ประกาศโรงพยาบาลเชียงกลาง
เรื่อง นโยบายแผนการปฏิบัติงานและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

เพื่อให้การดำเนินการใดๆ ต่อระบบสารสนเทศโรงพยาบาลเชียงกลาง เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจส่งผลทำให้ระบบสารสนเทศไม่สามารถดำเนินงานต่อไปได้จากภัยคุกคามด้านเครือข่ายต่างๆ ซึ่งอาจส่งผลทำให้เกิดความเสียหายต่อระบบสารสนเทศโรงพยาบาลเชียงกลาง มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจนและเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และกฎหมายอื่นๆ ที่เกี่ยวข้อง โรงพยาบาลเชียงกลางจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของโรงพยาบาลเชียงกลางทำให้ดำเนินงานได้อย่างปลอดภัย และต่อเนื่อง

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลเชียงกลางได้รับทราบและถือปฏิบัติตามนโยบาย

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริการ เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลเชียงกลาง ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะมีการทบทวนนโยบายปีละ ๑ ครั้ง

อาศัยอำนาจตามในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โรงพยาบาลเชียงกลางจึงกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลเชียงกลาง ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลเชียงกลาง” เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลเชียงกลาง กำหนดประเด็นสำคัญดังต่อไปนี้

๒.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๒.๑.๑ ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๒.๑.๒ นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ

๒.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๒.๑.๔ กำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๒.๑.๕ กำหนดให้ทบทวนและปรับปรุงนโยบายปีละ ๑ ครั้ง

๒.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบายประกอบด้วย ๖ ส่วน คือ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงผู้ใช้งาน

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

แนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

แนวปฏิบัติในด้านรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบ

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลเชียงกลาง พ.ศ.๒๕๖๖ ซึ่งกำหนดผู้รับผิดชอบตาม ซึ่งสาระสำคัญ มีดังต่อไปนี้

(๑) นโยบายควบคุมการเข้าถึง เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตกำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

๑) ผู้อำนวยการโรงพยาบาลเชียงกลาง

๒) หัวหน้ากลุ่มงานประกันสุขภาพและสารสนเทศทางการแพทย์

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติ ดังต่อไปนี้

๑) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

๒) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย

๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๔) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น

(๒) นโยบายเกี่ยวกับการสำรองและการกู้คืนข้อมูล กำหนดให้มีการจัดทำระบบสำรองข้อมูลสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและกำหนดให้จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในการให้บริการสารสนเทศกำหนดผู้รับผิดชอบตามนโยบาย ดังนี้

๑) ผู้อำนวยการโรงพยาบาลเชียงกลาง

๒) หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

โดยมีมาตรการควบคุมการเข้าถึงตามแนวปฏิบัติ ดังต่อไปนี้

๑) แนวปฏิบัติการสำรองและการกู้คืนข้อมูล

๒) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๓ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลเชียงกลางเกิดความเสียหาย หรือได้รับอันตรายจากภัยคุกคามทางด้านต่างๆ ผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย ละเว้น หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของโรงพยาบาลเชียงกลางเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๔ ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้าย ประกาศนี้

ข้อ ๕ ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๖

(นายอภิชิต สถาวรวิวัฒน์)
นายแพทย์ชำนาญการพิเศษ ปฏิบัติหน้าที่
ผู้อำนวยการโรงพยาบาลเชียงกลาง

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลเชียงกลาง

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดหลักเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจ

๓. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ (๑) ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ หรือเจ้าของข้อมูล หรือเจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ (๒) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลบ้านด่าน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้ากลุ่มงานของหน่วยงาน และหัวหน้าศูนย์คอมพิวเตอร์พิจารณา

ข้อ (๓) ผู้ดูแลระบบ จะต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

๑.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๑.๒ กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลเชียงกลาง จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้ากลุ่มงานของหน่วยงาน และหัวหน้าศูนย์คอมพิวเตอร์พิจารณา

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๒.๑ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๒.๒ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายรายแรงที่สุด
- ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายร้ายแรง
- ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๓ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหารโรงพยาบาลเชียงกลาง
- ระดับชั้นสำหรับผู้ดูแลระบบของโรงพยาบาลเชียงกลาง
- ระดับชั้นสำหรับเจ้าหน้าที่ของโรงพยาบาลเชียงกลาง
- ระดับชั้นสำหรับบุคคลทั่วไปมาใช้บริการของโรงพยาบาลเชียงกลาง

ข้อ (๔) ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของโรงพยาบาลเชียงกลาง และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ (๕) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ (๖) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ (๗) กำหนดระยะเวลาการเข้าถึงระบบสารสนเทศ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงผู้ใช้งาน (User Access Management)

ข้อ (๘) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูและระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ (๙) ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ (๑๐) ผู้ดูแลระบบ ต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ข้อ (๑๑) การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้และรหัสผ่านต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๔) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) ในกรณีที่มีความจำเป็นต้องใช้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยมีการกำหนดระยะเวลาในการใช้งานและระงับการใช้งานทันทีเมื่อพ้นกำหนดระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษ

ข้อ (๑๒) ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(๑) ควบคุมการเข้าถึงชั้นตุละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) กำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการส ารองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๖) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ข้อ (๑๓) ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศของโรงพยาบาลเชียงกลาง พิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่เชื่อมโยงเข้าด้วยกัน เช่น ระหว่างโรงพยาบาลเชียงกลางกับหน่วยงานที่ขอมาเชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคคลใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ (๑๔) การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้งาน และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามท าการเผยแพร่แจกจ่าย รหัสผ่าน

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งประกอบด้วยตัวเลข ตัวอักษร และตัวอักษรพิเศษ

(๓) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๕) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคล ไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๖) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๗) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ (๑๕) การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากล

ข้อ (๑๖) การกระทำใดๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน อันมีกฎหมายกำหนดให้ เป็นความรับผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ (๑๗) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของโรงพยาบาลเชียงกลางและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากการใส่รหัสผิดเกิน ๓ ครั้งก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

ข้อ (๑๘) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลเชียงกลางหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ (๑๙) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของโรงพยาบาลเชียงกลางห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลเชียงกลาง

ข้อ (๒๐) ผู้ใช้งานมีส่วนร่วมในการดุแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลเชียงกลาง และข้อมูลของผู้มารับบริการ หากเกิดการสูญเสีย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ (๒๑) มาตรการควบคุมการเข้า-ออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องมาติดต่อผู้ดูแลระบบเพื่อขออนุญาตเข้าไปยังห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ทุกครั้ง ผู้ดูแลระบบจะกำกับดูแลตลอดเวลาเมื่อหน่วยงานภายนอกอยู่ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ต้องมาติดต่อผู้ดูแลระบบเพื่อขออนุญาตเข้าไปยังห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ทุกครั้ง ผู้ดูแลระบบจะกำกับดูแลตลอดเวลาเมื่อหน่วยงานภายนอกอยู่ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

ข้อ (๒๒) ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของโรงพยาบาลเชียงกลาง ต้องได้รับอนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์และปฏิบัติตามแนวปฏิบัตินี้โดยเคร่งครัด

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ (๒๓) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลเชียงกลาง (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก เป็นต้น

ข้อ (๒๔) กำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูก
กำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

(๔) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งานและรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของโรงพยาบาลเชียงกลาง ร่วมกัน

(๕) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่ได้อยู่ที่หน้าจอเป็นเวลานาน

(๖) ซอฟต์แวร์ที่โรงพยาบาลเชียงกลาง จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานท าการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อไปใช้งานที่อื่น

(๗) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเชียงกลาง เพื่อประโยชน์ทางการค้า(๘) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปแบบไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๙) ห้ามผู้ใช้งานของโรงพยาบาลเชียงกลาง ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาต

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ (๒๕) ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกโรงพยาบาลเชียงกลาง เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ (๒๖) การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีกาเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำมาส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากการประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น