



นโยบายและแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
โรงพยาบาลพระมงกุฎเกล้า

บทนำ

๑) นโยบายนี้จัดทำขึ้นสำหรับข้าราชการหรือเจ้าหน้าที่ในสังกัดโรงพยาบาลพระมงกุฎเกล้า จะเข้าใช้งานระบบคอมพิวเตอร์ของโรงพยาบาลพระมงกุฎเกล้า รวมไปถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตโดยผ่านทางเครือข่ายของโรงพยาบาลพระมงกุฎเกล้าโดยให้ถือปฏิบัติโดยเคร่งครัด

๒) โรงพยาบาลพระมงกุฎเกล้าสงวนสิทธิ์ในการเข้าตรวจสอบ เก็บหลักฐานและดำเนินการอันสมควรหากพบว่ามีกรณีละเมิดนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต

๓) นโยบายของระบบคอมพิวเตอร์และอุปกรณ์ประกอบของโรงพยาบาลพระมงกุฎเกล้า มีดังนี้

- ระบบคอมพิวเตอร์
- เครื่องคอมพิวเตอร์
- อุปกรณ์ประกอบ
- ซอฟต์แวร์
- เครือข่ายภายในอินทราเน็ต
- เครือข่าย อินเทอร์เน็ต
- การใช้งานจากภายนอกองค์กร remote access
- โปรแกรมการใช้งาน Application
- โปรแกรมป้องกัน Firewall

หมวดทั่วไป

- ๑) ระบบคอมพิวเตอร์เครื่องคอมพิวเตอร์และอุปกรณ์ต่อเชื่อมของโรงพยาบาลพระมงกุฎเกล้า จัดทำเพื่อให้บริการที่เกี่ยวข้องกับกิจการของโรงพยาบาลพระมงกุฎเกล้าและหากไม่ได้รับอนุญาต ห้ามนำบุคคลภายนอกมาใช้งานเครื่องคอมพิวเตอร์ และเครือข่ายของโรงพยาบาลพระมงกุฎเกล้า
- ๒) การเข้าใช้งานระบบคอมพิวเตอร์และการต่อเชื่อมทางอินเทอร์เน็ตของโรงพยาบาลพระมงกุฎเกล้า จะต้องปฏิบัติตามระเบียบในการขออนุญาตเจ้าใช้โดยจะมีการลงทะเบียนการใช้งานตามขั้นตอนของโรงพยาบาลพระมงกุฎเกล้า
- ๓) บัญชีผู้ใช้งาน (User Account) ที่ให้ผู้ใช้งานไว้นั้น ผู้ใช้งานต้องรับผิดชอบผลต่าง ๆ อันอาจเกิดขึ้นรวมถึงผลเสียหายต่างๆที่เกิดขึ้นจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- ๔) บัญชีผู้ใช้งาน ให้เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกสิทธินั้นให้กับผู้อื่นไม่ได้
- ๕) ในการขออนุญาตเข้าใช้งาน ให้ผู้ที่ขอใช้บริการเป็นผู้ขอโดยปฏิบัติตามขั้นตอนการขอเข้าใช้งานระบบที่กำหนดไว้

- ๖) ผู้ใช้งานจะต้องทำความเข้าใจและลงนามเพื่อยืนยันว่าจะปฏิบัติตามนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตและจะต้องทำความเข้าใจในส่วนเปลี่ยนแปลงแก้ไข (หากมี) โดยลงนามเพื่อยืนยันทุกรอบปี
- ๗) ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆที่กำหนดขึ้นโดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายมิได้
- ๘) นโยบายการใช้ระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตนี้ ถือเป็นส่วนหนึ่งของข้อกำหนดในการปฏิบัติงานของข้าราชการและเจ้าหน้าที่ทุกคน และจะถือเป็นกรณีวินัยหรือระเบียบในการปฏิบัติงานเช่นเดียวกันหากไม่ปฏิบัติตาม
- ๙) หากพบว่าข้าราชการหรือเจ้าหน้าที่มีการละเมิดนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตจะถูกลงโทษตามกฎหมายระเบียบของการเป็นข้าราชการหรือเจ้าหน้าที่ รวมไปถึงอาจจะส่งตัวเพื่อดำเนินคดีตามกฎหมาย หากการละเมิดนั้นมีความผิดตามกฎหมายหรือพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่๒)พ.ศ.๒๕๖๐
- ๑๐) ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแลระบบคอมพิวเตอร์

หมวดที่ ๑ ว่าด้วยระเบียบการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต

- ๑) โรงพยาบาลพระมงกุฎเกล้าดำเนินกิจการภายใต้กฎหมายไทยดังนั้นการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อทางอินเทอร์เน็ตจะต้องปฏิบัติตามพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่๒) พ.ศ.๒๕๖๐ และกฎหมายประกอบอื่นๆที่เกี่ยวข้องโดยข้าราชการหรือเจ้าหน้าที่สามารถศึกษาข้อกฎหมายจาก พรบ.ดังกล่าวได้
- ๒) โรงพยาบาลพระมงกุฎเกล้า ไม่สนับสนุนหรือยินยอมให้ข้าราชการหรือเจ้าหน้าที่ของโรงพยาบาลพระมงกุฎเกล้ากระทำความผิดต่อพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่๒) พ.ศ.๒๕๖๐ และกฎหมายประกอบอื่นๆที่เกี่ยวข้อง
- ๓) โรงพยาบาลพระมงกุฎเกล้าจะจัดให้มีผู้ใช้ (User ID) และรหัสผ่าน (Password) ให้กับข้าราชการหรือเจ้าหน้าที่ ที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ตเป็นรายบุคคลและมีกฎในการใช้งานรหัสผ่าน เช่น ความยาวของตัวอักษรหรือระยะเวลาที่ต้องเปลี่ยนรหัส ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม

- ๔) รหัสผ่านของข้าราชการหรือเจ้าหน้าที่ถือเป็นทรัพย์สินของโรงพยาบาลพระมงกุฎเกล้าและไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และข้าราชการหรือเจ้าหน้าที่ทุกคนมีหน้าที่ในการป้องกันรหัสผ่านขององค์กรอย่างเคร่งครัด
- ๕) โรงพยาบาลพระมงกุฎเกล้าไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน
- ๖) ข้าราชการหรือเจ้าหน้าที่อาจจะได้รับมอบหมายให้เข้าใช้ระบบงานอื่นๆที่โรงพยาบาลพระมงกุฎเกล้ากำหนดให้ใช้ ข้าราชการหรือเจ้าหน้าที่จะต้องปฏิบัติตามกฎการใช้ระบบเก็บรักษาชื่อและรหัสผ่านไว้มิให้เปิดเผยกับผู้อื่น ยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาโดยตรงเป็นลายลักษณ์อักษร
- ๗) หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่านให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอลีกใช้โดยจะต้องกระทำทันทีที่จะเลิกใช้งานหรือบัญชีผู้ใช้งานใดๆที่มีได้มีการใช้งานภายในระยะที่กำหนดไว้จะถูกระงับหรือยกเลิกการใช้งาน
- ๘) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของโรงพยาบาลพระมงกุฎเกล้า ข้าราชการหรือเจ้าหน้าที่ที่เป็นผู้รับผิดชอบจะต้องมีหน้าที่ดูแลบำรุงรักษาเบื้องต้น
- ๙) ไม่อนุญาตให้ใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มีใช้ของโรงพยาบาลพระมงกุฎเกล้าในการเชื่อมต่อเข้ากับเครือข่ายของโรงพยาบาลพระมงกุฎเกล้าเว้นแต่ได้รับอนุญาตจากศูนย์คอมพิวเตอร์

หมวดที่ ๒ ว่าด้วยการใช้จดหมายอิเล็กทรอนิกส์, การสนทนาและการติดต่อสื่อสารทางอิเล็กทรอนิกส์ อื่นๆ E-mail, chat, social network and others digital communication เช่น การส่ง file หรือการส่งโทรสาร

- ๑) ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์หรือการติดต่อสื่อสารใดๆให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎหมายการรับ-ส่งหนังสือหรือจดหมายของโรงพยาบาลพระมงกุฎเกล้า ได้แก่ การรักษาความลับของเอกสาร ห้ามส่งเอกสารความลับโดยจดหมายอิเล็กทรอนิกส์ ยกเว้นได้รับการเข้ารหัสและรับรองจากหน่วยงานคอมพิวเตอร์
- ๒) ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อโรงพยาบาลพระมงกุฎเกล้าหรือบุคคลอื่นๆ
- ๓) ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร
- ๔) การส่งข้อมูลใดๆให้ปฏิบัติพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๕๐

- ๕) หากพบว่ามี การส่งข้อมูลที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ผิดต่อกฎหมายระเบียบของโรงพยาบาลพระมงกุฎเกล้า ให้แจ้งต่อผู้บังคับบัญชา โดยตรงหรือเจ้าหน้าที่หน่วยงานคอมพิวเตอร์
- ๖) ให้ใช้ข้อความสุภาพในการส่งจดหมายอิเล็กทรอนิกส์ การสนทนา chat หรือการสื่อสารทาง อิเล็กทรอนิกส์อื่นๆ
- ๗) ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง (SPAM E-mail)
- ๘) ไม่อนุญาตให้ข้าราชการหรือเจ้าหน้าที่ใช้ (E-mail) อื่นใดที่โรงพยาบาลพระมงกุฎเกล้าไม่ได้ กำหนดให้ใช้

หมวดที่ ๓ ว่าด้วยการใช้ Portal ขององค์กร และการเข้าใช้อินเทอร์เน็ต

- ๑) ห้ามข้าราชการหรือเจ้าหน้าที่ post และ/หรือ download file รูป/หรือข้อมูลใดๆบน Portalของ โรงพยาบาล Portal อื่นๆที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์(ฉบับที่๒) พ.ศ.๒๕๖๐
 - ๑.๑ มีไวรัสหรือชุดคำสั่งไม่พึงประสงค์
 - ๑.๒ ไม่เกี่ยวข้องกับกิจการขององค์กร
- ๒) การเปิดให้บริการการเข้าเว็บไซต์
 - ๒.๑ ให้บริการเว็บไซต์ที่เกี่ยวข้องการให้บริการและกิจการของโรงพยาบาลพระมงกุฎเกล้า เป็นหลักหากตรวจพบว่าความเร็วอินเทอร์เน็ตของระบบช้า จะงดให้บริการอินเทอร์เน็ต ในกิจการอื่นๆที่มีใช้ของโรงพยาบาลพระมงกุฎเกล้าก่อน
 - ๒.๒ กำหนดช่วงเวลาหรือระดับการเข้าใช้งานของเว็บไซต์ ที่กำหนดโดยศูนย์คอมพิวเตอร์

หมวดที่ ๔ ว่าด้วยการใช้งาน Application และโปรแกรมต่างๆ

- ๑) การเข้าใช้งาน Application ต่างๆ จะต้องได้รับอนุญาตจากเจ้าของระบบ
- ๒) ให้ข้าราชการหรือเจ้าหน้าที่ใช้โปรแกรมและApplication ที่โรงพยาบาลพระมงกุฎเกล้ากำหนด ให้ใช้เท่านั้น
- ๓) ห้ามข้าราชการหรือเจ้าหน้าที่นำโปรแกรมหรือ Application ใดๆ มาติดตั้งบนเครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่นๆ โดยไม่ได้รับความยินยอมจากหน่วยงาน ผู้ดูแลคอมพิวเตอร์โดยตรง

- ๔) ห้ามข้าราชการหรือเจ้าหน้าที่ใช้โปรแกรมหรือ Application ที่ไม่ถูกลิขสิทธิ์ หากก่อให้เกิดความเสียหายหรือมีการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว
- ๕) ผู้ที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่างๆเป็นไปตามมาตรฐานและไม่เกิดผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของโรงพยาบาลพระมงกุฎเกล้า
- ๖) การขออนุญาตนำเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายและขอหมายเลขไอพี (IP ADDRESS) ของหน่วยงานใดๆ หน่วยงานนั้นจะต้องทำหนังสือขออนุญาต
- ๗) ห้ามบุคคลใดกระทำการเคลื่อนย้ายหรือทำการใดๆต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของโรงพยาบาลพระมงกุฎเกล้าได้
- ๘) ในกรณีที่ตรวจสอบพบว่า เครือข่ายส่วนใดก่อให้เกิดความผิดปกติของระบบเครือข่ายหลักของโรงพยาบาลพระมงกุฎเกล้าศูนย์คอมพิวเตอร์ อาจพิจารณาระงับการให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน
- ๙) ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับการอนุญาต ทั้งนี้รวมถึงการติดตั้งเครือข่ายแบบไร้สาย
- ๑๐) โรงพยาบาลพระมงกุฎเกล้าจะติดตั้งโปรแกรมควบคุมการใช้งานผ่านเครือข่าย เพื่อติดตามช่วยเหลือแก้ไขและควบคุมการใช้งานเครื่องคอมพิวเตอร์
- ๑๑) ผู้ใช้งานห้ามทำการเก็บหรือสำรองข้อมูลส่วนบุคคลไว้ในเครื่องคอมพิวเตอร์ของโรงพยาบาลพระมงกุฎเกล้า หากเกิดปัญหาจำเป็นต้องมีการซ่อมบำรุงหรือมีการติดตั้งระบบปฏิบัติการใหม่ อาจมีการล้างข้อมูลในเครื่องคอมพิวเตอร์ทั้งหมดของศูนย์คอมพิวเตอร์

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลพระมงกุฎเกล้า เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลพระมงกุฎเกล้าจึงเห็นควรกำหนดนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน(Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

๒. วัตถุประสงค์

๒.๑ การจัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ อ้างอิงตามมาตรฐานHA และมีการปรับปรุงอย่างต่อเนื่อง

๒.๓ นโยบายและแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๔ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๕ นโยบายและแนวทางปฏิบัตินี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

๓.นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาลพระมงกุฎเกล้า

๓.๑ โรงพยาบาลพระมงกุฎเกล้าส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๓.๒ โรงพยาบาลพระมงกุฎเกล้ามีหน้าที่จำกัด ระบุ เป้ากอนสิทธิหรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติ ในกรณีสำคัญศูนย์คอมพิวเตอร์และคณะกรรมการสารสนเทศรายงานการฝ่าฝืนให้ผู้บังคับบัญชาของหน่วยทราบหรือผู้อำนวยการโรงพยาบาลพระมงกุฎเกล้าเพื่อพิจารณาลงโทษ

๓.๓ โรงพยาบาลพระมงกุฎเกล้าสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๔ โรงพยาบาลพระมงกุฎเกล้าสนับสนุนการรักษาความมั่นคงปลอดภัยของข้อมูลตามระเบียบปฏิบัติเพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

๔.องค์ประกอบของแนวปฏิบัติ

๔.๑ คำนิยาม

๔.๒ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๔.๓ การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

๔.๔ การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔.๕ การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๔.๖ การรักษาความมั่นคงปลอดภัยของไฟล์วอลล์

๔.๗ การรักษาความมั่นคงปลอดภัยของอีเมล

๔.๘ การรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

๔.๙ การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

๔.๑๐การรักษาความมั่นคงปลอดภัยของการสำรองข้อมูล

๔.๑๑ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ (Objective) แนวทางปฏิบัติ(Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กรเพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัยช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลพระมงกุฎเกล้า

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายถึงผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของโรงพยาบาลพระมงกุฎเกล้า ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ศูนย์คอมพิวเตอร์และสารสนเทศของโรงพยาบาล หมายถึง ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลพระมงกุฎเกล้า

หัวหน้าและคณะกรรมการด้านความมั่นคงปลอดภัยระบบสารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการจัดการ ระบบเทคโนโลยีสารสนเทศโรงพยาบาลพระมงกุฎเกล้า และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในโรงพยาบาลพระมงกุฎเกล้า

การรักษาความมั่นคงปลอดภัย หมายถึงการรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลพระมงกุฎเกล้า

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึงแนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งโรงพยาบาลพระมงกุฎเกล้ากำหนดไว้ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลพระมงกุฎเกล้า เช่นผู้อำนวยการโรงพยาบาลพระมงกุฎเกล้า รองผู้อำนวยการโรงพยาบาล หัวหน้ากลุ่มงาน เป็นต้น

ผู้ดูแลระบบ (System Administrator) หมายถึงเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่น เพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ User Account หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (E-mail Account) เป็นต้น

เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราวและเจ้าหน้าที่ประจำโครงการต่างๆของโรงพยาบาลพระมงกุฎเกล้า

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลพระมงกุฎเกล้าอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกส์ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึงระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้เช่น ระบบแลน(LAN)ระบบอินทราเน็ต(Intranet) ระบบอินเทอร์เน็ต เป็นต้น

ระบบแลน(LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้ บริหาร การพัฒนาและการควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร(Information System Workspace) หมายถึง พื้นที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

- พื้นที่ของผู้ดูแลระบบ (System administrator area) หมายถึง พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)

- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) หมายถึง พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึงการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางการภาพรวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ(Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นเป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืน นโยบายด้านความมั่นคงปลอดภัย หรือ เหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิกส์ ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POPM และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ให้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เป็นผู้กำหนดพื้นที่ผู้ให้บริการพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจนและจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายพื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๒ ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓ ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ กำหนดมาตรการควบคุมการเข้า-ออก พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงานจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกหรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงักรวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคล ที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่าย ของหน่วยงานได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลพระมงกุฎเกล้า

๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑.๑ โรงพยาบาลพระมงกุฎเกล้ากำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงาน หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์คอมพิวเตอร์กอ.รพ.ร.๖

๒.๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานและตรวจสอบการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

๒.๑.๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิต่างๆและการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๒.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลพระมงกุฎเกล้า กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒.๒ ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่นระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้นโดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างสม่ำเสมอ

๒.๒.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

- ๒.๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน
- ๒.๒.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน
- ๒.๒.๓.๓ ควรกำหนดให้ผู้ให้บริการตอบยืนยันการได้รับรหัสผ่าน
- ๒.๒.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- ๒.๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- ๒.๒.๓.๖ ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้ รหัสผู้ใช้งานต่างๆจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- ๒.๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- ๒.๒.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
- ๒.๒.๔.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๒.๔.๔ ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๒.๔.๕ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๒.๓.๑ ผู้ให้บริการต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๒.๓.๒ ผู้ให้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงาน

๒.๓.๓ ผู้ให้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอเพื่อทำการล๊อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

๒.๓.๔ ผู้ให้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานมากกว่า๑ชั่วโมง

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้บริการได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายรวมทั้งทำความเข้าใจตลอดปฏิบัติตาม เพื่อเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงาน ให้มีความลับ ความถูกต้องและมีความพร้อม ใช้งานอยู่เสมอ

๒. แนวทางปฏิบัติในการใช้งานเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์แม่ข่ายโรงพยาบาล

กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย(Server) ดังนี้

๒.๑ ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุม ป้องกัน การบุกรุกได้อย่างเป็นระบบ

๒.๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานต้องได้รับอนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศโรงพยาบาลและต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนเนมย่อย(Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศและจะต้องไม่ติดตั้งโปรแกรมใดๆที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้บริการอื่นๆ

๒.๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆต่ออุปกรณ์ส่วนกลางได้แก่ อุปกรณ์จัดเส้นทาง อุปกรณ์กระจายสัญญาณข้อมูล (Router) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก (Switch) โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๒.๕ ผู้ดูแลระบบต้องการควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๒.๕.๑ มีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๒.๕.๒ ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ

๒.๕.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

- ๒.๕.๔ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่ใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ
- ๒.๕.๕ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการบันทึกเข้า(Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ
- ๒.๕.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้
- ๒.๕.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ๒.๕.๘ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
- ๒.๕.๙ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่ายในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆของซอฟต์แวร์ระบบ (Systems Software)
- ๒.๖ โรงพยาบาลพระมงกุฎเกล้า กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้
- ๒.๖.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย
- ๒.๖.๒ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบบันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วันนับตั้งแต่การใช้บริการสิ้นสุดลง
- ๒.๖.๓ ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ
- ๒.๖.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒.๗ โรงพยาบาลพระมงกุฎเกล้ากำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทางดังต่อไปนี้

- ๒.๗.๑ บุคคลจากหน่วยงานนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศ
- ๒.๗.๒ มีการควบคุมช่องทาง ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
- ๒.๗.๓ วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศ
- ๒.๗.๔ การเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ
- ๒.๗.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบ ในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ต้องปฏิบัติ ดังนี้

๒.๑ การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจาก ผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งานเพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒.๒ ห้ามผู้ใช้งาน(User) นำอุปกรณ์ Wireless มาติดตั้งหรือปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็ Access point, Wireless Router, Wireless USB client หรือ Wireless card

๒.๓ ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

๒.๔ กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

๒.๔.๑ ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสมโดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายในที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

๒.๔.๒ ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ (User name) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๒.๔.๓ ให้เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งานและต้องปิดคุณสมบัติการ Auto Broadcast SSID ด้วย

๒.๔.๔ ผู้ดูแลระบบต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสมรวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๒.๔.๕ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๒.๔.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้เกิดบุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๒.๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายและจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือนและในกรณีที่ต้องตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานให้หัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศทราบทันที

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

๒. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความมั่นคงปลอดภัยไฟร์วอลล์ (Firewall) ของโรงพยาบาลพระมงกุฎเกล้า มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑ ศูนย์คอมพิวเตอร์และสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาลพระมงกุฎเกล้า

๒.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิบัติทั้งหมด

๒.๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก(Block) โดยไฟร์วอลล์

๒.๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User Password)

๒.๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่นค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๒.๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๒.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อย กว่า ๙๐ วัน

๒.๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลพระมงกุฎเกล้าอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่ออื่นที่กำหนดจะต้องได้รับอนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์และสารสนเทศของโรงพยาบาลก่อน

๒.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายชื่อเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่อง

คอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องอนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์คอมพิวเตอร์ และสารสนเทศของโรงพยาบาล โดยต้องระบุข้อมูลดังนี้

๒.๙.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๒.๙.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๒.๙.๓ วัตถุประสงค์หรือชื่อแอปพลิเคชันที่ต้องการใช้งาน นั้นๆ

๒.๙.๔ วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

๒.๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟล်วอลเป็นประจำทุกสัปดาห์หรือ ทุกครั้งที่มีการเปลี่ยนแปลงค่า

๒.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีๆไป

๒.๑๒ โรงพยาบาลพระมงกุฎเกล้ามีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลหรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศจนกว่าจะได้รับการแก้ไข

๒.๑๓ ภายหลังจากการอนุญาตให้ใช้งานหาก พบว่า มีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาล หรือกฎหมาย หรืออาจจะทำให้เกิดความเสียด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางระบบงานโรงพยาบาล ทางระบบประกัน สุขภาพและระบบอื่นๆที่เกี่ยวข้องจะยกเลิกการให้บริการทันที

๒.๑๔ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรือ อุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากโรงพยาบาล

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของโรงพยาบาลพระมงกุฎเกล้า ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต ผู้ใช้งานต้องเข้าใจกฎเกณฑ์ ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิกระทำการใดๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

ผู้ใช้งานเครือข่ายอินเทอร์เน็ตของโรงพยาบาลพระมงกุฎเกล้ามีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๒.๑ การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่ศูนย์คอมพิวเตอร์และสารสนเทศของโรงพยาบาล โดยรอการตรวจสอบตัวบุคคลและอนุมัติการใช้งานโดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลพระมงกุฎเกล้า สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากเจ้าหน้าที่ ฝ่ายงานอินเทอร์เน็ตของศูนย์คอมพิวเตอร์และสารสนเทศของโรงพยาบาลเป็นผู้ดำเนินการพิจารณาเป็นกรณีไป

๒.๒ ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่ก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๓ ผู้ใช้งานอินเทอร์เน็ต พึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๒.๔ ผู้ใช้งานต้องไม่ให้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๒.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๖ รมัตระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้แจ้งผู้ที่ได้รับมอบหมาย

๒.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ Face book โปรแกรมอื่นๆ ที่มีลักษณะคล้ายกัน ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๒.๘ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควร (Logout) ออกจากระบบทุกครั้ง

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
(Intrusion Detection System/ Intrusion System Policy: IDS/IPS Policy)

๑. วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในโรงพยาบาลพระมงกุฎเกล้าให้มีความมั่นคงปลอดภัย

๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

๒.๑ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของโรงพยาบาลพระมงกุฎเกล้าและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๒.๒ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ต หรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๒.๓ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และเปิดให้บริการ

๒.๔ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๒.๕ มีการตรวจสอบและ Update Patch /Signature ของ IDS/IPS เป็นประจำ

๒.๖ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งานกิจกรรม และปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำโดยผู้ดูแลระบบ

๒.๗ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ

๒.๘ เครื่องแม่ข่ายที่มีการติดตั้ง host - based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๒.๙ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบพฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจสอบ

๒.๑๐ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๒.๑๑ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๒.๑๒ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจสอบพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตและดำเนินการตามแผน

๒.๑๓ โรงพยาบาลพระมงกุฎเกล้า มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๒.๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลพระมงกุฎเกล้า การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับพ.ร.บ.ว่าด้วยการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของโรงพยาบาลพระมงกุฎเกล้า จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอีเมล (E-mail Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กรซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ตผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ไม่ละเมิดสิทธิกระทำการใดๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัดจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของโรงพยาบาลพระมงกุฎเกล้ามีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๒.๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์คอมพิวเตอร์ของโรงพยาบาลพระมงกุฎเกล้า

๒.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที

๒.๓ ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๒.๔ ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๒.๕ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

๒.๖ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการหรือตามภารกิจของโรงพยาบาลพระมงกุฎเกล้า ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลพระมงกุฎเกล้าเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลพระมงกุฎเกล้าขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๒.๗ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๒.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่นยั่วยุยเสียดสี ส่อเสียด ไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของโรงพยาบาล

๒.๙ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลพระมงกุฎเกล้า เพื่อเผยแพร่ข้อมูล ข้อมูลรูปภาพหรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมายหรือกระทบต่อ

การดำเนินงานของโรงพยาบาลพระมงกุฎเกล้าตลอดจนเป็นการรวบรวมผู้ใช้งานอื่น รวมทั้งผู้รับบริการของ
โรงพยาบาลพระมงกุฎเกล้า

๒.๑๐ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมาย
อิเล็กทรอนิกส์

๒.๑๑ การแนบไฟล์ข้อมูลสามารถแนบไฟล์ได้ไม่เกิน ๑๐ เมกะไบต์

๒.๑๒ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการสำรองข้อมูล
(Backup Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย(Sever) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

๒.๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูล ระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๒.๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบ ซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

๒.๓ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจนข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่อื่นและต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๔ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

แนวทางการปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถทำไปปฏิบัติ ได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง โดยอาจจัดรวมกับการสัมมนาอื่นด้วยก็ได้และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจ ความต้องการของผู้ใช้บริการ

แนวทางการปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการอำนวยการและกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลพระมงกุฎเกล้าเพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยเชื่อถือได้ซึ่งเป็นตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และเพื่อให้เจ้าหน้าที่ทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

ผู้จัดทำ

พ.อ.



(ธนกร เทียนศรี)

รองหน.ศูนย์คอมพิวเตอร์ กอ.รพ.ร.๖