นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศโรงพยาบาล

วันที่ประกาศใช้ 1 เมษายน 2567	**ประเภทเอกสาร** ❑ ควบคุม ❑ ไม่ควบคุม	
จัดทำโดย	นายสรศักดิ์ นาคจิตร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ผู้ทบทวน	นางสาวศรีสุดา ชิตกุล	หัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์
ผู้อนุมัติ	นายแพทย์เอกพล พิศาล	ผู้อำนวยการโรงพยาบาลบ้านตาขุน

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับองค์กรที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่างๆ เป็นต้น แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่างๆ ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเตอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ ของหน่วยงาน ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัย ด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น โรงพยาบาลบ้านตาขุน จึงจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และเพื่อดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

งานสารสนเทศ

เมษายน 2567

สารบัญ

บทนำ

1. นโยบาย

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเป็นไปอย่างเหมาะสม มีประสิทธิภาพมีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและถูกคุกคามจากภัยต่างๆ โรงพยาบาล จึงเห็นสมควรกำหนดนโยบาย ดังนี้

1.1. ส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

1.2. มีหน้าที่ จำกัด ระงับ เพิกถอนสิทธิ หากมีการละเมิดหรือฝ่าฝืนแนวปฏิบัติ คณะกรรมการสารสนเทศและคอมพิวเตอร์รายงานการฝ่าฝืนให้ต้นสังกัดหรือโรงพยาบาลพิจารณาลงโทษ

1.3. สนับสนุนให้เทคโนโลยีสารสนเทศมีความถูกต้อง สมบูรณ์และพร้อมใช้งานอยู่เสมอ

1.4. สนับสนุนการรักษาความปลอดภัยของข้อมูลตามแนวปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

2. วัตถุประสงค์

2.1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเพื่อให้มีความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

2.2. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ นโยบายนี้ต้อง เผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลบ้านตาขุน ได้รับทราบและถือปฏิบัติตาม นโยบายนี้อย่างเคร่งครัด

2.3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

2.4. เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆเข้าล่วงรู้ข้อมูล แก้ไขหรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ

2.5. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี

3. ขอบเขต

3.1. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ นโยบายนี้ต้องเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาล ได้รับทราบและถือปฏิบัติตาม นโยบายนี้อย่างเคร่งครัด

3.2. ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบตระหนักถึงความสำคัญของการรักษาความมั่นคง

ปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

4. หน้าที่รับผิดชอบ

ด้วยในปัจจุบันโรงพยาบาลมีการใช้ระบบสารสนเทศเป็นเครื่องมือในการดำเนินงาน ไม่ว่าจะเป็น ฮาร์ดแวร์ ซอร์ฟแวร์ข้อมูล เครือข่ายอินเตอร์เน็ต อินทราเน็ต จึงจำเป็นต้องมีการรักษาความปลอดภัยด้านเทคโนโลยี สารสนเทศ การควบคุมการเข้าถึงคอมพิวเตอร์เพื่อป้องกันความเสียหาย การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมความพร้อมในกรณีฉุกเฉิน โดยมีมาตรฐานมาตรวจสอบภายในเป็นตัวควบคุม

ดังนั้น โรงพยาบาลบ้านตาขุน จึงขอมอบหมายหน้าที่รับผิดชอบนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล ได้แก่

1. นายสรศักดิ์ นาคจิตร นักวิชาการคอมพิวเตอร์ปฏิบัติการ
2. นางสาวจิติมา ศรีสาคร นักวิชาการคอมพิวเตอร์ปฏิบัติการ
3. นางสาวเบญจวรรณ ชูพรม นักวิชาการคอมพิวเตอร์

โดยมีหน้าที่และกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน ดังนี้

1) การใช้งานรหัสผ่านผู้ใช้งานต้องปฏิบัติดังนี้

(1) ผู้ใช้งานมีหน้าที่ในการป้องดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่ายให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(2) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว

(3) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(4) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(5) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(6) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดาและการส่งมอบรหัสผ่านให้กับ ผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(7) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) อย่างน้อย 2 ครั้งต่อปี

2) การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษา ความลับทางราชการพ.ศ. และต้องใช้วิธีการเข้ารหัส 2544(Encryption) ที่เป็นมาตรฐานสากล

3) การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิดไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตามให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

4) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของ

หน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดีหรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทางดังนี้

(1) คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(2) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่ง สามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(4) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อกหน้าจอทุกครั้งและต้องทำการพิสูจน์ ตัวตนก่อนการใช้งานทุกครั้ง

(5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลา อย่างน้อย 15 นาที

5) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาล หรือเป็นข้อมูลของบุคคลภายนอก

6) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงานห้าม ไม่ให้ทำการเผยแพร่เปลี่ยนแปลง หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

7) ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาล และข้อมูลของผู้รับบริการหากเกิดการสูญหายโดยนำ ไปใช้ในทางที่ผิดการเผยแพร่โดยไม่ได้รับอนุญาตผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

8) ผู้ใช้งานต้องป้องกันดูแลรักษาไว้ซึ่งความลับความถูกต้องและความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

9) ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษาใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาล จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิด ต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้นยกเว้นในกรณีที่โรงพยาบาลต้องการ ตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาลซึ่งโรงพยาบาลอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

10) ห้ามเปิดหรือใช้งาน(Run) โปรแกรมประเภท Peer-to-Peer หมายถึงวิธีการจัดเครือข่ายคอมพิวเตอร์ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกันหมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลการจัดแบบนี้ไว้เองให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม(File Server) เท่านั้น หรือโปรแกรมที่มีความเสี่ยงในระดับ เดียวกัน เช่น บิทเทอร์เรนท์ (Bit-torrent), อีมูล(E-mule) เป็นต้นเว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

11) ห้ามเปิดหรือใช้งาน(Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟัง เพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

12) ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูลข้อความรูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของประเทศกฎหมายหรือกระทบต่อภารกิจของโรงพยาบาล

13) ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวนก่อให้เกิดความเสียหรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรมหรือกระทบต่อภารกิจของโรงพยาบาล

14) ห้ามใช้สินทรัพย์ของโรงพยาบาลเพื่อประโยชน์ทางการค้า

15) ห้ามกระทำการใดๆ ไม่ว่าจะเป็นข้อความภาพ เสียงหรือสิ่งอื่นใด เครือข่ายระบบสารสนเทศของโรงพยาบาลโดยเด็ดขาดไม่ว่าจะด้วยวิธีการใดๆก็ตาม

16) ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงั

17) ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

18) ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่า กรณีใดๆเพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากร

19) ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

5. นิยามศัพท์เฉพาะ

โรงพยาบาล หมายถึง โรงพยาบาลบ้านตาขุน

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านตาขุน

มาตรการ หมายถึง วิธีการที่ตั้งเป็นกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเป็นต้น

วิธีปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวปฏิบัติ หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลบ้านตาขุน

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และลูกจ้างเหมา

สารสนเทศ หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปแบบของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่

ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได้ เช่น ระบบแลน) LAN (ระบบอินเตอร์เน็ต) Internet(ระบบแลน) LAN (หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเตอร์เน็ต) Internet (หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูลและสารสนเทศ เป็นต้น
“การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ”หมายถึง การตรวจสอบการอนุมัติและการกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้

เครื่องเซิร์ฟเวอร์) Server (หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ที่เป็นลูกข่ายในระบบเครือข่าย

อุปกรณ์ UPS หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการไฟฟ้าเกิดปัญหาขึ้นมา เช่น ไฟตก ไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้น โดยที่อุปกรณ์ UPS จะจ่ายพลังงานออกมาอย่างต่อเนื่องและมีคุณภาพในทุกสถานการณ์ ตลอดจนเป็นอุปกรณ์ที่ช่วย ป้องกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟ้า และอุปกรณ์อิเล็กทรอนิกส์) โดยเฉพาะคอมพิวเตอร์และอุปกรณ์เชื่อมต่อ (รวมถึงมีหน้าที่ในการจ่ายพลังงานไฟฟ้าสำรองจากแบตเตอรี่ให้แก่อุปกรณ์ไฟฟ้าหรือคอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า

ซอฟต์แวร์) Software (หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน ซอฟต์แวร์จึงหมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหล่านี้เรียงกันเป็นโปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียงการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รูปภาพ หรือแม้แต่เป็นเสียงพูดก็ได้ โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์ เพราะเป็นลำดับขั้นตอนการทำงานของคอมพิวเตอร์ คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน ซอฟต์แวร์จึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้

ไวรัสคอมพิวเตอร์ หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูล ไวรัสก็อาจ แพร่ระบาดได้เช่นกัน

การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสจะเข้าไปอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว

เนื่องจากไวรัสเป็นแค่โปรแกรมหนึ่ง การที่ไวรัสเข้าไปอยู่ในหน่วยความจำได้นั้น จะต้องมีการถูกเรียกให้ทำงานได้ขึ้นอยู่กับประเภทของไวรัสแต่ละตัว ปกติผู้ใช้มักจะไม่ทราบว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสนั้นๆ ขึ้นมาทำงานแล้ว

เวชระเบียน หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งที่เป็นเอกสารและข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลบ้านตาขุน

หมวดที่ 1
การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและคงปลอดภัย

2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิ์และการมอบอำนาจให้เข้าถึง

3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อที่ 1. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้อนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบตามความจำเป็นต่อการใช้งาน เท่านั้น

ข้อที่ 2. บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหาร

ข้อที่ 3. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งทบทวน สิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

1) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับ อนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

(2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงาน ผู้ดูแลระบบที่ได้รับมอบหมาย

2) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสาร อิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

(1) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูล ผู้ป่วยข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

(2) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(3) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน ก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะ ก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไป

(4) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(5) รูปแบบของเอกสารอิเล็กทรอนิกส์แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจาก เครื่องมือที่เป็นซอฟต์แวร์ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์ พอที่จะอ่านข้อความนั้นได้ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ TEXT เช่น Format, Document Format, PDF Format (Portable Document Format)
- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์มีรูปแบบที่ใช้ JPEG เช่นFormat, PNG or GIF Format, Bitmapping Format เป็นต้น

ข้อที่ 4. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อที่ 5. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อที่ 6. ผู้ดูแลระบบต้องจัดให้มีการล็อกประตูทางเข้าและบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็น หลักฐานในการตรวจสอบ

ข้อที่ 7. กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

1) ระบบงานบริการ (e-Service Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอดเวลา

2) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด

ส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อที่ 8. ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ดังนี้

1) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศ

2) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

3) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ 3)

4) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าใช้เทคโนโลยีสารสนเทศ

ข้อที่ 9. ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต(Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อที่ 10. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน การใช้งานสิทธิอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

1) จัดทำบัญชีรายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน

2) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อ และตรวจสอบสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

3) ดำเนินการแก้ไขข้อมูลต่างๆสิทธิให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

4) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน 3 วัน หรือ อาจเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 7 วัน

ข้อที่ 11. การบริหารจัดการรหัสผ่าน

1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่งงานหรือยกเลิกการใช้งาน

2) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

3) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการ

ใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการ ส่งรหัสผ่าน (Password)

4) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

5) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

6) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้อง ได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษ ที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้กำหนดให้รหัสผู้ใช้งานต่างจากรหัสและต้องผู้ใช้งานตามปกติ

ข้อที่ 12. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับการในการควบคุมเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

ส่วนที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน(User Responsibilities)

ข้อที่ 13. การใช้งานรหัสผ่านผู้ใช้งานต้องปฏิบัติดังนี้

1) ผู้ใช้งานมีหน้าที่ในการป้องดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่ายให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

2) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว

3) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

4) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

5) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

6) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดาและการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

7) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) อย่างน้อย 2 ครั้งต่อปี

ข้อที่ 14. การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการพ.ศ. 2544 และต้องใช้วิธีการเข้ารหัส(Encryption) ที่เป็นมาตรฐานสากล

ข้อที่ 15. การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน(Username) อันมีกฎหมายกำหนดให้เป็นความผิดไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตามให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อที่ 16. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดีหรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทางดังนี้

1) คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

2) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

3) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

4) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อกหน้าจอทุกครั้งและต้องทำการพิสูจน์ ตัวตนก่อนการใช้งานทุกครั้ง

5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย 15 นาที

ข้อที่ 17. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาล หรือเป็นข้อมูลของบุคคลภายนอก

ข้อที่ 18. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงานห้าม ไม่ให้ทำการเผยแพร่เปลี่ยนแปลง หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อที่ 19. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาล และข้อมูลของผู้รับบริการหากเกิดการสูญหายโดยนำ ไปใช้ในทางที่ผิดการเผยแพร่โดยไม่ได้รับอนุญาตผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อที่ 20. ผู้ใช้งานต้องป้องกันดูแลรักษาไว้ซึ่งความลับความถูกต้องและความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

ข้อที่ 21. ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษาใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาล จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิด ต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้นยกเว้นในกรณีที่โรงพยาบาลต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาล ซึ่งโรงพยาบาลอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อที่ 22. ห้ามเปิดหรือใช้งาน(Run) โปรแกรมประเภท Peer-to-Peer หมายถึงวิธีการจัดเครือข่ายคอมพิวเตอร์ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกันหมายความว่าแต่ละเครื่อง ต่างมีโปรแกรมหรือมีแฟ้มข้อมูลการจัดแบบนี้ไว้เองให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์ เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม(File Server) เท่านั้น หรือโปรแกรมที่มีความเสี่ยงในระดับ เดียวกัน เช่น บิทเทอร์เรนท์(Bittorrent), อีมูล(Emule) เป็นต้นเว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อที่ 23. ห้ามเปิดหรือใช้งาน(Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟัง เพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อที่ 24. ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูลข้อความรูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของประเทศกฎหมายหรือกระทบต่อภารกิจของโรงพยาบาล

ข้อที่ 25. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวนก่อให้เกิดความเสียหรือใช้ในการโจรกรรม

ข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรมหรือกระทบต่อภารกิจของโรงพยาบาล

ข้อที่ 26. ห้ามใช้สินทรัพย์ของโรงพยาบาลเพื่อประโยชน์ทางการค้า

ข้อที่ 27. ห้ามกระทำการใดๆ ไม่ว่าจะเป็นข้อความภาพ เสียงหรือสิ่งอื่นใด เครือข่ายระบบสารสนเทศของโรงพยาบาลโดยเด็ดขาดไม่ว่าจะด้วยวิธีการใดๆก็ตาม

ข้อที่ 28. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อที่ 29. ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อที่ 30. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่า กรณีใดๆเพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากร

ข้อที่ 31. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 4 การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อที่ 32. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์(Operation Center) หมายถึง สถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่ายที่เป็นเขตหวงห้ามโดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อที่ 33. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อที่ 34. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อที่ 35. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กับการใช้งานก่อนได้รับอนุญาตและผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ

ข้อที่ 36. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูลแฟ้มข้อมูลก่อนที่จะกำจัดอุปกรณ์ดังกล่าวและใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สาหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภทดังนี้

ประเภทสื่อบันทึกข้อ	วิธีทำลาย
กระดาษ	ใช้การทำลายด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.00 M ของกระทรวงกลาโหมสหรัฐอเมริกาซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ
	- ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่นCD/DVD	ใช้การทำลายด้วยเครื่องหั่นทำลายเอกสาร

เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	เขียนทับข้อมูลเดิมหลายรอบกระทรวงกลาโหมสหรัฐอเมริกาซึ่งเป็นมาตรฐานการทลายข้อมูลโดยการเขียนทับข้อมูลเดิม - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อที่ 37. ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศต่างๆที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้นห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่างๆไปใช้ในกิจกรรมที่หน่วยงานไม่ได้หรือทำให้เกิดความเสียหายต่อโรงพยาบาล

ส่วนที่ 5 การควบคุมการเข้าถึงเครือข่าย(Network Access Control)

ข้อที่ 38. มาตรการควบคุมการเข้าออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย(Server)

1) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่ายต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาต เข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

2) ผู้ดูแลระบบต้องตรวจสอบความถูกต้องของข้อมูลในสมุดแบบฟอร์มบันทึกการขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อที่ 39. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัดโดยผู้ใช้งานต้อง กรอกแบบฟอร์ม“การขอเชื่อมต่อเครือข่าย”

ข้อที่ 40. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย(Sub Domain Name) ที่หน่วยงาน รับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงานและจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผล กระทบต่อการกระทบของระบบและผู้ใช้งานอื่นๆ

ข้อที่ 41. ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหรือการกระทำใดๆต่ออุปกรณ์ส่วนกลางได้แก่ อุปกรณ์จัดเส้นทาง(Router) อุปกรณ์กระจายสัญญาณข้อมูล(Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อที่ 42. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมี ประสิทธิภาพดังต่อไปนี้

1) จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานาระบบเครือข่ายที่ได้รับเฉพาะอนุญาตเท่านั้น

2) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

3) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆได้

4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ หน่วยงาน

ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกรวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรม ประสงค์ร้าย (Malware) ด้วย

5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

6) การเข้าสู่ระบบเครือข่ายภายในหน่วยโดยงานผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

7) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

8) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆพร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

9) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่ายได้แก่รายชื่อผู้ขอใช้บริการรายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอกต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อที่ 43. ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย(Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย(Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆของซอฟต์แวร์ระบบ (Systems Software)

ข้อที่ 44. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อที่ 45. กำหนดให้มีการจัดเก็บรหัสต้นฉบับ (source code), คลังโปรแกรม(Library) และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อที่ 46. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางคอมพิวเตอร์ พ.ศ.2550

ข้อที่ 47. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย(Server) จากผู้ใช้งานภายนอกหน่วยงานเพื่อดูแลรักษาความปลอดภัยของระบบตามแนวทางปฏิบัติดังต่อไปนี้

1) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่อง

คอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากหัวหน้าหน่วยงาน

2) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

3) วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

4) การเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

5) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลง บันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อที่ 48. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

1) Internet แบ่งแยกเครือข่ายเป็นเครือข่าย เพื่อควบคุมการเข้าถึง เครือข่ายที่ไม่ได้รับอนุญาต

2) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอกเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อที่ 49. กำหนดการป้องกันเครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต่างๆ ต้องทบทวนการกำหนดค่า Parameter ต่างๆเช่น IP Address อย่างน้อยปีละ 1 ครั้งนอกจากนี้การกำหนด แก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อที่ 50. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่นๆรวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อที่ 51. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก(IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติโดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อที่ 52. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่ เชื่อมต่อสามารถมองเห็นได้เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของเครือข่ายได้โดยง่าย

ข้อที่ 53. การใช้เครื่องมือ(Tools)ต่างๆ เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแล ระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ 6 การควบคุมการเข้าถึงระบบปฏิบัติการ(Operating System Access Control)

ข้อที่ 54. ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน(โดยปฏิบัติตามข้อ8) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน(โดยปฏิบัติตามข้อ10) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงานเป็นต้น

ข้อที่ 55. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

1) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

2) หลังจากระบบติดตั้งเสร็จต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

3) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

4) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

5) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

6) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเวลานาน

7) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงานโรงพยาบาล

8) ซอฟต์แวร์ที่โรงพยาบาลฯ ใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามความจำเป็นในหน้าที่ และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

9) ซอฟท์แวร์ที่โรงพยาบาลจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นห้ามมิให้ผู้ใช้งานทำการติดตั้งถอดถอนเปลี่ยนแปลงแก้ไขหรือทำสำเนาเพื่อไปใช้งานที่อื่น

10) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเพื่อประโยชน์ทางการค้า

11) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมกรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

12) ห้ามผู้ใช้งานของหน่วยงานควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อที่ 56. การระบุและยืนยันตัวตนของผู้ใช้งาน(User Identification and Authentication) กำหนดให้ ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความ ถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อที่ 57. การใช้งานโปรแกรมประเภทยูทิลิตี้(Use of system utilities) ต้องจำกัดและควบคุมการใช้งาน โปรแกรมยูทิลิตี้สาหรับโปรแกรมคอมพิวเตอร์ที่สำคัญเนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการดังนี้

1) การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบและต้องมีการพิสูจน์ยืนยันตัวตนสาหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้เพื่อจำกัดและควบคุมการใช้งาน

2) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

3) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

4) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

5) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานจำเป็นในการใช้งานรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี

ข้อที่ 58. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

1) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานรวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 15 นาที

2) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานเร็วขึ้นสำหรับระบบสารสนเทศ ที่มีความเสี่ยงสูง

ข้อที่ 59. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

1) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจากัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดและกำหนดให้ใช้งานได้ตามช่วงเวลาการทำงานที่หน่วยงานกำหนดเท่านั้น

2) กำหนดให้ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะหรือพื้นที่ภายนอกหน่วยงานมีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ 7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ(Application and Information Access Control)

ข้อที่ 60. ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่(โดยปฏิบัติตามข้อ8)ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสาหรับการยกเลิกสิทธิการใช้งาน(โดยปฏิบัติตามข้อ10) เช่นการลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงานเป็นต้น

ข้อที่ 61. ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่นระบบคอมพิวเตอร์โปรแกรมประยุกต์(Application) จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต(Internet) เป็นต้นโดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อที่ 62. ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆเมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน 15 นาทีระบบจะยุติการใช้งานผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน(Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อที่ 63. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

2) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

รูปแบบที่ไม่ได้ป้องกันการเข้าถึง

3) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

4) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานโดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อที่ 64. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ ละประเภทชั้นความลับดังต่อไปนี้

1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการผ่านระบบงาน

2) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือXML Encryption เป็นต้น

5) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่นบำรุงรักษาตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อที่ 65. ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงให้ปฏิบัติดังนี้

1) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่นๆ

2) มีการควบคุมสภาพแวดล้อมของตนเองโดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

3) มีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

ข้อที่ 66. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังต่อไปนี้

1) ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้ งานหรือไม่และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้วให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

4) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

5) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ 8 การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malwares)

ข้อที่ 67. โรงพยาบาลได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญาดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาต ให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่หากไม่มีลิขสิทธิ์การตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ถือว่าเป็น ความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อที่ 68. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอนเปลี่ยนแปลงแก้ไขหรือทำสำเนาเพื่อนไปใช้งานที่อื่นๆยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิในลิขสิทธิ์

ข้อที่ 69. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์(Antivirus) ตามที่หน่วยงาน ได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาโดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อที่ 70. บรรดาข้อมูลไฟล์ซอฟต์แวร์หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อที่ 71. ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ(Update Patch) ให้ใหม่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อที่ 72. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลารวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อที่ 73. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัสผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

ข้อที่ 74. ห้ามลักลอบทำสำเนาเปลี่ยนแปลงลบทิ้งซึ่งข้อมูลข้อความเอกสาร หรือสิ่งใดๆที่เป็นสินทรัพย์ของหน่วยงานหรือของผู้อื่นโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อที่ 75. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใดๆที่อาจก่อให้เกิดความ เสียหายมาสู่สินทรัพย์ของหน่วยงานสิทธิที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆสามารถดำเนินการได้แต่ต้องไม่ดำเนินการดังนี้

1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่านการลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของ บุคคลอื่น

2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

3) พัฒนาโปรแกรมใดที่จะทำให้ตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นใน

ลักษณะเช่นเดียวกับหนอนวนัสคอมพิวเตอร์

4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

5) นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทยกรณีที่ผู้ใช้งานสร้างเว็บเพลบนเครือข่ายคอมพิวเตอร์

ข้อที่ 76. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก(Outsourced software development)

1) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

2) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ (source code) ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

3) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องขอซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ไว้กับผู้ให้บริการภายนอกนั้น

4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

5) หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายหน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่างๆให้พร้อมใช้งาน

ส่วนที่ 9 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อที่ 77. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอตามที่หน่วยงานกำหนด

ข้อที่ 78. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกลการจัดเก็บข้อมูลและอุปกรณ์ สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อที่ 79. ผู้ใช้งานจากระยะไกลทุกคนต้องผ่านการพิสูจน์ตัวตนเพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่านหรือวิธีการเข้ารหัส เป็นต้น

ข้อที่ 80. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

ข้อที่ 81. ต้องกำหนดชนิดของงานชั่วโมงการทำงาน ชั้นความลับของข้อมูลระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อที่ 82. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการขอยกเลิกการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงานและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ 10 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย(Wireless LAN Access Control)

ข้อที่ 83. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย(Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อที่ 84. ผู้ดูแลระบบต้องทำการเปลี่ยนค่าSSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดย

ปริยาย(Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย(Access Point) มาใช้งานและกำหนดให้ซ่อน SSID (Service Set Identifier)

ข้อที่ 85. ผู้ดูแลระบบต้องกำหนดค่าWireless Security เป็นแบบWEP (Wired Equivalent Privacy) หรือWPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่างWireless LAN Client และอุปกรณ์ กระจายสัญญาณแบบไร้สาย(Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อที่ 86. ผู้ดูแลระบบเลือกใช้วิธีการควบคุมMAC Address (Media Access Control Address) และชื่อผู้ใช้งาน(Username) รหัสผ่าน(Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มีMAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และรหัสผ่าน(Password) ตามที่กำหนดไว้เท่านั้นให้ใช้เข้าระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อที่ 87. ผู้ดูแลระบบต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อที่ 88. ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายหน่วยงานผ่านทางVPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อที่ 89. ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อที่ 90. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายและจัดส่งรายงานผลการ ตรวจสอบทุก 3 เดือนและในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อที่ 91. ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบ เครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต(Intranet) และฐานข้อมูลภายในต่างๆของหน่วยงาน

ข้อที่ 92. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลจะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อที่ 93. ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้ เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิ การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่ 11 การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย(Firewall Control)

ข้อที่ 94. หน่วยงานมีหน้าที่ในการบริหารจัดการการติดตั้งและกำหนดค่าของFirewall ทั้งหมด

ข้อที่ 95. การกำหนดค่าเริ่มต้นของFirewall ต้องกำหนดเป็นปฏิเสธทั้งหมด(Deny)

ข้อที่ 96. ทุกบริการ(Services) และเส้นทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตPolicyจะต้องถูกบล็อก (Block) โดย Firewall

ข้อที่ 97. ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน(Login) ก่อนการใช้งานทุกครั้ง

ข้อที่ 98. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้งหากมีการเปลี่ยนแปลงค่าต่างๆขอ Firewall

ข้อที่ 99. การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูจัดการเท่านั้น

ข้อที่ 100. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewallจะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

ข้อที่ 101. การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งานซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อที่ 102. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้อง กำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อทีเป็นต่อการให้บริการเท่านั้น

ข้อที่ 103. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆของอุปกรณ์Firewall เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อที่ 104. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆภายในหน่วยงานที่มีเป็นอินทราเน็ตจะต้องไม่อนุญาตการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ตให้มีเว้นแต่มีความจำเป็นโดยจะต้องอนุญาตเป็นกรณีไป

ข้อที่ 105. หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที การใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อที่ 106. การเชื่อมต่อในลักษณะของการRemote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการของการดเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายและจะต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานก่อน

ข้อที่ 107. ผู้ละเมิดนโยบายด้านความปลอดภัยของFirewall จะถูกระงับการใช้งานอินเตอร์เน็ตทันที

ส่วนที่ 12 การควบคุมการใช้จดหมายอิเล็กทรอนิกส์(E-Mail)

ข้อที่ 108. ไม่บันทึกหรือเก็บรหัสผ่าน(Password) ไว้ในระบบคอมพิวเตอร์

ข้อที่ 109. เปลี่ยนรหัสผ่าน(Password) ทุก 3 - 6 เดือน

ข้อที่ 110. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์(E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์(E-Mail) เป็น ผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์(E-Mail)ของตน

ข้อที่ 111. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์(E-Mail) เสร็จสิ้นต้องลงบันทึกออก Logout) ทุกครั้ง

ข้อที่ 112. การส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์(E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลE-Mailที่หน่วยงานกำหนดไว้ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อที่ 113. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายขยะ(Spam Mail)

ข้อที่ 114. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อที่ 115. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อที่ 116. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา ข้อ127. ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป

ข้อที่ 117. ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ตามความจำเป็นอย่างสม่ำเสมอ(แม้ว่าหน่วยงาน จะทำการสำรองข้อมูลาE-Mail ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่ง ดังนั้นE- Mail ที่เก่ามากๆและจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ข้อที่ 118. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็นExecutable file เช่น.exe .com เป็นต้น

ข้อที่ 119. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ใช้

ข้อที่ 120. ผู้ใช้งานต้องใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงานทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อที่ 121. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจนวนน้อยที่สุดและควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการอจากระบบเพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ข้อที่ 122. ข้อควรระวังผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังคอมพิวเตอร์ของตนเพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อที่ 123. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ 18 ธันวาคม 2550 เรื่องการพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่ 13. การควบคุมการใช้อินเตอร์เน็ต(Internet)

ข้อที่ 124. ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้นเช่นProxy ,Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อที่ 125. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บบราวเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อที่ 126. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อที่ 127. ไม่ใช้ระบบอินเตอร์เน็ต(Internet) ของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนาพระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคมละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อที่ 128. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต(Internet)ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อที่ 129. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อที่ 130. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงานการทลายความสัมพันธ์กับบุคลากรของหน่วยงาน อื่นๆ

ข้อที่ 131. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรอันเป็นความผิดเกี่ยวกับการก่อการร้ายหรือภาพที่มีลักษณะอันไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

ข้อที่ 132. หลังจากใช้งานระบบอินเตอร์เน็ต(Internet) เสร็จแล้วให้ปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อที่ 133. หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้วให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ข้อที่ 134. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

ส่วนที่ 14 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อที่ 135. แนวทางปฏิบัติการใช้งานทั่วไป

1) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมหน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

3) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

4) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของโรงพยาบาลเท่านั้น

5) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

6) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

7) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง ทำการตั้งค่าScreen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อก หน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาทีเพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

8) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับหน่วยงานยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

ข้อที่ 136. การใช้รหัสผ่าน

1) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

2) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

3) ควรเปลี่ยนรหัสผ่านทุก 3–6 เดือน

ข้อที่ 137. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware)

1) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

2) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

3) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหายถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อที่ 138. การสำรองข้อมูลและการกู้คืน

1) ผู้ใช้งานต้องรับผิดชอบในการสรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆเช่น CD, DVD, External Hard Disk เป็นต้น

2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

3) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บ Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญไว้เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ 15 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อที่ 139. แนวทางปฏิบัติการใช้งานทั่วไป

1) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และ นำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

3) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ

4) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

5) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

6) หลีกเลี่ยงการใช้นิ้วหรือของแข็งเช่น ปลายปากกา กดสัมผัสหน้าจอLCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

7) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

8) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุดและต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

9) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

10) การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อที่ 140. ความปลอดภัยทางด้านกายภาพ

1) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อนความชื้นฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อที่ 141. การควบคุมการเข้าถึงระบบปฏิบัติการ

1) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

2) ผู้ใช้งานต้องกหนดรหัสผ่านให้มีคุณภาพดีและรัดกุม

3) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาทีให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

4) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเวลานาน

ข้อที่ 142. การใช้รหัสผ่านให้ผู้ใช้งาน

1) ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

2) ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

3) ควรเปลี่ยนรหัสผ่านทุก 3–6 เดือน

ข้อที่ 143. การสำรองข้อมูลและการกู้คืน

1) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาโดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

2) ผู้ใช้งานต้องจัดเก็บรักษาข้อมูลสื่อสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

3) แผ่นสื่อสำรองข้อมูลต่างๆที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

4) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

5) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บ Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียจะไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ 16 การตรวจจับการบุกรุก(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

ข้อที่ 144. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ความมั่นคงปลอดภัยเป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมกับบทบาทความรับผิดชอบที่เกี่ยวข้อง

ข้อที่ 145. IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเตอร์เน็ตทุกเส้นทาง

ข้อที่ 146. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบระบบ IDS/IPS

ข้อที่ 147. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อที่ 148. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่านIDS/IPSจะต้องมีการบันทึกผลการตรวจสอบ

ข้อที่ 149. ระบบ IDS/IPS จะต้องมีการตรวจสอบและUpdate Patch/Signature เป็นประจำ

ข้อที่ 150. ต้องมีการตรวจสอบเหตุการณ์ข้อมูลจราจรพฤติกรรมการใช้งานกิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อที่ 151. พฤติกรรมการใช้งานกิจกรรมหรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก ระบบพฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบประสบความสำเร็จและไม่ประสบความสำเร็จ ทั้งที่จะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบ

ข้อที่ 152. พฤติกรรมกิจกรรมที่น่าสงสัยหรือระบบการทางานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบ ภายใน 1 ชั่วโมงที่ตรวจพบ

ข้อที่ 153. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

ข้อที่ 154. หน่วยงานมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรม การ

บุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อที่ 155. ผู้ที่ถูกตรวจสอบว่าพยายามการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาล การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศหรือจะถูกระงับการใช้เครือข่ายทันทีหากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล ทรัพยากรและระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ 17 การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อที่ 156. การปรับปรุงระบบปฏิบัติการ(Operating System Update)

1) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ
2) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน
3) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน (User)
4) กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name / IP Address)
5) ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update) ติดตั้งโปรแกรม Antivirus/ปรับปรุง Virus Definition และการกำหนดค่าตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

ข้อที่ 157. การบริหารบัญชีผู้ใช้งาน/สิทธิการเข้าถึงและการใช้งานระบบ (User Account Management)

1) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)
2) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)
3) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อที่ 158. การปรับปรุงการรักษาความปลอดภัย (System Security & Anti-virus/Anti-Virus)

1) ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ
2) ประสิทธิภาพของระบบ (Performance) หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง
3) ปรับปรุง/กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา
4) ปรับปรุงโปรแกรม Anti-virus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์
5) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์ เป็นประจำ

ข้อที่ 159. ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

1) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้
2) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้อง และมีประสิทธิภาพ
3) สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล(Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิการใช้

4) ปรับปรุง/กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

ข้อที่ 160. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ /กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

1) ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

2) กำหนดค่าให้เป็นไปตามโปรแกรม หรือบริการ หรือทำงานร่วมกับระบบปฏิบัติการตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

3) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการกำหนดทดสอบการให้บริการตามระบบงานนั้น

4) แจ้งผู้ใช้งานหรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้โดยแจ้งรายชื่อรหัสผ่านและสิทธิการเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

5) กำหนดเกณฑ์การสำรอง สำเนา ทดสอบกู้คืน (Restore Test)

6) บันทึกข้อกำหนดค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

ส่วนที่ 18 การจัดเก็บข้อมูลจราจรคอมพิวเตอร์(Log)

ข้อที่ 161. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ข้อมูลที่ใช้ในการจัดเก็บและกำหนดชั้นต้องการความลับในการเข้าถึง

ข้อที่ 162. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่เก็บรักษาไว้(Log)

ข้อที่ 163. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้า สู่ระบบ เป็นต้นเพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อที่ 164. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ 2
ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินข้อมูล

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

2. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้หน่วยงานปฏิบัติอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วิธีปฏิบัติ

ส่วนที่ 1 การรักษาความปลอดภัยฐานข้อมูล

ข้อที่ 1. กำหนดสิทธิและความสำคัญของข้อมูลและฐานข้อมูล

1) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

2) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

(2) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบได้รับมอบหมาย

3) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(1) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

(2) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับสำคัญมากที่สุด

- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อยที่สุด

(3) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุดหมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความ เสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(4) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(5) การกำหนดเวลาที่ได้เข้าถึง

(6) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อที่ 2. ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิเข้าใช้ หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่เป็นต่อมาตรการรักษาความปลอดภัย

ข้อที่ 3. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับ พ.ศ. 2544 และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 1 ข้อหมวดที่12

ข้อที่ 4. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งาน และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็นเพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อที่ 5. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยนขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

1) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

2) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

3) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

4) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อ

การป้องกันการปฏิเสธ

5) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

6) กำหนดสิทธิการเข้าถึงข้อมูล

7) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

8) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูลซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ

ส่วนที่ 2 การสำรองข้อมูล

ข้อที่ 6. พิจารณาคัดเลือกระบบสารสนเทศที่สูญหายและจัดทาระบบสำรองที่เหมาะสมให้อยู่ในสภาพ พร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อที่ 7. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อที่ 8. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองและจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

ข้อที่ 9. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยให้มีการกำหนดความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

1) กำหนดประเภทของข้อมูลที่ต้องทาการสำรองเก็บไว้และความถี่ในการสำรอง

2) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

3) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อ ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

4) ตรวจสอบการตั้งค่า (Configuration) ต่าง ๆ ของระบบการสำรองข้อมูล

5) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

6) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานทีนั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

7) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

8) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

9) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

10) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความ เสี่ยงต่างๆ ที่จะเกิดขึ้น

11) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเข้าเก็บไว้

12) สำรองข้อมูลอย่างน้อย 3 ชุด

13) ใช้ 2 เทคโนโลยีในการสำรองข้อมูลเป็นอย่างน้อย เพื่อจะได้ไม่เสียหายด้วยสาเหตุเดียวกัน

14) มีการสำรองข้อมูล 1 ชุดไปที่อื่น สถานที่อื่น หรือ แบบออฟไลน์

15) มีไฟล์สำรองรายวัน

16) มีเอกสารตรวจสอบ เครื่อง Slave สามารถใช้งานได้

17) มีเอกสารการตรวจสอบความสมบูรณ์ของไฟล์ Backup

18) มีเอกสารระบุผู้รับผิดชอบ ข้อมูลสำรองและความสมบูรณ์ของข้อมูล เมื่อมีการ Restore เดิมกลับมาใช้งาน

ส่วนที่ 3 แผนเตรียมความพร้อมกรณีฉุกเฉิน

ข้อที่ 10. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

1) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานานน้ำท่วมไฟไหม้แผ่นดินไหว การชุมนุมประท้วงให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการ เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น

6) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อที่ 11. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

ข้อที่ 12. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์

ข้อที่ 13. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อที่ 14. มีการทบทวนระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

หมวดที่ 3
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
2. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ
3. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

วิธีปฏิบัติ

ส่วนที่ 1 การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ 1 ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อที่ 1. จัดลำดับความสำคัญของความเสี่ยง

ข้อที่ 2. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อที่ 3. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อที่ 4. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อที่ 5. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อที่ 6. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

1) กำหนดให้ผู้ตรวจสอบ สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

2) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือต้องจัดเก็บ ไว้โดยมีการป้องกันเป็นอย่างดี

3) กำหนดให้มีการะบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

4) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

5) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ 2 ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ 4 ประเภท ดังนี้

ประเภทที่ 1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน(Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักหรือหยุดทำงาน และอาจส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพกำหนดได้แนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้

ประเภทที่ 2 ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วยไวรัสคอมพิวเตอร์(Computer Virus), หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจัน(Trojan Horse), และข่าวไวรัสหลอกลวง(Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software

ประเภทที่ 3 ภัยจากไฟไหม้ หรือระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

1) ติดตั้งอุปกรณ์สองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสรองข้อมูลไว้อย่างปลอดภัย

2) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีเหตุเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนไปยังห้องฉุกเฉินเพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินได้ทันท่วงที

3) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉินอัคคีภัย โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานสม่ำเสมอ

ประเภทที่ 4 ภัยจากน้ำท่วม(อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

1) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

2) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเครื่องปรับอากาศไฟ เพื่อป้องกัน เครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

3) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย

4) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าใน

ห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่าย สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

5) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้ งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือตรวจสอบระบบ Network ว่า สามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูก ข่ายได้หรือไม่ เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูล ได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้ตามปกติ

หมวดที่ 4
การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม
(Physical and environment security)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สนที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อที่ 1. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบ ที่ติดตั้งประจำโต๊ะทำงาน

ข้อที่ 2. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

1) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

2) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า ออก ของบุคคลเป็นจำนวนมาก-

3) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

4) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

5) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจาก บริเวณดังกล่าว

6) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

7) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศ จัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อที่ 3. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

1) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่รับ อนุญาต รวมทั้งป้องกัน'ได้'ไม่' ความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกันโดยการกำหนด พื้นที่ดังกล่าวอาจ

แบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบ เทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อที่ 4. การควบคุมการเข้าออก อาคารสถานที่

1) กำหนดสิทธิผู้ใช้งาน ที่มีสิทธิผ่านเข้าออก และช่วงเวลาที่มี-สิทธิในการผ่านเข้าออก ในแต่ละอย่างชัดเจน ”พื้นที่ใช้งานระบบ“

2) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตร ประชาชนใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและ รับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

3) ให้มีการบันทึกวันและเวลาการเข้า ออกพื้นที่สำคัญของผู้ที่มาติดต่อ-(Visitors)

4) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

5) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

6) จัดเก็บบันทึกการเข้า มีความสำคัญ เช่นออกสำหรับพื้นที่หรือบริเวณที่-(Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

7) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

8) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

9) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

10) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

11) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

12) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้าก ออก- ในพื้นที่หรือบริเวณที่มีความสำคัญ(Data Center)

13) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงาน ในพื้นที่หรือบริเวณที่มีความสำคัญ

14) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ อย่างน้อยปีละ ครั้ง 1

ข้อที่ 5. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

1) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

2) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ครั้ง เพื่อให้ 1 มั่นใจได้ ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของ ระบบ

3) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

ข้อที่ 6. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security)

1) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

2) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเลียหาย

3) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

4) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

5) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

6) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ บิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

7) พิจารณาใช้งานสายไฟเบอร์ออปติก แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณ) แบบCoaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

8) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อที่ 7. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

1) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

2) ปฏิบัติตามดำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะน่า

3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ ในการตรวจสอบหรือประเมินในภายหลัง

4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

5) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

6) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างให้บริการจาก

ภายนอก อนุ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับ (ที่มาทำการบำรุงรักษาอุปกรณ์)ญาต

ข้อที่ 8. การน่าทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

1) ให้มีการขออนุญาตก่อนน่าอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

2) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือน่าอุปกรณ์ออกนอกหน่วยงาน

3) กำหนดระยะเวลาของการน่าอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

4) เมื่อมีการน่าอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเลียหายของอุปกรณ์ด้วย

5) บันทึกข้อมูลการน่าอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไจ้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อน่าอุปกรณ์ส่งคืน

ข้อที่ 9. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

1) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการน่าอุปกรณ์หรือ ทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

2) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยสำพังในที่สาธารณะ

3) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

หมวดที่ 5
การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อที่ 1. ระบบป้องกันผู้บุกรุก

1) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อที่ 2. ระบบไฟร์วอลล์

1) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ 1 ครั้ง

2) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

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

3) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อที่ 3. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

1) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในกระทรวงสาธารณสุขไปยังภายนอกหรือไม่

2) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจ พบว่ากระจายอยู่ในเครือข่ายของกระทรวงสาธารณสุข

3) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการ แก้ไขเครื่องนั้นทันที

หมวดที่ 6
การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1. เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของกระทรวงสาธารณสุข

2. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

3. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อที่ 1. จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อย ปีละ 1 ครั้ง

ข้อที่ 2. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อที่ 3. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า 1 ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อที่ 4. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกียวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือ ข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อที่ 5. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อที่ 6. ให้มีการสร้างความตระหนักเกียวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าทีมีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อที่ 7. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อที่ 8. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ทีได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของกระทรวงสาธารณสุข และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ 7
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อที่ 1. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารระดับสูงสุด (Chief Executive Office: CEO) ของหน่วยงาน
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือเทียบเท่าระดับผู้อำนวยการ

1) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

2) รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆแก่หน่วยงานหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อที่ 2. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้ากลุ่ม/หัวหน้าศูนย์เทคโนโลยีสารสนเทศ หรือเทียบเท่าหัวหน้ากลุ่ม

1) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

2) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อที่ 3. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการกระทรวงสาธารณสุข เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์

1) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

4) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

5) ป้องกันการถูกเจาะระบบและแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

6) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต

7) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข ผู้รับผิดชอบได้แก่

- นายสรศักดิ์ นาคจิตร ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ
- นางสาวจิติมา ศรีสาคร ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ
- นางสาวเบญจวรรณ ชูพรม ตำแหน่งนักวิชาการคอมพิวเตอร์

หมวดที่ 8
การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก

วัตถุประสงค์

เพื่อให้หน่วยงานภายนอกได้ปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข ทำให้ระบบสารสนเทศดำเนินไปได้อย่างต่อเนื่องและมีประสิทธิภาพ

แนวปฏิบัติ

ข้อที่ 1. ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูลและระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

ข้อที่ 2. การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอก ต้องมีการขออนุญาตอย่างเป็นทางการและได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

ข้อที่ 3. การบริการและการดำเนินงานจากหน่วยงานภายนอกจะต้องปฏิบัติตามนโยบายการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศแนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ของกระทรวงสาธารณสุข

ข้อที่ 4. ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

ข้อที่ 5. ต้องมีการทำสัญญาการรักษาความลับขององค์กรระหว่างหน่วยงานและหน่วยงานภายนอกที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ

ข้อที่ 6. ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน และวิธีการดำเนินงาน เป็นอย่างน้อย เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขต ที่ได้กำหนดไว้

ข้อที่ 7. สัญญาระหว่างหน่วยงาน และ หน่วยงานภายนอก ในการให้บริการต้องระบุถึงหัวข้อต่างๆดังต่อไปนี้ เป็นอย่างน้อย

- รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ
- ระดับการให้บริการ (Service Level)
- หน้าที่และความรับผิดชอบขององค์กรและหน่วยงานภายนอก ในการให้บริการในครั้งนี้
- ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้
- ราคา และเงื่อนไขการชำระเงิน
- ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อ หรือ พัฒนาขึ้น (ถ้ามี)
- การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์การ
- แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้

ผ่านการพิจารณาจากคณะกรรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลบ้านตาขุน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

(นายแพทย์เอกพล พิศาล)
ผู้อำนวยการโรงพยาบาลบ้านตาขุน
วันที่ เมษายน 2567