3.1

บันทึกข้อความ

ส่วนราชการ งานคอมพิวเตอร์ โรงพยาบาลท่าตะเกียบ อำเภอท่าตะเกียบ จังหวัดฉะเชิงเทรา ๒๔๑๖๐

ที่ ฉช. ๐๐๒๗.๓ / ๖๗๑ **วันที่** ๑ เดือน ตุลาคม พ.ศ. ๒๕๖๒

เรื่อง ประกาศใช้นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศโรงพยาบาล

เรียน ผู้อำนวยการโรงพยาบาลท่าตะเกียบ

ตามที่ งานคอมพิวเตอร์ ได้จัดทำนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของโรงพยาบาลเพื่อสร้างความตระหนักของการให้ความสำคัญข้อมูลสารสนเทศ ความลับของผู้ป่วย ข้อมูลส่วนบุคคล รวมทั้งระเบียบปฏิบัติต่าง ๆ และแนวทางปฏิบัติของระบบสารสนเทศแก่เจ้าหน้าที่ของโรงพยาบาล ให้เป็นไปตามมาตรการที่เหมาะสมและถูกต้อง

ดังนั้น งานคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศ จึงขออนุญาตประกาศใช้นโยบาย ระเบียบปฏิบัติต่าง ๆ และแนวทางปฏิบัติของระเบียบสารสนเทศแก่เจ้าหน้าที่ของโรงพยาบาล ดังต่อไปนี้

๑.นโยบาย

- ๑.๑ นโยบายหลักด้านความมั่นคงปลอดภัยระบบสารสนเทศ

๒.ระเบียบปฏิบัติ

- ๒.๑ ระเบียบปฏิบัติการแก้ปัญหาการใช้งาน Hardware และ Software
- ๒.๒ ระเบียบปฏิบัติเมื่อระบบ HIS ใช้งานไม่ได้
- ๒.๓ ระเบียบปฏิบัติการเผยแพร่ข้อมูลลงเว็บไซต์ของโรงพยาบาล

๓.แนวทางปฏิบัติ

- ๓.๑ แนวทางปฏิบัติการใช้งานห้องแม่ข่าย
- ๓.๒ แนวทางปฏิบัติเมื่อระบบ HIS ใช้งานไม่ได้
- ๓.๓ แนวทางปฏิบัติการสำรองข้อมูล
- ๓.๔ แนวทางปฏิบัติการสำรองข้อมูล และนำข้อมูลกลับมาใช้
- ๓.๕ แนวทางปฏิบัติกรณีไฟฟ้าดับ
- ๓.๖ แนวทางปฏิบัติการรักษาความปลอดภัยและป้องกันการสูญหายของแฟ้มเวชระเบียบที่จัดเก็บในรูปแบบ Electronics
- ๓.๗ แนวทางปฏิบัติการลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่
- ๓.๘ แนวทางปฏิบัติการทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล
- ๓.๙ แนวทางปฏิบัติเอกสารที่เกี่ยวข้องกับระบบ

จึงเรียนมาเพื่อโปรดพิจารณาอนุมัติต่อไปด้วย จะเป็นพระคุณ

วีระชาติ บัวตุม

(นายวีระชาติ บัวตุม)

นักวิชาการคอมพิวเตอร์

เรียน ผู้อำนวยการโรงพยาบาลท่าตะเกียบ

เพื่อโปรดพิจารณาอนุมัติต่อไปด้วย จะเป็นพระคุณ

ชนันธร

(นางชนันธร เสียงล้ำ)

เจ้าพนักงานเวชสถิติ ชำนาญงาน

อนุมัติ

(นายเกริกภัทร ลิมปพยอม)

ผู้อำนวยการโรงพยาบาลท่าตะเกียบ

ประกาศโรงพยาบาลท่าตะเกียบ

เรื่อง นโยบายหลักด้านการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศ

ด้วย งานคอมพิวเตอร์ โรงพยาบาลท่าตะเกียบ มีหน้าที่ในการกำกับดูแลการใช้งานระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ พบว่าบางส่วนมีการใช้งานผิดประเภท ทำให้อาจเกิดความเสียหายในหน่วยงาน ดังนั้น เพื่อให้เป็นแนวทางปฏิบัติเดียวกัน จึงได้กำหนดนโยบายหลักเพื่อประกอบการควบคุม ดังนี้

1. นโยบายการรักษาความปลอดภัยมั่นคงปลอดภัยในระบบ HOSxP

1.1 ห้ามบุคคลภายนอกหรือผู้ที่ไม่มีหน้าที่เกี่ยวข้อง เข้าใช้งานในระบบ HOSxP

1.2 ห้ามไม่ให้ดูประวัติของผู้ป่วย นอกจากเป็นประวัติผู้ป่วยที่อยู่ในความรับผิดชอบและกำลังทำการรักษาอยู่เท่านั้น ยกเว้น กรณีต้องติดตามประวัติผู้ป่วยเพื่อการดูแลต่อเนื่อง หรืออื่น ๆ เพื่อเกิดประโยชน์แก่การรักษาพยาบาลผู้ป่วย

1.3 ตั้งรหัสผ่านในการเข้าใช้งานระบบ HOSxP ให้คาดเดาได้ยาก ปกปิดรหัสผ่านเป็นส่วนตัว ไม่อนุญาตให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้ เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ เช่น ทุก ๆ 3 เดือน

1.4 ห้ามนำอุปกรณ์ต่อพ่วงทุกชนิด มาใช้กับคอมพิวเตอร์ในระบบ HOSxP นอกจากได้รับอนุญาตจากงานคอมพิวเตอร์

1.5 ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ หรือปรับเปลี่ยนหมายเลขไอที (IP Address) ของเครื่องคอมพิวเตอร์ในระบบ HOSxP

1.6 ห้ามมิให้เปิดเผยประวัติผู้ป่วยกับผู้อื่น ในกรณีไม่มีหนังสือลายลักษณ์อักษร มาแสดง

1.7 มีการจำกัดการเข้าถึงข้อมูลที่เป็นความลับ เช่น ประวัติผู้ป่วย ให้เข้าถึงได้เฉพาะที่ตนเองได้รับอนุญาตตามหน้าที่ที่ปฏิบัติและความเหมาะสมเท่านั้น

1.8 ห้ามแก้ไข/ดัดแปลง ประวัติผู้ป่วยจากความเป็นจริง นอกจากมีลายลักษณ์อักษร ยินยอมหรืออยู่ในความรับผิดชอบเจ้าหน้าที่ที่เกี่ยวข้อง

1.9 ห้ามใช้คอมพิวเตอร์ที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วย ในการติดต่อกับอินเตอร์เน็ตทุกกรณี ยกเว้น เครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเตอร์เน็ต ซึ่งได้รับอนุญาตจากผู้อำนวยการ

1.10 กำหนดให้ระบบ HOSxP มีการตัดและหมดระยะเวลาการใช้งาน รวมทั้งปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา 15 นาที

1.11 ตำแหน่งที่ตั้งจอภาพ และเครื่องพิมพ์ ให้อยู่ในตำแหน่งที่ ผู้ป่วยหรือญาติ ไม่สามารถมองเห็นหรือเข้าถึงได้

2. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

2.1 ห้ามนำอุปกรณ์ Wireless มาติดตั้ง หรือเปิดใช้งานเองภายในโรงพยาบาล โดยไม่ได้รับอนุญาต

2.2 ห้ามให้ User และ Password แก่ผู้อื่น ต้องรักษาเป็นความลับ

2.3 ห้ามเคลื่อนย้ายอุปกรณ์ Wireless Lan โดยไม่ได้รับอนุญาต

3. นโยบายการใช้สื่อสังคมออนไลน์ (Social Media)

3.1 ขอให้สมาชิกกลุ่มไลน์ต่าง ๆ ห้ามมิให้แสดงข้อความ รูปภาพที่ไม่เหมาะสม ส่อไปในทางลามก อนาจาร การปลุกเร้าให้เกิดการแตกแยก การทำลายสถาบันต่าง ๆ หรือเอกสารที่สามารถระบุตันตนผู้ป่วย แสดงถึงการเปิดเผยความลับของผู้ป่วย

3.2 ขอให้สมาชิกกลุ่มไลน์ต่าง ๆ ห้ามมิให้แสดงรูปภาพ ชื่อ ที่อยู่ ที่จะนำไปสู่การระบุตัวตนผู้ป่วยอย่างชัดเจน หากกระทำเผื่อประโยชน์ทางการรักษาพยาบาล ควรปกปิดใบหน้าและควรขออนุญาตผู้ป่วยก่อน เมื่อดำเนินการเสร็จสิ้นต้องลบภาพนั้นทันที

3.3 ห้ามใช้โปรแกรม Line ในการสื่อสารการรักษาพยาบาล ยกเว้น เพื่อประโยชน์ในการรักษาพยาบาลผู้ป่วย เมื่อดำเนินการเสร็จ ต้องลบข้อมูลหรือรูปภาพนั้นทันที ทั้งผู้ส่งและผู้รับ

4. นโยบายการใช้อินเตอร์เน็ต

4.1 ห้ามเข้าเว็บไซต์ ลามก อนาจาร สิ่งผิดกฎหมาย ผิดศีลธรรม จริยธรรม การวิพากษ์วิจารณ์ชาติ ศาสนา และพระมหากษัตริย์

4.2 ห้ามเข้าเว็บไซต์ เล่นเกมส์ ดูภาพยนตร์ ฟังเพลง ในขณะปฏิบัติงาน หรือกำลังให้บริการผู้ป่วย

4.3 ห้ามดาวน์โหลดหรือส่ง กระจาย แจกจ่าย ข้อมูลลามก อนาจาร ข้อมูลส่วนบุคคล สื่อสิ่งพิมพ์ ซึ่งเป็นการละเมิดลิขสิทธิ์ทางปัญหา

4.4 ห้ามกระทำการใด ๆ ซึ่งขัดต่อ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

5. นโยบายการป้องกันโปรแกรมไม่พึงประสงค์

5.1 ห้ามนำโปรแกรมใด ๆ มาติดตั้งภายในเครื่องคอมพิวเตอร์ หากต้องการติดตั้งเนื่องจากมีผลกับการปฏิบัติราชการต้องติดต่องานคอมพิวเตอร์

6.นโยบายการป้องกันไวรัส บนเครื่องคอมพิวเตอร์

6.1 ห้ามใช้ USB Port กับเครื่องในระบบเครือข่าย HOSxP

6.2 ห้ามดาวน์โหลด หรือติดตั้งโปรแกรมใด ๆ โดยไม่ได้รับอนุญาต

6.3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านอินเตอร์เน็ต จะต้องมีการตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับและส่งข้อมูลทุกครั้ง

7.นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

7.1 ห้ามจด หรือบันทึก User และ Password ไว้ในที่ง่ายต่อการสังเกต เช่น ที่โต๊ะทำงาน บนหน้าจอ ,(Clear Desk, Clear Screen Policy) แป้นพิมพ์ หรือ ไวท์บอร์ด ควรเก็บเป็นความลับ หรือจดไว้ในสมุดที่เก็บในลิ้นชักส่วนตัว

7.2 กรณีที่จำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อให้สามารถปฏิบัติงานแทนเพื่อประโยชน์ในการรักษาพยาบาล หลังจากที่ทำงานเสร็จแล้ว ให้ทำการเปลี่ยนรหัสผ่านทันที

7.3 เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการติดตั้งเวลาพักหน้าจอ โดยตั้งเวลาอย่างน้อย 15 นาที

7.4 ผู้ใช้งานต้องสำรองข้อมูล (Backup) ที่สำคัญทุกวัน จากเครื่องคอมพิวเตอร์ ไปไว้บนสื่อบันทึกอื่น ๆ เช่น Flash Drive หรือ External Hard Disk เป็นต้น

7.5 เครื่องคอมพิวเตอร์ทุกเครื่องที่ต้องทำการเปลี่ยนทดแทน หรือต้องจำหน่ายด้วยกระบวนการทางพัสดุ ให้ดำเนินการทำลายข้อมูลที่อยู่ในฮาร์ดดิสก์ ด้านวิธีการเปลี่ยนโครงสร้างทางกายภาพ (Disk) ของฮาร์ดดิสก์ก่อนส่งไปงานพัสดุ

8.นโยบายการป้องกันทรัพย์สินทางคอมพิวเตอร์

8.1 ห้ามเคลื่อนย้ายคอมพิวเตอร์ เครื่องพิมพ์ อุปกรณ์ต่อพ่วงต่าง ๆโดยไม่ได้รับอนุญาตจากงานคอมพิวเตอร์

8.2 ห้ามนำวัสดุ หรือ ครุภัณฑ์คอมพิวเตอร์ ออกนอกโรงพยาบาลโดยไม่ได้รับอนุญาตจากงานคอมพิวเตอร์ หรือกระบวนการทางพัสดุ

8.3 ห้ามมิให้บุคคลภายนอกใช้วัสดุและครุภัณฑ์คอมพิวเตอร์ นอกเหนือจากที่ได้จัดสถานที่ไว้บริการ เช่น ห้องสมุด

นโยบายการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดเป็นมาตรการด้านความปลอดภัยในการใช้งานระบบสารสนเทศของโรงพยาบาล ซึ่งเจ้าหน้าที่ของโรงพยาบาลท่าตะเกียบ จะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ เดือน ตุลาคม พ.ศ. ๒๕๖๒

(นายเกริกภัทร ลิมปพยอม)
ผู้อำนวยการโรงพยาบาลท่าตะเกียบ