ประเมินการรับรู้และการละเมิดแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลน้ำเกลี้ยง

งานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์

โรงพยาบาลน้ำเกลี้ยง

ประกาศนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลน้ำเกลี้ยง จึงกำหนดนโยบาย ดังนี้

๑. ส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร
๒. มีหน้าที่ควบคุม ดูแล ระงับเพิกถอนสิทธิ หรือบทลงโทษตามความเหมาะสม หากมีการละเมิดหรือ ฝ่าฝืนระเบียบปฏิบัติในกรณีสำคัญ งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์รายงานการฝ่าฝืนให้ต้นสังกัด หรือโรงพยาบาลเพื่อพิจารณาลงโทษ
๓. สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ
๔. สนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้ และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ.๒๕๖๕

(นายอธิบ ลีธีระประเสริฐ)
ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง

โรงพยาบาลน้ำเกลี้ยง

ประกาศระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลน้ำเกลี้ยง ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลน้ำกเลี้ยง จึงกำหนดระเบียบปฏิบัติ ดังนี้

ข้อ	ระเบียบปฏิบัติ
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHimProทุกๆ ๓๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรมHimPro ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน(Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
๔	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นท์เตอร์,อุปกรณ์กระจายสัญญาณต่างๆ ฯลฯ) มาเชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาลโดยไม่ได้รับอนุญาต
๕	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัพเดทซอฟแวร์อื่นใด ในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด
๖	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น
๗	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
๘	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
๙	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ
๑๐	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ.๒๕๖๕

(นายอธิบ ลีธีระประเสริฐ)

ผู้อำนวยการโรงพยาบาลน้ำเกลี้ยง

ประเมินการรับรู้และการละเมิดแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

กิจกรรมที่ ๑

ร่างนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
๑	ผ่านมติที่ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ	√
๒	ผ่านมติที่ประชุมคณะกรรมการระบบเวชระเบียน (MRS)	√
๓	ผ่านมติที่ประชุมคณะกรรมการบริหารโรงพยาบาล (กกบ)	√

กิจกรรมที่ ๑

ประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
๑	ประกาศใช้ วันที่ ๑ ตุลามคม ๒๕๖๕	√
๒	เวียนหนังสือแจ้งประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ทุกหน่วยงานพร้อมกับเซ็นต์รับทราบทุกคน ส่งรายชื่อกลับงานประกัน สุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เพื่อติดตามประเมินผลต่อไป	√

กิจกรรมที่ ๓

ประเมินการรับรู้นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
๑	ประเมินการรับรู้ฯ ผู้ใช้งานทุกคน จำนวน ๑๖๐ คน ทั้งหมด ๑๕ หน่วยงาน	๑๐๐%
๒	วิธีการประเมินการรับรู้ฯ โดยแบบสอบถาม	๑๐๐%
๓	หัวหน้ากลุ่มงานควบคุม กำกับ ติดตามผล	√
๔	งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ สรุปผลการประเมิน และหาแนวทางพัฒนาต่อไป	√

กิจกรรมที่ ๔

ประเมินการละเมิดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ		
๑	ประเมินการรับรู้ฯ ผู้ใช้งานทุกคน จำนวน ๑๖๐ คน ทั้งหมด ๑๕ หน่วยงาน	๑๐๐%
๒	วิธีการประเมินการรับรู้ฯ โดยแบบสอบถาม	๑๐๐%
๓	หัวหน้ากลุ่มงานควบคุม กำกับ ติดตามผล	√
๔	งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ สรุปผลการประเมิน และหาแนวทางพัฒนาต่อไป	√

<u>กิจกรรมที่ ๕</u> สรุปผลการประเมินการรับรู้ และการละเมิดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๕

ลำดับ	แนวปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ/แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม Himpro ทุกๆ ๓๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	๑๖๐	๑๐๐	๐	๐	๕	๘.๐๐	๑๕๕	๙๒	• ผู้ใช้งานต้องติดต่อขอเปิดใช้งานใหม่
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม Himpro ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร									• งานประกันสุขภาพ ฯ ประเมินทุกราย เมื่อพบให้แจ้งดำเนินการแก้ไขทันที
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน (User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม									• เตือน แนะนำผู้ละเมิดและประเมินผลซ้ำ • เพิ่มบัญชีผู้ใช้งานให้แก่บุคคลที่ยังไม่มี
๔	ห้ามผู้ใช้งานนำอุปกรณ์กระจ่ายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล									• เตือน แนะนำผู้ละเมิดและประเมินผลซ้ำ
๕	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟแวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ									• ติดตั้งโปรแกรม Winlock ผู้ใช้งานจะไม่สามารถติดตั้งซอฟแวร์อื่นได้ยกเว้นผู้ดูแลระบบเท่านั้น
๖	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น									• เตือน แนะนำ ผู้ละเมิดและประเมินผลซ้ำ

ลำดับ	แนวปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ/แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
๗	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ									• เตือน แนะนำ ผู้ละเมิดและประเมินผลซ้ำ
๘	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ									• เตือน แนะนำ ผู้ละเมิดและประเมินผลซ้ำ
๙	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ									• เตือน แนะนำ ผู้ละเมิดให้ดำเนินการลบข้อมูลและประเมินผลซ้ำ
๑๐	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน									• กำหนดสิทธิ์การเข้าถึงข้อมูล
หมายเหตุ : ผู้ใช้งานทั้งหมด จำนวน ๑๖๐ คน										

ภาคผนวก

ภาคผนวก ก

สื่อประชาสัมพันธ์

สื่อประชาสัมพันธ์

ภาคผนวก ข
แบบสอบถามประเมินการรับรู้และการละเมิดแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๕

.....

ตอนที่ ๑ ข้อมูลทั่วไป

ชื่อ – สกุล.....ตำแหน่ง.....

หน่วยงาน / กลุ่มงาน.....

ตอนที่ ๒ การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยฯ

ข้อ	แนวปฏิบัติ	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHimpro ทุกๆ ๓๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน				
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม Himpro ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร				
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม				
๔	ห้ามผู้ใช้งานนำอุปกรณ์กระจ่ายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล				
๕	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟแวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ				
๖	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น				
๗	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ				
๘	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ				
๙	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ				
๑๐	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน				

ภาคผนวก ค
แบบสอบถามประเมินการรับรู้และการละเมิดแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ตัวอย่างการประเมิน)

แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๕

.....

ตอนที่ ๑ ข้อมูลทั่วไป

ชื่อ – สกุล น.ส. ศิริลักษณ์ สมศิริ ตำแหน่ง พนักงานสาธารณสุขปฏิบัติการ

หน่วยงาน / กลุ่มงาน ประกันสุขภาพฯ

ตอนที่ ๒ การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยฯ

ข้อ	แนวปฏิบัติ	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHimpro ทุกๆ ๓๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	✓			✓
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม Himpro ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	✓			✓
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม	✓			✓
๔	ห้ามผู้ใช้งานนำอุปกรณ์กระจ่ายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	✓			✓
๕	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟแวร์อื่นใดในโรงพยาบาลโดยที่ไม่อนุญาตจากผู้ดูแลระบบ	✓			✓
๖	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	✓			✓
๗	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	✓			✓
๘	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	✓			✓
๙	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	✓			✓
๑๐	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	✓			✓

แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๕

.....

ตอนที่ ๑ ข้อมูลทั่วไป

ชื่อ – สกุล น.ส.ยุ้ยพนา สิงปะมงม์ ตำแหน่ง จพ.เวชสถิติ

หน่วยงาน / กลุ่มงาน งานประกัน

ตอนที่ ๒ การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยฯ

ข้อ	แนวปฏิบัติ	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHimpro ทุกๆ ๓๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	/			/
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม Himpro ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	/			/
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม	/			/
๔	ห้ามผู้ใช้งานนำอุปกรณ์กระจ่ายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	/			/
๕	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟแวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ	/			/
๖	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	/			/
๗	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	/			/
๘	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	/			/
๙	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	/			/
๑๐	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	/			/

ภาคผนวก ง

ภาพกิจกรรม

แบบสอบถามประเมินการรับรู้และการละเมิด
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ.๒๕๖๕

ตอนที่ ๑ ข้อมูลทั่วไป
ชื่อ – สกุล นส. ศิริลักษณ์ สุมศิริ ตำแหน่ง พนก. สาธารณสุขปฏิบัติการ
หน่วยงาน / กลุ่มงาน ประกันสุขภาพฯ

ตอนที่ ๒ การประเมินการรับรู้และการละเมิดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยฯ

ข้อ	แนวปฏิบัติ	การรับรู้		การปฏิบัติ	
		รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
๑	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรมHimpro ทุกๆ ๓๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน	✓			✓
๒	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม Himpro ให้มี ๖ ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร	✓			✓
๓	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account)ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม	✓			✓
๔	ห้ามผู้ใช้งานนำอุปกรณ์กระจ่ายสัญญาณมาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล	✓			✓
๕	ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟแวร์อื่นใดในโรงพยาบาล โดยที่ไม่อนุญาตจากผู้ดูแลระบบ	✓			✓
๖	ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น	✓			✓
๗	ห้ามผู้ใช้งานนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ	✓			✓
๘	ห้ามผู้ใช้งานเคลื่อนย้ายเครื่องคอมพิวเตอร์ และ อุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ	✓			✓
๙	ห้ามผู้ใช้งานเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, Line, Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้Lineในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ	✓			✓
๑๐	ห้ามผู้ใช้งานเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบของตนเองในปัจจุบัน	✓			✓