าพระยาดังนี้ จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งานข้อมูลโดยการจับเก็บ Audit Log เป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้ เพื่อตรวจสอบว่าใครเข้ามาใช้งานระบบการตรวจสอบการบุกรุก รวมไปถึงการตรวจสอบข้อผิดพลาดที่เกิดขึ้น โดยจัดทำรายงานเบื้องต้นสรุปข้อมูลว่า ใคร (Who) ทำอะไร (What) เมื่อไหร่ (When) ที่ไหน (Where) และอย่างไร (How) ดังนั้นข้อมูลที่ควรจัดเก็บมีดังนี้

๔๔.๑ ข้อมูลชื่อบัญชีผู้ใช้ระบบงาน

๔๔.๒ ข้อมูลวันเวลาที่เข้าถึงระบบงาน

๔๔.๓ ข้อมูลวันเวลาที่ออกจากระบบงาน

๔๔.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๔๔.๕ ข้อมูลชื่อเครื่องคอมพิวเตอร์ที่ใช้ใช้งาน

๔๔.๖ ข้อมูลการเข้าถึงระบบ (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

๔๔.๗ ข้อมูลความพยายามในการเข้าถึงทรัพยากร เช่น ข้อมูลบัญชีผู้ใช้งาน ข้อมูลสำคัญของระบบงาน เป็นต้น ทั้งที่สำเร็จและไม่สำเร็จ

๔๔.๘ ข้อมูลการเปลี่ยนแปลงสิ่งแวดล้อมหรือการกำหนดค่า (Configuration) ของระบบงาน

๔๔.๙ ข้อมูลแสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบ เป็นต้น

๔๔.๑๐ ข้อมูลแสดงการใช้งานโปรแกรมประยุกต์ (Application Program)

๔๔.๑๑ ข้อมูลแสดงการเข้าถึงแฟ้มข้อมูล (File) และการกระทำกับแฟ้มข้อมูล (File) เช่น เปิด ปิด เขียน อ่านแฟ้มข้อมูล เป็นต้น

๔๔.๑๒ ข้อมูลไอพีแอดเดรสที่เข้าถึง

๔๔.๑๓ ข้อมูลโพรโตคอลของเครือข่ายที่ใช้งาน

๔๔.๑๔ ข้อมูลการแจ้งเตือนเกี่ยวกับการเข้าถึงระบบจากการบุกรุก

๔๔.๑๕ ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

๔๔.๑๖ ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญ

๔๔.๑๗ ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

หมวด ๙

การบริหารจัดการการเข้าถึงระบบเครือข่ายสื่อสารข้อมูล

ข้อ ๔๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดมาตรการทางเครือข่ายสื่อสารข้อมูล (Network Controls) เพื่อป้องกันข้อมูลในเครือข่ายระบบงาน หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๔๕.๑ กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติ สำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

๔๕.๒ กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งาน และอุปกรณ์ที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๔๕.๓ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญ เมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

๔๕.๔ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๔๕.๕ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๔๕.๖ มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่าย เพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๔๕.๗ มีการใช้ฮาร์ดแวร์หรือซอฟต์แวร์ สำหรับการบริหารจัดการเครือข่าย เพื่อระบุเฝ้าตรวจ ติดตามสถานะ อุปกรณ์ในระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

ข้อ ๔๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการควบคุมการเข้าถึงระบบเครือข่ายดังนี้

๔๖.๑ ผู้ดูแลระบบ ต้องมีการออกแบบแบ่งระบบเครือข่ายตามกลุ่มของบริการ ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น เขตภายใน (Internal Zone) เขตภายนอก (External Zone) เป็นต้น เพื่อเป็นการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๔๖.๒ ผู้ดูแลระบบ ควรดำเนินการแยกและติดตั้ง เครื่องคอมพิวเตอร์ให้บริการไว้ในวงเครือข่ายที่แยกต่างหากจากวงเครือข่ายของผู้ใช้งาน และใช้ Firewall หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อจำกัดให้เฉพาะกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้น จึงจะสามารถเชื่อมต่อเข้าไปยังเครื่องคอมพิวเตอร์ให้บริการนั้นได้ และสำหรับแนวทางปฏิบัติการใช้งานของไฟร์วอลล์ (Firewall) ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยามีดังนี้

๔๖.๒.๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

๔๖.๒.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๔๖.๒.๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๔๖.๒.๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login Account ก่อนการใช้งานทุกครั้ง

๔๖.๒.๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าให้บริการ และการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๔๖.๒.๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๔๖.๒.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๔๖.๒.๘ การกำหนดระเบียบในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาก่อน

๔๖.๒.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

๔๖.๒.๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๔๖.๒.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๔๖.๒.๑๒ ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

๔๖.๒.๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาต ดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

๔๖.๒.๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตหรือเชื่อมต่อเครือข่ายภายในโดยทันที

๔๖.๓ การเข้าสู่ระบบเครือข่ายภายในของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาโดยผ่านทางอินเทอร์เน็ต จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ ในทุกกรณี

๔๖.๔ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๔๖.๕ ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๔๖.๖ ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ เช่น ในการเชื่อมต่อเข้าสู่เครื่องคอมพิวเตอร์ให้บริการเพื่อบริหารจัดการระบบ ให้กำหนดเฉพาะชุดไอพีแอดเดรสของผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงเครื่องคอมพิวเตอร์ให้บริการนั้นได้

๔๖.๗ ผู้ดูแลระบบ ตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๔๖.๘ กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า ตัวแปร (Parameter) ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนด ค่าตัวแปร (Parameter) ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๔๖.๙ ระบบเครือข่ายทั้งหมดของหน่วยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ เป็นต้น

๔๖.๑๐ มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง และสำหรับแนวทางปฏิบัติการใช้งานของอุปกรณ์ป้องกันการบุกรุก (IDS/IPS) ดังนี้

๔๖.๑๐.๑ เป็นการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๔๖.๑๐.๒ ให้ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ทั้งที่เชื่อมต่อสู่เครือข่ายภายนอก และ เครือข่ายภายในทุกเส้นทาง

๔๖.๑๐.๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากเครือข่ายภายนอกหรือเครือข่ายสาธารณะต่างๆ จะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๔๖.๑๐.๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๔๖.๑๐.๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๔๖.๑๐.๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

๔๖.๑๐.๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๔๖.๑๐.๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๔๖.๑๐.๙ เครื่องคอมพิวเตอร์ที่ให้บริการที่มีการติดตั้ง Host-Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๔๖.๑๐.๑๐ พฤติกรรมการใช้งานกิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๔๖.๑๐.๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๔๖.๑๐.๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๔๖.๑๐.๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผนเผชิญเหตุที่เกิดขึ้น

๔๖.๑๐.๑๔ ผู้ดูแลระบบมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของ เครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๔๖.๑๐.๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดระเบียบของสถาบันจิตเวชศาสตร์สมเด็จพระยาการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อ การทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการ กระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของสถาบันจิตเวชศาสตร์ สมเด็จพระยา จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมายต่อไป

๔๖.๑๑ การเข้าสู่ระบบงานเครือข่ายภายในหน่วย ผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๔๖.๑๒ ข้อมูลหมายเลขชุดอินเทอร์เน็ตของคอมพิวเตอร์ (IP Address) ภายใน (Local) ของระบบงานเครือข่ายภายในของหน่วยจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศของหน่วยได้โดยง่าย

๔๖.๑๓ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๔๖.๑๔ การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๔๖.๑๕ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศของหน่วย และจะต้องจัดทำเป็นบัญชีไว้สำหรับระบุอุปกรณ์บนเครือข่ายได้

๔๖.๑๖ การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงาน ของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึก ดังกล่าวไว้ อย่างน้อยกว่า ๓ เดือน หรือไม่ต่ำกว่า ๙๐ วัน

๔๖.๑๗ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

หมวด ๑๐ การควบคุม

การพัฒนาหรือจัดหาระบบงาน (Control of Application Development or Acquisition)

ข้อ ๔๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จพระยาต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัยเพียงพอ ดังนี้

๔๗.๑ ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษรข้อกำหนดดังกล่าวอย่างน้อยควรมี

๔๗.๑.๑ คุณสมบัติของการล็อกอินเข้าสู่ระบบงานที่มีความมั่นคงปลอดภัยของระบบสารสนเทศ ตามหมวด ๘

๔๗.๑.๒ การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับเข้าถึงระบบสารสนเทศตามหมวด ๔

๔๗.๑.๓ การเข้ารหัสข้อมูลสำคัญที่มีการรับ - ส่งข้อมูลระหว่างเครื่องผู้ใช้งานกับเครื่องคอมพิวเตอร์ให้บริการ

๔๗.๑.๔ การเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

๔๗.๑.๕ การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ - ๓๐ นาที เป็นต้น

๔๗.๑.๖ การบันทึกบัญชีชื่อผู้ใช้งานที่ล็อกอินเข้าระบบ หมายเลขไอพีแอดเดรส วันเวลาที่เข้าใช้ระบบ ความสำเร็จหรือไม่สำเร็จในการล็อกอินของผู้ใช้งาน

๔๗.๒ พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคง ปลอดภัยของระบบสารสนเทศที่ระบุไว้

๔๗.๓ พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสําหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

๔๗.๔ กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบนำเสนอแผนดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้บังคับบัญชาหรือผู้ที่ได้รับการมอบอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้ผู้บังคับบัญชาได้รับทราบ เพื่อให้คำแนะนำในการปรับปรุงต่างๆ ที่จำเป็น แผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

๔๗.๔.๑ แผนการทดสอบ UAT (User Acceptance Test)

๔๗.๔.๒ แผนการทดสอบ System Integration Test

๔๗.๔.๓ แผนการทดสอบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Test)

๔๗.๕ ไม่อนุญาตการนำข้อมูลสำคัญของสถาบันจิตเวชศาสตร์สมเด็จพระยาไปใช้ในการทดสอบกับ ระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชา ระดับสูงก่อนและหากเป็นไปได้ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไปให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

หมวด ๑๑

การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์ที่ให้บริการ (Server)

ข้อ ๔๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ (Control of Operational Software)

๔๘.๑ ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของหน่วยเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

๔๘.๒ ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้นที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วย

๔๘.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๔๘.๔ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๔๘.๕ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงาน เป็นต้น

๔๘.๖ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๔๘.๗ ทำการปรับปรุงไลบรารีสำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัย และสอดคล้องกับทั้งหมดที่การติดตั้ง

๔๘.๘ ในกรณีที่เป็นกรติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกูเรชัน หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

๔๘.๙ ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้งให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

๔๘.๑๐ ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่นๆ

๔๘.๑๑ สำหรับซอฟต์แวร์ที่จะทำการติดตั้งให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

๔๘.๑๒ ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ที่จะทำการติดตั้งอย่างเคร่งครัด

๔๘.๑๓ สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้

๔๘.๑๔ ติดตั้งโปรแกรมแก้ไขช่องโหว่ต่างๆ (Patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการโปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๔๘.๑๕ ตรวจสอบและปิดพอร์ต (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

๔๘.๑๖ จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

๔๘.๑๗ จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้น จึงจะสามารถเชื่อมต่อเพื่อเข้าสู่ระบบงานที่ทำการติดตั้งนั้น

ข้อ ๔๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating System Changes) ดังนี้

๔๙.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๔๙.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงานรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

หมวด ๑๒

การจ้างงานหน่วยงานภายนอกให้บริการด้านเทคโนโลยีสารสนเทศ (Information Technology Service Delivery)

ข้อ ๕๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องกำหนดแนวทางการควบคุมการจ้างงานสำหรับการให้บริการด้านเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ดังนี้

๕๐.๑ จัดให้มีการควบคุมโครงการที่มีการจัดจ้างดำเนินการโดยหน่วยงานภายนอก

๕๐.๒ กำหนดให้มีการประเมินและจัดทำแผนการลดความเสี่ยงสำหรับกรณีการเข้าถึงระบบงานหรือสารสนเทศโดยหน่วยงานภายนอก โดยปฏิบัติตามแนวทางการประเมินตามหมวด ๒๑

๕๐.๓ กำหนดให้มีการอ้างอิงข้อปฏิบัติที่เกี่ยวข้องในระเบียบของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาฉบับนี้ไว้ในสัญญาจ้างเพื่อให้ผู้รับจ้างปฏิบัติตามอย่างเคร่งครัด

๕๐.๔ กำหนดให้มีการทำสัญญาการไม่เปิดเผยข้อมูลสำคัญที่ได้รับจากสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาให้แก่ผู้อื่น

๕๐.๕ สำหรับบริการต่างๆ ที่เป็นงานให้บริการตามวงรอบระยะเวลาที่กำหนดไว้ หรือตามคำร้องขอจากหน่วยงานผู้ว่าจ้าง เช่น บริการบำรุงรักษาฮาร์ดแวร์ บริการแก้ไขปัญหาฮาร์ดแวร์ บริการแก้ไขปัญหาระบบงาน บริการจ้างในลักษณะ Help Desk ให้กำหนดรายละเอียดการบริการหรือตามที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยากำหนดลงในสัญญาจ้างดังนี้

- ๕๐.๕.๑ รายละเอียดของบริการ
- ๕๐.๕.๒ ระดับการให้บริการ (Service Level Agreement)
- ๕๐.๕.๓ ผู้รับผิดชอบในการเฝ้าระวังหรือติดตามการให้บริการ
- ๕๐.๕.๔ วิธีการติดตามการให้บริการ
- ๕๐.๕.๕ วงรอบระยะเวลาที่ชัดเจนของการทบทวนการปฏิบัติงาน เช่น ทุก

๓ เดือน เป็นต้น

- ๕๐.๕.๖ รูปแบบของรายงานที่ต้องการและความถี่ในการจัดส่งรายงาน

๕๐.๖ กำหนดให้มีการติดตามการให้บริการตามข้อ ๕๐.๕ อย่างสม่ำเสมอ และบันทึกผลการติดตามนั้นไว้ด้วย

๕๐.๗ ทบทวนการให้บริการตามข้อ ๕๐.๕ จากผลการปฏิบัติงานในช่วงเวลาที่ผ่านมา หรือผลที่ได้บันทึกไว้ร้องขอให้ผู้ให้บริการปรับปรุงการให้บริการเพิ่มเติมตามที่ต้องการ และ/หรือ แก้ไขสัญญาจ้างตามความเหมาะสมและจำเป็น

๕๐.๘ กรณีการจ้างพัฒนาซอฟต์แวร์หรือระบบงานโดยหน่วยงานภายนอก (Outsourced Software Development) ให้ปฏิบัติตามแนวทางดังนี้

๕๐.๘.๑ กำหนดให้มีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยของซอฟต์แวร์หรือระบบงานที่จะทำการพัฒนาขึ้นมาอย่างเป็นลายลักษณ์อักษร

๕๐.๘.๒ ควรพิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนาซอฟต์แวร์ที่มีการจัดจ้างดำเนินการจากผู้รับจ้างภายนอก

๕๐.๘.๓ ควรพิจารณากำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้รับจ้างภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้รับจ้างภายนอกนั้น

๕๐.๘.๔ ให้มีการตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์ในซอฟต์แวร์ต่างๆ ที่ถูกพัฒนาขึ้นก่อนดำเนินการติดตั้งหรือทดสอบการใช้งานจริง

หมวด ๑๓
การตรวจสอบการใช้งานระบบ
(Monitoring System Use)

ข้อ ๕๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่ใช้งานเพื่อกำหนดแนวทางในการเฝ้าระวังและดูแลระบบเหล่านั้น และกำหนดให้มีการเฝ้าระวังและดูแลระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่หน่วยต้องปฏิบัติตามอย่างสม่ำเสมอ โดยการตรวจสอบดังต่อไปนี้

- ๕๑.๑ ชื่อบัญชีผู้ใช้งาน
- ๕๑.๒ กิจกรรมการใช้งานและประเภทของกิจกรรม
- ๕๑.๓ วัน/เวลาที่เข้าถึง
- ๕๑.๔ แพ้มข้อมูลหรือข้อมูลที่ถูกเข้าถึง
- ๕๑.๕ โปรแกรมทั่วไปและอรรถประโยชน์ต่างๆ (Utilities) ที่ถูกเรียกใช้งาน
- ๕๑.๖ การใช้บัญชีผู้ใช้งานในระดับสูง เช่น Supervisor, Root, Administrator เป็นต้น
- ๕๑.๗ การเปิด - ปิดการทำงานของระบบ
- ๕๑.๘ การถอดถอนหรือติดตั้งอุปกรณ์สำหรับนำเข้าและส่งออกข้อมูล (I/O) เช่น ฮาร์ดดิสก์ เป็นต้น
- ๕๑.๙ การใช้คำสั่งของผู้ใช้งานที่ได้รับการปฏิเสธโดยระบบ เช่น พยายามใช้คำสั่งทั้งที่ไม่มีสิทธิการพยายามเข้าถึงระบบอย่างไม่ถูกต้อง เป็นต้น
- ๕๑.๑๐ ความพยายามในการเข้าถึงข้อมูลหรือทรัพยากรของระบบที่ได้รับการปฏิเสธโดยระบบ
- ๕๑.๑๑ การแจ้งเตือนจากไฟร์วอลล์หรือระบบป้องกันการบุกรุก
- ๕๑.๑๒ การแจ้งเตือนจากอุปกรณ์แจ้งเตือน (Console) ของผู้ดูแลระบบ
- ๕๑.๑๓ การแจ้งเตือนเมื่อระบบทำงานผิดปกติ เช่น ฮาร์ดดิสก์เต็ม เป็นต้น
- ๕๑.๑๔ การแจ้งเตือนจากโปรแกรมบริหารจัดการเครือข่าย
- ๕๑.๑๕ การแจ้งเตือนการทำงานของระบบล้มเหลวหรือหยุดชะงัก
- ๕๑.๑๖ ความพยายามในการเปลี่ยนแปลงค่าการติดตั้งระบบ (Configuration) ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

หมวด ๑๔

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์คอมพิวเตอร์ (Use of Personal Computers and Computer Devices)

ข้อ ๕๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดแนวทางปฏิบัติในการใช้งานทั่วไป

๕๒.๑ เครื่องคอมพิวเตอร์ที่หน่วยอนุญาตให้ผู้ใช้ ใช้งานเป็นสิ่งอุปกรณ์หรือทรัพย์สินของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาดังนั้นผู้ซึ่งจควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่อ งานของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาเท่านั้น

๕๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วย ต้องเป็นโปรแกรม ที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอก โปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิด กฎหมาย

๕๒.๓ ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่อง คอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

๕๒.๔ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่น ที่มีไขของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาเชื่อมต่อเข้ากับระบบและเครือข่ายคอมพิวเตอร์ของสถาบัน จิตเวชศาสตร์สมเด็จเจ้าพระยา

๕๒.๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้อง ดำเนินการโดยเจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ที่ได้ทำสัญญากับสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาเท่านั้น

๕๒.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัส โดย โปรแกรมป้องกันไวรัส

๕๒.๗ ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่อง

ข้อ ๕๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดแนวทางปฏิบัติในการใช้รหัสผ่าน ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน เอกสารที่หน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

ข้อ ๕๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการป้องกันจากโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ (Malware) ดังนี้

๕๔.๑ ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่นๆ เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของสถาบันจิตเวชศาสตร์ สมเด็จเจ้าพระยา

๕๔.๒ ผู้ใช้งานควรตรวจสอบแฟ้ม (File) ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (E-mail) หรือแฟ้ม (File) ที่ได้รับ (Download) มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๕๔.๓ ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นๆ เกิดความเสียหาย ถูกทำลาย แก้ไข เปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๕๕ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการสำรองข้อมูลและการกู้คืนดังนี้

๕๕.๑ ผู้ใช้งานคอมพิวเตอร์ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๕๕.๒ ผู้ใช้งานคอมพิวเตอร์มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

หมวด ๑๕

การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

(Use of Notebook Computer)

ข้อ ๕๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดแนวทางปฏิบัติการใช้งานทั่วไป ดังนี้

๕๖.๑ เครื่องคอมพิวเตอร์แบบพกพาที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา อนุญาตให้ผู้ใช้งานเป็นสิ่งอุปกรณ์หรือทรัพย์สินของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ดังนั้นผู้ใช้งานควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เท่านั้น

๕๖.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องเป็นโปรแกรมที่สถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๕๖.๓ ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๕๖.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๕๖.๕ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๕๖.๖ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา ปลายดินสอ กดสัมผัส หน้าจอแสดงผลให้เป็นรอยขีดข่วนหรือทำให้จอแสดงผลของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๕๖.๗ ไม่วางของที่มีน้ำหนักมากทับบนหน้าจอแสดงผลและแป้นพิมพ์

๕๖.๘ การขีดทำความสะอาดหน้าจอแสดงผลควรเช็คอย่างเบาเมื่อที่สุด และควรเช็คไปในแนวทางเดียวกันห้ามขีดแบบหมุนวน เพราะจะทำให้หน้าจอแสดงผลมีรอยขีดข่วนได้

ข้อ ๕๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดความปลอดภัยทางด้านกายภาพ ดังนี้

๕๗.๑ ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรเก็บเครื่องไว้ในสถานที่ที่มีอุปกรณ์ป้องกันขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

๕๗.๒ ผู้ใช้ไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้นฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ ๕๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการ ควบคุมการเข้าถึงระบบปฏิบัติการ ดังนี้

๕๘.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๕๘.๒ ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตามที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

๕๘.๓ ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาหน้าจอแสดงผล (Screen Saver) โดยตั้งเวลาในกรณีไม่ได้ใช้งานในห้วงระยะเวลาขณะหนึ่ง เช่น ตั้งไว้ ๑๐ นาที เป็นต้น ให้ทำการปิดกั้นการ ใช้งาน (Lock) สำหรับหน้าจอแสดงผล หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๕๘.๔ ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอแสดงผลเป็นเวลานาน

๕๘.๕ ห้ามบันทึกชื่อผู้ใช้งานและรหัสผ่านไว้บนสถานที่ที่พบเห็นได้ง่าย เช่น บันทึกไว้บนอุปกรณ์คอมพิวเตอร์ บันทึกไว้บนโต๊ะทำงาน เป็นต้น

ข้อ ๕๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดแนวทางปฏิบัติในการใช้รหัสผ่าน ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

ข้อ ๖๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดการสำรองข้อมูลและการกู้คืน ดังนี้

๖๐.๑ ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาโดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

๖๐.๒ ผู้ใช้ควรที่จะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๖๐.๓ แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

๖๐.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้นำไปใช้งานได้ อีกให้ปฏิบัติตามแนวทางการทำลายสื่อบันทึกข้อมูลในหมวด ๘

หมวด ๑๖
การใช้งานอินเทอร์เน็ต
(Use of the Internet)

ข้อ ๖๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดแนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตดังนี้

๖๑.๑ ให้ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS/IDS เป็นต้น

๖๑.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตเพื่อใช้งานโปรแกรมเข้าชมเว็บไซต์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่โปรแกรมเข้าชมเว็บไซต์ติดตั้งอยู่ก่อนการใช้งาน

๖๑.๓ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๖๑.๔ ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา โดยผ่านความเห็นชอบจากผู้บังคับบัญชา

๖๑.๕ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับทางราชการและที่เกี่ยวข้องกับสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา โดยไม่ได้รับอนุญาตอย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต เช่น เอกสารที่กำหนดชั้นความลับร่างหนังสือ ประกาศหรือคำสั่งต่างๆ เป็นต้น

๖๑.๖ ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๖๑.๗ การใช้งานกระดานสนทนา (Web Board) ของหน่วย ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลส่วนบุคคล และเป็นความลับของทางราชการ โดยไม่ได้รับอนุญาต รวมทั้งต้องไม่บันทึกข้อมูลที่เป็นการใส่ร้าย ให้ร้ายบุคคลอื่น และการบันทึกข้อมูลที่ผิดกฎหมายต่างๆ

๖๑.๘ หลังจากใช้งานอินเทอร์เน็ตเสร็จเรียบร้อยแล้ว ให้ทำการออกจากระบบ (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๖๑.๙ ผู้ใช้ต้องปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

ข้อ ๖๒ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดมาตรการป้องกันและรักษาความปลอดภัยจากการเชื่อมต่ออินเทอร์เน็ตความเร็วสูงดังนี้

๖๒.๑ การขอเปิดให้บริการเชื่อมต่ออินเทอร์เน็ตความเร็วสูงผ่านโทรศัพท์ เลขหมายเอกชน หน่วยผู้ขอใช้จะต้องเสนอขออนุมัติสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาผ่านกลุ่มเทคโนโลยีสารสนเทศเพื่อพิจารณาความเหมาะสมและความจำเป็นในการใช้งานต่อไป

๖๒.๒ การเชื่อมต่ออินเทอร์เน็ตความเร็วสูง จะต้องไม่เชื่อมต่อกับเครื่องคอมพิวเตอร์ของทางราชการที่เชื่อมต่อกับเครือข่ายภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา(Intranet) หรือเครื่องคอมพิวเตอร์ ส่วนตัวที่มีข้อมูลข่าวสารของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาที่เป็นชั้นความลับและ/หรือข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงของประเทศโดยเด็ดขาด

ข้อ ๖๓ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ กรณีที่มีการให้บริการเข้าถึงระบบอินเทอร์เน็ตจากภายในหน่วยงานโดยการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจร ทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

หมวด ๑๗

การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

ข้อ ๖๔ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาต้องกำหนดแนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์ ดังนี้

๖๔.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอเช่น การเปลี่ยนตำแหน่ง เปลี่ยนต้นสังกัด การลาออกจากราชการ การเกษียณอายุ เป็นต้น

๖๔.๒ ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๖๔.๓ การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสารของหน่วยที่รับผิดชอบระบบสารสนเทศเป็นผู้กำหนดขึ้น

๖๔.๔ รหัสผ่านของจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O” ในการ พิมพ์แต่ละตัวอักษร

๖๔.๕ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา หรือ จดหมายอิเล็กทรอนิกส์ (E-mail) ของภาครัฐเพื่อใช้ในการติดต่อกับราชการ

๖๔.๖ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๖๔.๗ ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน เป็นต้น

๖๔.๘ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อสถาบันจิตเวชศาสตร์สมเด็จพระยาหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบันจิตเวชศาสตร์สมเด็จพระยา

๖๔.๙ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการออกจากระบบ (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๖๔.๑๐ ผู้ใช้ควรทำการตรวจสอบเอกสารที่แนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบแฟ้มข้อมูลโดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดแฟ้มข้อมูลที่เป็น Executable File เช่น .exe, .com เป็นต้น

๖๔.๑๑ ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๖๔.๑๒ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๖๔.๑๓ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

หมวด ๑๘

การใช้งานทรัพย์สินทางปัญญา (Use of Intellectual Property)

ข้อ ๖๕ ผู้ใช้งานระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จพระยาควรจะต้องปฏิบัติตามเงื่อนไขการใช้งานและไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น ดังนี้

๖๕.๑ ปฏิบัติตามเงื่อนไขการใช้งานหรือที่กำหนดไว้ของซอฟต์แวร์หรือทรัพย์สินทางปัญญาอื่นๆ ที่สถาบันจิตเวชศาสตร์สมเด็จพระยาหรือผู้ใช้งานมีใช้งานหรือครอบครอง

๖๕.๒ ห้ามทำซ้ำ เปลี่ยนแปลง หรือแก้ไขทรัพย์สินทางปัญญาไปสู่รูปแบบอื่นที่เป็นการละเมิดเงื่อนไขหรือข้อตกลงการใช้งาน

๖๕.๓ ห้ามสำเนาทั้งหมดหรือบางส่วนของหนังสือ บทความ เพลง ภาพยนตร์ รายงาน หรือเอกสารอื่นๆ ที่เป็นการละเมิดเงื่อนไขของเจ้าของทรัพย์สินทางปัญญา

หมวด ๑๙
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

ข้อ ๖๖ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดแนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สายดังนี้

๖๖.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาจะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

๖๖.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๖๖.๓ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

๖๖.๔ การระบุอุปกรณ์ที่จะเข้าใช้งานในเครือข่ายไร้สายของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยานอกจากการลงทะเบียนการใช้งานแล้ว จะต้องแจ้งค่า MAC Address ของเครื่อง หรืออุปกรณ์ที่จะเข้ามาใช้งาน เพื่อให้ผู้รับผิดชอบเครือข่ายไร้สายของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาบันทึกเป็นหลักฐานการเข้าใช้งานต่อไป

หมวด ๒๐
ระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน
(Backup System and Contingency Plan)

ข้อ ๖๗ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนดแนวทางปฏิบัติในการคัดเลือกและจัดทำระบบสำรองและกู้คืนระบบ ดังนี้

๖๗.๑ กำหนดระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้

๖๗.๒ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๖๗.๓ กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

๖๗.๔ กำหนดความถี่ในการสำรองข้อมูลของระบบงาน เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อยควรมีความถี่ในการสำรองข้อมูลมากขึ้น เป็นต้น

๖๗.๕ ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้ในสถานที่อย่างน้อย ๑ ชุด

๖๗.๖ ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วนหรือไม่

๖๗.๗ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

๖๗.๘ แนวทางปฏิบัติสำหรับการสำรองข้อมูล ดังนี้

๖๗.๘.๑ ผู้ดูแลระบบต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามแนวทางการสำรองข้อมูลของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๖๗.๘.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูล ที่บันทึก เป็นต้น

๖๗.๘.๓ การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๖๗.๘.๔ ให้ผู้ดูแลระบบมอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรองในกรณีที่ผู้ดูแลระบบและ/หรือผู้ดูแลเครือข่ายไม่สามารถปฏิบัติงานได้

๖๗.๘.๕ ในกรณีพบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้รับผิดชอบระบบสารสนเทศของหน่วยทราบ

๖๗.๘.๖ ให้ผู้ดูแลระบบและผู้ดูแลเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสมพร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิดคือการสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๖๗.๘.๗ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๖๗.๘.๘ แนวทางที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

๖๗.๘.๙ สำหรับความถี่ในการสำรองข้อมูลมีดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรอง
๑. ระบบ E-Mail	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลในส่วน Mailbox	๑ ครั้งต่อเดือน
๒. Web Server	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลต่างๆที่เผยแพร่บนเว็บไซต์	๑ ครั้งต่อเดือน
๓. Database Server	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ฐานข้อมูลที่มีความสำคัญ	๑ ครั้งต่อเดือน
๔. Active Directory	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูล Rule ของอุปกรณ์นั้น	๑ ครั้งต่อเดือน
๕. อุปกรณ์ Firewall	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูล Rule ของอุปกรณ์นั้น	๑ ครั้งต่อเดือน

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรอง
๖. อุปกรณ์ IDS/IPS	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูล Rule ของอุปกรณ์นั้น	๑ ครั้งต่อเดือน
๗. อุปกรณ์ Server อื่นๆ	ค่าติดตั้งของระบบ (Configure)	ช่วงก่อนและหลังการเปลี่ยนค่า
	ข้อมูลที่มีความสำคัญของระบบงานที่ถูกเก็บในอุปกรณ์ต่างๆเหล่านั้น	๑ ครั้งต่อเดือน

๖๗.๘.๑๐ ผู้ดูแลระบบและผู้ดูแลเครือข่ายสารสนเทศรับผิดชอบ ความถูกต้องและความสมบูรณ์ของข้อมูล ตามความถี่ในข้อ ๖๗.๘.๙

๖๗.๙ แนวทางปฏิบัติสำหรับการกู้คืนระบบ ดังนี้

๖๗.๙.๑ ในกรณีพบปัญหาที่อาจสร้างความเสียหายต่อระบบ คอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบและ/หรือผู้ดูแล เครือข่าย ดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อ ผู้รับผิดชอบ ระบบสารสนเทศของหน่วย หรือผู้ที่ได้รับมอบหมายทราบ

๖๗.๙.๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้ หรือ ตามความเหมาะสมเพื่อกู้คืนระบบ

๖๗.๙.๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบ เครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

ข้อ ๖๘ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องกำหนด แนวทางเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ดังนี้

๖๘.๑ กำหนดระบบงานที่มีความสำคัญทั้งหมดของสถาบันจิตเวชศาสตร์ สมเด็จเจ้าพระยาและจัดทำเป็นบัญชีรายชื่อของระบบงาน ดังกล่าวรวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความ ทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

๖๘.๒ ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนด มาตรการเพื่อลดความเสี่ยงที่พบ โดยให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๖๘.๓ กำหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบงานและ ข้อมูลในฐานข้อมูล เป็นต้น รวมถึงกำหนดความถี่ในการสำรองข้อมูล วิธีการสำรองข้อมูล เช่น แบบ Full Backup หรือแบบ Incremental Backup เป็นต้น สำหรับระบบงานที่มีความสำคัญเหล่านั้น

๖๘.๔ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน (Contingency Plan) เพื่อรับมือกับภัยพิบัติ ที่อาจเกิดขึ้นได้ ทั้งวิธีการทางอิเล็กทรอนิกส์ และทางกายภาพ อีกทั้งให้กำหนดหัวงในการ ทดสอบแผนดังกล่าวในหัวงรอบ ๖ เดือน ของทุกปี โดยแผนฯ ต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

๖๘.๔.๑ การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๖๘.๔.๒ การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุม ประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

- ๖๘.๔.๓ การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
- ๖๘.๔.๔ การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบ กู้คืนข้อมูลสำรองไว้
- ๖๘.๔.๕ การกำหนดช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่างๆ เช่น เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น
- ๖๘.๔.๖ การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน
- ๖๘.๕ ให้ทำการปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง โดยมุ่งเน้นไปที่ระบบที่มีความสำคัญสูง
- ๖๘.๖ ให้ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลสำรองไปนั้นมีความครบถ้วน
- ๖๘.๗ ให้ทำการทดสอบกู้คืนข้อมูลสำรองไว้นั้นว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่อย่างน้อยปีละ ๑ ครั้ง ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร
- ๖๘.๘ ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินรวมทั้งเมื่อมีการปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

หมวด ๒๑

การตรวจสอบและประเมินความเสี่ยง

ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

- ข้อ ๖๙ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดให้มีการ ตรวจสอบด้านความมั่นคงปลอดภัยของข้อมูล ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่ตนเองรับผิดชอบ อย่างสม่ำเสมอ ดังนี้
- ๖๙.๑ ตรวจสอบและประเมินด้านการบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศ
- ๖๙.๒ ตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม
- ๖๙.๓ ตรวจสอบและประเมินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลและการปฏิบัติการ
- ๖๙.๔ ตรวจสอบและประเมินการควบคุมการเข้าถึง
- ๖๙.๕ ตรวจสอบและประเมินด้านการพัฒนาระบบสารสนเทศ เช่น ด้านการจัดซื้อจัดจ้างพัฒนาระบบฯ รวมทั้งด้านการดูแลระบบสารสนเทศ เป็นต้น
- ๖๙.๖ ตรวจสอบและประเมินด้านความพร้อมการรับมือกับเหตุการณ์เฉพาะหน้า
- ๖๙.๗ ตรวจสอบความสอดคล้องกับระเบียบฉบับนี้และทางเทคนิคกับระเบียบฉบับนี้

ข้อ ๗๐ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา ต้องจัดให้มีการประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ ซึ่งประกอบด้วยทรัพย์สิน ๕ หมวด ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบงาน ที่หน่วยรับผิดชอบอย่างน้อยปีละ ๑ ครั้ง โดยปฏิบัติตามแนวทางการประเมินดังนี้

- ๗๐.๑ กำหนดให้มีการจัดทำบัญชีทรัพย์สินสารสนเทศ
- ๗๐.๒ ระบุและประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศ
- ๗๐.๓ จัดลำดับความเสี่ยงจากสูงมาต่ำ
- ๗๐.๔ จัดทำแผนการลดความเสี่ยงโดยคำนึงถึงการจัดการกับความเสี่ยงสูงก่อน
- ๗๐.๕ กำหนดให้มีการปฏิบัติตามแผนการลดความเสี่ยงที่กำหนดไว้และติดตาม

จนกระทั่งแล้วเสร็จ

- ๗๐.๖ ความรับผิดชอบในการตรวจสอบและประเมินความเสี่ยง
 - ๗๐.๖.๑ กรณีการตรวจสอบภายในหน่วยงานของสถาบันจิตเวชศาสตร์

สมเด็จเจ้าพระยา (Internal Auditor)

๗๐.๖.๑.๑ ให้ผู้รับผิดชอบระบบสารสนเทศภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาแต่งตั้งหน่วยงาน หรือคณะกรรมการสำหรับการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๗๐.๖.๑.๒ วงรอบการตรวจสอบปีละ ๑ ครั้ง

๗๐.๖.๑.๓ ภายหลังจากการตรวจสอบ ให้รายงานผลการตรวจสอบให้หน่วยที่ได้รับการตรวจสอบ และผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

๗๐.๖.๒ กรณีผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๗๐.๖.๒.๑ ให้ผู้รับผิดชอบระบบสารสนเทศภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาพิจารณาจัดทำโครงการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๗๐.๖.๒.๒ โดยให้มีการจัดจ้างดำเนินการในวงรอบ ๑ ปีงบประมาณ

๗๐.๖.๒.๓ ภายหลังจากการตรวจสอบให้รายงานผลการตรวจสอบให้หน่วยที่ได้รับการตรวจสอบ และผู้บังคับบัญชาตามลำดับชั้นทราบต่อไป

หมวด ๒๒

การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๗๑ ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานภายในสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่ตรวจพบให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๗๑.๑ ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด ได้แก่ ระดับสูง ระดับกลาง หรือระดับต่ำ

๗๑.๒ แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้นตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

๗๑.๓ วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็นกรณีการบุกรุก การโจมตีระบบ หรือระบบได้รับความเสียหาย กรณีที่ไม่สามารถวิเคราะห์และแก้ไขโดยหน่วยงานเองได้ ให้ประสานงานขอความช่วยเหลือจากผู้ที่มีความรู้และความเชี่ยวชาญ เช่น ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (Thai CERT) หรือหน่วยงานภายนอกอื่นๆ เป็นต้น

๗๑.๔ กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ให้ผู้ผ่านการอบรม หรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัย และจำกัดการเข้าถึงหลักฐานนั้น

๗๑.๕ จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบ ตั้งแต่ระดับปานกลางขึ้นไป และแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงานดังนี้

๗๑.๕.๑ รายละเอียดเหตุการณ์

๗๑.๕.๒ วันเวลาที่เกิดขึ้น

๗๑.๕.๓ ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง

๗๑.๕.๔ สถานะของเหตุการณ์ในแต่ละช่วงเวลา

๗๑.๕.๕ ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา

๗๑.๕.๖ สาเหตุและวิธีการแก้ไข

๗๑.๕.๗ ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

หมวด ๒๓ หน้าที่และความรับผิดชอบ

ข้อ ๗๒ ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัติตามระเบียบนี้โดยเฉพาะในกรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามระเบียบสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาว่าด้วยการรักษาความปลอดภัยสารสนเทศของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยาพ.ศ. ๒๕๖๐ ให้ผู้บังคับบัญชาสูงสุดในพื้นที่และรับผิดชอบระบบสารสนเทศของหน่วย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยมีแนวทางปฏิบัติดังนี้

๗๒.๑ ให้แจ้งรายงานการละเมิดตามสายการบังคับบัญชาให้หน่วยเหนือและหน่วยที่เกี่ยวข้องทราบ

๗๒.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๗๒.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๗๒.๔ ให้พิจารณาสั่งการลงโทษทางวินัยตามระเบียบของราชการหรือดำเนินคดีตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิดและผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้จะโดยเจตนาหรือไม่เจตนา และการละเมิดนั้นจะเกิดความเสียหายหรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๗๓ ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัย ให้ส่วนราชการเจ้าของระบบสารสนเทศดำเนินการดังนี้

๗๓.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่างๆ ประมวลลับ หรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนหรือเกิดเสียหายอย่างไรหรือไม่

๗๓.๒ จัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันที ในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ ๗๔ ความรับผิดชอบของผู้ใช้งานต่อระเบียบฉบับนี้มีดังนี้

๗๔.๑ ปฏิบัติตามระเบียบฯ อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๗๔.๒ ไม่เข้าถึงเปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๗๔.๓ ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ของสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา

๗๔.๔ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังผู้บังคับบัญชาและผู้รับผิดชอบระบบสารสนเทศโดยเร็วที่สุด

ข้อ ๗๕ ในกรณีที่การละเมิดการรักษาความปลอดภัยเกิดผลกระทบกระเทือนเสียหายอย่างร้ายแรงให้อยู่ในดุลพินิจของของผู้บังคับบัญชาสามารถแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติ หากจำเป็นให้รายงานหน่วยเหนือได้ตามความเหมาะสม

ข้อ ๗๖ ให้ส่วนราชการที่มีศูนย์สารสนเทศหรือศูนย์กรรมวิธีข้อมูลอัตโนมัติอยู่ในสังกัดสามารถออกระเบียบปลีกย่อยได้โดยไม่ขัดต่อระเบียบนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑ มีนาคม พ.ศ. ๒๕๖๕



(นายศรุตพันธุ์ จักรพันธุ์ ณ อยุธยา)

ผู้อำนวยการสถาบันกัลยาณ์ราชนครินทร์ รักษาราชการแทน

ผู้อำนวยการสถาบันจิตเวชศาสตร์สมเด็จเจ้าพระยา