



โรงพยาบาลแก่งหางแมว  
KEANGHANGMEOW HOSPITAL

นโยบายรักษาความปลอดภัย  
ของระบบเทคโนโลยีสารสนเทศ  
(Information Security Policy)

โรงพยาบาลแก่งหางแมว  
ระยะเวลา 5 ปี (พ.ศ. 2565- พ.ศ. 2569)

## คำนำ

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

แม้ระบบ เทคโนโลยีสารสนเทศจะมีประโยชน์ และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง ละอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหาย ต่อการปฏิบัติราชการได้เช่นกันเพราะการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อติดต่อเชื่อมโยงข้อมูล ไปยังหน่วยงานต่างๆ ทำให้มีโอกาส ถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อวินาศกรรมระบบใช้การไม่ได้ รวมถึงการขโมย ข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการ สร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ ของหน่วยงาน ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยี สารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแล บำรุงรักษา และการควบคุม รักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นอย่างยิ่ง

ดังนั้น โรงพยาบาลแก่งหางแมวจึงจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคง ปลอดภัย และเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความ ร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศ จากทุกหน่วยงาน และต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยี ที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการเทคโนโลยีสารสนเทศจึงหวังเป็นอย่างยิ่งว่า แนวปฏิบัติการรักษาความมั่นคงปลอดภัย ฉบับนี้ จะเป็นแนวทางให้กับผู้ใช้บริการ ผู้ดูแลระบบ และผู้ที่ เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมวต่อไป

## สารบัญ

เรื่อง	หน้า
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ.....	1
บทนำ.....	1
หมวดทั่วไป.....	1
หมวดที่ 1 ว่าด้วยระเบียบการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต.....	2
หมวดที่ 2 ว่าด้วยการใช้จดหมายอิเล็กทรอนิกส์ การสนทนาและการติดต่อสื่อสารทาง อิเล็กทรอนิกส์.....	3
หมวดที่ 3 ว่าด้วยการใช้ Portal ขององค์กร และการเข้าใช้อินเทอร์เน็ต.....	3
หมวดที่ 4 ว่าด้วยการใช้งาน Application และโปรแกรมต่างๆ.....	4
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ .....	4
1.หลักการและเหตุผล.....	4
2.วัตถุประสงค์.....	5
3.นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ.....	5
4.องค์ประกอบของแนวทางปฏิบัติ.....	6
คำนิยาม.....	7
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security).....	10
1.วัตถุประสงค์.....	10
2.แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม .....	10
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy).....	10
1.วัตถุประสงค์.....	10
2.แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	10
2.1การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	10
การบริหารจัดการ การเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	11
การควบคุมการเข้าถึงระบบปฏิบัติการ.....	12
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy) .....	12
1.วัตถุประสงค์.....	12
2.แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย.....	12

เรื่อง	หน้า
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy) .....	15
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy) .....	16
1.วัตถุประสงค์.....	16
แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์.....	16
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)	18
1.วัตถุประสงค์.....	18
2.แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์.....	18
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)	19
1.วัตถุประสงค์.....	19
2.แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต.....	19
นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy) .....	20
1.วัตถุประสงค์.....	20
2.แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย.....	20
นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)	21
1.วัตถุประสงค์.....	21
2.แนวทางปฏิบัติในการสำรองข้อมูล.....	21
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ .....	21
1.วัตถุประสงค์.....	21
2.แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ.....	21

## นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

### บทนำ

- 1) นโยบายนี้จัดทำขึ้นสำหรับข้าราชการหรือเจ้าหน้าที่ในสังกัดโรงพยาบาลแก่งหางแมว จะเข้าใช้งานระบบคอมพิวเตอร์ของโรงพยาบาลแก่งหางแมว รวมไปถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ต โดยผ่านทางเครือข่ายของโรงพยาบาลแก่งหางแมวโดยให้ถือปฏิบัติโดยเคร่งครัด
- 2) โรงพยาบาลแก่งหางแมว สงวนสิทธิ์ในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามีกรณีละเมิดนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต
- 3) นิยามของระบบคอมพิวเตอร์และอุปกรณ์ประกอบของ โรงพยาบาลแก่งหางแมว มีดังนี้
  - ระบบคอมพิวเตอร์
  - เครื่องคอมพิวเตอร์
  - อุปกรณ์ประกอบ
  - ซอฟต์แวร์
  - เครือข่ายภายใน อินทราเน็ต
  - เครือข่าย อินเทอร์เน็ต
  - การใช้งานจากภายนอกองค์กร Remote Access
  - โปรแกรมการใช้งาน Application

### หมวดทั่วไป

- 1) ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์ต่อเชื่อมของโรงพยาบาลแก่งหางแมว จัดหาเพื่อให้บริการที่เกี่ยวข้องกับกิจการของโรงพยาบาลแก่งหางแมวเท่านั้น ไม่อนุญาตให้ใช้ในกิจการที่ไม่เกี่ยวข้องกับกิจการของโรงพยาบาลแก่งหางแมว และหากไม่ได้รับอนุญาตห้ามนำบุคคลภายนอก มาใช้งานเครื่องคอมพิวเตอร์ และเครือข่ายของโรงพยาบาลแก่งหางแมว
- 2) การเข้าใช้งานระบบคอมพิวเตอร์ และการต่อเชื่อมทางอินเทอร์เน็ต ของโรงพยาบาลแก่งหางแมว จะต้องปฏิบัติตามระเบียบในการขออนุญาตเข้าใช้โดยจะมีการลงทะเบียนการเข้าใช้งานตามขั้นตอนของโรงพยาบาลแก่งหางแมว
- 3) บัญชีผู้ใช้งาน (USER ACCOUNT) ที่ให้ผู้ใช้ในวันนั้น ผู้ใช้งานต้องรับผิดชอบผลต่างๆ อันอาจเกิดขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดขึ้นจากบัญชีผู้ใช้งาน (USER ACCOUNT) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่า ผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น
- 4) บัญชีผู้ใช้งาน (USER ACCOUNT) ให้เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ นั้น ให้กับผู้อื่นไม่ได้

- 5) ในการขออนุญาตเข้าใช้งาน ให้ผู้ที่ขอใช้บริการเป็นผู้ขอโดยปฏิบัติตามขั้นตอนการขอเข้าใช้ระบบที่กำหนดไว้
- 6) ผู้เข้าใช้งานจะต้องทำความเข้าใจและลงนามเพื่อยืนยันว่าจะปฏิบัติตามนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ต และจะต้องทำความเข้าใจในส่วนเปลี่ยนแปลงแก้ไข (หากมี) โดยลงนามเพื่อยืนยันทุกรอบปี
- 7) ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้นโดยจะอ้างว่าไม่ทราบกฎระเบียบ หรือนโยบาย มิได้
- 8) นโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตนี้ ถือเป็นส่วนหนึ่งของข้อกำหนดในการปฏิบัติงานของข้าราชการและเจ้าหน้าที่ทุกคน และจะถือเป็นการผิดวินัยหรือระเบียบในการปฏิบัติงานเช่นเดียวกันหากไม่ปฏิบัติตาม
- 9) หากพบว่าข้าราชการหรือเจ้าหน้าที่มีการละเมิดนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ต จะถูกลงโทษตามกฎระเบียบของการเป็นข้าราชการหรือเจ้าหน้าที่ รวมถึงอาจจะส่งตัวเพื่อดำเนินคดีตามกฎหมาย หากการละเมิดนั้นมีความผิดตามกฎหมายหรือพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560
- 10) ผู้ใช้งานต้องต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแลระบบคอมพิวเตอร์

### หมวดที่ 1 ว่าด้วยระเบียบการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ต

- 1) โรงพยาบาลแก่งหางแมว ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และ การเชื่อมต่อทางอินเทอร์เน็ต จะถือปฏิบัติตามพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้องโดยข้าราชการหรือเจ้าหน้าที่ สามารถศึกษาข้อกำหนดจาก พรบ. ดังกล่าวได้
- 2) โรงพยาบาลแก่งหางแมว ไม่สนับสนุนหรือยินยอมให้ข้าราชการหรือเจ้าหน้าที่ของโรงพยาบาลแก่งหางแมว กระทำผิดต่อพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง
- 3) โรงพยาบาลแก่งหางแมว จะจัดให้มีชื่อผู้ใช้ (USERID) และรหัสผ่าน(Password) ให้กับข้าราชการหรือเจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตเป็นรายบุคคล และมีกฎในการใช้งานรหัสผ่าน เช่น ความยาวของตัวอักษร หรือระยะเวลาที่ต้องเปลี่ยนรหัส ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม

- 4) รหัสผ่านของข้าราชการหรือเจ้าหน้าที่ถือเป็นทรัพย์สินของโรงพยาบาลแก่งหางแมว และไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และข้าราชการหรือเจ้าหน้าที่ทุกคนมีหน้าที่ในการป้องกันรหัสผ่านขององค์กรอย่างเคร่งครัด
- 5) โรงพยาบาลแก่งหางแมว ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน
- 6) ข้าราชการหรือเจ้าหน้าที่อาจจะได้รับมอบหมายให้เข้าใช้ระบบงานอื่นๆ ที่โรงพยาบาลแก่งหางแมว กำหนดให้ใช้ ข้าราชการหรือเจ้าหน้าที่จะต้องปฏิบัติตามกฎการใช้ระบบเก็บรักษาชื่อและรหัสผ่านไว้ ห้ามมิให้เปิดเผยกับผู้อื่น ยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาโดยตรงเป็นลายลักษณ์อักษร
- 7) หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่านให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอลีกใช้ โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน หรือบัญชีผู้ใช้งานใดๆ ที่มีได้มีการใช้งานภายในระยะที่กำหนดไว้ จะถูกระงับหรือยกเลิกการใช้งาน
- 8) เครื่องคอมพิวเตอร์และอุปกรณ์ประกอบถือเป็นทรัพย์สินของโรงพยาบาลแก่งหางแมว ข้าราชการหรือเจ้าหน้าที่ ที่เป็นผู้รับผิดชอบจะต้องมีหน้าที่ดูแลบำรุงรักษาเบื้องต้น
- 9) ไม่อนุญาตให้ใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มีไซของโรงพยาบาลแก่งหางแมว ในการเชื่อมต่อเข้ากับเครือข่ายของโรงพยาบาลแก่งหางแมว เว้นแต่ได้มีการขออนุญาตเข้าใช้ระบบเครือข่ายคอมพิวเตอร์จากงานเทคโนโลยีสารสนเทศ

**หมวดที่ 2 ว่าด้วยการใช้จดหมายอิเล็กทรอนิกส์, การสนทนา และการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่นๆ (E-mail), chat, social network and others digital communication เช่นการส่ง file หรือการส่งโทรสาร**

- 1) ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ หรือการติดต่อสื่อสารใดๆ ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรือจดหมายของโรงพยาบาลแก่งหางแมว ได้แก่ การรักษาความลับของเอกสาร ห้ามส่งเอกสารความลับโดยจดหมายอิเล็กทรอนิกส์ ยกเว้นได้รับการเข้ารหัสและรับรองจากหน่วยงานคอมพิวเตอร์
- 2) ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อโรงพยาบาลแก่งหางแมว หรือบุคคลอื่นๆ 3) ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร
- 4) การส่งข้อมูลใดๆ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2440
- 5) หากพบว่ามี การส่งข้อมูลผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2440 หรือผิดต่อกฎระเบียบของโรงพยาบาลแก่งหางแมว ให้แจ้งต่อผู้บังคับบัญชาโดยตรง หรือเจ้าหน้าที่หน่วยงานคอมพิวเตอร์
- 6) ให้ใช้ข้อความสุภาพในการส่งจดหมายอิเล็กทรอนิกส์ การสนทนา chat หรือการสื่อสารทางอิเล็กทรอนิกส์อื่นๆ

- 7) ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง (SPAM (E-mail))
- 8) ไม่อนุญาตให้ข้าราชการหรือเจ้าหน้าที่ใช้ (E-mail) อื่นใดที่โรงพยาบาลแก่งหางแมว ไม่ได้กำหนดให้ใช้

### หมวดที่ 3 ว่าด้วยการใช้ Portal ขององค์กร และการเข้าใช้อินเทอร์เน็ต

- 1) ห้ามข้าราชการหรือเจ้าหน้าที่ post และ/หรือ download file รูป หรือข้อมูลใดๆ บน Portal ของโรงพยาบาลแก่งหางแมว หรือ Portal อื่นๆ ที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560
  - 1.1 มีไวรัส หรือชุดคำสั่งไม่พึงประสงค์
  - 1.2 ไม่เกี่ยวข้องกับกิจการขององค์กร
- 2) การเปิดให้บริการการเข้าถึงเว็บไซต์
  - 2.1 ให้บริการเว็บไซต์ที่เกี่ยวข้อง การให้บริการและกิจการของโรงพยาบาลแก่งหางแมวเป็นหลัก หากตรวจพบว่าความเร็วอินเทอร์เน็ตของระบบช้า จะงดให้บริการอินเทอร์เน็ตในกิจการอื่นๆ ที่มีใช้ของโรงพยาบาลแก่งหางแมวก่อน
  - 2.2 กำหนดช่วงเวลาหรือระงับการเข้าใช้งานของเว็บไซต์ ที่กำหนดโดยงานเทคโนโลยีสารสนเทศ

### หมวดที่ 4 ว่าด้วยการใช้งาน Application และโปรแกรมต่างๆ

- 1) การเข้าใช้งาน Application ต่างๆ จะต้องได้รับอนุญาตจากเจ้าของระบบ
- 2) ให้ข้าราชการหรือเจ้าหน้าที่ใช้โปรแกรมและ Application ที่โรงพยาบาลแก่งหางแมว กำหนดให้ใช้เท่านั้น
- 3) ห้ามข้าราชการหรือเจ้าหน้าที่นำโปรแกรม หรือ Application ใดๆ มาติดตั้งบนเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่นๆ โดยไม่ได้รับความยินยอมจากหน่วยงานคอมพิวเตอร์โดยตรง
- 4) ห้ามข้าราชการหรือเจ้าหน้าที่ใช้โปรแกรม หรือ Application ที่ไม่ถูกลิขสิทธิ์ หากก่อให้เกิดความเสียหาย หรือมีการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว
- 5) ผู้ที่ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามนโยบายนี้ โดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่างๆ เป็นไปตามมาตรฐานและไม่เกิดผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของโรงพยาบาลแก่งหางแมว
- 6) การขออนุญาตนำเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายและหมายเลขไอพี (IP ADDRESS) ของหน่วยงานใดๆ หน่วยงานนั้นจะต้องทำหนังสือขออนุญาต มายังงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เพื่อพิจารณาดำเนินการ



- 7) ห้ามบุคคลใดกระทำการเคลื่อนย้ายหรือทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการเพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของโรงพยาบาลแก่งหางแมวได้
- 8) ในกรณีที่ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติของระบบเครือข่ายหลักของโรงพยาบาลแก่งหางแมว งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ อาจจะพิจารณา ระวังการให้บริการ จากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน
- 9) ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับการอนุญาต ทั้งนี้รวมถึงการติดตั้งเครือข่ายแบบไร้สาย
- 10) โรงพยาบาลแก่งหางแมว จะติดตั้งโปรแกรมควบคุมการใช้งานผ่านเครือข่าย (REMOTE ACCESS) เพื่อติดตามช่วยเหลือ แก้ไข และควบคุมการใช้งานเครื่องคอมพิวเตอร์
- 11) ผู้ใช้งานห้ามทำการเก็บหรือสำรองข้อมูลส่วนบุคคลไว้ในเครื่องคอมพิวเตอร์ ของโรงพยาบาล เมืองจันทร์ หากเกิดปัญหาจำเป็นต้องมีการซ่อมบำรุงหรือมีการติดตั้งระบบปฏิบัติการใหม่ อาจมีการ ล้างข้อมูลในเครื่องคอมพิวเตอร์ทั้งหมด งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ จะไม่รับผิดชอบต่อการสูญหายของข้อมูลส่วนบุคคลนั้นๆ

## นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

### 1. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมว เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลแก่งหางแมวจึงเห็นสมควรกำหนดนโยบายและแนวทาง ปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความ มั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

### 2. วัตถุประสงค์

- 2.1 การจัดทำนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

- 2.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อ้างอิงตามมาตรฐาน HA และมีการปรับปรุงอย่างต่อเนื่อง
- 2.3 นโยบายและแนวทางปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- 2.4 เพื่อกำหนดมาตรฐานแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กร ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
- 2.5 นโยบายและแนวทางปฏิบัตินี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย 1 ครั้ง ต่อปี

### 3. นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลแก่งหางแมว

- 3.1 โรงพยาบาลแก่งหางแมวส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร
- 3.2 โรงพยาบาลแก่งหางแมวมีหน้าที่จำกัด ระบุ รับ เพิกถอนสิทธิหรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติ ในกรณีสำคัญงานเทคโนโลยีสารสนเทศ ทางกายภาพ ทรัพยากร การแพทย์ รายงานการฝ่าฝืนให้ต้นสังกัดหรือโรงพยาบาลเพื่อพิจารณาลงโทษ
- 3.3 โรงพยาบาลแก่งหางแมวสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อม ใช้งานอยู่เสมอ
- 3.4 โรงพยาบาลแก่งหางแมวสนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

### 4. องค์ประกอบของแนวทางปฏิบัติ

- 4.1 คำนิยาม
- 4.2 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- 4.3 การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
- 4.4 การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
- 4.4 การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
- 4.6 การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์
- 4.7 การรักษาความมั่นคงปลอดภัยของอีเมลล์
- 4.8 การรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

- 4.9 การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
- 4.10 ความมั่นคงปลอดภัยของการสำรองข้อมูล
- 4.11 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ แต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ (Objective) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กร มีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอก จะต้องปฏิบัติตามอย่างเคร่งครัด

## คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

**ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลแก่งหางแมว

**ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมวซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุม ดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

**งานเทคโนโลยีสารสนเทศทางการแพทย์** หมายถึง ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษา ระบบ คอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลแก่งหางแมว

**หัวหน้างานยุทธศาสตร์และสารสนเทศทางการแพทย์** หมายถึง ผู้บังคับบัญชา สูงสุดในการบริหารจัดการ ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมวและมีอำนาจตัดสินใจ เกี่ยวกับระบบสารสนเทศภายในโรงพยาบาลแก่งหางแมว

**การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมว

**มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

**ขั้นตอนการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

**แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

**ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งโรงพยาบาลเมืองจันทร์กำหนดไว้ดังนี้

- **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลแก่งหางแมว เช่น ผู้อำนวยการโรงพยาบาลแก่งหางแมว รองผู้อำนวยการโรงพยาบาล หัวหน้าตึก หัวหน้ากลุ่มงาน เป็นต้น
- **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจาก ผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่น เพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

- **เจ้าหน้าที่** หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการต่างๆ ของโรงพยาบาลแก่งหางแมว
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลแก่งหางแมว อนุญาต ให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ

ในการใช้ระบบตาม อำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

**ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบ คอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

**สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถ เข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

**ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

**ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

**ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

**ระบบอินเทอร์เน็ต (Internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

**ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของ หน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้าง สารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้ บริหารการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

**พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

-**พื้นที่ทำงานทั่วไป (General working area)** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

-**พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)** หมายถึง พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)

-**พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)** หมายถึง พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

**เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

**สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

**สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

**ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

**เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืน นโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าจะเกี่ยวข้องกับ ความมั่นคงปลอดภัย

**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

**จดหมายอิเล็กทรอนิกส์ (Email)** หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดย

ผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐาน ที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POPm และ IMAP เป็นต้น

**รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

**ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

## แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

### 1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่ เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ให้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

### 2. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

2.1 ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้ง และจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

2.2 ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.3 ให้งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ กำหนดมาตรการควบคุมการเข้า - ออก พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่าย ภายใน หน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

## แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

### 1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคล ที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่าย ของหน่วยงานได้อย่างถูกต้อง

### 2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมว

#### 2.1 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.1.1 โรงพยาบาลแก่งหางแมวกำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงาน หน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทาง การแพทย์

2.1.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

2.1.3 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

2.1.4 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

#### 2.2 การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.2.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลแก่งหางแมว กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น



- 2.2.2 ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างสม่ำเสมอ
- 2.2.3 ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้
- 2.2.3.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- 2.2.3.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน
- 2.2.3.3 ควรกำหนดให้ผู้ให้บริการตอบยืนยันการได้รับรหัสผ่าน
- 2.2.3.4 ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- 2.2.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- 2.2.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้อง กำหนดให้ รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ
- 2.2.4 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้
- 2.2.4.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- 2.2.4.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
- 2.2.4.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

2.2.4.4 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

2.2.4.5 ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

2.2.4.6 ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่ เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

### 2.3 การควบคุมการเข้าถึงระบบปฏิบัติการ

2.3.1 ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

2.3.2 ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่านของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

2.3.3 ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถอมหน้าจอ เพื่อทำการล๊อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ให้บริการ ต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

2.3.4 ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็น เวลานานมากกว่า 1 ชม.

### แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

#### 1. วัตถุประสงค์

เพื่อช่วยให้ผู้บริการได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์ และระบบเครือข่ายรวมทั้งทำความเข้าใจตลอดจนปฏิบัติตาม เพื่อเป็นการป้องกันทรัพยากร และข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อม ใช้งานอยู่เสมอ

#### 2. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายโรงพยาบาลแก่งหางแมว

กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

2.1 ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุม ป้องกัน การบุกรุกได้อย่างเป็นระบบ

- 2.2 ผู้ให้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ และต้องปฏิบัติตามนโยบายนี้ โดยเคร่งครัด
- 2.3 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงาน รับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างาน ประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผล กระทบต่อการกระทำของระบบและผู้ให้บริการอื่นๆ
- 2.4 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัด เส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย หลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)
- 2.5 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้
- 2.5.1 มีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ให้บริการให้สามารถใช้งาน เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
  - 2.5.2 ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยัง เครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ให้บริการสามารถใช้เส้นทางอื่นๆ
  - 2.5.3 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการ ตรวจสอบโปรแกรมประสงค์ร้าย (Malware) ด้วย
  - 2.5.4 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบ เครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ
  - 2.5.5 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการ บันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความ ถูกต้องของผู้ใช้บริการ
  - 2.5.6 เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมี การป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

- 2.5.7 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของ ระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็น ปัจจุบันอยู่เสมอ
- 2.5.8 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจาก ผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
- 2.5.9 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบ ในการ ดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่า ต่างๆ ของซอฟต์แวร์ ระบบ (Systems Software)
- 2.6 โรงพยาบาลแก่งหางแมว กำหนดมาตรการควบคุมการจับเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้
- 2.6.1 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความ ครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ใน การจับเก็บต้อง กำหนดขึ้นความลับในการเข้าถึงข้อมูล และผู้ดูแลระบบไม่ได้รับ อนุญาตในการแก้ไขข้อมูลที่เกิดขึ้นไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยี สารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย
- 2.6.2 กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึก การพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง
- 2.6.3 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ
- 2.6.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึง บันทึก เหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
- 2.7 โรงพยาบาลแก่งหางแมว กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่อง คอมพิวเตอร์ แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตาม แนวทาง ดังต่อไปนี้
- 2.7.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่าย และ เครื่อง คอมพิวเตอร์แม่ข่าย ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลาย

ลักษณะอักษร เพื่อขอ อนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ หัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

2.7.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

2.7.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการ อนุญาตจาก ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และ สารสนเทศทางการแพทย์

2.7.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความ จำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

2.7.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

### แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

#### 1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนด สิทธิของ ผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบ ในการปฏิบัติงานรวมทั้งมีการทบทวน สิทธิการ เข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแล ระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

#### 2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ต้องปฏิบัติ ดังนี้

2.1 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา ในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งานเพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

2.2 ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

2.3 ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

2.4 กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

2.4.1 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสมโดยจะต้องวาง Access

Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายในที่เป็น

Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption) 2.4.2

ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่อง คอมพิวเตอร์ที่

อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้  
เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

2.4.3 ให้เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point  
มาใช้งานและต้องปิดคุณสมบัติการ Auto Broadcast SSID ด้วย

2.4.4 ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration  
ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

2.4.4 ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected  
Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ  
(Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

2.4.6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้อุบัติการณ์หรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งาน  
ระบบเครือข่ายไร้สาย ในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของ  
หน่วยงาน

2.4.7 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ  
เครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่าย ไร้สาย  
และจัดส่งรายงานผลการตรวจสอบ ทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบ  
เครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้หัวหน้างานประกันสุขภาพ ยุทธศาสตร์และ  
สารสนเทศทางการแพทย์ ทราบทันที

### แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

#### 1. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆ ให้เหมาะสม ตามความ  
ต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ผู้ที่ควบคุมดูแล ต้องเป็น  
ผู้ดูแลระบบที่มีสิทธิในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคง ปลอดภัย  
ของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

#### 2. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของโรงพยาบาลแก่งหางแมว มีหน้าที่และ ความ  
รับผิดชอบที่ต้องปฏิบัติ ดังนี้

- 2.1 งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาลแก่งหางแมว
- 2.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
- 2.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์
- 2.4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User password)
- 2.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อ ที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง
- 2.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
- 2.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บ ข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อย กว่า 90 วัน
- 2.8 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ต การเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลแก่งหางแมว อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากหัวหน้างาน ประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ก่อน
- 2.9 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้อง กำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้อง ถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายชื่อเครื่องที่ให้บริการจริง และการกำหนดค่าการ ให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์ อักษร ต่อหัวหน้างานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ โดยต้องระบุข้อมูล ดังนี้
  - 2.9.1 หมายเลข Port ที่ต้องการขอให้เปิด
  - 2.9.2 หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
  - 2.9.3 วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ
  - 2.9.4 วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้
- 2.10 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุก ครั้งที่มีการเปลี่ยนแปลงค่า

- 2.11 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มี ความจำเป็นโดยจะต้องกำหนดเป็น กรณี ไป
- 2.12 โรงพยาบาล เมืองจันทร์ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาล เมืองจันทร์ หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มี ความ เสี่ยง ต่อความปลอดภัยของระบบ เทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข
- 2.13 ภายหลังจากการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศระเบียบของโรงพยาบาล เมืองจันทร์ หรือกฎหมาย หรืออาจจะทำให้เกิดความ เสี่ยง ด้านความ ปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศ ของหน่วยงาน ทางงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ จะยกเลิกการให้บริการทันที
- 2.14 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการ เกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

### แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์

#### (E-mail Policy)

#### 1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้ จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ กระทบการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่าย เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

#### 2. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของโรงพยาบาลแก้งหางแมวมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

- 2.1 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ โรงพยาบาลแก้งหางแมว
- 2.2 เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที



- 2.3 ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้
- 2.4 ควรเปลี่ยนรหัสผ่านทุก 3 - 6 เดือน
- 2.5 ไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
- 2.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของโรงพยาบาลแก่งหางแมวผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลแก่งหางแมวเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ ของโรงพยาบาลแก่งหางแมวขัดข้อง และได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
- 2.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง
- 2.8 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของโรงพยาบาลแก่งหางแมว หรือก่อให้เกิดความเสียหายต่อโรงพยาบาลแก่งหางแมว
- 2.9 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลแก่งหางแมว เพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของโรงพยาบาลแก่งหางแมว ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของโรงพยาบาลแก่งหางแมว
- 2.10 การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- 2.11 การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน 10 เมกะไบต์
- 2.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

### แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

#### (Internet Security Policy)

#### 1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของโรงพยาบาลแก่งหางแมว ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเทอร์เน็ต เป็นไปอย่างปลอดภัย และมีประสิทธิภาพ

## 2. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

ผู้ใช้งานเครือข่ายอินเทอร์เน็ตของโรงพยาบาลแก่งหางแมวมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

- 2.1 การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ หรือทำการสมัครผ่านระบบอินเทอร์เน็ตของโรงพยาบาลแก่งหางแมว โดยรอการตรวจสอบตัวบุคคลและอนุมัติการใช้งานโดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลแก่งหางแมว สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากหัวหน้างานเทคโนโลยีและสารสนเทศ ทางทางการแพทย์ หรือผู้ที่ได้รับมอบหมาย
- 2.2 ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่น่าจะก่อให้เกิดความเสียหายให้กับหน่วยงาน
- 2.3 ผู้ใช้งานอินเทอร์เน็ต พึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่าน ระบบเครือข่าย
- 2.4 ผู้ใช้งานต้องไม่ให้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ
- 2.4 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต
- 2.6 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้แจ้งผู้ที่ได้รับมอบหมาย
- 2.7 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ Facebook โปรแกรมอื่นๆ ที่มีลักษณะคล้ายกัน ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ
- 2.8 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควร (Logout) ออกจากระบบทุกครั้ง

## นโยบายความมั่นคงปลอดภัยของการตรวจจัดการบุกรุก

### (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

#### 1. วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัย ของเครือข่าย เพื่อป้องกันทรัพยากรระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในโรงพยาบาล เมืองจันทร์ให้มีความมั่นคงปลอดภัย

#### 2. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

2.1 IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของโรงพยาบาลแก่งหางแมวและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง 2.2 ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ต หรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

2.3 ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และเปิดให้บริการ

2.4 โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

2.5 มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

2.6 มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งานกิจกรรม และปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำโดยผู้ดูแลระบบ

2.7 IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ

2.8 เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

2.9 พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การ โจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จ และไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

2.10 พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน 1 ชั่วโมงที่ตรวจพบ

2.11 การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า 90 วัน

2.12 มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจ เกิดอีกในอนาคต และดำเนินการตามแผน

2.13 โรงพยาบาลแก่งหางแมว มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

2.14 ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลแก่งหางแมว การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2440 หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาลแก่งหางแมว จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

### นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

#### 1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิด ความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

#### 2. แนวทางปฏิบัติในการสำรองข้อมูล

2.1 จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูล ระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2.2 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบ ซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศ แต่ละระบบ

2.3 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดง ถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรอง ซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการ ทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

2.4 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายใน ระยะเวลาที่เหมาะสม

### นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

#### 1. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถ นำไปปฏิบัติได้อย่างถูกต้อง

#### 2. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- 2.1 จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
- 2.2 จัดสัมมนาเพื่อเผยแพร่แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง โดยอาจจัดรวมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้
- 2.3 ประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
- 2.4 ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจ ความต้องการของผู้ใช้บริการ

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการอำนวยการและกำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลแก่งหางแมว เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทราบ และถือปฏิบัติอย่างเคร่งครัดต่อไป

(นพ.อภิสิทธิ์ คุจวรรณ)

ผู้อำนวยการโรงพยาบาลแก่งหางแมว



## โรงพยาบาลแก่งหางแมว

### ประกาศนโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศเพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมว ดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัย ต่างๆ โรงพยาบาลแก่งหางแมว จึงกำหนดนโยบาย ดังนี้

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

ประกาศ ณ วันที่ 28 เมษายน พ.ศ.2566

(นพ.อภิสิทธิ์ คุจวรรณ)

ผู้อำนวยการโรงพยาบาลแก่งหางแมว



## โรงพยาบาลแก่งหางแมว

### ประกาศระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลแก่งหางแมวดำเนินไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลแก่งหางแมวจึงกำหนดระเบียบปฏิบัติ ดังนี้

ข้อ	ระเบียบปฏิบัติ
1	ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) โปรแกรม HOSxP ทุกๆ 30 วันหรือทุกครั้งที่มีการแจ้งเตือน ให้เปลี่ยนรหัสผ่าน
2	ผู้ใช้งานต้องกำหนดรหัสผ่าน โปรแกรม HOSxP ให้มี 6 ตัวขึ้นไป ประกอบด้วยตัวเลขและตัวอักษร
3	ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีของผู้ใช้งาน (User Account) และรหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (User Account) ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม
4.	ในการเข้าสู่ระบบเพื่อใช้งาน โปรแกรม HOSxP ของสหสาขาวิชาชีพต่าง ๆ ที่เกี่ยวข้องกับการรักษา ผู้ป่วย ให้สามารถเข้าสู่ระบบได้เฉพาะที่กำหนด ในตารางการปฏิบัติหน้าที่เท่านั้น ยกเว้นแต่มีเหตุฉุกเฉินที่จำเป็น
5	ห้ามนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (เช่น ปริ้นท์เตอร์, อุปกรณ์กระจายสัญญาณต่างๆ ฯลฯ) มาต่อกับระบบคอมพิวเตอร์หรือระบบเครือข่ายของโรงพยาบาลโดยไม่ได้รับอนุญาต
6	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัปเดตซอฟต์แวร์อื่นใดในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด
7	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น

ข้อ	ระเบียบปฏิบัติ
8	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CDRom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
9	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
10	ห้ามนำเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น <ul style="list-style-type: none"><li>- Facebook</li><li>- Line</li><li>- tiktok</li><li>- instagram</li><li>- Website หรือ โปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยให้ยินยอม เผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่มและลบข้อมูลผู้ป่วย ทุกครั้งที่ปรึกษาเสร็จ</li></ul>
11	ห้ามนำเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง

ประกาศ ณ วันที่ 28 เมษายน พ.ศ.2566

(นพ.อภิสิทธิ์ คุจวรรณ)

ผู้อำนวยการโรงพยาบาลแก่งหางแมว






## ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

### ข้อควรปฏิบัติ

1. ควรทำการเปลี่ยนรหัสผ่านทุกๆ 30 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
2. รหัสผ่านต้องมีความยาวอย่างน้อย 6 ตัว ประกอบด้วยตัวเลขและตัวอักษร
3. เก็บรักษาข้อมูลบัญชีของผู้ใช้งานและรหัสผ่าน ห้ามให้ผู้อื่นใช้

### ข้อห้าม

	ห้ามผู้ใดนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง(เช่นปริ้นเตอร์,อุปกรณ์กระจาย สัญญาณต่างๆ ฯลฯ) มาเชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาล โดยไม่ได้รับอนุญาต
	ห้ามผู้ใช้งานทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตมาติดตั้งหรือการอัปเดตซอฟต์แวร์ ใดๆ ในโรงพยาบาล นอกเหนือจากที่ผู้ดูแลระบบกำหนด
	ห้ามเปิดหรือใช้งานโปรแกรมเพื่อความบันเทิงส่วนบุคคล ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง เล่นเกมส์ เป็นต้น
	ห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก (Flash Drive, External Drive ,CD-Rom) กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
	ห้ามเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆ ต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาล โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ
	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line, tiktok, instagram ,Website หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเทอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์ อักษรจากผู้ป่วยให้ยินยอมเผยแพร่ได้ กรณีใช้ Line ในการปรึกษาให้ส่งโดยตรงส่วนตัว ห้ามส่งปรึกษาในกลุ่ม และลบข้อมูลผู้ป่วยทุกครั้งที่ปรึกษาเสร็จ
	ห้ามเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบโดยไม่ขออนุญาตจากแพทย์หรือผู้รับผิดชอบโดยตรง