โรงพยาบาลทุ่งเขาหลวง อำเภอทุ่งเขาหลวง จังหวัดร้อยเอ็ด

นโยบายคุณภาพ เลขที่ QM-IM-001-01

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

	ชื่อ-สกุล	ลายเซ็น	วัน เดือน ปี
จัดทำโดย	1.นายธงไชย พ้องเสียง		
ทบทวนโดย	1.นายบูชา บัวภา		
	2.นางปทุมทอง พงศ์ศาสตร์		
	3.นายชัชชัย วันทอง		
	4.นายกฤษณะพล สุระ		
ตรวจสอบโดย	นายบูชา บัวภา		
อนุมัติโดย	นายชาญชัย วันทอง		

ประวัติการแก้ไข **จำนวนหน้า ..... หน้า**

ครั้งที่	วันที่ประกาศใช้	รายละเอียด	แผ่นที่

โรงพยาบาลทุ่งเขาหลวง	**หน้าที่ 1/27** **วันที่อนุมัติใช้ .....** **รหัสเอกสาร QM-IM-001-01**
เรื่อง: แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลทุ่งเขาหลวง	**ผู้จัดทำ : นายธงไชย พ้องเสียง**
ระดับเอกสาร : นโยบายคุณภาพ	**ผู้ตรวจสอบ : หัวหน้ากลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์**
หน่วยงานที่เกี่ยวข้อง : งานสารสนเทศทางการแพทย์	**ผู้อนุมัติ : ผู้อำนวยการโรงพยาบาลทุ่งเขาหลวง**

1. วัตถุประสงค์

1.1 เพื่อให้มีนโยบายและแนวทางปฏิบัติการรักษาความมั่งคงปลอดภัยทางด้านสารสนเทศ โรงพยาบาลทุ่งเขาหลวง

1.2 เพื่อเป็นกรอบและแนวทางปฏิบัติในการกำหนดมาตรฐาน ขั้นตอนปฏิบัติ รวมถึงสิ่งอำนวยความสะดวกด้านคอมพิวเตอร์สำหรับการติดตั้งและการใช้ระบบงานเพื่อรักษาความมั่นคงปลอดภัยทางด้านระบบสารสนเทศ

1.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและ บุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.4 มุ่งกำหนดแนวปฏิบัติแนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิด หรือ ฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและ ตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

1.5 เผยแพร่ความรู้ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงาน เองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

1.6 ติดตามตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

2. ขอบเขต

นโยบายจัดทำขึ้นโดยอาศัยกรอบตามมาตรฐานสากลด้านความปลอดภัยระบบสารสนเทศ อ้างอิงตามมาตรฐาน ISO/IEC 27001 รวมทั้งข้อกำหนดตามกฎหมายและระเบียบปฏิบัติกับความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อเป็นกรอบและแนวปฏิบัติด้านสารสนเทศของโรงพยาบาลทุ่งเขาหลวงจากภาวะคุกคามทุกประเภทที่อาจเกิดขึ้นทั้งภายในและภายนอกโรงพยาบาล โดยเจตนาหรือรู้เท่าไม่ถึงการณ์ ซึ่งเป็นแนวนโยบายในภาพรวมเพื่อการตัดการด้านบริหารความมั่นคงปลอดภัยของสารสนเทศโดยแบ่งสาระออกเป็น 7 หมวด ประกอบด้วย

1. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
2. การรักษาความมั่นคงปลอดภัยของการควบคุมการใช้งานระบบสารสนเทศ
3. การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
4. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
5. การรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต
6. ความมั่นคงปลอดภัยของการสำรองข้อมูล
7. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
8. นโยบายการใช้สื่อสังคมออนไลน์ในโรงพยาบาล

3. ผู้รับผิดชอบ

3.1 บุคลากรโรงพยาบาลทุ่งเขาหลวง

3.2 บุคลากรภายนอกที่ใช้ระบบสารสนเทศโรงพยาบาลทุ่งเขาหลวง

4. นิยามศัพท์

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลทุ่งเขาหลวง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หมายถึง ผู้มีอำนาจใน ด้านเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งเขาหลวงซึ่งมีบทบาทหน้าที่และความ

รับผิดชอบใน ส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ศูนย์สารสนเทศ หมายถึง ศูนย์สารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลทุ่งเขาหลวง

ผู้อำนวยการศูนย์สารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศ และมีอำนาจตัดสินใจเกี่ยวกับระบบ สารสนเทศภายในโรงพยาบาลทุ่งเขาหลวง

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศของโรงพยาบาลทุ่งเขาหลวง

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตาม วัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร **ผู้รับบริการ** หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแล รักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับ

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลทุ่งเขาหลวง เช่น ผู้อำนวยการโรงพยาบาล รองผู้อำนวยการ เป็นต้น

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลทุ่งเขาหลวงอนุญาต ให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้ สามารถ เข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่ง ข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการ ติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของ หน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้าง สารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้ บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบ เครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

1. พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
2. พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
3. พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
4. พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
5. พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์

และทาง กายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

คามมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความ ถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึง คุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้าม ปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิด เหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบาย ด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจ เกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคง ปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน เครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพ กราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของ ข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือ ชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ ตรงตามคำสั่งที่กำหนดไว

วิธีปฏิบัติ

นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environment Security)

วัตถุประสงค์

1. เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตาม ความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สนที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายในองค์กร ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวทางปฏิบัติ

2. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

2.1 ให้ศูนย์สารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บ อุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

2.2 ให้ศูนย์สารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.3 ให้ศูนย์สารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบ เครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่อง คอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

นโยบายการรักษาความมั่นคงปลอดภัยของการรควบคุมการใช้งานระบบสารสนเทศ

(Access Control Policy)

วัตถุประสงค์

1. เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และ ป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่าย ของหน่วยงานได้อย่างถูกต้อง
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์และการมอบอำนาจของหน่วยงานของรัฐ
3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

ในการควบคุมการเข้าถึงระบบ แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งเขาหลวง มีดังนี้

ส่วนที่ 1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

1.1 โรงพยาบาลทุ่งเขาหลวง กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบ เทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร ต่อผู้อำนวยการศูนย์สารสนเทศ

1.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

1.3 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบ เทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความ ปลอดภัย ที่มีต่อระบบข้อมูล

1.4 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

1.5 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

1.5.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

ส่วนที่ 2 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

2.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ โรงพยาบาลทุ่งเขาหลวง กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

2.2 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ อินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานใน หน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2.3 ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของ บุคลากรดังต่อไปนี้

2.3.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

2.3.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

2.3.3 ให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน การกำหนดรหัสผ่านใหม่เอง

2.3.4 ให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

2.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้ รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับ การใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2.3.7 ผู้ดูแลระบบจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

3.1 การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

3.1.1 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้น ความลับของข้อมูล ดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

3.1.2 กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

3.1.3 ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของ ระดับความสำคัญของข้อมูล ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

3.1.4 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่าย คอมพิวเตอร์

3.2 การควบคุมการเข้าถึงระบบปฏิบัติการ

3.2.1 ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน ระบบโปรแกรมบันทึกข้อมูลสารสนเทศ

3.2.2 กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

3.2.3 ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

3.2.4 ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.2.5 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

3.2.6 ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของ หน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้า หน่วยงาน

3.2.7 ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลทุ่งเขาหลวง และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

3.2.8 ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

3.2.9 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

3.2.10 ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของ โรงพยาบาลทุ่งเขาหลวง

3.2.11 ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการ โจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกระทรวงสาธารณสุข

3.2.12 ห้ามใช้สินทรัพย์ของโรงพยาบาลทุ่งเขาหลวง เพื่อประโยชน์ทางการค้า

3.2.13 ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

3.2.14 ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายระบบสารสนเทศของโรงพยาบาลทุ่งเขาหลวง โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

3.2.15 ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

3.2.16 ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลทุ่งเขาหลวงโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

วัตถุประสงค์

1. เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์ และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและ ข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

2. ในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย โรงพยาบาลทุ่งเขาหลวงกำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่อง คอมพิวเตอร์แม่ข่าย (Server) ดังนี้

2.1 ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุม ป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการศูนย์สารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

2.3 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับ ระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

2.4 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้ อย่างมีประสิทธิภาพ ดังต่อไปนี้

2.4.1 ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งาน เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการ เข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

2.4.2 ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

2.4.3 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกรวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

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

2.4.5 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

2.4.6 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

2.4.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.4.8 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.4.9 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และ รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

2.5 โรงพยาบาลทุ่งเขาหลวง กำหนดมาตรการควบคุมการใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทางดังต่อไปนี้

2.5.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการศูนย์สารสนเทศ

2.5.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

2.5.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการศูนย์สารสนเทศ

2.5.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

2.5.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

(Wireless Policy)

วัตถุประสงค์

1. เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการ กำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวทางปฏิบัติ

2. ในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของโรงพยาบาลทุ่งเขาหลวง มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

2.1 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจาก ผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

2.2 ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

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

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

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

2.6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

2.7 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบ และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการศูนย์สารสนเทศทราบทันที

นโยบายการรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต

(Internet Security Policy)

วัตถุประสงค์

1. เพื่อกำหนดมาตรการการใช้งานอินเตอร์เน็ตของโรงพยาบาลทุ่งเขาหลวง ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเตอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวทางปฏิบัติ

2. ในการใช้เครือข่ายอินเตอร์เน็ต ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของโรงพยาบาลทุ่งเขาหลวงมีหน้าที่และความรับผิดชอบที่ ต้องปฏิบัติดังนี้

2.1 การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการ เครือข่ายอินเตอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์สารสนเทศโรงพยาบาลทุ่งเขาหลวง โดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลทุ่งเขาหลวง สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศ หรือผู้ที่ได้รับมอบหมาย

2.2 ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคลและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่ มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

2.3 ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเองทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

2.4 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

2.5 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

2.6 ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการ อัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ไม่ดาวน์โหลดไฟล์ ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

2.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้ เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของ หน่วยงานอื่นๆ

2.8 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจากเครือข่ายอินเตอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกัน การเข้าใช้งานโดยบุคคลอื่นๆ

นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล

(Backup Policy)

วัตถุประสงค์

1. เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

แนวทางปฏิบัติ

2. แนวทางปฏิบัติในการสำรองข้อมูล

2.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

2.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

2.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

แนวทางปฏิบัติ

2. เพื่อสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.1 จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

2.2 จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

2.3 ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

2.4 ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจ ความต้องการของผู้ใช้บริการ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการสารสนเทศโรงพยาบาลทุ่งเขาหลวง ซึ่งมีหน้าที่ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลทุ่งเขาหลวง เพื่อใช้เป็นแนวทางในการดำเนินงาน

ด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ขอให้เจ้าหน้าที่ที่เกี่ยวข้องทราบและถือปฏิบัติ อย่างเคร่งครัดต่อไป

นโยบายการใช้สื่อสังคมออนไลน์ในโรงพยาบาล

(Social Media Policy)

1. วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแล การเผยแพร่ข้อมูล และการเข้าถึงเครือข่ายสังคมออนไลน์ ของโรงพยาบาลทุ่งเขาหลวง หรือต่อไปนี้เรียกว่า “องค์กร” รวมถึงบริการอิเล็กทรอนิกส์ ตลอดจนการแสดงความคิดเห็นของบุคลากรในองค์กร ผ่านสื่อสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม มีความเป็นระเบียบเรียบร้อยและเกิดประโยชนสูงสุด ดังนั้น เพื่อให้ผู้ปฏิบัติงานในองค์กรทุกท่าน สามารถใช้สื่อสังคมออนไลน์ได้อย่างมีประสิทธิภาพ จึงเห็นสมควรกำหนดนโยบาย และแนวปฏิบัติการใช้สื่อสังคมออนไลน์ โดยมีวัตถุประสงค์ ดังนี้

1.1 เพื่อให้มีการกำหนดขอบเขตของการใช้สื่อสังคมออนไลน์ทั้งในระดับตัวบุคลและองค์กร

1.2 เพื่อสร้างภาพลักษณ์ของบุคลากรและการดำเนินงานขององค์กร

1.3 เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาอันอาจจะเกิดขึ้นจากการใช้สื่อสังคมออนไลน์

1.4 เพื่อป้องกันการเปิดเผยข้อมูลความลับในทุกระดับทั้งองค์กร

1.5 เพื่อให้บุคลากรที่ปฏิบัติงานใช้สื่อสังคมออนไลน์ได้อย่างเหมาะสม

1.6 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้บุคลากรในองค์กรตระหนักถึงความสำคัญของ การรักษาความมั่นคงปลอดภัย ในการใช้ประโยชน์จากสื่อสังคมออนไลน์ และปฏิบัติตามอย่างเคร่งครัด

2. ขอบเขตนโยบาย

ภายใต้นโยบายนี้ การเข้าถึงสื่อสังคมออนไลน์ และการเผยแพร่ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง หรือข้อมูลใดๆ หรือแสดงความคิดเห็นส่วนตัวผ่านสื่อสังคมออนไลน์ มีผลบังคับเหมือนกับการเผยแพร่ข้อมูลหรือแสดงความคิดเห็นผ่านช่องทางอื่นๆ โดยการใช้งานสื่อสังคมออนไลน์ทุกประเภทจะต้องปฏิบัติ และสอดคล้องตามนโยบายขององค์กรอย่างเคร่งครัด

1. หลักการและแนวปฏิบัติทั่วไป

1.1 องค์กรอนุญาตให้ใช้ระบบเครือข่าย สำหรับสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบบณองค์กร

1.2 เคารบกฎหมาย จริยธรรมแห่งวิชาชีพกฎระเบียบองค์กรในการใช้สื่อออนไลน์

1.3 หน่วยงานภายในองค์กร บุคลากร สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ ประชาสัมพันธ์ในการติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ชัดเจนว่า ข้อความใดเป็น “ข่าวประชาสัมพันธ์” ข้อความใดเป็น “ความคิดเห็น” หรืออื่นๆ และความคิดเห็นดังกล่าวควรคำนึงถึงสาธารณะด้วย

1.4 พึงระมัดระวังการใช้ถ้อยคำ ภาษาที่ใช้อาจดูหมิ่น หรือหมิ่นประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์

1.5 พึงงดเว้นการโต้ตอบด้วยความรุนแรง กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง การละเว้นการโต้ตอบจะทำให้ความขัดแย้ง ไม่บานปลายจนหาที่สิ้นสุดไม่ได้

1.6 พึงงดเว้นการใช้สื่อสังคมวิพากษ์ วิจารณ์ ตลอดจนแสดงความเห็นในเรื่องที่เป็นข้อมูลภายในองค์กร หรืออาจส่งผลกระทบต่อองค์กรได้

1.7 พึงระมัดระวังข้อความที่ส่งผลกระทบต่อผู้ป่วย หรือละเมิดสิทธิมนุษยชน

1.8 รักษาความเป็นวิชาชีพ มีพฤติกรรมออนไลน์เหมาะสม แยกเรื่องส่วนตัวกับวิชาชีพ กำหนดขอบเขตการเป็นวิชาชีพกับผู้ป่วยและผู้อื่นอย่างเหมาะสม

2. หลักการส่งต่อข้อมูล

2.1 ควรส่งข้อมูลข่าวสารเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่กรงาน สถานะชัดเจนเท่านั้น

2.2 ละเว้นการส่งข้อมูลที่เป็นข่าวลือ ข่าวไม่ทราบปรากฏที่มา หรือเป็นเพียงการคาดเดา

2.3 ละเว้นการส่งต่อข้อมูลหรือข้อความเกี่ยวกับองค์กรทุกกรณี ยกเว้นข้อมูลนั้นๆที่เผยแพร่ต่อสาธารณะแล้ว

2.4 พึงระลึกเสมอว่า การส่งต่อข้อความที่เป็นเท็จ หรือข้อความที่เจ้าของประสงค์กระจายข่าวสร้างความสับสนวุ่นวายในบ้านเมือง เท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น

2.5 การส่งต่อข้อความเชิญชวนไปร่วมชุมนุมหือกิจกรรมทางสังคมใดๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

2.6 ไม่ควรปรึกษาการดูแลผู้ป่วยทางไลน์ ได้แก่ ภาพถ่าย x-ray ด้วยกล้องที่มีความละเอียดต่ำซึ่งอาจนำมาสู่การวินิจฉัยที่ผิดพลาด

2.7 ใช้ไลน์ลักษณะบุคคลต่อบุคคล หลีกเลี่ยงการใช้ไลน์กลุ่ม โดยกำหนดผู้ส่งข้อมูลคือผู้ตรวจการเวร พยาบาลเป็นผู้ส่งต่อข้อมูลให้กับแพทย์ผู้อยู่เวร หรือผู้ที่ได้รับมอบหมาย เพื่อป้องกันการรั่วไหลของข้อมูล

2.8 หลีกเลี่ยงการขอคำปรึกษาผู้ป่วยพร้อมกันมากกว่า 1 ราย ในการปรึกษา 1 ครั้ง เพราะอาจมีการสลับข้อมูลของบุคคลได้

2.9 ผู้ที่ให้คำปรึกษาต้องรักษาความลับของผู้ป่วย และทำลายข้อมูลที่ได้รับ เมื่อกระบวนการให้คำปรึกษานั้นเสร็จ เพื่อป้องกันการรั่วไหลของข้อมูล

3. หลักความรับผิดชอบ

3.1 ควรแสดงความรับผิดชอบ ด้วยการขอโทษหรือแสดงความเสียใจทันที เมื่อรู้ว่ามีการเผยแพร่ข้อมูลที่ผิดพลาดหรือกระทบต่อบุคคลอื่น และอาจได้รับความผิดตามกฎหมาย พรบ. คุ้มครองข้อมูลส่วนบุคคล PDPA อีกด้วย

3.2 หากพบข้อมูลใดๆที่ไม่เหมาะสมความดำเนินการอย่างรวดเร็ว โดยลบข้อมูลดังกล่าวออกทันทีเพื่อลดโอกาศที่จะขัดแย้งทางกฎหมาย และส่งผลกระทบด้านลบต่อองค์กร

4. การไม่เปิดเผยข้อมูลที่เป็นความลับ

4.1 ต้องไม่เปิดเผยส่งต่อข้อมูล ชื่อ-นามสกุล เลขประจำตัวผู้ป่วย ข้อมูลการเจ็บป่วย รูปภาพ การตรวจต่างๆ รวมถึงคลิปวีดีโอการรักษาของผู้ป่วยผ่านสื่อสังคมออนไลน์ เช่น โปรแกรม Line, Facebook

4.2 ระมัดระวังในการให้คำปรึกษาออนไลน์ บันทึกการสื่อสารออนไลน์ที่เกี่ยวข้อง

5. ความน่าเชื่อถือของข้อมูล

ไม่ควรโพสต์ข้อความที่เป็นเท็จหรือก่อนให้เกิดความเข้าใจผิด และระบุของที่มาข้อมูลนั้นอย่างชัดเจน การโพสต์ข้อความใดๆ ควรพิจารณาข้อความอย่างรอบครอบและระมัดระวัง โดยเฉพาะการเปิดเผยข้อมูลส่วนบุคคล

6. การคำนึงถึงผลการะทบต่อการปฏิบัติงาน

การใช้สื่อสังคมออนไลน์ต้องไม่รบกวนการปฏิบัติงาน หรือหน้าที่รับผิดชอบที่ได้รับมอบหมาย

7. คำนึงถึงผู้เข้าชมและผู้เกี่ยวข้อง

บุคลากรขององค์กรไม่ควรโพสต์ข้อมูลใดๆ ที่ขัดแย้งต่อข้อกำหนดขององค์กร รวมถึงละเว้นการแสดงออกถึงความคิดเห็นที่ก้าวร้าว หมิ่นประมาท ดูถูกเป็นการส่วนตัวลามกอนาจาร และอื่นๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม เช่นการเมือง ศาสนา เป็นต้น