โรงพยาบาลโพธิ์ไทร

ประกาศนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลโพธิ์ไทร ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัย ต่างๆ โรงพยาบาลโพธิ์ไทร จึงกำหนดนโยบาย ดังนี้

1. ส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร
2. มีหน้าที่ควบคุม ดูแล ระงับเพิกถอนสิทธิ หรือบทลงโทษตามความเหมาะสม หากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติในกรณีสำคัญ งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ รายงานการฝ่าฝืนให้ต้นสังกัด หรือโรงพยาบาลเพื่อพิจารณาลงโทษ
3. สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ
4. สนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้ และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ 1 ตุลาคม พ.ศ. 2565

(นางสาวธรรมพร ปรัสพันธ์)

ผู้อำนวยการโรงพยาบาลโพธิ์ไทร

โรงพยาบาลโพธิ์ไทร

ประกาศระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลโพธิ์ไทร ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหา ที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลโพธิ์ไทร จึงกำหนดระเบียบปฏิบัติ ดังนี้

ข้อ	ระเบียบปฏิบัติ
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม HI ทุก ๆ 90 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม HI ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน(User Account) และรหัสผ่าน (Password) และ ต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน(User Account) ไม่ว่าการกระทำนั้นจะเกิด จากผู้ใช้งานหรือไม่ก็ตาม
4.	ในการเข้าสู่ระบบเพื่อใช้งาน โปรแกรม HI ของสหสาขาวิชาชีพต่าง ๆ ที่เกี่ยวข้องกับการรักษาผู้ป่วย ให้สามารถเข้าสู่ระบบได้เฉพาะที่กำหนด ในตารางการปฏิบัติหน้าที่เท่านั้น ยกเว้นแต่มีเหตุฉุกเฉินที่จำเป็น
5	ห้ามนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นท์เตอร์, อุปกรณ์กระจายสัญญาณต่างๆ ฯลฯ) เชื่อมต่อกับระบบคอมพิวเตอร์หรือระบบเครือข่ายของโรงพยาบาลโดยไม่ได้รับอนุญาต
6	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัพเดทซอฟแวร์อื่นใดในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด

7	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น
8	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive, CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
9	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใด ๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาล โดยไม่ได้รับ อนุญาตจากผู้ดูแลระบบ
10	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น - Facebook - Line - Tiktok - Instagram - Website หรือ โปรแกรมอื่น ๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอม เผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วย ทุกครั้งที่ปรึกษาเสร็จ
11	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบโดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

ประกาศ ณ วันที่ 1 ตุลาคม พ.ศ. 2565

(นางสาวธรรมพร ปรัสพันธ์)

ผู้อำนวยการโรงพยาบาลโพธิ์ไทร

ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ข้อควรปฏิบัติ

1. ควรทำการเปลี่ยนรหัสผ่านทุก ๆ 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
2. รหัสผ่านต้องมีความยาวอย่างน้อย 6 ตัว ประกอบด้วยตัวเลขและตัวอักษร
3. เก็บรักษาข้อมูลบัญชีของผู้ใช้งานและรหัสผ่าน ห้ามให้ผู้อื่นใช้

ข้อห้าม

	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่นปริ้นท์เตอร์,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, tiktok, instagram ,Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์ อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ
	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยสารสนเทศ

ประกาศนโยบายรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

(Information Security Policy)

โรงพยาบาลโพธิ์ไทร

คำนำ

การเข้าถึงข้อมูลเป็นสิ่งสำคัญในโลกปัจจุบันที่พัฒนาไปอย่างรวดเร็ว และเทคโนโลยีทำให้ง่ายขึ้นกว่าที่เคยเป็นมา ด้วยช่องทางการสื่อสารที่มีประสิทธิภาพ เช่น อีเมล การส่งข้อความ การประชุมทางวิดีโอ และการบันทึกจัดเก็บข้อมูลข้อมูลผู้รับบริการ ทำให้สามารถแบ่งปันข้อมูลได้อย่างรวดเร็วและง่ายดายในระยะทางไกล นอกจากนี้ การมีเว็บไซต์เพื่อการประชาสัมพันธ์ยังเป็นช่องทางให้องค์กรได้กระจายข้อมูลข่าวสาร ให้ประชาชนได้รับทราบเกี่ยวกานดำเนินงานของหน่วยงาน

แม้ระบบ เทคโนโลยีสารสนเทศจะมีประโยชน์ และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง ละอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกันเพราะการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่างๆ ทำให้มีโอกาส ถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมย ข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยี สารสนเทศและการสื่อสารจึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแล บำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นอย่างยิ่ง

ดังนั้น โรงพยาบาลโพธิ์ไทรจึงจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคง ปลอดภัย และเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ จากทุกหน่วยงาน และต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยี ที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการเทคโนโลยีสารสนเทศจึงหวังเป็นอย่างยิ่งว่า แนวปฏิบัติการรักษาความมั่นคง ปลอดภัย ฉบับนี้จะเป็นแนวทางให้กับผู้ใช้บริการ ผู้ดูแลระบบ และผู้ที่ เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลโพธิ์ไทรต่อไป

สารบัญ