นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) และบริษัทย่อย

นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) (**"บริษัท"**) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ บริษัทจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

วัตถุประสงค์

1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
2. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง
3. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
5. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย 1 ครั้งต่อปี

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. การจัดทำนโยบายต้องมีผู้บริหาร เจ้าหน้าที่ปฏิบัติงานด้านคอมพิวเตอร์ และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย
2. นโยบายต้องจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของบริษัท
3. มีการกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวไว้ชัดเจน
4. มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง

5. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

6. มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานอย่างทั่วถึง โดยให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

7. มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

8. มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

9. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

10. มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

11. การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

12. มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ เผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) ประกอบด้วย

   1.1 มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยเป็นสำคัญ

   1.2 ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

   1.3 ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ซึ่งได้รับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ประกอบด้วย

   2.1 สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

2.2 การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

2.3 การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

2.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ประกอบด้วย

3.1 การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

3.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

3.3 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

3.4 ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

4. การควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ประกอบด้วย

4.1 การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

4.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

4.3 การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

4.5 การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

4.7 การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ประกอบด้วย

5.1 กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

5.2 ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

5.3 การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำ หรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

5.4 การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัด และควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

5.5 เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) ประกอบด้วย

6.1 การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศ และฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

6.2 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

6.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

6.4 การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

7. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

7.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

7.2 หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงาน หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

7.3 สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

7.4 ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

8. การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ประกอบด้วย

8.1 การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

8.2 การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

8.3 ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

8.4 ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

8.5 มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

9. การจัดทำแผนเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน ประกอบด้วย

9.1 ต้องมีการจัดทำแผนด้านระบบสารสนเทศ

9.2 ต้องมีการจัดทำแผนด้านระบบคอมพิวเตอร์และระบบเครือข่าย

9.3 ต้องมีการจัดทำแผนด้านบุคลากรผู้รับผิดชอบ สถานที่ในการปฏิบัติงาน เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน

10. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ประกอบด้วย

10.1 ต้องมีการจัดทำแผนบริหารความเสี่ยงด้านระบบสารสนเทศ

10.2 ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง

11. บริษัทกำหนดความรับผิดชอบให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

11.1 ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงเป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

11.2 ระดับปฏิบัติ

1) การกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

1.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

1.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน ผู้รับผิดชอบ ได้แก่

2.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

2.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

2.3) ผู้ใช้งาน

3) การควบคุมการเข้าถึงเครือข่าย ผู้รับผิดชอบ ได้แก่

3.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

3.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

3.3) ผู้ใช้งาน

4) การควบคุมการเข้าถึงระบบปฏิบัติการ ผู้รับผิดชอบ ได้แก่

4.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

4.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

5) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ผู้รับผิดชอบ ได้แก่

5.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

5.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

6) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

6.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

6.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

7) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ผู้รับผิดชอบ ได้แก่

7.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

7.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

8) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

8.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

8.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

9) การจัดทำแผนเตรียมความพร้อมในการใช้งานฉุกเฉิน ผู้รับผิดชอบ ได้แก่

9.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

9.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

10) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

10.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

10.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

11) นโยบายการสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

11.1) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

11.2) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

องค์ประกอบของนโยบาย

1. คำนิยาม
2. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อม (Physical and Environment Security)
3. นโยบายและแนวปฏิบัติการควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศ (Access Control Policy)
4. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)
5. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)
6. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)
7. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)
8. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)
9. นโยบายและแนวปฏิบัติระบบสำรองของสารสนเทศ (Backup Policy)
10. นโยบายและแนวปฏิบัติการประเมินความเสี่ยง
11. นโยบายและแนวปฏิบัติการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ และระบบคอมพิวเตอร์
12. การกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัย
13. ขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Scope of Information Security Management System)
14. บริบทขององค์กร (Context of the organization)
15. ความเป็นผู้นำ (Leadership)
16. การประเมินผลการดำเนินการ (Performance evaluation)
17. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)
18. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
19. การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Compliance)
20. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)
21. นโยบายและแนวปฏิบัติการกำหนดบัญชีผู้ใช้งานและรหัสผ่าน (User Management Policy)

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน)

ฝ่ายเทคโนโลยีสารสนเทศ หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายใน บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน)

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หมายถึง ผู้บังคับบัญชาในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในบริษัท

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของบริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน)

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำเพื่อให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role)

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) เช่น กรรมการผู้จัดการ เป็นต้น

ผู้ดูแลระบบ หรือเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่น เพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

เจ้าหน้าที่ หมายถึง พนักงานแผนกต่างๆ ของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน)

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

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

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information system Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็นพื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือมอบอำนาจการใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบครัน (Integrity) และสภาพพร้อมใช้งาน (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธการรับผิด (non-repudiation) และความหน้าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัส (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพ และสิ่งแวดล้อม
(Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่การใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวนโยบายและแนวปฏิบัติ

แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ของบริษัท มีดังนี้

1. **ด้านการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม** (Physical and Environmental Security)

    1.1 ศูนย์กลางข้อมูลและระบบเครือข่าย (Data Center and Network Center) ผู้ดูแลระบบเครือข่าย ผู้ดูแลข้อมูลสารสนเทศ มีหน้าที่ปฏิบัติดังนี้

        1.1.1 ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ใช้งาน ได้แก่ ข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสารภายใน ระบบเครือข่ายสื่อสารภายนอก ห้องควบคุมการปฏิบัติงาน พื้นที่จัดเก็บอุปกรณ์ต่าง ๆ พื้นที่จัดเก็บเอกสาร สื่อบันทึก เป็นต้น ให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน

        1.1.2 ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิและลำดับชั้นในการเข้าถึงพื้นที่ใช้งานข้อมูลระบบสารสนเทศระบบเครือข่ายสื่อสาร

        1.1.3 ให้ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้าออกพื้นที่ และกำหนดพื้นที่ที่มีความเสี่ยงห้ามมิให้บุคคลภายนอกหรือผู้มีส่วนเกี่ยวข้องเข้าถึงได้

        1.1.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาเชื่อมต่อกับระบบเครือข่ายภายในหน่วยงาน จะต้องขออนุญาตใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

        1.1.5 มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำ และเครื่องดับเพลิง ระบบปรับอากาศ และควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ

1.2 การติดตั้งระบบสายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security) ผู้ดูแลระบบเครือข่ายมีหน้าที่ปฏิบัติดังนี้

1.2.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

1.2.2 ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

1.2.3 ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

1.2.4 ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

1.2.5 วางแผนการใช้งานสายไฟเบอร์ออฟติก (Fiber Obtics) แทนสายสัญญาณสื่อสารแบบเดิมกับข้อมูลที่มีความสำคัญ

1.3 การบำรุงรักษาอุปกรณ์ (Equipment maintenance) ผู้ดูแลทรัพย์สิน บริษัทผู้รับจ้างบริการ มีหน้าที่ปฏิบัติดังนี้

1.3.1 ผู้ดูแลทรัพย์สินกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่หน่วยงานกำหนด

1.3.2 บริษัทผู้รับจ้างปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่กำหนด

1.3.3 บริษัทผู้รับจ้างจัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

1.3.4 บริษัทผู้รับจ้างจัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

1.3.5 ผู้ดูแลทรัพย์สิน ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

1.3.6 ผู้ดูแลทรัพย์สิน จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอกเป็นลายลักษณ์อักษร

1.4 การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of property) ผู้ดูแลทรัพย์สิน หรือผู้ได้รับมอบหมายจากผู้บริหาร มีหน้าที่ปฏิบัติดังนี้

1.4.1 ผู้บริหารมอบอำนาจ หรือกำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน

1.4.2 กำหนดมาตรการความปลอดภัยและผู้รับผิดชอบเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน

1.4.3 ควบคุมดูแลให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน และต้องได้รับอนุญาตจากผู้มีอำนาจ เท่านั้น

1.4.4 กำหนดระยะเวลาของการนำทรัพย์สินออกไปใช้งานนอกหน่วยงาน

1.4.5 บันทึกข้อมูลการนำทรัพย์สินของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำทรัพย์สินส่งคืน พร้อมทั้งมีการบันทึกผู้รับผิดชอบในการดูแลรักษาทรัพย์สินหรืออุปกรณ์นอกพื้นที่

1.4.6 เมื่อมีการนำทรัพย์สินส่งคืน ให้ตรวจสอบจำนวนทรัพย์สินกับเอกสาร การชำรุดเสียหายของทรัพย์สินด้วยทุกครั้ง

1.4.7 บุคลากรที่มีส่วนเกี่ยวข้องทุกคนต้องไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะโดยไม่มีผู้รับผิดชอบ

1.4.8 เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

1.5 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment) ผู้ดูแลทรัพย์สินมีหน้าที่ปฏิบัติดังนี้

1.5.1 ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

1.5.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

1.5.3 เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

(1) คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับ และไม่แน่ใจว่าลับหรือไม่ให้อยู่ในกลุ่มเอกสารลับ

(2) ทำลายข้อมูลในสื่อบันทึกข้อมูล เพื่อป้องกันการกู้คืน โดยใช้วิธีการ ดังนี้

- ☐ ประเภท Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย
- ☐ ประเภทกระดาษ ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- ☐ ประเภทแผ่น CD/DVD ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น CD/DVD
- ☐ ประเภทเทป ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
- ☐ ประเภทฮาร์ดดิสก์ ใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์

1.6 การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ ผู้ดูแลระบบ ผู้ดูแลข้อมูล และเจ้าหน้าที่ที่เกี่ยวข้อง มีหน้าที่ปฏิบัติดังนี้

1.6.1 จัดแบ่งหมวดหมู่ประเภทของเอกสารและจัดหาสถานที่จัดเก็บเอกสารที่เหมาะสม

1.6.2 จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัยตามที่กำหนด

1.6.3 ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

1.6.3 ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

2. ด้านการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

2.1 ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ผู้ดูแลเครือข่าย และผู้ดูแลระบบ มีหน้าที่ปฏิบัติดังนี้

2.1.1 ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

2.1.2 จัดเก็บบันทึกการติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ

2.1.3 ไม่ควรติดตั้งซอร์สโค้ด และคอมไพเลอร์ (complier) ของระบบงานในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

2.1.4 จัดเก็บซอร์สโค้ดและไลบรารี่ของซอฟต์แวร์ระบบ ไว้ในสถานที่ที่มีความมั่นคงปลอดภัยและกำหนดลำดับชั้นของสิทธิการเข้าถึงข้อมูล

2.1.5 ให้มีการระบุความต้องการทางสารสนเทศ สำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

2.1.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศให้ถูกต้องตรงตามความต้องการของระบบ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ไว้ให้บริการ

2.1.7 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวน ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

2.1.8 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำ เป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

2.2 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก ผู้ดูแลระบบ และผู้ดูแลข้อมูล มีหน้าที่ปฏิบัติดังนี้

2.2.1 กำกับ ควบคุม ดูแล โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างจากภายนอก

2.2.2 ระบุชื่อผู้รับผิดชอบ หน้าที่ความรับผิดชอบ โครงการพัฒนาซอฟต์แวร์โดยบริษัทผู้รับจ้างให้บริการจากภายนอก

2.2.3 ให้กำหนดเรื่องลิขสิทธิ์ของซอฟต์แวร์ ซอร์สโค้ด และซอฟต์แวร์ที่ใช้ในการพัฒนาและติดตั้งต้องเป็นของหน่วยงานทั้งหมด

2.2.4 ศูนย์จัดหาสถานที่ที่ใช้ในการพัฒนาซอฟต์แวร์ในกรณีที่บริษัทผู้รับจ้างต้องเข้ามาดำเนินการพัฒนา และทดสอบซอฟต์แวร์ระบบในหน่วยงาน

2.2.5 กำหนดสิทธิการเข้าถึงอุปกรณ์และสารสนเทศเพื่อใช้ในการพัฒนาซอฟต์แวร์ให้กับบริษัทผู้รับจ้างได้เท่าที่จำเป็น

2.2.6 จัดเก็บบันทึกข้อมูลการเข้า-ออกพื้นที่ของเจ้าหน้าที่หน่วยงานภายนอก (Outsource) และบันทึกการเข้าใช้งานระบบเครือข่ายของหน่วยงาน

2.2.7 ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

2.2.8 ผู้ดูแลระบบจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับจัดการช่องโหว่ของซอฟต์แวร์ระบบต้องมีรายละเอียดอย่างน้อย

- ☐ ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน
- ☐ หน่วยงานที่ติดตั้ง
- ☐ เครื่องที่ติดตั้ง
- ☐ ผู้ผลิตซอฟต์แวร์
- ☐ ชื่อผู้รับผิดชอบซอฟต์แวร์หรือระบบงาน

2.2.9 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

2.3 มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ผู้ดูแลระบบมีหน้าที่บันทึกข้อมูลดังนี้

2.3.1 ชื่อบัญชีผู้ใช้งาน

2.3.2 วันเวลาที่เข้าออก-ระบบ

2.3.3 เหตุการณ์สำคัญที่เกิดขึ้น

2.3.4 การเปลี่ยนคอนฟิกกูเรชั่น (configuration) ของระบบ

2.3.5 แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

2.3.6 ไอพีแอดเดรสที่เข้าถึง

2.3.7 โพรโตคอลเครือข่ายที่ใช้

2.4 ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

2.5 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

3. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์

3.1 การใช้งานทั่วไป

3.1.1 ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลและรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของหน่วยงาน

3.1.2 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

3.1.3 การรับหรือคืนทรัพย์สินจะต้องถูกบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแล

3.1.4 ผู้ใช้งานจะต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงาน หรือเป็นข้อมูลส่วนบุคคล

3.1.5 ผู้ใช้งานจะต้องรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง โดยผู้ใช้งานแต่ละคนจะต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองโดยเฉพาะ ห้ามมิให้ใช้ร่วมกับผู้อื่น ห้ามมิให้ทำการเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

3.1.6 ห้ามไม่ให้ผู้ใช้งานใช้โปรแกรมบางประเภท เช่น บิตทอร์เรนต์ (BitTorrent), อีมู (emule) เป็นต้น เว้นแต่จะได้รับอนุญาต

3.1.7 ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์

3.1.8 คอมพิวเตอร์ของผู้ใช้งานจะติดตั้งโปรแกรมป้องกันโปรแกรมประสงค์ร้าย (Anti-Mailware) ตามที่หน่วยงานได้กำหนด

3.1.9 ตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องในศูนย์ฯให้ตรงกันโดยให้อิงกับเวลามาตรฐานกลางของโลก เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

3.2 การสำรองข้อมูลและการกู้คืน

3.2.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

3.2.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

3.2.3 ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

4. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

4.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

4.2 เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล หรือใช้การพิสูจน์ตัวตนด้วย Token Key

4.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

4.5 มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

5. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

5.1 การใช้งานสำหรับผู้ใช้งาน

5.1.1 ห้ามมิให้มีการส่งหรือใช้ E-mail ที่ผิดกฎระเบียบของฝ่ายเทคโนโลยีสารสนเทศ หรือกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

5.1.2 E-mail จะถูกเก็บเป็นความลับ ห้ามผู้ใดพยายามเข้าถึง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิใน E-mail ดังกล่าว

5.1.3 ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายลูกโซ่ ข่มขู่ ลามกอนาจาร หรือไม่สุภาพ

5.1.4 ห้ามมิให้มีการส่งหรือใช้ E-mail ที่เป็นจดหมายกระจาย โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ

5.1.5 การรับส่งเอกสารจะต้องใช้อีเมล์ของหน่วยงาน ที่ฝ่ายเทคโนโลยีสารสนเทศออกให้เท่านั้น

5.2 แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (system administrator)

5.2.1 กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

5.2.2 กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (password) ผิดพลาดได้ไม่เกิน 3 ครั้ง

5.2.3 มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

5.2.4 มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (user access management) ที่ได้กำหนดไว้อย่างเคร่งครัด

6. **การใช้งานระบบอินเทอร์เน็ต** (internet)

6.1 การควบคุมการใช้งาน (Access Control Policy)

6.1.1 ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบเครือข่ายของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงานเท่านั้น

6.1.2 มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

6.1.3 มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

6.1.4 มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

6.1.5 การเข้าถึงระบบด้วย Remote User ต้องได้รับการอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และควบคุมดูแลโดยเจ้าหน้าที่ที่ได้รับมอบหมาย

6.1.6 ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสมหากผู้ใช้งานกระทำการใดๆ ในทางที่ผิด

6.1.7 ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบด้วย

6.2 การใช้และการเปลี่ยนรหัสผ่าน สำหรับใช้ในการเข้าถึงฐานข้อมูลของเจ้าหน้าที่ ต้องปฏิบัติดังนี้

6.2.1 การกำหนดให้รหัสผ่านควรมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยต้องผสมผสานกันระหว่างตัวอักษรตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

6.2.2 ไม่ควรกำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

6.2.3 ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

6.2.4 ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

6.2.5 ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

6.2.6 ถ้ารหัสผ่านถูปกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

6.2.7 เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น

6.2.8 ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

6.3 การใช้งานเครือข่ายไร้สาย (Wireless Policy) ปฏิบัติดังนี้

6.3.1 ไม่อนุญาตให้ผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer network

6.3.2 การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

6.3.3 เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

6.3.4 ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็น access point, wireless routers, wireless USB client, หรือ wireless card ภายในบริษัท ยกเว้นจะได้รับอนุญาตจากหน่วยงานผู้รับผิดชอบ

6.3.5 การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan) จะต้องได้รับอนุญาตจากผู้ดูแลระบบและมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายขององค์กร

6.4 การใช้งานระบบไฟร์วอล และระบบ IDS/IPS ปฏิบัติดังนี้

6.4.1 มีการระบุขอบเขต (Truth Zones) ของเครือข่าย เช่น เครือข่าย Internet, web servers, remote access โซนการเชื่อมต่อภายนอกในองค์กร และโซนภายในเครือข่าย และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

6.4.2 มีการระบุการควบคุมระบบ firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

6.4.3 มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

6.4.4 มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

6.5 การใช้งานเครือข่าย (Internet Security Policy) ปฏิบัติดังนี้

6.5.1 มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

6.5.2 มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

6.5.3 มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

6.5.4 มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

6.5.5 จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

6.6 ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับเครือข่ายอื่น นอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

6.7 ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันทีถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

6.8 การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่าย ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

6.9 ตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

6.10 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

6.11 ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้ดูแลระบบ

นโยบายและแนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control Policy)

วัตถุประสงค์

เพื่อให้ผู้รับผิดชอบ และผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงานได้รับรู้เข้าใจ นโยบายในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) (**"บริษัท"**) และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

แนวนโยบายและแนวปฏิบัติ

แนวนโยบายและแนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control Policy) ของบริษัท มีดังนี้

1. **การควบคุมการเข้าถึงและใช้งานสารสนเทศ** (Access Control)

   1.1 **แนวนโยบาย**

   (1) ผู้ที่เข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

   (2) มีการจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มเข้าใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

   (3) มีการกำหนดสิทธิการใช้งานและการเข้าถึงตามระดับความสำคัญของผู้ใช้งาน ซึ่งเห็นชอบโดยผู้บริหารของหน่วยงาน

   (4) มีการกำหนดสิทธิในการเข้าใช้งานแก่ผู้ใช้งานให้ตรงตามหน้าที่ความรับผิดชอบ โดยสามารถตรวจสอบสิทธิได้

   (5) การเข้าถึงระบบด้วยการ Remote User ต้องได้รับการอนุญาตและสิทธิการเข้าใช้งานระบบผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และควบคุมดูแลโดยเจ้าหน้าที่ที่ได้รับมอบหมาย

   (6) ผู้ดูแลระบบสามารถควบคุมหรือตัดสิทธิการใช้งานของผู้ใช้งานได้ตามความเหมาะสม หากผู้ใช้งานกระทำการใดๆ ในทางที่ผิดตามประกาศของบริษัท

   (7) ผู้ใช้งานที่ผ่านการตรวจสอบสิทธิทุกคนจะต้องทราบถึงข้อตกลงในการใช้งานระบบสารสนเทศนั้น ๆ ด้วย

(8) จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(9) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(9.1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- ☐ อ่านอย่างเดียว (Read Only)
- ☐ สร้างข้อมูล (Create)
- ☐ ป้อนข้อมูล
- ☐ แก้ไข (Edit)
- ☐ อนุมัติ (Authorize)

(9.2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(9.3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

1.2 แนวทางปฏิบัติ

หน่วยงานได้กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ การจัดแบ่งระดับการเข้าถึงข้อมูลและสิทธิ เวลา และช่องทางการเข้าถึงข้อมูล ดังนี้

(1) การจัดแบ่งประเภทสิทธิของผู้เข้าถึงข้อมูลแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- ☐ อ่านอย่างเดียว (Read Only)
- ☐ สร้างข้อมูล (Create)
- ☐ แก้ไข (Edit)
- ☐ ลบ (Delete)
- ☐ อนุมัติ (Authorize)

(2) การจัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ ระดับความสำคัญมากที่สุด ระดับความสำคัญปานกลาง ระดับความสำคัญน้อย

(3) การจัดแบ่งลำดับชั้นความลับของข้อมูล ได้แก่

- ☐ ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ☐ ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

☐ ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

☐ ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

ตารางการกำหนดความสำคัญและการเข้าถึงข้อมูล

ข้อมูล	ข้อมูลลับที่สุด	ข้อมูลลับมาก	ข้อมูลลับ	ข้อมูลทั่วไป
1.ข้อมูลเงินเดือน ค่าตอบแทน	✓			
2.ข้อมูลส่วนบุคคล		✓		
3.ข้อมูลการรักษาพยาบาล	✓			
4.ข้อมูลการจัดซื้อ-จัดจ้าง			✓	
5.ข้อมูลด้านการเงิน การบัญชี		✓		
6.ข้อมูลสถิติ				✓
7.ข้อมูล Packet โปรโมชั่น				✓

(4) การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท ประเภทผู้เกี่ยวข้องที่สามารถเข้าถึงข้อมูล ได้แก่

☐ ระดับชั้นสำหรับผู้บริหารระดับสูง หมายถึง กรรมการผู้จัดการ

☐ ระดับชั้นสำหรับผู้บริหารทั่วไป หมายถึง ผู้อำนวยการฝ่าย ผู้จัดการฝ่าย

☐ ระดับชั้นสำหรับผู้ใช้งานทั่วไป หมายถึง บุคลากรในบริษัท

☐ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย หมายถึง ผู้ที่มีหน้าที่รับผิดชอบดูแลในระบบงานนั้นๆ

(5) การกำหนดเวลาที่สามารถเข้าถึงได้ ตลอดเวลา 24 ชั่วโมง 7 วัน

(6) การกำหนดช่องทางการเข้าถึง ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้นั้น จะต้องได้รับสิทธิจากหน่วยงาน โดยมีการกำหนดบัญชีผู้ใช้งานตามระดับการเข้าถึง ให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น โดยมีช่องทางการเข้าถึง ดังนี้

☐ ระบบเครือข่ายภายใน (Intranet)

☐ ระบบเครือข่ายอินเตอร์เน็ต (Internet)

☐ ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(7) กำหนดเงื่อนไขในการระงับหรือยกเลิกสิทธิของผู้ใช้งานในการใช้งานระบบสารสนเทศในแต่ละประเภทของข้อมูล

(8) ผู้ดูแลระบบต้องมีการทบทวนและปรับปรุงสิทธิให้สอดคล้องกับข้อกำหนดการใช้งานตามข้อกำหนดด้านความมั่นคงปลอดภัยของบริษัท

2. **การควบคุมสิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ** (High Privilege User ID)

2.1 **แนวนโยบาย**

นโยบายและแนวปฏิบัติการควบคุมสิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ (High Privilege User ID) ของมีดังนี้

(2.1) การควบคุมสิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ (High Privilege User ID)

(1.1) ผู้ที่ใช้งานและได้รับสิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศโดยตำแหน่ง

☐ กรรมการผู้จัดการ

☐ ผู้จัดการฝ่ายเทคโนโลยีสารสเทศ

(1.2) ผู้ที่ใช้งานและได้รับสิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ โดยหน้าที่และการปฏิบัติงาน

☐ เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศจะได้รับสิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ เป็นครั้งคราวจาก ผู้ได้รับสิทธิ์พิเศษในข้อ 1

☐ ผู้ใช้งานหรือบุคคลภายในที่เข้ามาดูแลระบบ เป็นครั้งคราวจาก ผู้ได้รับสิทธิ์พิเศษในข้อ 1 และมีการกับกำดูแลอย่างใกล้ชิด และมีระยะเวลาการครอบครองชัดเจน

2.2 **แนวปฏิบัติ**

(1) การขอสิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ

การใช้ใช้สิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศจะต้องมีการกรอกแบบฟอร์มขอใช้งานเมื่อเหตุจำเป็นเมื่อมีเหตุเร่งด่วนและต้องยืนยันตัวตนของผู้รองขอ โดยมีขั้นตอนและคุณสมบัติประกอบดังนี้

☐ ต้องมีความเกี่ยวข้องกับระบบสารสนเทศนั้นๆ

☐ ต้องได้รับมอบหมายจากผู้มีส่วนเกี่ยวข้องของระบบ

☐ ต้องมีเอกสารยืนยันตัวตนที่ชัดเจน เช่น บัตรพนักงาน หรือ บัตรประชาชน

☐ ต้องกรอกแบบฟอร์มการขอใช้สิทธิ์สูงสุด และระบุเวลาการขอใช้สิทธิ์ให้ชัดเจนเป็นรายครั้ง

(2.1) การใช้สิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ

ผู้ที่ได้รับสิทธิ์ต้องใช้งานอย่างระมัดระวังตลอดระยะเวลาที่ได้รับสิทธิ์โดยสิทธิ์นั้นจะมีระยะเวลาตามที่ได้รับอนุญาต และต้องไม่ส่งต่อสิทธิ์ที่ได้รับให้บุคคลอื่น หากตรวจสอบพบจะดำเนินการตามบทลงโทษสูงสุด

(2.1) การสิ้นสุดระยะเวลาการใช้สิทธิ์พิเศษการเข้าถึงและใช้งานระบบสารสนเทศ

เมื่อผู้ขอใช้งานสิทธิ์ครบระยะเวลาที่ได้รับอนุญาต ผู้ที่ให้สิทธิ์จะทำการยกเลิกสิทธิ์ทันที และผู้ให้สิทธิ์จะมีการตรวจสอบความถูกต้อง สำรวจความเสียหายที่อาจเกิดขึ้น โดยผู้ขอใช้สิทธิ์จะไม่สามารถเข้าถึงสิทธิ์ที่ได้รับอีก จนกว่าจะมีการขอใช้สิทธิ์อีกครั้ง

2.3 **บทลงโทษ**

(1) ผู้ที่ได้รับสิทธิ์การใช้งานต้องใช้งานอย่างระมัดระวัง ในช่วงเวลาที่ดีรับสิทธิ์นั้น

(2) หากมีข้อผิดพลาดขณะถือครองสิทธิ์ และผู้ดูแลระบบตรวจสอบได้ว่าการกระทำใดๆ ที่เกิดขึ้นแล้วมีผลกระทบต่อระบบหรือเสียหาย ให้ถือเป็นความรับผิดชอบของผู้ใช้สิทธิ์และไม่สามารถปฏิเสธความรับผิดชอบได้

(3) หากระบบสารสนเทศเกิดความเสียหายและความเสียหายที่เกิดขึ้นนั้นประเมินเป็นมูลค่าได้ ผู้ที่กระทำให้เกิดความเสียหายนั้นต้องกระทำการใดๆ ให้ระบบสามารถใช้งานได้สมบูรณ์ ไม่เช่นนั้นผู้ให้สิทธิ์มีสิทธิ์นำบุคคลอื่นเข้ามาดำเนินการเพื่อทำให้ระบบสารสนเทศสามารถใช้งานได้ดังเดิม หากมีค่าใช้จ่ายเกิดขึ้น ผู้กระทำให้เกิดความเสียหาย ต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

3. **การบริหารจัดการการเข้าถึงของผู้ใช้งาน** (User Access Management)

3.1 **แนวนโยบาย**

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และเพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต จะต้องประกอบด้วย

(1) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (user access) ประกอบด้วย

(1.1) ประชาสัมพันธ์ให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(2) การลงทะเบียนผู้ใช้งาน (user registration) ประกอบด้วย

(2.1) ต้องกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานระบบตามความเหมาะสมในแต่ละระบบงานที่ได้รับอยู่ในความรับผิดชอบของบริษัท

(2.2) ต้องจัดทำบัญชีผู้ใช้งานระบบ อย่างน้อยต้องประกอบด้วย

- ☐ รายชื่อผู้ขออนุญาตเข้าใช้งานระบบ
- ☐ รายชื่อผู้ได้รับการอนุมัติเข้าใช้งานระบบ
- ☐ กำหนดสิทธิการเข้าใช้งานข้อมูล
- ☐ ผู้อนุมัติ หรือผู้ดูแลระบบที่ได้รับมอบหมาย
- ☐ การยกเลิกหรือเพิกถอนสิทธิการเข้าใช้งานระบบ

(2.3) ต้องกำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(2.4) ต้องกำหนดหลักเกณฑ์ในการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(2.5) ต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบหรือความต้องการของบริษัท

(3) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ประกอบด้วย

(3.1) มีการแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ซึ่งหมายรวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงข้อมูลสารสนเทศ

(3.3) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูล ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

(3.3) ผู้ใช้มีสิทธิเข้าใช้งานผ่านระบบเครือข่าย ระบบงาน และระบบปฏิบัติการตามที่ผู้ดูแลระบบกำหนด

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ประกอบด้วย

(4.1) มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานให้มีความมั่นคงปลอดภัยอย่างรัดกุม

(4.2) มีการกำหนดให้เครื่องแม่ข่ายต้องกำหนดรหัสผ่านของผู้ดูแลระบบของแต่ละระบบโดยเฉพาะ และให้ทราบรหัสผ่านเฉพาะผู้เกี่ยวข้องเท่านั้น และไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน

(4.3) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(4.4) ผู้ใช้งานระบบควรทำการแจ้งผู้ดูแลระบบ หากต้องการทำกิจกรรมที่อาจมีผลกระทบต่อความปลอดภัยของระบบ และผู้ใช้งานระบบควรจะแจ้งผู้ดูแลระบบความปลอดภัยของระบบทันที ถ้าหากสงสัยว่าได้กระทำกิจกรรมที่มีผลต่อความปลอดภัยของระบบ

(4.5) การละเมิดหรือบุกรุกโดยผู้ไม่มีสิทธิในการเข้าถึงข้อมูลหรือระบบเครือข่าย ผู้ละเมิดจะถูกลงโทษตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

(4.6) มีการตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy เป็นต้น

(4.7) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

(5) การทบทวนสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน (review of user access rights) ประกอบด้วย

(5.1) สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอโดยผู้ดูแลระบบอย่างน้อยปีละ 1 ครั้ง

(5.2) สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวนและจัดสรรใหม่ เมื่อมีการเคลื่อนย้ายบุคลากรภายในหน่วยงาน

(5.3) การกำหนดสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อมั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

(5.4) การเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

3.2 แนวทางปฏิบัติ

(1) การลงทะเบียนผู้ใช้งาน (user regitration) มีดังนี้

(1.1) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ

(1.2) จัดทำคู่มือการใช้งานระบบสารสนเทศให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบสารสนเทศทราบ

(1.3) ให้ผู้ใช้งานกรอกข้อมูลการขอใช้ระบบงานสารสนเทศลงในแบบฟอร์ม และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานระบบ

(1.4) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย พิจารณาคำขอลงทะเบียนอนุมัติ กำหนดระดับการเข้าใช้งานสารสนเทศเท่าที่จำเป็นในแต่ละระบบงาน และทำการบันทึกจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศทุกครั้ง

(1.5) ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล และไม่ซ้ำซ้อนกัน

(1.6) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(1.7) กำหนดบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และกำหนดสิทธิการใช้งานระบบเท่าที่จำเป็นในแต่ละระบบงาน

(1.8) ต้องตรวจสอบและมอบหมายสิทธิที่เหมาะสมต่อหน้าที่ความรับผิดชอบ หรือความต้องการของบริษัทให้ผู้มีส่วนเกี่ยวข้องกับระบบงาน

(1.9) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(1.10) ผู้ดูแลระบบจัดทำการบันทึกการเปลี่ยนแปลงบัญชีผู้ใช้งานแต่ละรายในระบบเมื่อได้รับรายงาน บัญชีรายชื่อผู้ใช้งานได้ถูกเพิกถอนสิทธิ หรือลาออก หรือเปลี่ยนแปลงตำแหน่ง หรือย้ายหน่วยงาน

(2) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายต้องดำเนินการ ดังนี้

(2.1) ผู้ดูแลระบบแสดงกระบวนการในการมอบหมาย หรือการกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(2.2) ผู้ดูแลระบบสามารถบันทึกการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศตามที่ได้รับอนุมัติ หรือตามอำนาจหน้าที่ความรับผิดชอบ หรือตามความจำเป็นในการใช้งานระบบเท่านั้น

(2.3) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศมอบอำนาจหน้าที่ความรับผิดชอบให้ผู้ดูแลระบบหรือมอบหมายสิทธิการบริหารจัดการบัญชีผู้ใช้งานให้ผู้อื่นที่มีส่วนเกี่ยวข้องกับระบบงานดำเนินการแทนก็ได้

(2.4) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานระบบ

(2.5) บันทึกและจัดเก็บข้อมูลการเปลี่ยนแปลงบัญชีผู้ใช้งาน การมอบหมายอำนาจหน้าที่หรือสิทธิการควบคุมการใช้งานทุกครั้ง

(2.6) ทำการทบทวนระดับและสิทธิของผู้ใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

(3) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) มีดังนี้

(3.1) จัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบ

(3.2) กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมผสานตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(3.3) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(3.4) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(3.5) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(3.6) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(3.7) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(3.8) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(3.9) ในกรณีระบบงานใดอนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันทีสำหรับการเข้าใช้งานครั้งแรก

(3.10) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(3.11) ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

(3.12) ไม่อนุญาตให้เจ้าหน้าที่หรือผู้ใช้งานระบบใช้รหัสผ่านร่วมกัน

(3.13) ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(4) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) มีดังนี้

(4.1) การทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ

(4.2) ปรับปรุงบัญชีผู้ใช้งาน และบันทึกการเปลี่ยนแปลงสิทธิบัญชีผู้ใช้งาน

(4.3) การทบทวนสิทธิการเข้าใช้งาน ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาโดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(4.4) ทบทวนสิทธิ์การเข้าถึง(User review)อย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนสิทธิ์การเข้าถึงและใช้งานระบบ ในโมดูลต่างๆ ของบัญชีผู้ใช้ ว่ามีความเหมาะสมหรือไม่

(4.5) ตรวจทานบัญชีผู้ใช้ที่ยังคงอยู่ในระบบอย่างน้อยปีละ 4 ครั้ง(ตามไตรมาส) เพื่อตรวจทานบัญชีผู้ใช้ที่อยู่ในระบบ ว่ายังคงสถานะเป็นพนักงานและมีสิทธิ์ใช้งานอยู่หรือไม่

4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

4.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ โดยได้กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานทุกคนในบริษัท และผู้ดูแลระบบครอบคลุมเรื่องต่าง ๆ ดังนี้

(1) ต้องกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ เพื่อกำหนดแนวทางในการป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงระบบและอุปกรณ์ต่าง ๆ ของหน่วยงานในขณะที่ไม่มีผู้ดูแลควรมี ดังนี้

(2.1) มีมาตรการป้องกันดูแลอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(2.2) สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหายหรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(2.3) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้งเสมอ

(2.4) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(2.5) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่มีการดูแลชั่วคราว

(2.6) ผู้บริหารมอบหมายหน่วยงานผู้รับผิดชอบ หรือแต่งตั้งผู้มีส่วนเกี่ยวข้องในการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหาย หรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศ

(3) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and Clear screen Policy) ควรมีดังนี้

(3.1) มีมาตรการการควบคุมดูแลบริหารทรัพย์สินของหน่วยงานไม่ให้เกิดความเสียหายหรือสูญหาย หรือถูกบุกรุกข้อมูลสารสนเทศจากผู้ไม่มีส่วนเกี่ยวข้อง

(3.2) หน่วยงานผู้รับผิดชอบจะต้องจัดหาสถานที่ที่ใช้ในการจัดเก็บเอกสาร สื่อบันทึกข้อมูลเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องให้มีความเหมาะสมไม่ให้ได้รับความเสี่ยง

(3.3) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ หรือระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(3.4) บุคลากรของบริษัททุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(3.5) ต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(3.6) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(3.7) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของบริษัท อย่างสม่ำเสมอ

(3.8) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(3.9) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่าง ๆ ของบริษัทจะต้องขออนุญาต เพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่าง ๆ ของบริษัท และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบอำนาจก่อนเข้าพื้นที่ เท่านั้น

(3.10) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น ชื่อผู้ใช้งานและรหัสผ่าน

(3.11) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(4) ข้อมูลสารสนเทศใดที่เป็นความลับ ผู้ดูแลระบบอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ

(5) กำหนดให้ต้องบันทึกการทำงานของระบบสารสนเทศ บันทึกการปฏิบัติงานของผู้ใช้งาน (application log) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเพื่อประโยชน์ในการตรวจสอบไว้เป็นเวลาอย่างน้อย 1 เดือน หรือตามที่หน่วยงานกำหนด

4.2 แนวทางปฏิบัติ

(1) วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password use) มีข้อปฏิบัติ ดังนี้

(1.1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(1.2) กำหนดรหัสผ่านต้องมีความยาวมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยต้องผสมผสานตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(1.3) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(1.4) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(1.5) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(1.6) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(1.7) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(1.8) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(1.9) ต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอทุก 3 เดือน หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(1.10) หลีกเลี่ยงการใช้รหัสผ่านเดียวกัน หรือรหัสผ่านเดิมสำหรับระบบงานอื่นๆ ที่ตนใช้งาน

(2) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ มีข้อปฏิบัติ ดังนี้

(2.1) ผู้ดูแลระบบ หรือผู้รับผิดชอบกำหนดข้อปฏิบัติในการป้องกันอุปกรณ์ระบบคอมพิวเตอร์และระบบสารสนเทศที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(2.2) สร้างให้ทุกคนต้องตระหนักและเอาใจใส่ต่อการป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหาย หรือสูญหาย หรือมีผู้ไม่พึงประสงค์เข้าถึงระบบและอุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

(2.3) เจ้าพนักงานเครื่องคอมพิวเตอร์ หรือผู้รับผิดชอบจะต้องมีมาตรการป้องกันระบบคอมพิวเตอร์และอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(2.4) ภายหลังการใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์เสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

(2.5) ติดตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(2.6) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

(3) การควบคุมทรัพย์สินและการใช้งานระบบ (Clear desk and Clear screen Policy) มีข้อปฏิบัติ ดังนี้

(3.1) ผู้ที่ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ หรือระบบเครือข่าย หรือระบบสารสนเทศของหน่วยงานจะต้องเป็นผู้ใช้งานที่ได้รับอนุญาตจากหน่วยงาน เท่านั้น

(3.2) บุคลากรของบริษัททุกคนอนุญาตให้เข้าใช้พื้นที่และอุปกรณ์ต่าง ๆ ได้ตามสิทธิที่หน่วยงานกำหนด เท่านั้น

(3.3) บุคลากรจะต้องตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(3.4) ต้องบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(3.5) ต้องจัดเก็บบันทึกเหตุการณ์การเข้า-ออกพื้นที่ของฝ่ายเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

(3.6) ต้องจัดเก็บบันทึกเหตุการณ์หรือกิจกรรมต่าง ๆ ของผู้ใช้งานตั้งแต่เริ่มใช้งานจนสิ้นสุดการใช้งาน เพื่อใช้เป็นฐานข้อมูลในการตรวจสอบ

(3.7) บุคคลภายนอกหรือเจ้าหน้าที่บริษัทที่เกี่ยวข้องกับโครงการต่าง ๆ ของบริษัทจะต้องขออนุญาต เพื่อเข้าใช้พื้นที่และใช้อุปกรณ์ต่าง ๆ ของฝ่ายเทคโนโลยีสารสนเทศ และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายอำนาจ ก่อนเข้าพื้นที่ฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

(3.8) ต้องตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(3.9) ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส การยืนยันตัวบุคคลผ่าน Proxy อย่างสม่ำเสมอ

(3.10) ผู้ดูแลระบบ หรือผู้รับผิดชอบจัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งระบุผู้รับผิดชอบเมื่อต้องให้บริการระบบเครือข่ายคอมพิวเตอร์

(3.11) ผู้ใช้งานระบบและเครื่องคอมพิวเตอร์ ต้องลงทะเบียนการใช้งานทุกครั้งเพื่อเป็นการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบทุกครั้ง

(3.12) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการการป้องกัน ดังนี้

- ☐ ให้ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- ☐ ต้องลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ☐ ต้องจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ☐ Log off เครื่องคอมพิวเตอร์ หรือล็อคหน้าจอทุกครั้งเมื่อไม่ได้ใช้งาน
- ☐ ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(3.13) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

5. **การควบคุมการเข้าถึงเครือข่าย** (Network Access Control)

5.1 **แนวนโยบาย**

เพื่อป้องกันการเข้าถึงระบบเครือข่าย บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด โดยไม่ได้รับอนุญาต ประกอบด้วย

(1) การกำหนดขอบเขตและสิทธิของผู้ใช้งานสามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานกำหนดเท่านั้น

(2) การกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(3) มีการทบทวนสิทธิการเข้าถึงบริการระบบเครือข่าย อย่างน้อยปีละ 4 ครั้ง และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานผู้รับผิดชอบ เท่านั้น

(4) มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้

(5) มีวิธีการระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) เพื่อใช้ในการตรวจสอบการเข้าถึงอุปกรณ์บนระบบเครือข่ายของหน่วยงาน

(6) มีการกำหนดหลักเกณฑ์ในการควบคุมและการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(7) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย และการตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(8) ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน

(9) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ของหน่วยงานที่มีการใช้ร่วมกัน หรือเชื่อมโยงระหว่างกันให้มีความสอดคล้องกับหน่วยงาน

(10) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย

(11) มีการกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน

5.2 แนวทางปฏิบัติ

(1) ผู้ดูแลระบบเครือข่ายจัดทำบันทึกการกำหนดขอบเขตและสิทธิของผู้ใช้งานที่สามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานตามที่กำหนดเท่านั้น

(2) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(3) ผู้ใช้งานต้องเข้าใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่หน่วยงานกำหนดขึ้นมา ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการ

ปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ 4 ครั้ง

(4) ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีกระบวนการในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้ ดังนี้

(4.1) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทุกครั้ง

(4.2) การอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ในการเข้าใช้งานต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิค รวมทั้งต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

(4.3) หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อน โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

(5) การระบุอุปกรณ์บนเครือข่าย (equipments identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(5.1) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศก่อนจึงจะสามารถดำเนินการได้

(5.2) ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

(5.3) จะต้องมีการจำกัดสิทธิการเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

(6) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(6.1) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล็อกอินเข้ามาใช้งาน

(6.2) ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันไว้ในห้องคอมพิวเตอร์แม่ข่ายที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(6.3) ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

(6.4) เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(6.5) ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง

(6.6) กำหนดสิทธิบุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

(6.7) บันทึกการเข้า-ออกพื้นที่บริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

(6.8) ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป

(6.9) ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลาง ที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) กันการโจรกรรม

(7) กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย และการตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(8) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(9) ทำการแบ่งแยกเครือข่าย (segregation in networks) สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น 2 เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

(10) มีการควบคุมการเชื่อมโยงเครือข่าย (network connection control) ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมโยงระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติอย่างน้อย ดังนี้

(10.1) การจำกัดสิทธิ การเข้าถึงเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตน

(10.2) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(10.3) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

(10.4) การเข้าใช้งานเชื่อมต่อเครือข่ายต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายทุกครั้ง

(10.5) ควบคุมไม่ให้เปิดเผยข้อมูลระบบเครือข่ายที่สำคัญในการเชื่อมต่อเข้าสู่ระบบได้แก่ หมายเลข IP Address Username และ Password เป็นต้น

(10.6) ผู้ใช้งานห้ามนำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

(11) มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

(11.1) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

(11.2) กำหนดให้มีการแปลงหมายเลขเครือข่ายย่อย

(11.3) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย หรือจำกัดสิทธิในการใช้บริการเครือข่ายของหน่วยงาน

(12) ผู้ดูแลระบบเครือข่ายกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก(remote access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน ที่ต้องผ่านการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน และต้องได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร เท่านั้น และผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดของหน่วยงานอย่างเคร่งครัด โดยดำเนินการดังนี้

(12.1) ผู้ดูแลระบบเครือข่ายต้องไม่เปิด port และ modem ทิ้งเอาไว้โดยไม่จำเป็น

(12.1) ปิดช่องทางการเชื่อมต่อเมื่อไม่ใช้งานแล้ว และเปิดใช้งานเมื่อมีการร้องขอเท่าที่จำเป็นเท่านั้น

(12.1) มีการควบคุมพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมตามความเหมาะสม

(12.1) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากภายนอก (remote access) ต้องได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

6. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

6.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ควรดำเนินการดังนี้

(1) การกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการจะต้องมีการควบคุม โดยการยืนยันตัวตนตามระบบรักษาความมั่นคงปลอดภัยของหน่วยงาน

(2) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้

(3) การระบุและยืนยันตัวตนของผู้ใช้งาน สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(4) การบริหารจัดการรหัสผ่าน (password management system) มีการแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(5) มีการจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้

(6) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(7) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

6.2 แนวทางปฏิบัติ

(1) ผู้ดูแลระบบ ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

(2) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

(2.1) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(2.2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(2.3) จำกัดการป้อนรหัสผ่านในกรณีป้อนรหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง

(2.4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

(3) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) กำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้ ดังนี้

(3.1) ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(3.2) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นของหน่วยงาน

(3.3) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key Hand Scan หรือ finger print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

(4) การบริหารจัดการรหัสผ่าน (password management system) ต้องแสดงผลการทำงานของการจัดการรหัสผ่านในลักษณะเชิงโต้ตอบ (interactive) หรือต้องทำงานในลักษณะอัตโนมัติ เพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านที่ได้ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(5) ต้องจำกัดการใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของหน่วยงานที่ได้กำหนดไว้ ให้ดำเนินการดังนี้

(5.1) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาต และยังไม่ผ่านการตรวจสอบ

(5.2) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อหน่วยงาน

(5.3) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(5.4) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(5.5) กำหนดให้ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(6) มีการกำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งานเป็นเวลา 15 นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา 10 นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(7) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(8) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

(9) กำหนดระยะเวลาในการจำกัดการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา 2 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง

7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

7.1 แนวนโยบาย

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ดำเนินการดังนี้

(1) กำหนดมาตรการการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

(2) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(3) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะได้รับการแยกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ

(4) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

7.2 แนวปฏิบัติ

(1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องดำเนินการ ดังนี้

(1.1) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามอำนาจหน้าที่ที่ควรได้รับจะต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

(1.2) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา 15 นาที ต้องทำการยุติการใช้งานทันที

(1.3) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

- ☐ กำหนดสิทธิให้กับผู้เข้าใช้งานระบบโดยการกำหนดรายชื่อผู้ใช้และรหัสผ่าน เพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น
- ☐ กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัสอย่างน้อย SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
- ☐ การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงาน กรณีข้อมูลที่เป็นความลับของหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

(1.4) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใดๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้นๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใดๆ ที่มีผลกระทบต่อระบบจะต้องเป็นผู้รับผิดชอบ

(2) ระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

(2.1) การแยกระบบสารสนเทศที่มีความสำคัญสูงและจำเป็นต้องได้รับการดูแลเป็นพิเศษ ฝ่ายเทคโนโลยีสารสนเทศต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ

ให้ทำงานอยู่บนเครื่องเซิร์ฟเวอร์ หรือคอมพิวเตอร์ไม่ใช้ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำ งานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องเครื่องคอมพิวเตอร์แม่ข่ายกลางที่มีสภาพแวดล้อมเหมาะสม

(2.2) ให้มีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ห้องคอมพิวเตอร์แม่ข่ายกลาง ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายกลาง และอื่นๆ เป็นต้น เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

(2.3) ควบคุมการเข้ามาใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกกำหนดสิทธิการเข้าใช้งานโดยกำหนดค่าที่ Firewall

(2.4) มีการควบคุมหรือป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

(3) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking)

(3.1) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย

(3.1) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในสำนักงานก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึง

(3.1) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นใด เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

(3.1) การขออนุมัติหรือยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย

8. **การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี** (Software Licensing and intellectual property and Preventing Malicious Software)

8.1 **แนวนโยบาย**

(1) บริษัทได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่บริษัทอนุญาตให้ใช้งานหรือที่บริษัทมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความรับผิดชอบ และความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดที่เกิดขึ้น รวมทั้งผู้บังคับบัญชาต้องรับผิดชอบความเสียหายที่เกิดขึ้นร่วมกัน

(2) ซอฟต์แวร์ที่บริษัทได้ติดตั้งบนคอมพิวเตอร์ไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากผู้บังคับบัญชา หรือผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

(3) คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่บริษัทได้ประกาศให้ใช้

(4) ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่พึงประสงค์ก่อนนำมาใช้งาน หรือเก็บบันทึกทุกครั้ง

(5) ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

(6) ผู้ใช้งานต้องพึงระวังไวรัส และโปรแกรมไม่พึงประสงค์ตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่แผนกเทคโนโลยีสารสนเทศ

(7) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องตัดการเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ต้องแจ้งแก่แผนกเทคโนโลยีสารสนเทศ

(8) ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาต

(9) ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของบริษัท สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

   (1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกการรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน ลักลอบทำเสานำข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

   (2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

   (3) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

   (4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

   (5) นำเสอนข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณี กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(10) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development) ดังนี้

(1) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(2) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(3) พิจารณากำหนดเรื่องการสงวนลิขสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการจากภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการจากภายนอกนั้น

(4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(5) หลังจากทำการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

(11) ซอฟต์แวร์ลิขสิทธิ์ที่กำหนดให้ติดตั้งบนเครื่องคอมพิวเตอร์ทุกเครื่อง เพื่อเป็นมาตรฐานในการใช้งานของบุคลากรของบริษัท มีรายการดังต่อไปนี้

ตารางซอฟต์แวร์ลิขสิทธิ์

โปรแกรม	วัตถุประสงค์การใช้งาน	License
HIMS	โปรแกรมสารสนเทศโรงพยาบาล	License
INFINITT MDHIH	โปรแกรมดูภาพ X-Ray	License
SBJ LIS	โปรแกรมสารสนเทศทางห้องปฏิบัติการ	License
Microsoft Office	โปรแกรม Word, Excel, Power Point, Outlook	License
Adobe Acrobat Reader	โปรแกรมเปิดไฟล์ .pdf	Freeware
Foxit Reader	โปรแกรมเปิดไฟล์ .pdf	Freeware
Google Chrome Browser	โปรแกรม Web Browser	Freeware
7 Zip	โปรแกรม Zip file ต่าง ๆ	Freeware
Kaspersky Security Antivirus	โปรแกรมป้องกันไวรัส	License
Adobe Creative Cloud	โปรแกรมสำหรับงานออกแบบ	License
Time Attendance	โปรแกรม Export ข้อมูลการมาทำงาน	License
Zoom	โปรแกรมประชุมออนไลน์	License

9. **การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย** (Wireless LAN Access Control)

9.1 **แนวนโยบาย**

หน่วยงานต้องมีการกำหนดมาตรการในการควบคุมและป้องกันการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) และหลักเกณฑ์การนำอุปกรณ์สื่อสารเคลื่อนที่เข้ามาใช้งานในระบบเครือข่ายไร้สาย เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของหน่วยงาน

9.2 **แนวปฏิบัติ**

(1) การใช้งานเครือข่ายไร้สาย (Wireless Policy)

(1.1) ไม่อนุญาตให้ผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer network

(1.2) การเข้าใช้ wireless จะต้องเข้าใช้ผ่าน username และ password ที่หน่วยงานกำหนด

(1.3) เจ้าหน้าที่มีสิทธิตรวจสอบเครื่องที่เชื่อมต่อผ่านระบบเครือข่ายไร้สายได้

(1.4) ห้ามมิให้ผู้ใดนำอุปกรณ์ wireless มาติดตั้งหรือเปิดใช้เองไม่ว่าจะเป็นอุปกรณ์กระจายสัญญาณ (access point), wireless routers, wireless USB client, หรือ wireless card ภายในหน่วยงาน ยกเว้นจะได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

(1.5) การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan) จะต้องได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และมีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์นั้น ๆ ก่อนเข้าใช้งานเครือข่ายของหน่วยงาน

(2) การใช้งานระบบไฟร์วอลล์ (Fire wall) และระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)

(2.1) มีการระบุขอบเขต (Trust Zones) ของเครือข่าย เช่น เครือข่าย Internet, web servers, โซนการเชื่อมต่อภายนอก เครือข่ายภายในองค์กร และโซน remote access และออกแบบการควบคุมการจราจรด้วยระบบ firewall ในแต่ละโซน

(2.2) มีการระบุการควบคุมระบบ firewall ในรูปแบบของเอกสาร เพื่อใช้ในกรณีที่มีการเปลี่ยนแปลงหรือเคลื่อนย้ายระบบ

(2.3) มีการจัดเก็บ Log file และการจราจรของเครือข่ายเป็นประจำและสม่ำเสมอ

(2.4) มีการตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นใน Host หรือเครือข่ายข้อมูล

(3) การใช้งานเครือข่าย (Internet Security Policy)

(3.1) มีการตรวจสอบสิทธิการใช้งานเครื่องคอมพิวเตอร์หรือเครือข่าย เช่น หมายเลขเครื่องคอมพิวเตอร์และรหัสผ่าน

(3.2) มีการตรวจสอบสิทธิการใช้งานในแหล่งทรัพยากรต่าง ๆ ตามลำดับความสำคัญ

(3.3) มีการบำรุงรักษาการบันทึกเหตุการณ์และการตรวจสอบระบบอยู่ตลอดเวลาพร้อมทั้งจัดเก็บไว้ในที่ที่ปลอดภัย

(3.4) มีการจัดเก็บบันทึกเหตุการณ์การเข้าถึงของระบบอย่างสม่ำเสมอ

(3.5) จัดทำกำหนดการการตรวจสอบระบบพร้อมทั้งผู้รับผิดชอบเมื่อมีการให้บริการระบบเครือข่ายคอมพิวเตอร์

(4) การเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่างๆ กับเครือข่าย

(4.1) ผู้ใช้ต้องไม่เชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กับเครือข่ายอื่นนอกเหนือจากเครือข่ายขององค์กร การติดต่อกับหน่วยงานภายนอกต้องผ่านระบบ Proxy Firewall ขององค์กรก่อน

(4.2) ผู้ที่นำคอมพิวเตอร์แบบพกพาของตนเองมาต่อเข้าระบบเครือข่ายขององค์กร ต้องได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

(5) ผู้ดูแลระบบ ต้องดำเนินการดังต่อไปนี้

(5.1) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(5.2) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(5.3) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(5.4) ควรทำการเปลี่ยนค่า SSID (service set identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

10. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Outsource Access Control)

10.1 แนวนโยบาย

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน ให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก ควรประกอบด้วย

(1) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

(2) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในหน่วยงานหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(3) สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของหน่วยงาน ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(4) ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

(5) สำหรับงานลักษณะโครงการ จะต้องมีการสรุปผลกำเนินการให้แก่ผู้บริหารทราบทุกครั้ง

10.2 แนวปฏิบัติ

(1) ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร

(2) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

(3) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้

(3.1) เหตุผลในการขอใช้

(3.2) ระยะเวลาในการใช้

(3.3) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(3.4) การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(3.5) กำหนดข้อตกลงการใช้งานข้อมูล เพื่อเป็นการป้องกันการเปิดเผยข้อมูล

(4) หน่วยงานภายนอก ที่ทำงานให้กับหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(5) หน่วยงานภายนอก ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(6) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(7) องค์กรมีสิทธิในการตรวจสอบตามสัญญา หรือข้อตกลงการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(8) ต้องกำหนดให้หน่วยงานภายนอก หรือผู้ให้บริการจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของหน่วยงานภายนอก หรือผู้ให้บริการ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดหรือตกลงไว้

11. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอก (Remote Access Control)

11.1 แนวนโยบาย

การเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอกอาจก่อให้เกิดความเสี่ยงได้ เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงาน ควรประกอบด้วย

(1) หน่วยงานที่ต้องการเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอก หน่วยงานต้องทำเรื่องขออนุญาต โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ วันที่ต้องการเข้าใช้งาน ระยะเวลาที่ใช้งาน วิธีการเข้าถึง เพื่อขออนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

(2) หน่วยงานที่ต้องการเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอก ต้องปฏิบัติและคำนึงถึงความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(3) ช่องทางการเข้าถึงควรมีความปลอดภัย น่าเชื่อถือ และตรวจสอบได้ เท่านั้น

(4) การเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอก จะต้องไม่สามารถเข้าถึงได้โดยตรง จะต้องมีการยืนยันตัวตน หรือมีการยอมรับจากบริษัท

(5) หน่วยงานภายนอก จะต้องทำสัญญาการรักษาข้อมูลภายในที่เป็นความลับ

11.1 แนวปฏิบัติ

(1) ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร

(2) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

(3) กำหนดแบบฟอร์มสำหรับให้หน่วยงานที่ต้องการเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอก ทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียด ดังนี้

(3.1) หน่วยงานที่ต้องการเข้าถึง

(3.1) วันที่และเวลาที่ต้องการเข้าถึง

(3.1) ระยะเวลาที่ต้องการเข้าถึง

(3.1) ช่องทางที่ต้องเข้าถึง

(3.1) เหตุผลที่ต้องเข้าถึง

(4) หน่วยงานภายนอก ที่ทำงานให้กับหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

(5) องค์กรมีสิทธิในการตรวจสอบตามสัญญา หรือข้อตกลงการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(6) ในกรณีเร่งด่วน เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศสามารถขออนุมัติผ่านช่องทางอื่นๆ เช่นทางโทรศัพท์ หรือทางไลน์ เพื่อขออนุมัติและเปิดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศจากภายนอกจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

12. การตรวจสอบการใช้งานของบัญชีผู้ใช้งาน

12.1 แนวนโยบาย

หน่วยงานต้องมีการกำหนดมาตรการในการตรวจสอบการเข้าใช้งานของบัญชีผู้ใช้ ทั้งผู้ใช้ทั่วไป และผู้ใช้ที่มีสิทธิ์สูง (High Privilege User ID) เพื่อตรวจสอบการปฏิบัติงานและตรวจเช็คความผิดปกติของระบบ รวมถึง การใช้งานตรงตามวัตถุประสงค์หรือไม่

12.2 แนวปฏิบัติ

(1) ต้องกำหนดระยะเวลาในการตรวจสอบอย่างเหมาะสม อย่างน้อยไตรมาสละ 1 ครั้ง

(2) ทำการตรวจสอบ Log การใช้งานว่ามีการใช้งานอย่างถูกต้องเหมาะสมหรือไม่

(2.1) บัญชีผู้ใช้ทั่วไป เป็นการสุ่มตรวจ ในหน่วยงานที่สำคัญ เช่น บัญชี,การเงิน,คลังยา, คลังสินค้า,ห้องจ่ายยา เป็นต้น

(2.2) บัญชีผู้ผู้ใช้ที่มีสิทธิ์สูง ตรวจสอบทุกบัญชีผู้ใช้

(3) รายงานผลการตรวจสอบแก่ผู้บังคับบัญชา

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย
(Network and Server Policy)

วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้บริการได้ทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวนโยบายและแนวปฏิบัติ

บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) (**"บริษัท"**) กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

1. ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ
2. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
3. การขออนุญาตใช้งานพื้นที่ Web Sever และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้บริการอื่นๆ
4. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
5. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้
    5.1 ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
    5.2 ต้องกำหนดให้มีวิธีเพื่อกำจัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆได้
    5.3 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

5.4 ระบบเครือข่ายต้องติดตั้งระบบจับการบุกรุก (Intrusion Prevention System / Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานลักษณะที่ผิดปกติ

5.5 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีบันทึกการลงเวลาเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

5.6 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในหน่วยงานจำเป็นต้องมีการป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

5.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.8 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.9 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆของซอฟต์แวร์ระบบ (Systems Software)

6. บริษัทกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

6.1 ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล

6.2 ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

6.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

6.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

7. บริษัทกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทางดังต่อไปนี้

7.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

7.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

7.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

7.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินการกับหน่วยงานอย่างเพียงพอ

7.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวนโยบายและแนวปฏิบัติ

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1. การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด
2. ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access Point, Wireless Router, Wireless USB client หรือ Wireless card
3. ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network
4. กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการดังนี้
   4.1 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internet Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)
   4.2 ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

4.3 ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติ Auto Broadcast SSID ของตัว Access Point ด้วย

4.4 ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

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

4.6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

4.7 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย ในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบทันที

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

แนวนโยบายและแนวปฏิบัติ

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1. ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาล
2. การกำหนดค่าเริ่มต้นของพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
3. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์
4. ผู้ใช้งานระบบอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการเข้าใช้งานด้วยรหัสผู้ใช้ (User account) และรหัสผ่าน (User Password)
5. ค่าการเปลี่ยนแปลงทั้งหมดของไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าการใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

6. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

7. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์ที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน

8. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทาง บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะต้องใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับการอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อน

9. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ โดยต้องระบุข้อมูลดังนี้

    9.1 หมายเลข Port ที่ต้องการขอให้เปิด

    9.2 หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

    9.3 วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

    9.4 วันที่เริ่มใช้งาน และวันที่สิ้นสุดการขอใช้

10. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

11. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

12. บริษัทมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมขัดต่อนโยบาย ประกาศ ระเบียบของบริษัท หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

13. ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด หรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางศูนย์หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศจะยกเลิกการให้บริการทันที

14. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกเข้ามายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อน

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์การกระทำใดๆ ที่สร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัย และมีประสิทธิภาพ

แนวนโยบายและแนวปฏิบัติ

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของบริษัทมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1. ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงาน โดยยื่นคำขอกับฝ่ายเทคโนโลยีสารสนเทศ
2. เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์เป็นครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที
3. ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้
4. ควรเปลี่ยนรหัสผ่านทุก 3 เดือน
5. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
6. การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้งานระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
7. การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง
8. การใช้งานจดหมายอิเล็กทรอนิกส์ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมายและผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท
9. ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของบริษัทตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งรับบริการของบริษัท
10. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
11. การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน 20 เมกะไบท์
12. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) (**"บริษัท"**) ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ตผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวนโยบายและแนวปฏิบัติ

ผู้ใช้งานเครือข่ายอินเทอร์เน็ตของบริษัท มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

1. การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต ต้องทำการกรอกข้อมูลการขอใช้บริการเครือข่ายอินเทอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับฝ่ายเทคโนโลยีสารสนเทศ เพื่อรอการตรวจสอบตัวบุคคล และอนุมัติการใช้งาน โดยผู้ใช้งานต้องเป็นบุคลากรสังกัดของบริษัท สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

2. ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชเป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

3. ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเองทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

4. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

5. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

6. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัพเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

7. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ เฟซบุ๊ก โปรแกรมอื่นๆที่มีลักษณะคล้ายกัน โดยต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

8. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้วให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจากเครือข่ายอินเทอร์เน็ตด้วยการ Logout จาก Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

นโยบายและแนวปฏิบัติระบบสำรองของสารสนเทศ (Backup Policy)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

แนวนโยบาย

1. ต้องจัดทำแผนและระบบสำรองสำหรับระบบสารสนเทศ เพื่อเตรียมความพร้อมใช้งานในกรณีฉุกเฉิน
2. การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
3. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
4. ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
5. ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง
6. ต้องปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

แนวทางปฏิบัติ

1. พิจารณาคัดเลือกและทบทวนระบบสารสนเทศที่มีความสำคัญ กำหนดประเภทของข้อมูล และกำหนดความถี่ในการจัดทำระบบสำรองที่เหมาะสมอย่างน้อยปีละ 1 ครั้ง
2. ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญ และจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความสำคัญของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานมากไปหาน้อย
3. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบสารสนเทศ
4. ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
5. มีการจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

6. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม สำหรับการกู้คืนระบบ
7. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง
8. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
9. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย จนเป็นเหตุต้องมีการดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบดำเนินการแก้ไข และรายงานปัญหาดังกล่าวต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบโดยด่วน
10. กรณีความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้รีบแจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบ เมื่อการดำเนินการกู้คืนระบบเสร็จสิ้นสมบูรณ์
11. กำหนดให้ผู้ดูแลระบบ ต้องสำรองข้อมูลที่สำคัญ ได้แก่ ข้อมูลและค่า Configure ของ Database Server, Web Server, Mail Server และ Firewall Server เป็นประจำอย่างน้อย 3 เดือนครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

นโยบายและแนวปฏิบัติการประเมินความเสี่ยง

วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจนและสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

แนวนโยบาย

1. ต้องมีการจัดแผนบริหารความเสี่ยงด้านระบบสารสนเทศ
2. ต้องมีการรายงานผลการบริหารความเสี่ยงด้านระบบสารสนเทศให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

แนวทางปฏิบัติ

1. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ควรประกอบด้วย
    1.1 ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)
    1.2 ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

1.3 ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

1.4 ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) ระบบสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

1.5 ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

2. มีการกำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

3. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้
   3.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
   3.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
   3.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

4. มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

5. มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง และป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

6. ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

7. ควรกำหนดให้แยกเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบายและแนวปฏิบัติการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ และระบบคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) ("บริษัท") มีความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ อันจะทำให้การดำเนินธุรกรรมมีความถูกต้องและน่าเชื่อถือ จึงกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของบริษัทเพื่อให้เจ้าหน้าที่ของบริษัททุกคนตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์และสารสนเทศ และตั้งใจปฏิบัติอย่างเคร่งครัด ตามแนวทางดังนี้

แนวนโยบายและแนวปฏิบัติ

1. เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงาน และของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

2. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการคุ้มครองข้อมูลส่วนบุคล ให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี รวมทั้งการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ
3. จัดทำแนวปฏิบัติและข้อกำหนดในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคลของบริษัทเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคลให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้
4. แจ้งหรือจัดให้มีประกาศแนวนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทให้แก่บุคลากรและบุคคลที่เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้
5. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน
6. ระดมการมีส่วนร่วมด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

การกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัย

วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินและอุปกรณ์ของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) (**"บริษัท"**) ซึ่งมีความสำคัญและคุณค่า ผู้บริหารจะให้การสนับสนุนในการกำหนดมาตรการป้องกัน ได้แก่ นโยบายความมั่นคงปลอดภัย ขั้นตอนปฏิบัติ และเอกสารสนับสนุนอื่นๆรวมทั้งกระบวนการในการทบทวนมาตรการดังกล่าว เพื่อให้สามารถปรับปรุงหรือแก้ไขข้อบกพร่องหรือปัญหาทางด้านความมั่งคงปลอดภัยได้อย่างมีประสิทธิภาพ

หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง ดังนี้

1. **ผู้บริหารระดับสูงสุด**
   1.1 กำกับให้มีการกำหนด จัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัยอยู่เสมอ
   1.2 กำกับให้มีการควบคุม และปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด ห้ามมิให้ผู้ใดฝ่าฝืนหรือละเลยการปฏิบัติตามแนวทางนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
   1.3 มอบหมาย อำนาจ หน้าที่ให้ผู้ดูแล ควบคุมและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

2. **ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ**
   2.1 กำหนดให้มีการกำหนดการจัดทำ ปรับปรุง นโยบายความมั่นคงปลอดภัย ขั้นตอนการปฏิบัติงาน (Procedures) กำหนดให้มีการจัดทำแผนรับมือกับเหตุภัยพิบัติ (disaster Recovery Plan)
   2.2 กำกับดูแลให้เจ้าหน้าที่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด
   2.3 กำหนดให้มีการตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของบริษัท
   2.4 จัดให้มีการศึกษากฎหมาย ระเบียบ พระราชบัญญัติ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย

3. **เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ**

3.1 ดูแลบัญชีผู้ใช้ กำหนดสิทธิ และทบทวนสิทธิการใช้งานของผู้ใช้ระบบ

3.2 บริหารจัดการเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายให้มีความมั่งคงปลอดภัย และสามารถใช้งานได้ตลอดเวลา

3.4 ตรวจสอบข้อมูลล็อกของเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายรวมทั้งจัดทำรายงานสรุปเสนอผู้บังคับบัญชา

3.5 ทำการสำรองข้อมูลและตรวจสอบข้อมูลที่สำรองไว้

3.6 ทำการทดสอบระบบหรือแอพพลิเคชั่นก่อนเริ่มต้นการใช้งานจริง

3.7 จัดทำคู่มือการใช้งาน คู่มือสำหรับระบบ และหรือคู่มือสำหรับการดำเนินงาน

3.8 บันทึกเหตุการณ์ ตรวจสอบการเข้าถึงระบบเครือข่ายของหน่วยงาน

3.9 ควบคุมดูแลระบบเครือข่ายสื่อสารให้สามารถใช้งานได้ตลอดเวลา

3.10 ควบคุมการดำเนินการข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นแนวทางตามที่ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดไว้

3.11 ตรวจสอบป้องกันการบุกรุกจู่โจมจากผู้ไม่ประสงค์ดี

3.12 ช่วยเหลือและแก้ปัญหาการใช้งานเครื่องคอมพิวเตอร์

3.13 ทำหน้าที่รับมือกับเหตุการณ์ความมั่งคงปลอดภัยตามที่ได้รับรายงานโดยปฏิบัติตามขั้นตอนปฏิบัติอย่างเคร่งครัด

3.14 บันทึกข้อมูลปัญหาการใช้งานเครื่องคอมพิวเตอร์และข้อมูลเหตุการณ์ความมั่งคงปลอดภัยและจัดทำรายงานสรุปปัญหาและเสนอผู้บังคับบัญชา

4. **ผู้ใช้งาน**

4.1 ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้โดยเคร่งครัด

ขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
(Scope of Information Security Management System)

บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) ("บริษัท") ได้ดำเนินการวิเคราะห์และประเมินเทคโนโลยีที่ใช้ของระบบที่มีความสำคัญต่อภารกิจและการบริการขององค์กร ได้แก่

- ☐ ระบบ Active Directory
- ☐ ระบบ HIMS
- ☐ ระบบ Website
- ☐ ระบบ Internet
- ☐ ระบบ Intranet

โดยการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA) จากการประเมินผลกระทบต่อการดำเนินงานและความเสี่ยงของระบบทั้งหมด สามารถสรุปถึงโอกาสที่จะเกิดความเสี่ยง ผลกระทบ และแนวทางการจัดการในแต่ละกรณีได้ดังนี้

ตารางสรุปผลการวิเคราะห์และประเมินผลกระทบต่อการดำเนินงาน

ปริการหลัก	กิจกรรม				ความสำคัญ	เป้าหมายการบริหารความต่อเนื่อง		
	ไฟฟ้า	ระบบเครือข่ายภายใน	ระบบเครือข่ายภายนอก	เครื่อง Server		MTPD	RTO	RPO
ระบบ Active Directory	●	●		●	Y	8 ชม.	4 ชม.	30 นาที
ระบบ HIMS	●	●		●	Y	8 ชม.	4 ชม.	30 นาที
ระบบ Website		●	●	●	Y	8 ชม.	4 ชม.	30 นาที
ระบบ Internet	●	●	●	●	Y	8 ชม.	4 ชม.	30 นาที
ระบบ Intranet	●	●	●	●	Y	8 ชม.	4 ชม.	30 นาที

หมายเหตุ:

(1) MTPD (Maximum Tolerable Period of Disruption) หมายถึง ระยะเวลาสูงสุดที่สามารถหยุดดำเนินการได้

(2) RTO (Recovery Time Objective) หมายถึง ระยะเวลาที่ต้องการดำเนินการกู้คืนสู่ระดับการดำเนินงานขั้นต่ำที่สามารถยอมรับได้

(3) RPO (Recovery Point Objective) หมายถึง ระดับการดำเนินงานขั้นต่ำที่สามารถยอมรับได้

บริบทขององค์กร (Context of the organization)

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ของบริษัทมีขอบเขตครอบคลุมการให้บริการภายในโรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล

1. ความเข้าใจในองค์กรและบริบทขององค์กร (Understanding the organization and its context)

องค์กรต้องกำหนดประเด็นทั้งภายในและภายนอกที่มีผลกระทบกับจุดประสงค์และความสามารถในการบรรลุถึงผลลัพธ์ตามเป้าหมายของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

2. ความเข้าใจในความต้องการ และความคาดหวังขององค์กรที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties) องค์กรต้องกำหนด

2.1 องค์กรที่เกี่ยวข้อง ซึ่งเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

2.2 ความต้องการขององค์กร ที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

หมายเหตุ : ความต้องการขององค์กรที่เกี่ยวข้องอาจรวมถึงกฎหมาย กฎระเบียบ และภาระผูกพันตามสัญญา

3. การกำหนดขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system) องค์กรต้องกำหนดขอบเขตและการจัดตั้งขอบเขตของระบบ

บริหารความมั่นคงปลอดภัยสารสนเทศ โดยระบุเป็นลายลักษณ์อักษร เมื่อกำหนดขอบเขต องค์กรจะพิจารณา

3.1 ประเด็นทั้งภายในและภายนอกองค์กร ซึ่งอ้างถึง 1

3.2 ความต้องการซึ่งอ้างถึง 2

3.3 ความเชื่อมต่อกันและความเกี่ยวข้องระหว่างกิจกรรม ที่ดำเนินการโดยองค์กรและโดยหน่วยงานอื่น

4. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) องค์กรต้องจัดตั้ง นำมาใช้งาน รักษาไว้ และพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

ความเป็นผู้นำ (Leadership)

1. **ความเป็นผู้นำและความมุ่งมั่น** (Leadership and commitment)

ผู้บริหารระดับสูง (กรรมการผู้จัดการ) ได้ให้คำมั่นและแสดงให้เห็นถึงความเป็นผู้นำต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศโดย

1.1 รับรองว่านโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดขึ้น สอดคล้องกับทิศทางยุทธศาสตร์ขององค์กร

1.2 รับรองว่ามีการบูรณาการความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ในกระบวนการขององค์กร

1.3 รับรองว่าให้การสนับสนุนทรัพยากรที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

1.4 สื่อสารความสำคัญของประสิทธิภาพระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และสอดคล้องกับความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

1.5 ให้ทิศทางและสนับสนุนบุคลากรเพื่อให้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีประสิทธิภาพ

1.6 ส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง

1.7 สนับสนุนอื่นๆ ที่แสดงถึงความเป็นผู้นำตามความรับผิดชอบ

2. **นโยบาย** (Policy)

ผู้บริหารระดับสูง (กรรมการผู้จัดการ) จะกำหนดนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

2.1 เหมาะสมกับวัตถุประสงค์ขององค์กร

2.2 ครอบคลุมถึงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ หรือเตรียมกรอบสำหรับจัดตั้งวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

2.3 ครอบคลุมถึงความมุ่งมั่นในการบรรลุถึงความต้องการเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

2.4 ครอบคลุมถึงความมุ่งมั่นในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

2.5 มีการจัดทำข้อมูลเป็นเอกสาร

2.6 มีการสื่อสารภายในองค์กร

2.7 มีการเผยแพร่ประชาสัมพันธ์ให้ผู้เกี่ยวข้อง ตามความเหมาะสม

3. **บทบาทหน้าที่ความรับผิดชอบและการมอบอำนาจ** (Organizational roles, responsibilities and authorities)

ผู้บริหารระดับสูงจะต้องมั่นใจว่าความรับผิดชอบและอำนาจหน้าที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศได้ถูกมอบหมายและสื่อสารอย่างครบถ้วน ผู้บริหารระดับสูงจะต้องมองหมายความรับผิดชอบและอำนาจหน้าที่โดย

3.1 ต้องมั่นใจว่าระบบบริหารความมั่นคงปลอดภัยสารสนเทศสอดคล้องกับความ ต้องการตามมาตรฐาน ISO/IEC 27001

3.2 มีการรายงานประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศต่อ ผู้บริหารระดับสูง

หมายเหตุ : ผู้บริหารระดับสูงอาจมอบหมายความรับผิดชอบและอำนาจหน้าที่ในการรายงานประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ให้บุคลากรภายในองค์กร

4. **การสนับสนุน** (Support)

1. ทรัพยากร (Resources)

องค์กรมีการระบุและเตรียมทรัพยากรที่จำเป็นในการจัดตั้งระบบบริหารความมั่นคงปลอดภัย นำมาใช้งาน บำรุงรักษา และพัฒนาอย่างต่อเนื่อง

2. ความสามารถ (Competence)

องค์กรดำเนินการดังนี้

2.1 ระบุความสามารถของบุคลากรที่จำเป็นในการปฏิบัติงานภายใต้มาตรการที่มีผลกับประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

2.2 ทำให้มั่นใจว่าบุคลากรมีความสามารถพื้นฐานที่เหมาะสมด้านการศึกษา การฝึกอบรมและประสบการณ์

2.3 ดำเนินการให้ได้รับความสามารถที่จำเป็นในการปฏิบัติงาน และประเมินผลประสิทธิภาพของการดำเนินการตามความเหมาะสม

2.4 เก็บรักษาเอกสารหลักฐานของความสามารถนั้นๆ

หมายเหตุ : ตัวอย่างการดำเนินการที่เหมาะสม เช่นวางแผนการฝึกอบรม การให้คำปรึกษา หรือมอบหมายงานให้บุคลากรที่มีอยู่ หรือว่าจ้างผู้ที่มีความสามารถนั้นๆ

3. ความตระหนัก (Awareness)

บุคลากรที่ปฏิบัติงานภายใต้มาตรการขององค์กรจะต้องตระหนักถึง

3.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

3.2 บุคลากรให้การสนับสนุนเพื่อให้ระบบบริหารความมั่นคงปลอดภัยมีประสิทธิภาพ รวมถึงประโยชน์ที่จะได้รับเมื่อสามารถปรับปรุงประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศได้

3.3 การดำเนินการที่ไม่สอดคล้องกับความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

4. การติดต่อสื่อสาร (Communication)

องค์กรระบุความจำเป็นของทั้งการสื่อสารภายในและภายนอก ที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยคลอบคลุมสิ่งต่อไปนี้

4.1 สิ่งที่จะสื่อสาร

4.2 เวลาที่จะสื่อสาร

4.3 ผู้ที่จะสื่อสาร

4.4 ผู้ที่รับหน้าที่ผู้สื่อสาร

4.5 กระบวนการ ของการสื่อสารที่มีประสิทธิภาพ

5. เอกสารหลักฐาน (Documented information)

5.1 บททั่วไป ระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร จะครอบคลุมถึง

5.1.1 ข้อมูลเอกสารที่ต้องการตามมาตรฐาน ISO/IEC 27001

5.1.1 ข้อมูลเอกสารที่ระบุโดยองค์กรว่ามีความจำเป็นต่อประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

5.2 การจัดทำและปรับปรุง เมื่อมีการจัดทำและปรับปรุงข้อมูลเอกสาร องค์กรจะต้องมั่นใจว่า

5.2.1 มีการระบุและคำอธิบาย (เช่น หัวเรื่อง วันที่ ผู้จัดทำหรือหมายเลขอ้างอิง)

5.2.2 จัดรูปแบบ (เช่น ภาษา ซอฟต์แวร์เวอร์ชั่น กราฟฟิก) และสื่อ เช่น กระดาษ อิเล็กทรอนิกส์)

5.2.3 มีการทบทวนและอนุมัติตามเหมาะสม

5.3 การควบคุมเอกสาร ข้อมูลเอกสารที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีการควบคุมเพื่อให้มั่นใจว่า

5.3.1 พร้อมใช้และเหมาะสมสำหรับการใช้งานในสถานที่ และเมื่อจำเป็น

5.3.2 มีการป้องกันอย่างพอเพียง (เช่น จากการเปิดเผยความลับ การใช้งานอย่าง ไม่เหมาะสม หรือขาดความสมบูรณ์) ในการควบคุมเอกสาร องค์กรจะระบุกิจกรรมดังต่อไปนี้

5.3.3 การแจกจ่าย การเข้าถึง การแก้ไข และการใช้งาน

5.3.4 การจัดเก็บและการป้องกัน รวมถึงการดำรงไว้ซึ่งความชัดเจน

5.3.5 การควบคุมการเปลี่ยนแปลง (เช่น การควบคุมเวอร์ชั่น)

5.3.6 การเก็บรักษาและการทำลาย

เอกสารที่มาจากภายนอก มีการกำหนดตามความจำเป็นสำหรับการวางแผนและการปฏิบัติงานสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการระบุและควบคุมตามความเหมาะสม

การเข้าถึงหมายถึงการตัดสินใจในการให้สิทธิ์ในการดูเอกสารเท่านั้น หรือการให้สิทธิ์และอำนาจในการดูแลแก้ไขเอกสารเอกสารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) รวมถึง แบบฟอร์ม และรูปแบบการบันทึกข้อมูลต่างๆ จะต้องมีการป้องกัน ควบคุม บำรุงรักษา และจัดการเอกสาร

การประเมินผลการดำเนินการ (Performance evaluation)

1. การเฝ้าระวัง การวัดผล การวิเคราะห์และประเมินผล (Monitoring, measurement, analysis and evaluation) องค์กรจะต้องประเมินผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศและประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศองค์กรจะต้องกำหนด
   1.1 ความจำเป็นในการเฝ้าระวัง และวัดผล รวมถึงกระบวนการและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ
   1.2 วิธีการเฝ้าระวัง วัดผล วิเคราะห์ และประเมิน ตามความเหมาะสม เพื่อให้ได้ผลที่ถูกต้อง

หมายเหตุ : วิธีการที่เลือกจะต้องสามารถเปรียบเทียบผลลัพธ์ได้ และทำซ้ำได้ผลลัพธ์ที่ถูกต้อง

   1.3 ช่วงเวลาในการเฝ้าระวังและวัดผล
   1.4 ผู้เฝ้าระวังและวัดผล
   1.5 ผลที่ได้จากการเฝ้าระวังและวัดผลแล้ว จะต้องมีการวิเคราะห์และประเมินผล
   1.6 ผู้ที่วิเคราะห์และประเมินผลองค์กรจะเก็บรักษาเอกสารข้อมูลการเฝ้าระวังและวัดผลไว้เป็นหลักฐาน

2. การตรวจสอบภายใน (Internal audit) องค์กรจะดำเนินการตรวจติดตามภายในตามรอบระยะเวลาที่กำหนดไว้ เพื่อเตรียมข้อมูลของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ดังนี้
   2.1 เพื่อให้สอดคล้องกับ
      ☐ ความต้องการด้านระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร
      ☐ ข้อกำหนดในมาตรฐาน ISO/IEC 27001
   2.2 มีการนำมาใช้งานและบำรุงรักษาอย่างมีประสิทธิภาพ
   2.3 มีการวางแผน จัดตั้ง นำมาใช้งานและบำรุงรักษาแผนการตรวจติดตาม รวมถึงความถี่ วิธีการ ความรับผิดชอบ ความต้องการของแผนและการรายงาน แผนการตรวจติดตามที่จะพิจารณาถึงความสำคัญของกระบวนการที่เกี่ยวข้องและผลจากการตรวจติดตามครั้งก่อน
   2.4 กำหนดเกณฑ์และขอบเขตการตรวจติดตาม
   2.5 เลือกผู้ตรวจติดตามและตรวจติดตามเพื่อให้มั่นใจว่าเป็นไปตามวัตถุประสงค์และความยุติธรรมของกระบวนการตรวจติดตาม
   2.6 ทำให้มั่นใจว่าผลของการตรวจติดตามได้รับการรายงานต่อผู้บริหารที่เกี่ยวข้อง
   2.7 การเก็บรักษาข้อมูลเอกสารแผนการตรวจติดตามและผลการตรวจติดตามไว้เป็นหลักฐาน

3. การทบทวนของฝ่ายบริหาร (Management review) ผู้บริหารระดับสูงต้องทบทวนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มีการดำเนินการที่เหมาะสมพอเพียงและสัมฤทธิผล การทบทวนของฝ่ายบริหารจะต้องพิจารณาดังนี้
   3.1 สถานะของการดำเนินการทบทวนของฝ่ายบริหารครั้งก่อน
   3.2 การเปลี่ยนแปลงทั้งภายในและภายนอกที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
   3.3 ข้อเสอนแนะเพื่อดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศรวมถึงแนวโน้มดังต่อไปนี้
      ☐ การไม่เป็นไปตามข้อกำหนด (Nonconformities) และการแก้ไข (Corrective Action)

- ☐ ผลการเฝ้าระวังและวัดผล
- ☐ ผลการตรวจติดตาม
- ☐ การบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

3.4 ข้อเสนอแนะจากผู้ที่เกี่ยวข้อง

3.5 ผลจากการประเมินความเสี่ยงและสถานะของแผนการจัดการความเสี่ยง

3.6 โอกาสในการพัฒนาอย่างต่อเนื่อง

ผลลัพธ์ของการทบทวนของฝ่ายบริหารจะรวมถึงการตัดสินใจที่เกี่ยวข้องกับโอกาสในการพัฒนาอย่างต่อเนื่องและความจำเป็นในการเปลี่ยนแปลงระบบบริหารความมั่นคงปลอดภัยสารสนเทศ องค์กรจะเก็บรักษาเอกสารข้อมูลการทบทวนของฝ่ายบริหารไว้เป็นหลักฐาน

ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

วัตถุประสงค์

เพื่อให้มีการป้องกันทรัพย์สินขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบายและแนวปฏิบัติ

1. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

หน่วยงานจะต้องกำหนดให้มีการจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างหน่วยงานกับผู้ให้บริการภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร โดยปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)

2.1 เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่าง หน่วยงานกับผู้ให้บริการภายนอก ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.2 ผู้ดูแลระบบต้องให้สิทธิการเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

2.3 การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอก ต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อนเสมอ

2.4 ผู้ให้บริการภายนอกต้องลงนามในเอกสารบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA)

2.5 สัญญาระหว่างหน่วยงาน และหน่วยงานภายนอกในการให้บริการ ต้องระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้

- ☐ รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ

- ☐ ระดับการให้บริการ (Service Level)
- ☐ หน้าที่และความรับผิดชอบขององค์การและหน่วยงานภายนอก ในการให้บริการในครั้งนี้
- ☐ ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้
- ☐ ราคา และเงื่อนไขการชำระเงิน
- ☐ ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)
- ☐ การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์การ

3. ห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

    3.1 ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศ

    3.2 ต้องมีการประเมินความเสี่ยงจากการเข้าถึงข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

นโยบายและแนวปฏิบัติ

1. การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

    1.1 เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับบริษัทที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก

    1.2 ต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

    1.3 การบริการและการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และกฎข้อบังคับต่าง ๆ ของบริษัท

2. การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

    2.1 การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของบริษัททุกครั้ง ต้องเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.2 การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องมีระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน) (**"บริษัท"**) ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

นโยบายและแนวปฏิบัติ

1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures) เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงานและขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

2. การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)
   2.1 ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทโดยผ่านช่องทางรายงานที่กำหนดไว้
   2.2 ผู้ใช้งานทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในบริษัทต่อผู้บังคับบัญชา หรือแผนกเทคโนโลยีสารสนเทศทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที
   2.3 ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศทันที
   2.4 ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศทันที
   2.5 ผู้ใช้งานที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในบริษัทต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชาและเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

3. การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)
   เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัทที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

4. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

4.1 สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นถือเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

4.2 จัดทำเกณฑ์ในการตัดสินเหตุการณ์ที่ถือว่าเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

5. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

5.1 เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องมีการกำหนดขั้นตอนไว้รองรับกรณีเกิดเหตุการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัย

5.2 เมื่อเกิดเหตุการณ์ความไม่มั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

5.3 โดยได้จัดทำแยกประเภทตามระบบต่าง ๆ ดังนี้

1) ระบบป้องกันผู้บุกรุก

1.1) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- ☐ มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ☐ ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ☐ ระดับความรุนแรงมากน้อยเพียงใด
- ☐ หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

2) ระบบไฟร์วอลล์

2.1) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ 1 ครั้ง

2.2) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้อง ตรวจสอบมีดังต่อไปนี้

- ☐ Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ☐ ลักษณะของ Packet ที่ถูก Block
- ☐ Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

2.3) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งผู้จัดการฝ่ายเทคโนโลยีสารสนเทศเพื่อตัดสินใจดำเนินการแก้ไขปัญหา

3) ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

3.1) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

☐ มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก

☐ มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด

☐ มีการส่งมัลแวร์จากเครือข่ายภายในบริษัทไปยังภายนอกหรือไม่

3.2) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของบริษัท

3.3) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

6. การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Information Security Incidents)

เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ปริมาณที่เกิดขึ้นและค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้วและเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

7. การเก็บรวบรวมหลักฐาน (Collection of Evidence)

เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศต้องรวบรวมและจัดเก็บหลักฐานตามกฎ หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Compliance)

การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญา ต่าง ๆ

นโยบายและแนวปฏิบัติ

1. การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

1.1 บริษัทต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

1.2 เจ้าหน้าที่บริษัททุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด

1.3 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท(ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดย สิทธิบัตร หรือลิขสิทธ์ของบุคคลภายนอก) ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

1.4 เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งาน เพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของ บริษัทกำหนดไว้

1.5 ห้ามเจ้าหน้าที่บริษัทใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัทกระทำการใด ๆ ที่ขัดแย้งต่อ กฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

1.6 การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศไม่ขัดต่อข้อกฎหมายใด ๆ ทั้งของราชอาณาจักรไทยระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษา ผู้บังคับบัญชา และผู้เชียวชาญด้านกฎหมายก่อนดำเนินการส่งออก

2. ทรัพย์สินทางปัญญา (Intellectual Property Rights)

2.1 ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

2.2 ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย

2.3 ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็น การละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัทโดยเด็ดขาด

3. การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบหน่วยงานว่าด้วยงานสารบรรณ และกฎหมาย

4. ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personaly identifiable information)

บริษัทต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญา ที่เกี่ยวกับบริษัท

5. การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

บริษัทต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

นโยบายและแนวปฏิบัติ

1. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องมีการทบทวนวิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติขององค์กร เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย ระเบียบปฏิบัติ ต่างๆ ให้ถูกต้องและเป็นปัจจุบันตามรอบระยะเวลาที่กำหนด อย่างน้อยปีละ 1 ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

2. การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

2.1 เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและระยะเวลาที่กำหนดไว้

2.2 เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

3. การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งานหรือให้บริการอยู่แล้วอย่างน้อยปีละ 1 ครั้ง ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และ/หรือ ทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย

นโยบายและแนวปฏิบัติการกำหนดบัญชีผู้ใช้งานและรหัสผ่าน (User Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติถึงการกำหนดบัญชีผู้ใช้งานและรหัสให้ได้มาตรฐานและมีความปลอดภัย การใช้งานยากต่อการคาดเดา เพื่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แนวนโยบาย

1. การกำหนดผู้ใช้ตามการปฏิบัติงาน

เพื่อให้การปฏิบัติงานสอดคล้องกับการให้บริการและการปฏิบัติหน้าที่ ทางบริษัทจึงจัดบัญชีผู้ใช้งานออกเป็น 2 ประเภท ได้แก่

(1.1) Personal User คือ User ที่ใช้เฉพาะบุคคล ตามการปฏิบัติงาน

(1.2) Share User คือ User ที่ใช้ในหน่วยงานที่ให้บริการ ไม่เจาะจงตัวบุคคลในการปฏิบัติงาน

2. การกำหนดบัญชีผู้ใช้และรหัสผ่านให้ปลอดภัยและได้มาตรฐาน ควรปฏิบัติดังนี้

   (2.1) รหัสผ่านจะต้องมีอย่างน้อย 8 ตัวอักษร

   (2.2) รหัสผ่านจะต้องประกอบไปด้วย ตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก และตัวเลข อย่างน้อย 1 ตัว

   (2.3) การตั้งรหัสผ่านจะต้องไม่ซ้ำกับรหัสผ่านเดิมกับ 3 ครั้งที่ผ่านมา

   (2.4) รหัสผ่านมีอายุ 90 วัน

3. ข้อกำหนดการใช้งานบัญชีผู้ใช้และรหัสผ่าน

   (3.1) ควรเปลี่ยนรหัสผ่านอย่างน้อยที่ 90 วัน

   (3.2) หากใส่รหัสผ่านผิดติดต่อกันเกิน 3 ครั้ง ระบบจะทำการล็อคชื่อบัญชีผู้ใช้ และจะปลดล็อคได้โดยผู้ดูแลระบบเท่านั้น

   (3.3) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

   (3.4) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

   (3.5) บัญชีผู้ใช้และรหัสผ่านถือเป็นความลับ

   (3.6) บัญชีผู้ใช้ Share User จะต้องมีการเปลี่ยนรหัสผ่านทันที ที่มีเจ้าหน้าที่ในหน่วยงานลาออกหรือพ้นสภาพการเป็นพนักงาน

แนวปฏิบัติ

ผู้ดูแลระบบ

1. ผู้ดูแลระบบแสดงกระบวนการในการมอบหมาย หรือการกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน
2. ผู้ดูแลระบบสามารถบันทึกการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศตามที่ได้รับอนุมัติ หรือตามอำนาจหน้าที่ความรับผิดชอบ หรือตามความจำเป็นในการใช้งานระบบเท่านั้น
3. ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศมอบอำนาจหน้าที่ความรับผิดชอบให้ผู้ดูแลระบบ หรือมอบหมายสิทธิการบริหารจัดการบัญชีผู้ใช้งานให้ผู้อื่นที่มีส่วนเกี่ยวข้องกับระบบงานดำเนินการแทนก็ได้
4. บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานระบบ
5. บันทึกและจัดเก็บข้อมูลการเปลี่ยนแปลงบัญชีผู้ใช้งาน การมอบหมายอำนาจหน้าที่ หรือสิทธิการควบคุมการใช้งานทุกครั้ง
6. ทำการทบทวนระดับและสิทธิของผู้ใช้งานระบบสารสนเทศอย่างสม่ำเสมอ
7. จัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบจัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบ
8. ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน

9. การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

ผู้ใช้งาน

1. กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมผสานตัวอักษร ระหว่างตัวอักษรตัวปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)
2. ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ-สกุล เบอร์โทรศัพท์ ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม
3. ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น
4. การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน
5. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา
6. ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที
7. ภายหลังการใช้งานเครื่องเสร็จสิ้น จะต้องทำการ Log off ออกจากระบบทุกครั้ง
8. จะต้องทำการเปลี่ยนรหัสผ่านทุกครั้งที่มีเจ้าหน้าที่ในหน่วยงานลาออกหรือพ้นสภาพการเป็นพนักงาน

อนุมัติโดย

มติที่ประชุมคณะกรรมการบริษัทครั้งที่ 5/2567 เมื่อวันที่ 5 สิงหาคม 2567 โดยเริ่มมีผลใช้บังคับนับตั้งแต่วันที่อนุมัติ

บริษัท โรงพยาบาลมุกดาหารอินเตอร์เนชั่นแนล จำกัด (มหาชน)

(นายบุญธรรม เลิศสุขีเกษม)
ประธานกรรมการ