ประกาศโรงพยาบาลภูเพียง

ประกาศนโยบายรักษาความมั่นคงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

ตามพระราชกฤษฎีกากำหนัดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียนปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลภูเพียง ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างถูกต้อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุมคามจากภัยต่าง ๆ โรงพยาบาลภูเพียง จึงกำหนดนโยบาย ดังนี้

๑. ส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๒. มีหน้าที่ควบคุม ดูแล ระงับเพิกถอนสิทธิหรือบทลงโทษตามความเหมาะสม หากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติในกรณีสำคัญ งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

๓. สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้อง สมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๔. สนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ ๒ ตุลาคม พ.ศ.๒๕๖๘

(นายภูวัส เฟยลุง)

นายแพทย์ชำนาญการพิเศษ (ด้านเวชกรรม)

รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลภูเพียง

ประกาศโรงพยาบาลภูเพียง

ประกาศระเบียบปฏิบัติการรักษาความมั่นคงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

ตามพระราชกฤษฎีกากำหนัดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียนปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลภูเพียง ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างถูกต้อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุมคามจากภัยต่าง ๆ โรงพยาบาลภูเพียง จึงกำหนดระเบียบปฏิบัติ ดังนี้

ข้อ	ระเบียบปฏิบัติ
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๙๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
๒	ผู้ใช้งานต้องกำหนัดรหัสผ่าน ให้มี ๖ ตัวขึ้นไปและประกอบด้วยตัวเลขและตัวอักษร
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน (User Account)และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของท่าน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
๔	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง มาเชื่อมต่อมกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ในโรงพยาบาลโดยไม่ได้รับอนุญาต
๕	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเตอร์เน็ตมาติดตั้งหรืออัพเดพซอฟแวร์อื่นใดในโรงพยาบาลนอกเหนือจากที่ผู้ดูแลระบบกำหนด
๖	ห้ามเปิดหรือใช้โปรแกรมเพื่อความบันเทิงส่วนบุคคลในระหว่างปฏิบัติราชการ
๗	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองภายนอกกับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย
๘	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆต่ออุปรณ์คอมพิวเตอร์ของโรงพยาบาลโดยไม่ได้รับอนุญาติจากผู้ดูแลระบบ
๙	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ ยกเว้นได้รับอนุญาติจากผู้ป่วย
๑๐	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผืดชอบโดยตรง

ประกาศ ณ วันที่ ๒ ตุลาคม พ.ศ.๒๕๖๘

(นายภูวัส เฟยลุง)

นายแพทย์ชำนาญการพิเศษ (ด้านเวชกรรม)

รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลภูเพียง

ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ควรทำ

๑. ควรทำการเปลี่ยนรหัสผ่านทุกๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
๒. รหัสผ่านต้องมีความยาวอย่างน้อย ๖ ตัว ประกอบด้วยตัวเลขและตัวอักษร
๓. เก็บรักษาข้อมูลบัญชีของผู้ใช้งานและรหัสผ่าน ห้ามให้ผู้อื่นใช้

ไม่ควรกระทำ

	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นท์เตอร์,อุปกรณ์กระจายสัญญาณต่างๆ ฯลฯ) มาเชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาลโดยไม่ได้รับอนุญาต
	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัพเดทซอฟแวร์อื่นใดในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด
	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น
	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ
	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

โรงพยาบาลภูเพียง
สำนักงานสาธารณสุขจังหวัดน่าน

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์: เพื่อสร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานสารสนเทศในโรงพยาบาล

มาตรการรักษาความปลอดภัย

1. กำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ	2. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยของระบบให้ตอบสนองต่อพันธกิจและนโยบาย
3. กำหนดแนวทางปฏิบัติ แนวทางแก้ไขหรือบทลงโทษตามความเหมาะสม หากมีการละเมิด หรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยของระบบ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ	4. เผยแพร่ความรู้ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานและหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง
5. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี	

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

1. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

กำหนดพื้นที่ของระบบอย่างเหมาะสม และจัดทำเป็นเอกสารกำหนดสิทธิให้กับเจ้าหน้าที่ให้เข้าถึงพื้นที่ใช้งานระบบให้ชัดเจน หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์เข้ามาในระบบเครือข่ายภายในหน่วยงานจะต้องแจ้งงาน IT ทราบทุกครั้ง

2. การควบคุมการเข้าออกห้องศูนย์

จัดระบบฯให้เป็นสัดส่วนชัดเจน มีการลงบันทึกตามแบบฟอร์ม "บันทึกการเข้าออกพื้นที่" ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องอย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้ง

3. การควบคุมการเข้าถึงระบบ ๆ

บริหารจัดการการเข้าถึงของผู้ใช้ การเข้าถึงระบบเครือข่าย แม่ข่าย การบันทึกและตรวจสอบการควบคุมการเข้าใช้งานระบบจากภายนอก การพิสูจน์ตัวตน

4. การควบคุมหน่วยงานภายนอกเข้าถึงระบบฯ

จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร ต้องลงนามเฉพาะบุคคลที่จำเป็นเท่านั้น มีการปรับปรุงให้ทันสมัยอยู่งพอ เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนด

5. การใช้งานเครื่องคอมพิวเตอร์และอินเทอร์เน็ต

จัดการรหัสผ่านที่ ระบุไว้ในเอกสาร ต้องทำการ Updateระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่จากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคาม Firewall เป็นระบบที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ เครื่องคอมฯทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus

6. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาต ลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย กำหนดการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น มีการติดตั้ง Firewall เฉพาะกับ VPN

จัดทำโดย งานสารสนเทศทางการแพทย์
กลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์