ประกาศ โรงพยาบาลคำม่วง
เรื่อง นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ โรงพยาบาลคำม่วง จังหวัดกาฬสินธุ์

.....

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลคำม่วง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคาม จากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลคำม่วง และหน่วยงานภายใต้สังกัดและเป็นความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ โรงพยาบาลคำม่วง จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น

ข้อ ๑. นโยบายนี้เรียกว่า “นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ โรงพยาบาลคำม่วง จังหวัดกาฬสินธุ์”

ข้อ ๒. นโยบายนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้วซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ ของโรงพยาบาลคำม่วง มีวัตถุประสงค์ ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของโรงพยาบาลคำม่วง ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดโรงพยาบาลคำม่วง และผู้ที่เกี่ยวข้องทั้งหมด ได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติตามนโยบายและแนวปฏิบัติ อย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งานผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาล ตระหนักถึงความสำคัญ ของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของโรงพยาบาลคำม่วง ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลคำม่วง กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนด สิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่ กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการ การเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบ สารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบ บัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการ ลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบ สารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การ ใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และ ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้ รหัสผ่าน ก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่โรงพยาบาลคำม่วง จัดสรรไว้ และมีการออกแบบระบบเครือข่าย โดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่างๆ รวมถึงจดหมาย อิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่างๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงาน รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่

และความรับผิดชอบของเจ้าหน้าที่ ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ข้อ ๖. กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๗. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศของโรงพยาบาลคำม่วง พ.ศ. ๒๕๖๕ ตามที่แนบท้ายประกาศนี้

ทั้งนี้ให้ทุกคนถือปฏิบัติตามนโยบายดังกล่าวตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๘ มกราคม ๒๕๖๗

(นายธนธร กานตอาภา)
นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลคำม่วง

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ
โรงพยาบาลคำม่วง จังหวัดกาฬสินธุ์ พ.ศ. 2567

หมวดที่ 1 ระบบความมั่นคงปลอดภัยของระบบสารสนเทศ ทางกายภาพ และสิ่งแวดล้อม

1.1 จัดทำบัญชีเครื่องคอมพิวเตอร์ วัสดุอุปกรณ์ของระบบสารสนเทศ โดยมีการบริหารจัดการอย่างชัดเจน มีระบบการเบิกจ่ายวัสดุอย่างมีประสิทธิภาพ

1.2 กำหนดให้ห้อง Server เป็นบริเวณที่ตองรักษาความปลอดภัย และจัดให้มีการควบคุมการเขา-ออก เฉพาะผู้ได้รับอนุญาต

1.3 ดูแลอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ที่ใช้งาน เช่นสายไฟ สายสื่อสารและสายสัญญาณต้องได้รับการป้องกันการเข้าถึงโดยไม้ได้รับอนุญาต เพื่อลดความเสี่ยงของการเสียหายต่อสายสัญญาณ หรืออุปกรณ์ระบบเครือข่าย

1.4 ตรวจสอบความเหมาะสมของข้อมูลที่เผยแพร่ออกสู่สาธารณะ ต้องไมขัดต่อกฎหมายที่เกี่ยวข้องและมีกลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไมไดรับอนุญาต

1.5 จัดระบบสำรองข้อมูลเพิ่มเติมจากระบบที่มีอยู่ด้วยการ Backupข้อมูลลง External HDD และแยกเก็บไว้ เพื่อความปลอดภัยกรณีมีปัญหาที่ห้อง Server

หมวดที่ 2 ระบบความมั่นคงปลอดภัยของระบบสารสนเทศด้านการใช้งาน

2.1 จัดระบบการป้องกันภัยคุกคามจาก ไวรัส เวิร์ม โทรจัน สปายแวร์ รวมทั้งอันตรายที่เกิดขึ้นจากโปรแกรมที่ไมประสงค์ดี .อย่างเหมาะสม

2.2 ติดตั้งระบบ Restore ที่เครื่องลูกข่าย ในระบบ HOSxP

2.3 ติดตั้งโปรแกรม anti-virus ที่เครื่องคอมพิวเตอร์ทุกเครื่อง ของโรงพยาบาล

2.4 ติดตั้งระบบกระจายสัญญาณ Wireless ให้ครอบคลุมพื้นที่โรงพยาบาลเพื่อลดการเชื่อมต่อระบบด้วยสายสัญญาณ ซึ่งเป็นช่องทางที่ไวรัสระบาดโดยง่าย

2.5 การติดตั้งโปรแกรมเพิ่มเติมในทุกเครื่องต้องทำโดยทีมผู้ดูแลระบบเท่านั้น

2.6 ผู้ใช้งานระบบเครือข่าย มีหน้าที่รับผิดชอบดังนี้

2.6.1 ผู้ใช้งานในระบบอินเตอร์เน็ตและ HOSxP ทุกคนจะมี username และ password ประจำตัว

2.6.2 ผู้ใช้งานในระบบอินเตอร์เน็ตและ HOSxP ต้องรับผิดชอบในการจัดเก็บและรักษารหัสผ่านของตนเอง ให้เป็นความลับและเปลี่ยนรหัสผ่านของตนเองทันที หลังจากได้รับรหัสผ่านจากผู้ดูแลระบบ

2.6.3 ห้าม ผู้ใช้งานนำเอา ฮาร์ดแวร์หรือ ซอฟต์แวร์มาติดตั้ง เปลี่ยนแปลง ทำซ้ำหรือต่อเติม โดยไม่ไดรับอนุญาต

2.6.4 ห้ามใช้งานระบบเครือข่ายคอมพิวเตอร์ เพื่อกระทำสิ่งที่ผิดกฎหมาย

2.6.5 รับผิดชอบ หมั่นตรวจตราเครื่องคอมพิวเตอร์ของตนเองด้วย โปรแกรม Anti-virus เพื่อให้มั่นใจว่าปลอดภัยจากโปรแกรมที่ไมประสงค์ดี หรือ ไวรัส เวิร์ม โทรจัน สปายแวร์

2.6.6 ห้ามใชชื่อและรหัสผานของผูใชงานคนอื่น

2.6.7 ห้ามเผยแพร่ข้อมูล หรือสารสนเทศที่เป็นเท็จ หรือดำเนินการใดๆ ที่จะส่งผลให้เกิดความเสียหาย แก่ผู้อื่นหรือโรงพยาบาล

2.6.8 ห้ามเผยแพร่ หรือจัดเก็บขอมูลที่มีลักษณะลามก อนาจาร และขัดตอศีลธรรมอันดี และห้ามเผยแพร่ข้อมูลภาพตัดต่อเติม หรือดัดแปลงภาพของบุคคลอื่น ด้วยวิธีการใดๆ ซึ่งจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือไดรับความอับอาย

2.6.9 ห้ามใช้บริการในระบบเครือข่าย เพื่อประกอบธุรกิจส่วนตัว

2.6.10 ห้ามกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่น

2.6.11 ห้ามทำลาย หรือพยายามทำลายระบบรักษาความปลอดภัยของระบบเครือข่าย

2.6.12 ห้ามลักลอบดักจับข้อมูลในระบบเครือข่าย

2.7 จัดทำระบบเก็บข้อมูลจราจรคอมพิวเตอร์ตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ด้วยระบบ Authen โดยผู้ใช้งานระบบอินเตอร์เน็ต ต้องแสดงตัวตนก่อนเข้าใช้งาน และข้อมูลที่ใช้งานจะถูกเก็บไว้ที่ server อย่างน้อย 90 วัน

หมวดที่ 3 การจัดการระบบความมั่นคงปลอดภัยของ Data Center

3.1 ห้ามนำบุคคลภายนอกเข้าไปในห้อง Data Center โดยไม่มีกิจที่จำเป็นหากจำเป็นต้องได้รับอนุญาต จากผู้ดูแลระบบ โดยมีบันทึกการเข้าห้องไว้เป็นลายลักษณ์อักษร ทุกครั้ง

3.2 ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้อง Data Center

3.3 ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้อง Data Center ให้ปิดล็อกอยู่เสมอ

3.4 ตรวจสอบสภาพการทำงานของอุปกรณ์ ระบบคอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ ได้แก่

• ระบบกระแสไฟ

• ระบบควบคุมอุณหภูมิ

• ระบบเครื่องสำรองไฟ

3.5 จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวัง การจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย

3.6 ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ1ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่

3.7 ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้อง Data Center อย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษ หรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้อง

3.8 ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย

3.9 ตรวจสอบสายสัญญาณสื่อสารให้มีการปิดล็อกอยู่เสมอ

3.10 จัดทำหรือต่อสัญญาการบำรุงรักษาระบบงานสำคัญ ไฟร์วอลล์เราท์เตอร์ อุปกรณ์เครื่องสำรองไฟ สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องให้ครบถ้วน

3.11 จัดให้ระบบงานสำคัญ เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์เครื่องสำรองไฟ และระบบกระแสไฟฟ้าสำรอง (electricity power generator) เพื่อสนับสนุนการทำงาน อย่างครบถ้วน

3.12 แต่งตั้งให้ หัวหน้าห้องปฏิบัติการคอมพิวเตอร์เป็นผู้ควบคุมดูแลห้องServer ให้มีอำนาจหน้าที่

- บันทึกการจัดเก็บกุญแจและกุญแจสำรอง (key card key หรือ Card สำรอง)
- ควบคุมการเข้าออกห้องทั้งผู้ดูแลและบุคคลทั่วไปด้วย เครื่องสแกนลายนิ้วมือ
- เสนอรายงานการใช้งานห้อง server ต่อประธานกรรมการสารสนเทศทุกเดือน