



ประกาศนโยบายความปลอดภัยด้านสารสนเทศ

เรื่อง แนวทางปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัย
ด้านเทคโนโลยีสารสนเทศของ บริษัท โรงพยาบาลอินเตอร์เมดิคัล แคร่ แอนด์ แล็บ จำกัด (มหาชน) (IMH)

เพื่อให้พนักงานบริษัท โรงพยาบาลอินเตอร์เมดิคัล แคร่ แอนด์ แล็บ จำกัด (มหาชน) รับทราบและรับนโยบายการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท โรงพยาบาลอินเตอร์เมดิคัล แคร่ แอนด์ แล็บ จำกัด (มหาชน) ได้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน บริษัท โรงพยาบาลอินเตอร์เมดิคัล แคร่ แอนด์ แล็บ จำกัด (มหาชน) จึงได้วางแนวทางให้บริษัทใช้ในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ จะทำให้บริษัทสามารถควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ซึ่งจะมีผลให้ได้รับการประเมินการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศอยู่ในระดับที่ดียิ่งขึ้น

แนวทางปฏิบัติฉบับนี้ได้ หากแสดงต่อสำนักงานได้ว่าแนวทางอื่นนั้นสามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศได้และมีประสิทธิภาพเพียงพอ ตลอดจนอยู่ในมาตรฐานที่ยอมรับได้สำหรับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทโดยสาระสำคัญของแนวทางปฏิบัติฉบับนี้ประกอบด้วย

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

การจัดให้มีนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบายรายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล้วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มีได้อำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติ

1. การบริหารจัดการข้อมูล

- ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น
- ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (input) ประมวลผล (Operate) และแสดงผล (Output) นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน
- ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2. การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)

- ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (Application System) สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- ในกรณีที่มีความจำเป็นต้องใช้ User ที่มีสิทธิพิเศษต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ในการพิจารณาว่าควรควบคุม User ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
 - ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
 - ควรควบคุมการใช้งาน User ที่มีสิทธิพิเศษอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งาน User ดังกล่าวในลักษณะ Dual Control โดยให้เจ้าหน้าที่ 2 รายถือรหัสผ่านคนละครึ่ง หรือเก็บของ Password ไว้ในตู้เซฟ เป็นต้น และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
 - ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
 - ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 120 วัน เป็นต้น
 - ในกรณีที่ไม่มีกรปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่ไม่ได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (log out) ในช่วงเวลาที่มีได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น
 - ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีเจตจำนงแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
 - ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติและต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
 - ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร
 - สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 120 วันในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
 - ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “123456” เป็นต้น
 - ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่
 - ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
 - ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไป
 - ไม่ควรเกิน 5 ครั้ง
 - ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
 - ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
 - ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
- ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง
- ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญ อย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มีได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของพนักงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือ เปลี่ยน Password เป็นต้น

4.การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

- ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการทำงานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที
- ต้องเปิดให้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม
- ต้องดำเนินการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web Server เป็นต้น อย่างสม่ำเสมอ ควรทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา
- ควรมีแนวทางปฏิบัติในการใช้งาน Software Utility เช่น Personal Firewall Password Cracker เป็นต้น และตรวจสอบการใช้งาน Software Utility อย่างสม่ำเสมอ
- ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

5. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

- ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก ส่วน DMZ เป็นต้น
- ต้องมีระบบป้องกันการบุกรุก เช่น Firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก

- ต้องมีระบบตรวจสอบการบุกรุกและการทำงานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ
 - ความพยายามในการบุกรุกผ่านระบบเครือข่าย
 - การใช้งานในลักษณะที่ผิดปกติ
 - การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า Parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical Disconnect) และจุดเชื่อมต่อ (Disable Port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง
- ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote Access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ Modem (Dial Out) ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด เช่น การใช้ระบบ Call Back การควบคุมการเปิดปิด Modem การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน การบันทึกรายละเอียดการใช้งาน และในกรณี Dial Out ก็ควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้นรวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว
- ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ก็ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
- การใช้เครื่องมือต่างๆ (Tools) เพื่อตรวจเช็คระบบเครือข่ายควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. การบริหารการเปลี่ยนแปลงระบบคอมพิวเตอร์ (Configuration Management)

- ก่อนการเปลี่ยนแปลงระบบและอุปกรณ์คอมพิวเตอร์ ควรมีการประเมินผลกระทบที่เกี่ยวข้อง และบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันอยู่เสมอ รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ
- ควรติดตั้งซอฟต์แวร์เท่าที่จำเป็นแก่การใช้งาน และถูกต้องตามลิขสิทธิ์

7. การวางแผนการรองรับประสิทธิภาพของระบบคอมพิวเตอร์ (Capacity Planning)

- ต้องประเมินการใช้งานระบบคอมพิวเตอร์สำคัญไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต

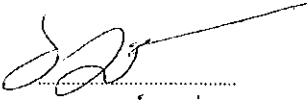
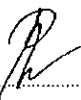
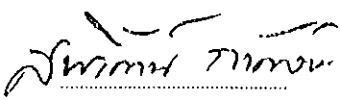
8. การป้องกันไวรัส และ Malicious Code

- ต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น
- ฝ่ายคอมพิวเตอร์ควรจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ รวมทั้งแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ๆ อย่างสม่ำเสมอ
- ควรควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (Disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส

9. บันทึกเพื่อการตรวจสอบ (Audit Logs)

- ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (Login-Logout Logs) บันทึกการพยายามเข้าสู่ระบบ (Login Attempts) บันทึกการใช้ Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน
- ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ประกาศ ณ วันที่ 6 กุมภาพันธ์ พ.ศ. 2566

ผู้ขออนุมัติ	ความเห็น/ผู้บังคับบัญชา	ผู้อนุมัติ
 (นายทรงศักดิ์ พลเยี่ยม) ผู้จัดการฝ่ายแผนกไอที	 (คุณปรมาภรณ์ ปาโจนกิจ) ผู้อำนวยการสาย บริหารทั่วไป	 (ดร.สิทธิวัฒน์ คำกัตวงศ์) ประธานเจ้าหน้าที่บริหาร