ประกาศโรงพยาบาลแม่ลาว
เรื่อง นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ระดับผู้ใช้งานสารสนเทศ โรงพยาบาลแม่ลาว

.....

โรงพยาบาลแม่ลาวมุ่งมั่นที่จะพัฒนาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความปลอดภัยสูงสุดแก่ระบบข้อมูลข่าวสาร การให้บริการผู้ป่วย การบริหารงานโรงพยาบาล ตลอดจนการตอบสนองต่อวิสัยทัศน์และพันธกิจของโรงพยาบาล ดังนั้น โรงพยาบาลแม่ลาว จึงขอประกาศนโยบายด้านความมั่นคงปลอดอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้ทุกหน่วยงานและบุคลากรทุกระดับ รับทราบและถือปฏิบัติ ดังนี้

๑. ยึดถือและปฏิบัติตามข้อกำหนด ตามกฎหมายเทคโนโลยีสารสนเทศของประเทศไทยในทุกขั้นตอนของการบริหารจัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลโดยเคร่งครัด

๒. ยึดถือหลักการปกปิดข้อมูลของผู้ป่วยตามคำประกาศสิทธิของผู้ป่วยของแพทย์สภา

๓. ถือเป็นหน้าที่ความรับผิดชอบของบุคลากรทุกระดับที่จะให้ความร่วมมือในการปฏิบัติตามมาตรการรักษาความปลอดภัยของระบบสารสนเทศที่โรงพยาบาลแม่ลาวกำหนดไว้

๔. วางแผนและดำเนินการพัฒนาศักยภาพระบบสารสนเทศอย่างต่อเนื่อง เพื่อให้มีประสิทธิภาพและทันสมัยตามความก้าวหน้า

๕. บริหารจัดการระบบรักษาความปลอดภัยของระบบสารสนเทศ เพื่อลดความเสี่ยงต่อการถูกโจมตีจากสิ่งคุกคามภายนอก

๖. จัดทำระบบฐานข้อมูลเพื่อเก็บรักษาข้อมูลสำคัญไว้อย่างมีประสิทธิภาพ และวางระบบในการกู้คืนข้อมูลเมื่อเกิดเหตุการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๗. กำกับและควบคุมการใช้งานระบบสารสนเทศของบุคลากรในโรงพยาบาลให้เป็นไปอย่างเหมาะสมกับหน้าที่และความจำเป็น รวมทั้งจำกัดสิทธิ์ในการเข้าถึงข้อมูลเท่าที่จำเป็น เพื่อลดโอกาสการนำข้อมูลของโรงพยาบาลไปใช้ในทางที่ก่อให้เกิดความเสียหาย

๘. เผยแพร่ข้อมูลที่มีความสำคัญ เป็นประโยชน์ต่อบุคลากรและผู้รับบริการ โดยอาศัยช่องทางที่เหมาะสมกับลักษณะของข้อมูล และผู้รับข้อมูล ทั้งนี้ต้องเป็นข้อมูลที่ไม่เป็นความลับ ไม่ละเมิดสิทธิ์ และไม่ก่อให้เกิดความเสียหายต่อผู้ใด หากผู้ใดละเมิดต่อนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พิจารณาบทราชการลงโทษตามวินัยราชการ รวมทั้ง พ.ร.บ.คอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ.๒๕๖๐

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๖ ตุลาคม พ.ศ. ๒๕๖๗

(นายคงศักดิ์ ชัยชนะ)
นายแพทย์เชี่ยวชาญ
ผู้อำนวยการโรงพยาบาลแม่ลาว

กิจกรรมที่ ๑

ปรับปรุงระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลแม่ลาว		
๑	ผ่านมติที่ประชุมคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศ (IT)	√
๒	ผ่านที่ประชุมคณะกรรมการพัฒนาระบบเวชระเบียนและสารสนเทศ (MIS)	√
๓	ผ่านมติที่ประชุมคณะกรรมการบริหารโรงพยาบาล (กกบ.) พร้อมได้ชี้แจ้งเพื่อทาความเข้าใจร่วมกัน	√

กิจกรรมที่ ๒

ประเมินการรับรู้ระเบียบปฏิบัติในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศของโรงพยาบาลแม่ลาว		
๑	ประเมินการรับรู้ฯ ผู้ใช้งานทุกคน จำนวน ๑๕๔ คน ทั้งหมด หน่วยงาน	√
๒	วิธีการประเมินการรับรู้ฯ ใช้แบบสอบถามโดยคณะกรรมการ IT แต่ละจุดบริการ	√
๓	คณะกรรมการ IT แต่ละจุดบริการ กำกับ ดูแลติดตามผล	√
๔.	คณะกรรมการ IT แต่ละจุดบริการ สรุปผลการประเมินส่งศูนย์คอมพิวเตอร์เพื่อสรุปผล และหาแนวทางพัฒนาต่อไป	√

สรุปผลการประเมินการรับรู้ และการละเมิด ระเบียบในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลแม่ลาว

ลำดับ	หัวข้อ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ/แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม HOSxpP ทุก ๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน									ปิดการใช้งานกรณีครบ ๙๐ วัน (+๓๐วัน) ผู้ใช้งานต้องติดต่อขอเปิดใช้งานใหม่
๒	ผู้ใช้งานต้องกำหนดรหัสผ่านโปรแกรม HOSxP ให้มี ๘ ตัวขึ้นไป บังคับรหัสผ่านต้องมีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก รหัสผ่านที่กำหนดใหม่ห้ามซ้ำกับรหัสผ่านเดิม									คณะกรรมการ IT แต่ละจุดบริการ ประเมินทุกราย เมื่อพบแจ้งดำเนินการแก้ไขทันที
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม									-เตือน แนะนา ผู้ละเมิดให้นาออกและประเมินผลซ้ า -เพิ่มบัญชีผู้ใช้งานแก่บุคคล
๔	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Driver,External Driver,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ									- ปิดช่องทางนาเข้า/ออกข้อมูลได้แก่ USB,CD-Rom - มีระบบรับส่งข้อมูล

๕	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่โรงพยาบาลแม่ลาวไม่อนุญาต									เมื่อต้องติดตั้งโปรแกรมอื่น ๆ ให้ประสานผู้ดูแลระบบเท่านั้น
๖	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรม เพื่อความบันเทิงส่วนบุคคล เช่นการดูหนัง เล่นเกมส์ เป็นต้นในระหว่างเวลาปฏิบัติราชการ									เตือน แนะนำ ผู้ละเมิดให้นำออก และประเมินผลซ้ำ
๗	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ									
๘	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook ,Line ,Website หรือโปรแกรมอื่น ๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ									- ประกาศนโยบายการสื่อสารช่องทาง LINE - เตือน แนะนำ ผู้ละเมิดให้ลบข้อมูล และประเมินซ้ำ
๙	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในนนนความรับผิดขอบของตนเองในปัจจุบัน									- ระบบป้องกันการเข้าถึงข้อมูลพร้อมกัน โดยมีแจ้งเตือนว่ามีใครเครื่องคอมพิวเตอร์ไหนใช้งานอยู่ ผู้รับผิดชอบปัจจุบันสามารถโทรประสานให้ออก - กำหนดการตั้งชื่อคอมฯ เช่น (DIAG ๑)

ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ

DO

เปลี่ยนรหัสผ่าน
ทุก 90 วัน

ต้องมีความยาวอย่างน้อย 8 ตัวอักษร
มีตัวอักษรภาษาอังกฤษผสมตัวเลข

DO NOT

ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งหรือทำการใด ๆ ต่ออุปกรณ์ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นเตอร์, อุปกรณ์กระจายสัญญาณต่าง ๆ ฯลฯ มาเชื่อมต่อกับระบบคอมพิวเตอร์หรือระบบเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต

ห้ามดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต หรือการอัพเดส (Update) โปรแกรมต่าง ๆ นอกเหนือจากที่ผู้ดูแลระบบกำหนด

ห้ามผู้ใช้งานระบบนำข้อมูลผู้ป่วยไปส่งต่อ หรือเปิดเผยข้อมูลต่อสาธารณะชนผ่านทาง Line , Facebook หรือโซเชียลมีเดีย (Socila Media) ต่าง ๆ หากมีความจำเป็นต้องได้รับการยินยอมจากผู้ป่วยหรือญาติเป็นลายลักษณ์อักษร

ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

แบบสอบถามการประเมินการรับรู้ และการละเมิด ระเบียนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลแม่ลาว

ตอนที่ ๑ ข้อมูลผู้รับการประเมิน

ชื่อ-สกุล ..... ตำแหน่ง .....

หน่วยงาน..... กลุ่มงานน .....

ตอนที่ ๒ การประเมินการรับรู้และเข้าใจ ระเบียบปฏิบัติฯ ข้อ ๑ และ ๒ สำหรับผู้ใช้งาน HOSxP เท่านั้น

ลำดับ	หัวข้อ	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม HOSxpP ทุก ๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน				
๒	ผู้ใช้งานต้องกำหนดรหัสผ่านโปรแกรม HOSxP ให้มี ๘ ตัวขึ้นไป บังคับรหัสผ่านต้องมีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก รหัสผ่านที่กำหนดใหม่ห้ามซ้ำกับรหัสผ่านเดิม				
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม				
๔	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Driver,External Driver,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ				
๕	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่โรงพยาบาลแม่ลาวไม่อนุญาต				
๖	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรม เพื่อความบันเทิงส่วนบุคคล เช่นการดูหนัง เล่นเกมส์ เป็นต้นในระหว่างเวลาปฏิบัติราชการ				
๗	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ				
๘	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook ,Line ,Website หรือโปรแกรมอื่น ๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ				
๙	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในนนนความรับผิดขอบของตนเองในปัจจุบัน				