ประกาศโรงพยาบาลค่ายกฤษณ์สีวะรา
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ของโรงพยาบาลค่ายกฤษณ์สีวะรา

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และ ระเบียบ ทบ. ว่าด้วย การรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทบ. (ฉบับที่ ๒) ปี ๒๕๖๐ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะราเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาลค่ายกฤษณ์สีวะรา จึงเห็นสมควรกำหนดนโยบาย ดังนี้

๑. โรงพยาบาลค่ายกฤษณ์สีวะราส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๒. โรงพยาบาลค่ายกฤษณ์สีวะรา กำหนดให้มีการควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้ข้อมูลของผู้ใช้งานและข้อมูลความลับของผู้ป่วยมีความปลอดภัย

๓. โรงพยาบาลค่ายกฤษณ์สีวะรา กำหนดให้มีการจัดทำระบบสำรองข้อมูลเพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ

๔. โรงพยาบาลค่ายกฤษณ์สีวะรา กำหนดให้มีการตรวจสอบ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

๕. โรงพยาบาลค่ายกฤษณ์สีวะรา กำหนดให้บุคลากรทุกระดับปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะรา พ.ศ. ๒๕๖๘ เพื่อให้การปฏิบัติงานมีความมั่นคงปลอดภัย และมีประสิทธิภาพ

ประกาศ ณ วันที่ ๑ เดือน ตุลาคม พ.ศ. ๒๕๖๗

พ.อ.

(จิตกานต์ อรรคธรรม)
ผอ.รพ.ค่ายกฤษณ์สีวะรา

ประกาศโรงพยาบาลค่ายกฤษณ์สีวะรา
เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลค่ายกฤษณ์สีวะรา พ.ศ. ๒๕๖๘

ตามระเบียบ ทบ. ว่าด้วย การรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทบ. (ฉบับที่ ๒) ปี ๒๕๖๐ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในหน่วย ทบ. และประกาศโรงพยาบาลค่ายกฤษณ์สีวะรา เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะรา ที่กำหนดให้บุคลากรทุกระดับปฏิบัติตามแนวปฏิบัติฯ นั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะรา เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกัน ปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ โรงพยาบาลค่ายกฤษณ์สีวะรา จึงได้ประกาศแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด ดังนี้

๑. ประกาศฉบับนี้มีวัตถุประสงค์เพื่อเผยแพร่แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะรา พ.ศ. ๒๕๖๘ ให้บุคลากรทุกระดับในหน่วยงาน และผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบ เข้าใจ และถือปฏิบัติ

๒. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

๓. ให้บุคลากรทุกระดับของโรงพยาบาลค่ายกฤษณ์สีวะรา ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะรา พ.ศ. ๒๕๖๘ ตามที่แนบท้ายประกาศ อย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ เดือน ตุลาคม พ.ศ. ๒๕๖๗

พ.อ.

(จิตกานต์ อรรคธรรม)
ผอ.รพ.ค่ายกฤษณ์สีวะรา

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลค่ายกฤษณ์สีวะรา มณฑลทหารบกที่ 29

คำนำ

โรงพยาบาลค่ายกฤษณ์สีวะรามีภารกิจในการให้บริการทางการแพทย์แก่ผู้ใช้บริการที่มีทั้งกำลังพลทหาร ครอบครัว ตลอดจนประชาชนทั่วไป โดยอาศัยระบบเทคโนโลยีสารสนเทศเป็นเครื่องมือที่สำคัญ เพื่อให้สามารถดำเนินงานและให้บริการได้อย่างถูกต้อง ปลอดภัย ครบถ้วนต่อเนื่องรวดเร็วและทันเวลา มีการติดต่อ ประสานงานและการสื่อสารมีประสิทธิภาพ อีกทั้งยังเป็นเครื่องมือที่สำคัญให้แก่คณะกรรมการบริหารโรงพยาบาลในการนำข้อมูลและสารสนเทศไปใช้ในการบริหารองค์กร เพื่อไปสู่วิสัยทัศน์ตามพันธะกิจที่ได้รับมอบหมายต่อไป

โรงพยาบาลค่ายกฤษณ์สีวะราจึงจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะรา เพื่อให้การดำเนินงานในระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพมีความมั่นคงปลอดภัย และเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยมุ่งหวังให้บุคลากรทุกระดับได้นำนโยบายและแนวทางปฏิบัตินี้ไปปฏิบัติอย่างเคร่งครัดเพื่อให้ระบบเทคโนโลยี สารสนเทศของโรงพยาบาลมีความเหมาะสม เกิดประสิทธิภาพสูงสุด มีความมั่นคงปลอดภัยด้านสารสนเทศ และ สามารถดำเนินงานได้อย่างต่อเนื่อง เต็มประสิทธิภาพรวมทั้งเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งาน ระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องจากการถูกคุกคามจากภัยคุกคามต่างๆหรือ ซึ่งอาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศของโรงพยาบาล

พ.อ. 

(จิตกานต์ อรรคธรรม)

ผอ.รพ.ค่ายกฤษณ์สีวะรา

...1..../....ต.ค.... /2567...

1. แนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

เพื่อป้องกันความเสียหายต่อระบบข้อมูลสารสนเทศ ซึ่งอาจเกิดขึ้นได้จากสาเหตุหลายประการเพื่อเพิ่มมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะราให้อยู่ใน ระดับมาตรฐานสากลจึงกำหนดแนวทางปฏิบัติด้านการรักษาความมั่นคงความปลอดภัยของระบบฯ ไว้ดังนี้

1. **การพิสูจน์ตัวตนและสิทธิในการเข้าถึงการใช้งาน (Authentication, Authorization and Accountability)**

1.1 ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีของตนเอง ได้แก่ชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

1.2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

1.3 ผู้ใช้งานควรตั้งรหัสผ่านให้เกิดความปลอดภัยโดยรหัสผ่านควรประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษรซึ่งประกอบด้วยตัวเลข (Numerical character), ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

1.4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่านในระบบทุกๆช่วงเวลาเป็น 3 หรือ 6 เดือน โดยเงื่อนไขในการตั้งรหัสผ่านใหม่ จะต้องมีความยาวตั้งแต่ 6 – 10 ตัวอักษร และรูปแบบจะต้อง ประกอบไปด้วย ตัวอักษรภาษาอังกฤษตัวใหญ่ ตัวเล็ก และ ตัวเลขผสมกันอย่างน้อย 1 ตัว

1.5 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของโรงพยาบาล และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านโดนล็อคหรือเกิดจากความผิดพลาดใดๆของผู้ใช้งาน ต้องแจ้งให้ผู้ดูแลระบบของศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราทราบทันที โดย

(1) คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการควรต้องทำการพิสูจน์ตัวตนทุกครั้ง

(2) การใช้งานระบบเครือขายอินเตอร์เน็ต จะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(3) การใช้งานระบบเครือข่ายอินเทอร์เน็ต ต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคล ผู้ใช้งานได้

(4) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ทุกเครื่องต้องการ logout โปรแกรมทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานใหม่ทุกครั้ง

(5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหนาจอ (screen saver) โดยตั้งเวลาอย่างน้อย 5 นาที

2. การบริหารจัดการทรัพย์สิน (Assets Management)

2.1 ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งเป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ ได้รับอนุญาตจากผู้ดูแลระบบ

2.2 ผู้ใช้งานต้องไม่น าอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะ ได้รับ อนุญาตจากผู้ดูแลระบบ

2.3 ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

2.4 ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ

2.5 ผู้ใช้งานต้องไม่คัดลอก หรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

2.6 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาลมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สิน ของผู้ใช้งานเอง โดยการรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้ง

2.7 กรณีที่มีการนำครุภัณฑ์ไปใช้ภายนอกศูนย์คอมพิวเตอร์ เช่น Notebook หรืออื่นๆ ผู้ใช้งานต้องดูแล และรับผิดชอบทรัพย์สินของโรงพยาบาลที่ได้รับมอบหมาย

2.8 ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สิน หาก ความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

2.9 ผู้ใช้งานต้องไม่ให้ผู้อื่นหยิบยืมคอมพิวเตอร์ตั้งโต๊ะหรือคอมพิวเตอร์แบบพกพาที่โรงพยาบาลมอบ ไว้ให้ ใช้งานไม่ว่าในกรณีใดๆ เว้นแต่การหยิบยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

2.10 ทรัพย์สินและระบบสารสนเทศต่างๆที่โรงพยาบาลจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งาน ของโรงพยาบาลค่ายกฤษณ์สีวะราเท่านั้นห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆไปใช้ใน กิจกรรมที่โรงพยาบาลค่ายกฤษณ์สีวะราไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อโรงพยาบาลค่ายกฤษณ์สีวะรา

2.11 ความเสียหายใดๆที่เกิดจากการละเมิดตามข้อ 2.10 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้อง รับผิดชอบต่อความเสียหายที่เกิดขึ้น

3. การบริหารจัดการข้อมูลองค์กร (Corporate Management)

3.1 ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลค่ายกฤษณ์สีวะรา หรือเป็นข้อมูลของบุคคลภายนอก

3.2 ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงพยาบาลค่ายกฤษณ์สีวะราถือเป็นทรัพย์สินของโรงพยาบาลค่ายกฤษณ์สีวะราห้ามไม่ให้ทำการเผยแพร่เปลี่ยนแปลงทำซ้ำหรือทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

3.3 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลค่ายกฤษณ์สีวะรา หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิดการเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

3.4 ผู้ใช้งานต้องป้องกัน ดูแลรักษาไว้ซึ่งความลับความถูกต้อง และความพร้อมใช้ของข้อมูล

3.5 ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษาใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลค่ายกฤษณ์สีวะราจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ โรงพยาบาลค่ายกฤษณ์สีวะราต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาลค่ายกฤษณ์สีวะรา ซึ่งโรงพยาบาลค่ายกฤษณ์สีวะราอาจแต่งตั้งผู้ทำหน้าที่ตรวจสอบให้ทำการตรวจสอบข้อมูล เหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

4. การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

4.1 ผู้ใช้งานต้องไม่ดำเนินการพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ดังต่อไปนี้

(1) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(2) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆซึ่งทำผู้ใช้มีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(3) พัฒนาโปรแกรมใดๆที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะ เช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(4) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายระบบหรือจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(5) นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อ ศีลธรรม ประเพณีอันดีงามของประเทศไทย

4.2 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับ เดียวกันเช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากโรงพยาบาลค่ายกฤษณ์สีวะรา

4.3 ห้ามเจ้าหน้าที่สำนักงานเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนังฟังเพลง การเล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

4.4 ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของโรงพยาบาลค่ายกฤษณ์สีวะราที่จัดเตรียมให้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคง ของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลค่ายกฤษณ์สีวะรา

4.5 ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภทรวมถึงอุปกรณ์อื่นใดของโรงพยาบาลค่ายกฤษณ์สีวะรา เพื่อการรบกวนก่อให้เกิดความเสียหายหรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและ ศีลธรรมหรือกระทบต่อภารกิจของโรงพยาบาลค่ายกฤษณ์สีวะรา

4.6 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลค่ายกฤษณ์สีวะราเพื่อประโยชน์ทางการค้า

4.7 ห้ามกระทำการใดๆเพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบ สารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะราโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆก็ตาม

4.8 ห้ามกระทำการรบกวน ทำลาย หรือให้ระบบสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะราต้อง หยุดชะงัก

4.9 ห้ามใช้ระบบสารสนเทศของโรงพยาบาลค่ายกฤษณ์สีวะราเพื่อการควบคุมคอมพิวเตอร์หรือระบบ สารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรา

4.10 ห้ามกระทำการใดๆอันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็น กรณีใดๆเพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

4.11 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆเพื่อให้สามารถเข้าถึงระบบสารสนเทศของโรงพยาบาลค่าย กฤษณ์สีวะราโดยไม่ได้รับอนุญาตจากศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรา

4.12 ห้ามติดตั้งโปรแกรมที่มีลักษณะเป็นรีโมทคอนโทรลจากระยะไกล หรือ RUN โปรแกรมรีโมท คอนโทรล โดยไม่ได้รับอนุญาตจากศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราหากประสงค์จะติดตั้งโปรแกรมดังกล่าวต้องขออนุมัติเป็นลายลักษณ์อักษรตามสายบังคับบัญชาก่อน

5. การปฏิบัติตามกฎหมาย และข้อบังคับ (Law and Compliance)

5.1 บรรดากฎหมายใดๆที่ได้ประกาศใช้ในประเทศไทยรวมทั้งประกาศและกฎระเบียบของโรงพยาบาลค่ายกฤษณ์สีวะราถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด

5.2 ผู้ใช้งานต้องไม่กระทำความผิดตามที่กฎหมายและระเบียบของโรงพยาบาลค่ายกฤษณ์สีวะราหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

6. ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

6.1 โรงพยาบาลค่ายกฤษณ์สีวะราได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่โรงพยาบาลค่ายกฤษณ์สีวะราอนุญาตให้ใช้งานหรือที่โรงพยาบาลค่ายกฤษณ์สีวะรามีลิขสิทธิ์ผู้ใช้งาน สามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และโรงพยาบาลค่ายกฤษณ์สีวะราห้ามไม่ให้ผู้ใช้งานทำการติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

6.2 ซอฟต์แวร์ (Software) ที่โรงพยาบาลค่ายกฤษณ์สีวะราได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลงแก้ไข หรือทำสำเนาเพื่อไปใช้งานที่อื่น

7. การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

7.1 คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราได้ประกาศให้ใช้

7.2 บรรดาข้อมูลไฟล์ซอฟต์แวร์หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

7.3 ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับการตรวจสอบ และปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

7.4 ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลารวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบโรงพยาบาลค่ายกฤษณ์สีวะรา

7.5 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบของโรงพยาบาลค่ายกฤษณ์สีวะรา

7.6 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆที่เป็นทรัพย์สินของโรงพยาบาลค่ายกฤษณ์สีวะราหรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

7.7 ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใดๆที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของโรงพยาบาลค่ายกฤษณ์สีวะรา

8. การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

8.1 ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

9. ความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Security)

9.1 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

9.2 ผู้ดูแลระบบ (System Administrator) ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

9.3 ผู้ดูแลระบบ (System Administrator) กำหนด WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้แสดงชื่อระบบเครือข่ายไร้สายตามที่กำหนดเท่านั้น

9.4 ผู้ดูแลระบบ (System Administrator) เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิในการเข้าใช้งานระบบ เครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

9.5 ผู้ดูแลระบบ (System Administrator) มีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สาย กับระบบเครือข่ายภายในหน่วยงาน

9.6 ผู้ดูแลระบบ (System Administrator) กำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สาย ติดต่อสื่อสารได้ เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบ

9.7 ผู้ดูแลระบบ (System Administrator) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคง ปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบ เครือข่าย ไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือนและในกรณีที่ตรวจสอบพบการใช้งานระบบ เครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ (System Administrator) รายงานต่อศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราทราบทันที

9.8 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเขาสู่ระบบอินทราเน็ต (Intranet) และฐานขอมูลภายในต่างๆของหน่วยงาน

10. ความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall security)

10.1 ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรามีหน้าที่ในการบริหารจัดการการติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมด

10.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

10.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

10.4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

10.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

10.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

10.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

10.8 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทางศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราก่อน

10.9 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้นโดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

10.10 ทำการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

10.11 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ตเว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

10.12 ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรามีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยง ต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

10.13 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับ เครื่อง

คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราก่อน

10.14 ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

11.ความมั่นคงปลอดภัยของอินเตอร์เน็ต (Internet Security)

11.1 ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือ เป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่นหรือ ข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับโรงพยาบาล

11.2 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของโรงพยาบาล หรือที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

11.3 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลด การอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

11.4 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของโรงพยาบาล

11.5 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของโรงพยาบาลการทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ หรือละเมิดกฎหมายต่างๆ

11.6 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

12. ความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)

12.1 การควบคุมการเข้าถึงระบบสารสนเทศ

(1) ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรากำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของโรงพยาบาล เพื่อดูแลรักษาความปลอดภัยโดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการ โรงพยาบาล

(2) ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

(3) ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

(4) ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า – ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

12.2 การบริหารจัดการเข้าระบบสารสนเทศ

12.2.1 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลค่ายกฤษณ์สีวะราควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งานเช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

12.2.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

12.2.3 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือ พ้นจากตำแหน่ง หรือ ยกเลิกการใช้งาน

(2) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(3) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(4) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(5) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(6) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และควรกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

12.2.4 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(5) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(6) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของโรงพยาบาล เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบขอมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

13. ความมั่นคงปลอดภัยของเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

13.1 ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรา กำหนดมาตรการควบคุมการ เข้า - ออก ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

(1) การติดตั้งประตูรหัส

(2) การบันทึกการเข้า - ออก

(3) ติดกล้องวงจรปิด

13.2 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบ เครือข่ายของโรงพยาบาลต้องได้รับอนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรา และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

13.3 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) จะต้องทำหนังสือขออนุญาตต่อหัวหน้าศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรา และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

13.4 ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหรือทำการใดๆต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัด เส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

13.5 ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการ ระบบเครือข่ายได้อย่างมีประสิทธิภาพดังตอไปนี้

(1) ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบ เครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) ต้องมีวิธีการจำกัดเส้นทางการเขาถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(3) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่อง คอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆได้

(4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกรวมทั้งควรมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(5) ระบบเครือข่ายควรติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของโรงพยาบาลในลักษณะที่ผิดปกติ

(6) การเข้าสู่ระบบเครือข่ายภายในโรงพยาบาลค่ายกฤษณ์สีวะราโดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อ ตรวจสอบความถูกต้องของผู้ใช้บริการ

(7) เลขที่อยู่ไอพี IP (Address) ภายในของระบบเครือข่ายภายในของโรงพยาบาลค่ายกฤษณ์สีวะราควรต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(8) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของ ระบบเครือข่ายภายใน และเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(9) การใช้เครื่องมือต่างๆเพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

13.6 ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆของซอฟต์แวร์ระบบ (Systems Software)

13.7 ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรากำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจร ทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังตอไปนี้

(1) ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความ ครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ยกเว้นผู้ตรวจสอบระบบสารสนเทศของโรงพยาบาล (IT Auditor) หรือบุคคลที่โรงพยาบาลมอบหมาย

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

(3) ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ และต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

13.8 ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรากำหนดมาตรการควบคุมการใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกที่ตองการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่อง คอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาลค่ายกฤษณ์สีวะรา หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานในโรงพยาบาลที่ได้ทำการฝากให้อยู่ในความดูแลของศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรา จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์โรงพยาบาล ค่ายกฤษณ์สีวะรา

(2) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(3) วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจาก หัวหน้าศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะรา

(4) การเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(5) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

14. ความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

14.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

14.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์ และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

14.3 ควรจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่นและควรมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

14.4 ควรมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินสามารถกู้ระบบกลับคืนมาได้ให้ภายในระยะเวลาที่เหมาะสม

2. นโยบายและแนวทางปฏิบัติด้านการรักษาความลับของผู้ป่วย

เพื่อให้การรักษาความลับของข้อมูลผู้ป่วยเป็นไปอย่างมีประสิทธิภาพ ครอบคลุมครบถ้วน ป้องกันการละเมิดสิทธิผู้ป่วย และความเสี่ยงต่อการฟ้องร้อง โรงพยาบาลค่ายกฤษณ์สีวะราจึงกำหนดให้ข้อมูลทั้งหมดในเวชระเบียนผู้ป่วยของโรงพยาบาลค่ายกฤษณ์สีวะราถือเป็นความลับของผู้ป่วย ซึ่งเจ้าหน้าที่ทุกคนรวมถึงบุคคลอื่นต้องปฏิบัติตามนโยบายและแนวทางปฏิบัติด้านการรักษาความลับผู้ป่วยดังนี้

1. การกำหนดผู้มีสิทธิเข้าถึงข้อมูล กำหนดให้ผู้มีสิทธิเข้าถึงข้อมูลผู้ป่วยได้ได้แก่ แพทย์ ทันตแพทย์ เภสัชกร พยาบาล นักกายภาพบำบัด นักเทคนิคการแพทย์ เจ้าหน้าที่ห้องเวชระเบียน เจ้าหน้าที่การเงิน เจ้าหน้าที่ผู้ มีหน้าที่บันทึกข้อมูลผู้ป่วยในห้องตรวจ โดยทุกคนจะมี username และ password เฉพาะตน และต้องรักษาไว้เป็นความลับห้ามมิให้ผู้อื่นนำไปใช้เจ้าหน้าที่ไม่เกี่ยวข้องจะไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้

2.การกำหนดระดับของเจ้าหน้าที่ในการเข้าถึงข้อมูล กำหนดให้เจ้าหน้าที่ที่มีสิทธิเข้าถึงข้อมูลสามารถเข้าถึงข้อมูลได้เฉพาะที่เกี่ยวกับการปฏิบัติงานของตนเท่านั้น เช่น เจ้าหน้าที่ห้องเวชระเบียนดูข้อมูลหน้าประวัติผู้ป่วยหน้าส่งต่อผู้ป่วยไปแผนกอื่น แพทย์ ทันตแพทย์ เภสัชกร พยาบาล นักกายภาพบำบัด นักเทคนิคการแพทย์ ดูได้ตั้งแต่การซักประวัติจนกระทั่งผู้ป่วยจำหน่าย การดูผลการตรวจ Anti-HIV, HBsAg, Acid phosphatase, urine amphetamine ให้สิทธิ์เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น

3. การเข้าถึงแฟ้มเวชระเบียนผู้ป่วย

3.1 แฟ้มเวชระเบียนผู้ป่วยต้องจัดเก็บที่ห้องเวชระเบียนซึ่งเป็นสถานที่เฉพาะและเป็นสัดส่วนจำกัดการเข้าถึง และให้สิทธิเฉพาะเจ้าหน้าที่งานเวชระเบียนในการค้นและจัดเก็บแฟ้มเวชระเบียนเท่านั้นและห้ามบุคคลภายนอกเข้าไปโดยไม่ได้รับอนุญาต

3.2 ในช่วงนอกเวลาราชการและวันหยุดราชการจะปิดประตูเวชระเบียนทุกด้านให้มีการเข้าออกทางเดียวเพื่อป้องกันการสูญหายของเวชระเบียน

3.3 จัดให้มีการจัดเวรอยู่ปฏิบัติงานตลอด 24 ชั่วโมง โดยจัดเจ้าหน้าที่ห้องเวชระเบียน หรือเจ้าหน้าที่อื่นที่ได้รับอนุญาตให้อยู่เวรห้องเวชระเบียนให้เพียงพอต่อการให้บริการแก่ผู้รับบริการ

3.4 การขอยืมข้อมูลประวัติในแฟ้มเวชระเบียนปฏิบัติตามแนวทางให้การยืม-คืนเวชระเบียน

4. การรักษาความลับของข้อมูลที่เก็บไว้ด้วยคอมพิวเตอร์

4.1 การดูข้อมูลในระบบให้เจ้าหน้าที่ใช้ username และ password เฉพาะของตนเองเท่านั้น

4.2 เมื่อใช้งานเสร็จแล้วต้องปิดหน้าจอ และออกจากระบบทันทีเพื่อป้องกันมิให้ผู้อื่นมาดู

4.3 ไม่อนุญาตให้เจ้าหน้าที่อื่น หรือบุคคลอื่นมาใช้ username และ password ของตนในการเข้าดูข้อมูลผู้ป่วย

5. การเปิดเผยข้อมูลผู้ป่วย

5.1 กำหนดให้ผู้อำนวยการโรงพยาบาล ประธานองค์กรแพทย์และแพทย์ผู้รักษา เป็นผู้เปิดเผยข้อมูลผู้ป่วยได้

5.2 การเปิดเผยข้อมูลการติดเชื้อ HIV ต้องได้รับความยินยอมจากตัวผู้ป่วยที่ติดเชื้อ HIV ด้วย

5.3 เมื่อต้องนำข้อมูลผู้ป่วยไปใช้ในการสอนหรือใช้ประกอบในการเขียนรายงานต่างๆให้เก็บเอกสารหรือรายงานเกี่ยวกับข้อมูลของผู้ป่วยไว้เป็นความลับเสมอ

5.4 ห้ามใส่ ชื่อ-นามสกุลผู้ป่วยในการเขียนรายงานผู้ป่วยเพื่อตีพิมพ์โดยทั่วไป

5.5 หลีกเลี่ยงการตีพิมพ์ หรือแสดงรูปผู้ป่วยที่เห็นใบหน้าชัดเจน ถ้าจำเป็นต้องมีรูปถ่ายผู้ป่วยให้ปิดส่วนหนึ่งของใบหน้าเพื่อให้ระบุตัวตนไม่ได้ ตามความเหมาะสม

5.6 การนำผู้ป่วยไปแสดงหรือปรากฏตัวต่อสาธารณชนเพื่อเป็นตัวอย่างในการให้ความรู้แก่ประชาชนต้องได้รับความยินยอมจากผู้ป่วยก่อนการนำเรื่องราวของผู้ป่วยไปเปิดเผยต่อสาธารณชน

5.7 ถ้าไม่จำเป็นควรหลีกเลี่ยงการนำเรื่องผู้ป่วยเข้าประชุมปรึกษาหารือกับกลุ่มบุคคลอื่นที่อยู่นอกวิชาชีพทางการแพทย์และไม่ควรเปิดเผยชื่อ-นามสกุลผู้ป่วย

5.8 ไม่อนุญาตให้เจ้าหน้าที่เวชระเบียนหรือผู้ไม่เกี่ยวข้องให้ข้อมูลทางโทรศัพท์โดยเด็ดขาด

5.9 กรณีเป็นบุคลากรที่มีหน้าที่ในการให้ข้อมูลหรือตอบคำถามเกี่ยวกับผู้ป่วย เช่น เจ้าหน้าที่ประชาสัมพันธ์ ควรจะต้องระมัดระวัง และตรวจสอบผู้ที่ถามนั้นว่า เกี่ยวข้องกับผู้ป่วยอย่างไรควรให้ข้อมูลตามความจำเป็นและตามขอบเขตที่ได้รับอนุญาตให้เปิดข้อมูลผู้ป่วยได้

3. นโยบายและแนวทางปฏิบัติด้านการกำกับดูแล ติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศ

เพื่อให้การกำกับดูแลและติดตามงานด้านเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม ได้ข้อมูลสารสนเทศที่ถูกต้อง ปลอดภัย ครบถ้วน รวดเร็ว ต่อเนื่อง และทันเวลา โรงพยาบาลค่ายกฤษณ์สีวะราจึงกำหนดแนวทางปฏิบัติ และผู้รับผิดชอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ดังนี้

1. การกำกับดูแลและติดงานด้านข้อมูลสารสนเทศและตัวชี้วัด

1.1 กำหนดให้คณะกรรมการสารสนเทศโรงพยาบาลค่ายกฤษณ์สีวะรา เป็นผู้ติดตามข้อมูลสารสนเทศและตัวชี้วัดที่เป็นข้อมูลกลางในระดับโรงพยาบาล เช่น อัตราครองเตียง อัตราการเสียชีวิต การรับส่งต่อ ผู้ป่วย(เข้า-ออก)

1.2 ให้คณะกรรมการระบบงานสำคัญอื่นๆติดตามข้อมูลสารสนเทศและตัวชี้วัดในส่วนที่เกี่ยวข้อง คณะกรรมการควบคุมการติดเชื้อในโรงพยาบาล ติดตามตัวชี้วัดอัตราการเกิดแผลผ่าตัดติดเชื้อ เป็นต้น

1.3 ศูนย์พัฒนาคุณภาพโรงพยาบาล (QIC), คณะกรรมการสารสนเทศ (IM) โรงพยาบาลค่ายกฤษณ์สีวะราติดตามรวบรวมข้อมูลสารสนเทศและตัวชี้วัดที่มีการเปรียบเทียบกับหน่วยงานภายนอก เช่น THIPII, AMEDstat เป็นต้น

2. การกำกับดูแลและติดตามงานด้านเทคโนโลยีสารสนเทศ

2.1 กำหนดให้ศูนย์คอมพิวเตอร์โรงพยาบาลค่ายกฤษณ์สีวะราเป็นผู้กำกับดูแลระบบอุปกรณ์ด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้ ปลอดภัย และทันสมัยอยู่เสมอ

2.2 ต้องมีระบบการสำรองข้อมูล (Backup) อัตโนมัติเป็นประจำทุกวัน

2.3 จัดหาอุปกรณ์ Hardware และ Software ที่มีประสิทธิภาพเพื่อการใช้งานได้อย่างรวดเร็ว ปลอดภัย ทันเวลาอยู่เสมอ

2.4 จัดให้มีระบบป้องกันและรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ เพื่อป้องกันภัยคุกคาม ในรูปแบบต่างๆ

4. แนวทางปฏิบัติด้านความครบถ้วนถูกต้องของข้อมูล

เพื่อให้ข้อมูลสารสนเทศมีความพร้อมใช้และเชื่อถือได้ จึงกำหนดนโยบายด้านความครบถ้วน ถูกต้อง แม่นยำ คงสภาพ และเป็นปัจจุบันของข้อมูลไว้ดังต่อไปนี้

1. **มีความถูกต้องแม่นยำ (accuracy)** ข้อมูลสารสนเทศต้องตรงกับความเป็นจริงและเชื่อถือได้ รวมถึงต้องมีความแม่นยำถูกต้องในการป้อนข้อมูลเข้าโปรแกรม และมีโปรแกรมประมวลผลที่ถูกต้องมีประสิทธิภาพ

2. **มีความสมบูรณ์ครบถ้วน (complete)** ข้อมูลสารสนเทศต้องมีความครบถ้วนซึ่งเกิดจากการเก็บข้อมูลได้ครบถ้วนและครอบคลุมทุกเรื่องและหัวข้อที่มีความเกี่ยวข้องสัมพันธ์กันเช่นข้อมูลผู้ป่วย (patient profile) จะต้องมีการเก็บรายละเอียดเกี่ยวกับผู้ป่วยให้ได้มากที่สุด เช่น ชื่อเพศ ที่อยู่อายุผู้ติดต่อชื่อ หมายเลขโทรศัพท์ โรคประจำตัวทั้งนี้เพื่อให้สามารถนำข้อมูลสารสนเทศไปใช้ประโยชน์ในการดูแล ผู้ป่วยได้อย่างถูกต้องรวดเร็ว ทันเวลา

3. **มีความสอดคล้องกับความต้องการของผู้ใช้ (relevancy)** ข้อมูลสารสนเทศจะต้องสอดคล้องกับความ ต้องการของผู้ใช้กล่าวคือการเก็บข้อมูลต้องมีการสอบถามการใช้งานและความต้องการของผู้ใช้ว่า ต้องการใช้งาน ในเรื่องใดจึงจะสามารถสรุปสารสนเทศได้ถูกต้องตรงกับความต้องการของผู้ใช้มากที่สุด

4. **ทันต่อเวลา (timeliness)** ข้อมูลสารสนเทศที่มีความครบถ้วนถูกต้องจะต้องทันต่อการใช้งานด้วย หมายถึง ข้อมูลที่ป้อนเข้าโปรแกรมคอมพิวเตอร์ต้องมีความเป็นปัจจุบันทันสมัยอยู่ตลอดเวลา เพื่อการนำไปใช้ประโยชน์ได้จริง

5. **สามารถพิสูจน์ได้ (verifiable)** ข้อมูลสารสนเทศจะต้องสามารถตรวจสอบแหล่งที่มาได้โดยง่ายมีความ ชัดเจน มีแหล่งที่มาของข้อมูลเป็นรูปธรรม สามารถอ้างอิงได้ตลอดเวลาทั้งนี้เพื่อให้ผู้ใช้มีความมั่นใจในการนำข้อมูล สารสนเทศไปใช้ประโยชน์ได้อย่างเต็มประสิทธิภาพ

****

ประวัติการแก้ไข/ทบทวนเอกสาร

ชื่อเอกสาร : แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
โรงพยาบาลค่ายกฤษณ์สีวะรา

วัน/เดือน/ ปี	ฉบับแก้ไข ครั้งที่	รายละเอียด	ลงชื่อ
1 ต.ค. 66	0	ฉบับแรก	ร.ท.ศาสตร์ศิลป์
1 ต.ค. 67	1	เพิ่มเติมนโยบายและแนวทางปฏิบัติอีก 3 เรื่อง ประกอบด้วย - ด้านการรักษาความลับของผู้ป่วย - ด้านการกำกับดูแล ติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศ - ด้านความครบถ้วนถูกต้องของข้อมูล	ร.ท.ศาสตร์ศิลป์