๓.

การบริหารความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ (SECURITY MANAGEMENT)

คำนำ

แผนบริหารจัดการความปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลอุดรธานี ประจำปี ๒๕๖๖ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศในการจัดทำแผนนโยบายและระเบียบปฏิบัติในความปลอดภัยและกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันและรักษาความปลอดภัยโดยมุ่งหวังให้บรรลุผลตามเป้าประสงค์ของหน่วยงาน เนื่องจากความปลอดภัยจะช่วยลดผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทปัญหาและโครงสร้างที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความปลอดภัยเหล่านั้นให้อยู่ในระดับที่องค์กรสามารถรองรับได้และทำให้การปฏิบัติงานมีประสิทธิภาพมากยิ่งขึ้นโรงพยาบาลอุดรธานี หวังเป็นอย่างยิ่งว่าแผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

ทั้งนี้โรงพยาบาลอุดรธานีจะนำแผนการจัดการความปลอดภัยไปใช้เพื่อลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ต่อไป

สารสนเทศทางการแพทย์ (ศูนย์คอมพิวเตอร์)

หน้า

การจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๑

แผนบริหารความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

การจัดการความมั่นคงและปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลอุดรธานี มีวัตถุประสงค์เพื่อทำให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทำงานได้อย่างราบรื่น ไม่หยุดชะงัก หรือสะดุดติดขัด โดยหัวใจหลักคือ การสร้างระบบจัดการความมั่นคงปลอดภัย (Security Management System) ให้มั่นใจว่ามาตรการต่างๆที่เกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยดำเนินไปได้อย่างต่อเนื่องและยั่งยืน

การจัดการความมั่นคงปลอดภัยเป็นกิจกรรรมที่สัมพันธ์กับการจัดการความเสี่ยง เพราะกิจกรรมจัดการความเสี่ยงเป็นส่วนหนึ่งของระบบความมั่นคงปลอดภัย แต่ในรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศของโรงพยาบาล (HA IT) ได้แยกจากการจัดการความเสี่ยงไว้เป็นหัวข้อหลักอีกหัวข้อหนึ่ง เพื่อให้เห็นว่า การจัดการความเสี่ยงเป็นกิจกรรมที่ต้องให้ความสำคัญโดยเฉพาะในระยะเริ่มต้นของการพัฒนาคุณภาพ

การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล สามารถแบ่งออกได้เป็น ๓ ระดับ ตามรูปแบบการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาลอุดรธานี

ระดับที่ ๑ การเริ่มต้นจัดการให้เกิดระบบ

ระดับที่ ๒ ระบบเกิดขึ้นและเริ่มต้นการขับเคลื่อน

ระดับที่ ๓ ระบบที่ขับเคลื่อนแล้ว เสริมให้แข็งแกร่งและมั่งคงยั่งยืน

วัตถุประสงค์

๑. การปกป้องข้อมูลทางการแพทย์: วัตถุประสงค์หลักของความปลอดภัยของเทคโนโลยีสารสนเทศในโรงพยาบาลคือการปกป้องข้อมูลทางการแพทย์ของผู้ป่วย ให้ได้รับการเก็บรักษาและใช้งานอย่างปลอดภัย โดยป้องกันการเข้าถึงและการแก้ไขข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต การใช้เทคนิคเข้ารหัสลับข้อมูลและการใช้ระบบควบคุมการเข้าถึงเพื่อรักษาความลับและความเป็นส่วนตัวของข้อมูล

๒. การรักษาความลับและความเป็นส่วนตัว: เทคโนโลยีสารสนเทศในโรงพยาบาลต้องมีวัตถุประสงค์ในการรักษาความลับและความเป็นส่วนตัวของข้อมูลผู้ป่วย เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่เหมาะสมและการละเมิดความเป็นส่วนตัวของผู้ป่วย นอกจากนี้ ยังควรมีการสร้างความตระหนักในบุคลากรทางการแพทย์เกี่ยวกับความสำคัญของความเป็นส่วนตัวของข้อมูลและการปฏิบัติตามนโยบายและข้อกำหนดที่เกี่ยวข้อง

๓. ความพร้อมใช้งานและประสิทธิภาพ: วัตถุประสงค์เพื่อความปลอดภัยของเทคโนโลยีสารสนเทศในโรงพยาบาลคือการให้บุคลากรทางการแพทย์สามารถเข้าถึงข้อมูลที่จำเป็นและสามารถใช้งาน

ระบบสารสนเทศได้อย่างรวดเร็วและมีประสิทธิภาพ โดยให้ระบบเทคโนโลยีสารสนเทศมีการออกแบบที่ใช้งานง่าย และมีประสิทธิภาพในการส่งเสริมกระบวนการทางการแพทย์ในโรงพยาบาล

๔. การรับรู้และการตรวจสอบ: เทคโนโลยีสารสนเทศในโรงพยาบาลควรมีวัตถุประสงค์ในการสร้างความรับรู้และการตรวจสอบความปลอดภัย โดยประเมินและตรวจสอบระบบที่เกี่ยวข้องเพื่อตรวจหาช่องโหว่และปัญหาที่อาจเกิดขึ้น และเพื่อให้มีการปรับปรุงและป้องกันอย่างต่อเนื่อง

ผลที่คาดว่าจะได้รับ

๑. การป้องกันการเข้าถึงข้อมูลที่ไม่เหมาะสม: การใช้มาตรการความปลอดภัยที่เหมาะสมจะช่วยลดความเสี่ยงในการเข้าถึงข้อมูลทางการแพทย์โดยบุคคลที่ไม่ได้รับอนุญาต ทำให้ข้อมูลที่เกี่ยวข้องกับผู้ป่วยนั้นปลอดภัยและไม่ถูกนำไปใช้อย่างไม่เหมาะสมหรือเกิดความเสียหาย

๒. ความละเอียดและความถูกต้องของข้อมูลทางการแพทย์: การรักษาความปลอดภัยของเทคโนโลยีสารสนเทศในโรงพยาบาลช่วยให้ข้อมูลทางการแพทย์มีความถูกต้องและเป็นปัจจุบัน ทำให้แพทย์และบุคลากรทางการแพทย์สามารถใช้ข้อมูลเหล่านี้ในการวินิจฉัย รักษา และดูแลผู้ป่วยได้อย่างมีประสิทธิภาพ

๓. ประสิทธิภาพในการดำเนินงาน: การใช้เทคโนโลยีสารสนเทศที่มีความปลอดภัยในโรงพยาบาลช่วยลดเวลาและค่าใช้จ่ายในกระบวนการทางการแพทย์ นอกจากนี้ยังช่วยเพิ่มประสิทธิภาพของการจัดการข้อมูลและกระบวนการทางการแพทย์ ทำให้โรงพยาบาลสามารถให้บริการที่ดีกว่าและออกแบบกระบวนการที่มีประสิทธิภาพมากยิ่งขึ้น

๔. ความเชื่อมั่นของผู้ป่วย: การให้ความสำคัญกับความปลอดภัยของข้อมูลแพทย์ในโรงพยาบาลช่วยสร้างความเชื่อมั่นให้กับผู้ป่วย ทำให้พวกเขามั่นใจว่าข้อมูลส่วนตัวของพวกเขาจะได้รับการรักษาและปกป้องอย่างเหมาะสม ซึ่งอาจส่งผลในการเพิ่มความพึงพอใจและความพึงพอใจของผู้ป่วยในการบริการทางการแพทย์ที่ได้รับ รวมถึงการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศในโรงพยาบาลยังช่วยลดความเสี่ยงทางกฎหมาย การละเมิดความเป็นส่วนตัว และการขาดความไว้วางใจจากผู้ป่วยหรือสาธารณชนทั่วไป ซึ่งส่งผลต่อภาพลักษณ์และชื่อเสียงของโรงพยาบาลได้เช่นกัน

ความหมายของการบริหารความปลอดภัย

ความปลอดภัย(Security) หมายถึง สภาวะที่มีความเสถียรและปลอดภัยจากความเสี่ยงหรืออันตรายที่อาจเกิดขึ้น ซึ่งสามารถป้องกันความเสียหายหรือการบาดเจ็บได้ ในบริบทต่างๆ ความปลอดภัยสามารถเกี่ยวข้องกับด้านต่างๆ

นโยบาย(Policy) หมายถึง แนวปฏิบัติหรือแนวทางที่กำหนดขึ้นเพื่อชี้นำการดำเนินงานและการตัดสินใจในองค์กรหรือสถาบันต่างๆ นโยบายเป็นแนวทางและแนวปฏิบัติที่สร้างมาเพื่อให้ความชัดเจนและเข้าใจวัตถุประสงค์ และวิสัยทัศน์ขององค์กรในการดำเนินงาน นโยบายส่วนใหญ่ถูกกำหนดขึ้นโดยระดับบริหารสูงสุดในองค์กร เพื่อให้เกิดการปฏิบัติที่สอดคล้องและเป็นระเบียบ รวมถึงช่วยสร้างความเข้าใจและการปฏิบัติของบุคลากรที่เกี่ยวข้องในองค์กร

ระเบียบปฏิบัติ(Regulation) หมายถึง ชุดข้อกำหนดหรือกฎระเบียบที่กำหนดขึ้นเพื่อกำกับและควบคุมการดำเนินงานหรือพฤติกรรมที่เกี่ยวข้องในองค์กรหรือสถาบันต่างๆ ระเบียบปฏิบัติมักจะระบุ

ข้อกำหนดและมาตรการที่ต้องปฏิบัติเพื่อให้การดำเนินงานเป็นไปอย่างเรียบร้อย สอดคล้องกับนโยบายและเป้าหมายขององค์กร

ความปลอดภัยทางไซเบอร์(Cyber Security) หมายถึง การปกป้องและรักษาความปลอดภัยของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ซึ่งรวมถึงการป้องกันและการตอบสนองต่อความเสี่ยง อันตราย และการละเมิดความเป็นส่วนตัวที่อาจเกิดขึ้นในโลกดิจิทัล ความปลอดภัยทางไซเบอร์เกี่ยวข้องกับการป้องกันและการรักษาความลับ ความครบถ้วน ความเข้าถึงข้อมูลที่ถูกต้อง และการรักษาความเสถียรของระบบ เพื่อป้องกันการบุกรุก การโจมตี การดักรับข้อมูล หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ขอบเขตการดำเนินการ

บริหารจัดการความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของโรงพยาบาลอุดรธานี

ระยะเวลาดำเนินการ

ลำดับที่	กิจกรรม	ปีงบปะมาณ ๒๕๖๖						หน่วยงานรับผิดชอบ
		เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑	ศึกษาข้อมูลในการจัดทำ แผนบริหารการจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศ							สารสนเทศทางการแพทย์
๒	จัดทำระเบียบปฏิบัติความปลอดภัยด้านเทคโนโลยีสารสนเทศ							ศูนย์คอมพิวเตอร์
๓	จัดทำนโยบายด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศ							สารสนเทศทางการแพทย์
๔	ประเมินความรับรู้ระเบียบด้านปฏิบัติความมั่นคงปลอดภัย							สารสนเทศทางการแพทย์

ตารางที่ ๑ ตารางแสดงระยะเวลาดำเนินการ

ส่วนที่ ๒

หัวข้อของนโยบายและระเบียบปฏิบัติทางด้านเทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติเทคโนโลยีสารสนเทศในโรงพยาบาลเป็นเอกสารที่กำหนดข้อกำหนดและมาตรการที่จำเป็นต้องปฏิบัติเพื่อรักษาความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นในการใช้เทคโนโลยีสารสนเทศ โดยเฉพาะในบริบทของโรงพยาบาลที่มีข้อมูลทางการแพทย์และข้อมูลสำคัญอื่นๆ ที่ต้องรักษาความลับและความปลอดภัย

ระเบียบปฏิบัติเทคโนโลยีสารสนเทศในโรงพยาบาลอุดรธานีสามารถรวมถึงข้อกำหนดและมาตรการดังต่อไปนี้

หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงสารสนเทศ (Access Control)
๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
๔. การบริหารจัดการสินทรัพย์ (Assets Management)
๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)
๘. การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware)
๙. การปฏิบัติงานจากภายนอกสานักงาน (Teleworking)
๑๐. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)
๑๑. การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)
๑๒. การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)
๑๓. การควบคุมการใช้อินเทอร์เน็ต (Internet)
๑๔. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
๑๕. คอมพิวเตอร์พกพา หรือ Notebook Computer
๑๖. การตรวจจับการบุกรุก (Intrusion Detection System Intrusion Prevention System Policy)
๑๗. การติดตั้งและกาหนดค่าของระบบ (System Installation and Configuration)
๑๘. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

หมวดที่ ๒ ระเบียบการรักษาความปลอดภัยฐานข้อมูล

๑. การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

๒. การสำรองข้อมูล (Backup)

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยง

๑. การตรวจสอบและประเมินความเสี่ยง

๒. ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

หมวดที่ ๘ การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก

นโยบายเทคโนโลยีสารสนเทศในโรงพยาบาลเป็นเอกสารที่กำหนดแนวทางและกรอบแนวทางในการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนและปรับปรุงการดำเนินงานทางการแพทย์และการบริการสุขภาพในโรงพยาบาล นโยบายเป็นแนวทางที่ชัดเจนและสอดคล้องกับนโยบายและวัตถุประสงค์ขององค์กรหรือสถาบันทางการแพทย์ และให้แนวทางสำหรับการดำเนินงานทางเทคโนโลยีสารสนเทศที่มีความปลอดภัยและประสิทธิภาพ

นโยบายเทคโนโลยีสารสนเทศในโรงพยาบาลอาจประกอบด้วยข้อกำหนดและมาตรการต่อไปนี้

๑. การรักษาความลับและความเป็นส่วนตัวของข้อมูล: นโยบายควรระบุถึงความสำคัญของการรักษาความลับและความเป็นส่วนตัวของข้อมูลทางการแพทย์และข้อมูลสำคัญอื่นๆ ที่เกี่ยวข้อง รวมถึงมาตรการที่เกี่ยวข้องเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการละเมิดความเป็นส่วนตัว

๒. การใช้เทคนิคเข้ารหัสลับข้อมูล: นโยบายควรระบุถึงการใช้เทคนิคเข้ารหัสลับข้อมูลทางการแพทย์และข้อมูลสำคัญอื่นๆ เพื่อปกป้องข้อมูลจากการถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต

๓. การบริหารจัดการระบบเทคโนโลยีสารสนเทศ: นโยบายควรระบุถึงการบริหารจัดการระบบเทคโนโลยีสารสนเทศในโรงพยาบาล เช่น การจัดการสิทธิ์การเข้าถึงข้อมูล การบำรุงรักษาระบบ และการดำเนินการเพื่อรักษาความเสถียรของระบบ

๔. การฝึกอบรมและการประเมินผล: นโยบายควรระบุถึงความจำเป็นในการฝึกอบรมบุคลากรทางการแพทย์และบุคลากรที่เกี่ยวข้องเกี่ยวกับเทคโนโลยีสารสนเทศและความปลอดภัย รวมถึงการประเมินผลเพื่อให้แน่ใจว่าบุคคลากรมีความรู้และความเข้าใจเพียงพอในการปฏิบัติตามมาตรการความปลอดภัยที่กำหนด

๕. การสำรวจและการตรวจสอบ: นโยบายควรระบุถึงการดำเนินการสำรวจและการตรวจสอบเพื่อตรวจสอบความปลอดภัยของระบบสารสนเทศที่ใช้ในโรงพยาบาล รวมถึงการตรวจสอบระบบการเข้าถึงข้อมูล การตรวจสอบระบบการสำรองข้อมูล และการตรวจสอบระบบการตรวจสอบความปลอดภัย

๖. *การปฏิบัติตามกฎหมายและการควบคุม: นโยบายควรระบุถึงความจำเป็นในการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศในโรงพยาบาล เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล และการปฏิบัติตามมาตรฐานและแนวทางที่รัฐบาลหรือองค์กรทางการแพทย์กำหนด*