นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

พ.ศ. ๒๕๖๖

ประกาศ ณ วันที่ ๑๘ ธันวาคม พ.ศ. ๒๕๖๖

(นายสมชาย แพรพิรุณ)

รองผู้อำนวยการด้านพัฒนาระบบบริการและสนับสนุนบริการสุขภาพ

ปฏิบัติราชการแทน ผู้อำนวยการโรงพยาบาลเฉลิมพระเกียรติ

สมเด็จพระเทพรัตราชสุดาฯ สยามบรมราชกุมารี ระยอง

๑. แนวนโยบายและแผน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ
สยามบรมราชกุมารี ระยอง พ.ศ. ๒๕๖๖

โดยประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ดังนั้น

คณะกรรมการพัฒนาระบบสารสนเทศและศูนย์ข้อมูลโรงพยาบาล (Data Center) ของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัดและเพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลฯเป็นไปอย่างเหมาะสมเกิดประสิทธิภาพสูงสุด มีความมั่นคงปลอดภัยด้านสารสนเทศและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาลฯ นั้น

โดยมีวัตถุประสงค์ ดังนี้

๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้มีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ
๒. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
๓. นโยบายนี้ต้องเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
๔. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด
๕. เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆเข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ
๖. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

ข้อ ๑ คำนิยาม

“โรงพยาบาล” หมายถึง โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

“มาตรการ” หมายถึง วิธีการที่ตั้งเป็นกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเป็นต้น

“วิธีปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถ บรรลุเป้าหมายได้ง่ายขึ้น

“ผู้บริหาร” หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาล

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการ ฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานราชการ และลูกจ้างชั่วคราว

“สารสนเทศ” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปแบบของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได้ เช่น ระบบแลน (LAN) ระบบอินเตอร์เน็ต (Internet)

- **ระบบแลน (LAN)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูล และสารสนเทศภายในหน่วยงาน
- **ระบบอินเตอร์เน็ต (Internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบ เครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

“ระบบเทคโนโลยีสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหารการสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูลและสารสนเทศ เป็นต้น

“การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ” หมายถึง การตรวจสอบ การอนุมัติ และการ กำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้

“เครื่องเซิร์ฟเวอร์ (Server)” หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรม คอมพิวเตอร์ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์หรือโปรแกรม คอมพิวเตอร์ที่เป็นลูกข่ายในระบบเครือข่าย

“อุปกรณ์ UPS” หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการไฟฟ้ามีปัญหา เช่น ไฟตก ไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้น โดยที่อุปกรณ์ UPS จะจ่ายพลังงานออกมาอย่างต่อเนื่องและมีคุณภาพในทุกสถานการณ์ ตลอดจนเป็นอุปกรณ์ที่ช่วยป้องกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟ้า และอุปกรณ์อิเล็กทรอนิคส์ (โดยเฉพาะคอมพิวเตอร์และอุปกรณ์เชื่อมต่อ) รวมถึงมีหน้าที่ในการจ่ายพลังงานไฟฟ้าสำรองจากแบตเตอรี่ให้แก่อุปกรณ์ไฟฟ้าหรือ คอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า

“ซอฟต์แวร์ (Software)” หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงานซอฟต์แวร์ จึงหมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหล่านี้เรียงกันเป็น โปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียงการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลข ตัวอักษร รูปภาพ หรือแม้แต่เป็นเสียงพูดก็ได้ โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์ เพราะเป็นลำดับขั้นตอนการทำงานของ คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน ซอฟต์แวร์จึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้

“ไวรัสคอมพิวเตอร์” หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสเป็นแค่โปรแกรมหนึ่งการที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้ขึ้นอยู่กับประเภทของไวรัสแต่ละตัว ปกติผู้ใช้มักจะไม่ทราบว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสนั้นๆขึ้นมาทำงานแล้ว

“เวชระเบียน” หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งที่เป็น เอกสารและข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

นโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศของหน่วยงานครอบคลุมทุกระดับ

วัตถุประสงค์

๑.เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒.เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์และการมอบอำนาจ

๓.เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

๑.๒.๑ การควบคุมการเข้าถึงห้องระบบปฏิบัติการระบบเครือข่าย (Access Control)

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนการเข้า-ออก ดังนี้

๑.๑ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบโดยใช้เครื่องสแกนลายนิ้วมือบันทึกในการเข้า-ออกห้องปฏิบัติการ

๑.๒ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้า-ออก ที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์(Application) จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

๑.๒.๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๑. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับ อนุญาตจากผู้รับผิดชอบ เจ้าของข้อมูล เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ ๒. บุคคลภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารที่ได้รับมอบหมาย

ข้อ ๓. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

๓.๑กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

๓.๒กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

๓.๒.๑ อ่านอย่างเดียว

๓.๒.๒ สร้างข้อมูล

๓.๒.๓ ป้อนข้อมูล

๓.๒.๔ แก้ไข

๓.๒.๕ อนุมัติ

๓.๒.๖ ไม่มีสิทธิ

ข้อ ๔. กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหาร จัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

ข้อ ๕. ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาต เป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๖. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบ ดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๖.๑ จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูล ยุทธศาสตร์ และคำรับรองข้อมูลบุคลากรข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูล ผู้ป่วย ข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

๖.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๖.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะ ก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้
- จัดแบ่งระดับชั้นการเข้าถึง
- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๖.๔ รูปแบบของเอกสารอิเล็กทรอนิกส์แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)
- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

ข้อ ๗. ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๘. ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไข เปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๙. กำหนดเวลาการเข้าถึงระบบสารสนเทศ ดังนี้

๙.๑ ระบบงานบริการ e-Service (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอดเวลา

๙.๒ ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด

๑.๒.๓ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่ายเพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัยเป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบ ที่เกี่ยวข้อ พฤติกรรมการใช้งานกิจกรรมหรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัยหรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบทันทีที่ตรวจพบพฤติกรรมกิจกรรมที่น่าสงสัยหรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบจะต้องมีการรายงานให้หัวหน้าหน่วยงานทราบภายใน ๑ ชั่วโมงที่ตรวจพบ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตและดำเนิน การตามแผน หน่วยงานมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยง ต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใด ที่เป็นการละเมิดนโยบายของโรงพยาบาล การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากร ระบบของหน่วยงานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๑.๒.๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (PC)

ข้อ ๑ แนวทางปฏิบัติการใช้งานทั่วไป

๑.๑ เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงาน ราชการ

๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วน บุคคลของหน่วยงาน

๑.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของโรงพยาบาลเท่านั้น

๑.๕ ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๑.๖ ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๑.๗ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๑.๘ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

๑.๘.๑ ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

๑.๘.๒ ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

๑.๘.๓ ควรเปลี่ยนรหัสผ่านทุก ๓ – ๖ เดือน

๑.๘.๔ ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๑.๘.๕ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๑.๘.๖ ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่ กำหนดไว้

๑.๙ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๑.๑๐ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่ เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑.๑๑ ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๑.๒.๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

ข้อ ๑. แนวทางปฏิบัติการใช้งานทั่วไป

๑.๑ เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๓ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ

๑.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มี สภาพเดิม

๑.๕ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่อง คอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือเป็นต้น

๑.๖ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑.๗ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑.๘ การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทาง เดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๑.๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑.๑๐ การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพ

๑.๑๐.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑.๑๑ ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่น ละอองสูงและต้องระวังป้องกันการตกกระทบ

๑.๑๑.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๑.๑๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีและรัดกุม

๑.๑๑.๓ ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

๑.๑๑.๔ ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๒ การใช้รหัสผ่านให้ผู้ใช้งาน

๒.๑ ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ

๒.๒ ไม่จดหรือบันทึกรหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์

๒.๓ ควรเปลี่ยนรหัสผ่านทุก ๓ – ๖ เดือน ข้อ ๑๕๕. การส ารองข้อมูลและการกู้คืน

๒.๔ ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

๒.๕ ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๒.๖ แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืน อย่างสม่ำเสมอ

๒.๗ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๒.๘ ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียจะไม่กระทบต่อการดำเนินการของหน่วยงาน

๑.๒.๖ การควบคุมการใช้อินเตอร์เน็ต (Internet)

๑. ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความ จำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการใช้งานอินเตอร์เน็ตผ่านเว็บบราวเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ ของระบบปฏิบัติการ

๓. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๔. ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือ ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๕. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

๖. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดป(Update) โปรแกรมต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

๗. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับ ของหน่วยงาน

๘. เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงาน อื่นๆ

๙. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความ มั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการ เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

๑๐. หลังจากใช้งานระบบอินเตอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๑. หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๒. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่าง เคร่งครัด

๑.๒.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒. ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier)

๓. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์ กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๔. ผู้ดูแลระบบต้องมีการติดตั้งไฟล์วอล (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๕. ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่าย ไร้สาย

๖. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๗. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

๘. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

๙. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลจะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

๑๐. ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้ เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

นโยบายและแนวปฏิบัติการสำรองข้อมูลและการกู้คืนระบบ

บทนำ

ในปัจจุบันโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง ใช้ระบบสารสนเทศมาช่วยสนับสนุนการดำเนินงานขององค์กรให้เป็นไปอย่างมีประสิทธิภาพข้อมูลสารสนเทศจึงมีความสำคัญต่อระบบที่สามารถสนับสนุนการดำเนินงานให้เป็นไปได้อย่างต่อเนื่องและมีประสิทธิภาพ การนำเทคโนโลยีสารสนเทศมาใช้จะทำให้องค์กรมีข้อมูลสารสนเทศสำหรับดูแล รักษาผู้ป่วยได้ถูกต้องรวดเร็วและทันต่อเหตุการณ์ในสถานการณ์ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลาความเสี่ยงที่กระทบต่อการดำเนินงานขององค์กรคือ ระบบสารสนเทศหยุดชะงัก ซึ่งเกิดจากปัจจัยอัน ได้แก่ อุบัติเหตุ ภัยธรรมชาติ ปัญหาการก่อการร้าย ปัญหาการเสื่อมสภาพของอุปกรณ์คอมพิวเตอร์ หรือ การมุ่งร้ายต่อองค์กร ตลอดจนการปัญหาการชุมนุมประท้วงทางการเมือง ซึ่งสร้างความเสียหายให้แก่ องค์กรเป็นมูลค่ามหาศาล ทั้งความเสียหายที่สามารถวัดมูลค่าได้และที่ไม่สามารถวัดเป็นมูลค่าได้ ดังนั้น องค์กรจึงตระหนักถึงปัญหาจึงควรมีมาตรการป้องกันเมื่อต้องประสบเหตุการณ์ที่ทำให้ระบบสารสนเทศ หยุดชะงัก มาตรการที่จะนำมาใช้ต้องอยู่บนพื้นฐานของการปฏิบัติที่รวดเร็วและทันต่อเหตุการณ์ซึ่งแต่ละกระบวนการที่จะนำมาใช้จะต้องอยู่บนพื้นฐานของการปฏิบัติที่เป็นเลิศ (Best Practice) แผนกู้คืนมีส่วนสำคัญในการตอบสนองความเสี่ยง ซึ่งในแผนกู้คืนจะมีรายละเอียดขั้นตอนการปฏิบัติเพื่อกู้คืนสถานการณ์ให้สามารถกลับมาดำเนินงานได้ตามปรกติภายใน ระยะเวลาที่กำหนดเพื่อให้การดำเนินงานขององค์กรเป็นไปอย่างต่อเนื่อง

๑. ปัญหาและแรงจูงใจ

ในปัจจุบันโรงพยาบาลยังขาดแผนกู้คืนระบบสารสนเทศและไม่มีขั้นตอนปฏิบัติเมื่อต้องประสบเหตุที่ไม่คาดคิดกับระบบเครือข่ายเครื่องเซิร์ฟเวอร์และฐานข้อมูล และหากสามารถกู้กลับคืนมาได้ข้อมูลอาจมีความสมบูรณ์ไม่เพียงพอที่จะนำไปใช้ดำเนินการดูแล รักษา ผู้ป่วย จากการประเมินความเสียหายเมื่อระบบ สารสนเทศไม่สามารถดำเนินการได้ ผู้ป่วยนอก อาจจะไม่ได้รับการรักษาที่ถูกต้อง จากแพทย์ผู้เชี่ยวชาญของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยองประมาณ ๑,๑๐๐ คน ต่อ ๑ วัน แผนกู้คืนจึงมีความสำคัญและจะช่วยบรรเทาความเสียหายที่เกิดขึ้นต่อโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยองอย่างเห็นได้ชัด ปี พ.ศ. ๒๕๖๓ เกิดปัญหาเครื่องคอมพิวเตอร์แม่ข่ายทำงานช้าไม่สามารถให้บริการได้ทุกแผนกสาเหตุเนื่องจากพื้นที่ฮาร์ดดิสก์ (Hard disk) ไม่เพียงพอให้โปรแกรมเรียกใช้งาน เนื่องจากขาด แผนการดูแลและขั้นตอนการปฏิบัติ

๒. ปัญหาที่ประสบครั้งนั้นก่อให้เกิดความเสียหายดังนี้

๑.ผู้ใช้งานไม่สามารถใช้งานระบบฐานข้อมูลในระหว่างการแก้ไขปัญหาเครื่องคอมพิวเตอร์แม่ข่าย

๒.ผู้ใช้งานระบบสารสนเทศต้องเขียนข้อมูลลงในกระดาษเนื่องจากเป็นข้อมูลที่ต้องใช้โดยเร่งด่วนไม่สามารถรอการกู้คืนได้

๓.การตัดสินใจของฝ่ายบริหารหยุดชะงักเนื่องจากต้องรอข้อมูลจากระบบฐานข้อมูลที่มาจากเครื่อง คอมพิวเตอร์แม่ข่ายที่พังไป

๔.ผู้ใช้งานระบบคอมพิวเตอร์รู้สึกไม่มีความมั่นใจในระบบคอมพิวเตอร์ที่ใช้งานอยู่จากปัญหาที่เกิดขึ้น ดังกล่าวมาแล้วนั้น ทางศูนย์คอมพิวเตอร์ได้ทำการวิเคราะห์สาเหตุต่างๆ ที่อาจจะก่อให้เกิดปัญหาพบว่า

๑. ไม่มีอุปกรณ์สำหรับการเก็บข้อมูลสำรองในกรณีฐานข้อมูลหลักเสียหาย

๒. ไม่มีแผนรองรับเมื่อเกิดเหตุการณ์เครื่องคอมพิวเตอร์แม่ข่ายหรือระบบหยุดการทำงาน

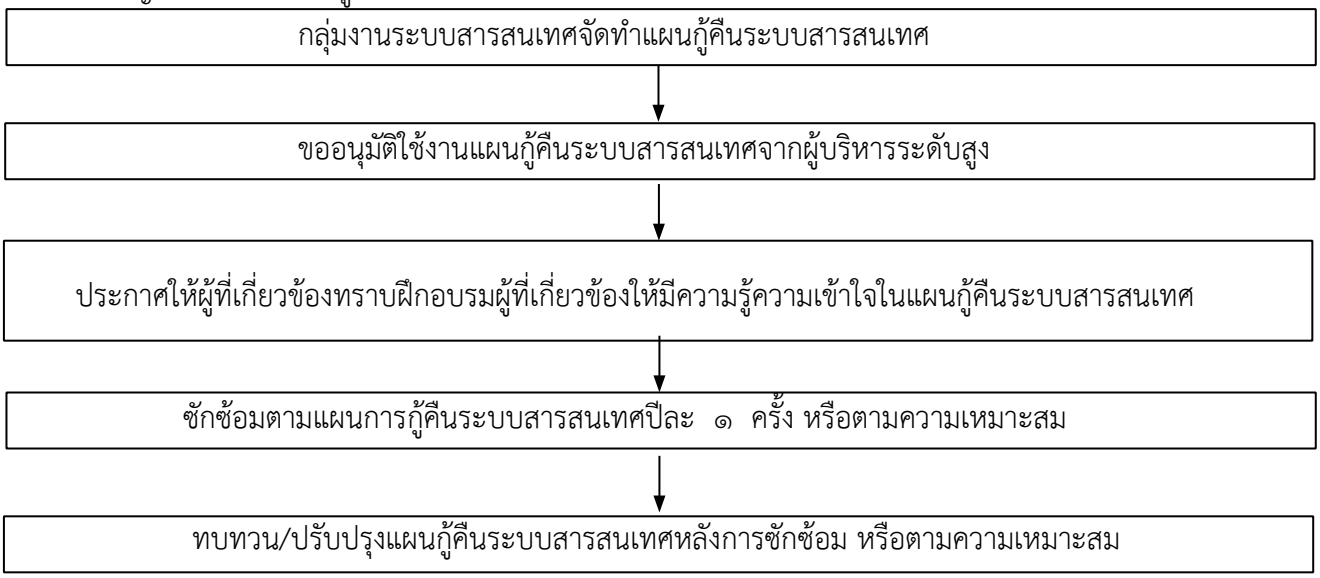
๓. ไม่มีการฝึกอบรมสร้างความรู้ ความเข้าใจและความพร้อมให้ผู้ที่เกี่ยวข้องเกี่ยวกับการกู้คืนระบบ

๔. ไม่สามารถระบุระยะเวลาที่ใช้ในการกู้คืนระบบสารสนเทศให้กลับคืนมาใช้งานได้ตามปกติ

๕. ไม่สามารถยืนยันได้ว่าระบบสารสนเทศที่กู้คืนมานั้นมีความสามารถเพียงพอที่จะใช้ในงานต่อไป ได้หรือไม่

๖. ไม่มีการกำหนดงบประมาณที่ใช้ในการกู้คืนระบบสารสนเทศ เมื่อปัญหาดังกล่าวได้รับ การประเมินผลกระทบ และมีการแก้ไขตามแผนกู้คืนระบบสารสนเทศจะทำให้โรงพยาบาลสามารถ ดำเนินงานได้อย่างต่อเนื่องแม้จะประสบปัญหาความเสียหายของฮาร์ดแวร์และประสบกับภัยธรรมชาติ

แนวทางแก้ไขปัญหา จากปัญหาที่กล่าวมาในหัวข้อก่อนนี้จึงเกิดแนวความคิดในการกู้คืนระบบสารสนเทศขึ้นมาเพื่อแก้ไขปัญหา ซึ่งแสดงไว้ดังรูปที่ ๑ งานระบบสารสนเทศประเมินความเสี่ยงและวิเคราะห์ผลกระทบ



รูปที่ ๑ แสดงขั้นตอนการจัดทำแผนกู้คืนระบบสารสนเทศ

จากรูปที่ ๑ ในขั้นตอนประเมินความเสี่ยงและวิเคราะห์ผลกระทบคณะทำงานสารสนเทศ จะทำการประเมินความเสี่ยงที่จะส่งผลให้ระบบสารสนเทศหยุดชะงัก และวิเคราะห์ผลกระทบที่เกิดขึ้นจากความเสี่ยง จากนั้นจึงเริ่มจัดทำแผนกู้คืนระบบสารสนเทศเพื่อขออนุมัติใช้แผนจากผู้บริหารระดับสูง เมื่อแผนได้รับการอนุมัติแล้ว ก็จะประกาศให้ผู้ที่เกี่ยวข้องทราบ อาทิ ผู้อำนวยการแผนกู้คืนระบบสารสนเทศ หัวหน้าแผนกทุกแผนก เจ้าหน้าที่ฝ่ายระบบสารสนเทศ เป็นต้น เมื่อแจ้งวัตถุประสงค์บุคคลที่เกี่ยวข้องและขั้นตอนการปฏิบัติโดยรวมของแผนกู้คืนระบบสารสนเทศให้ทราบแล้ว จะมีการจัดฝึกอบรมแก่บุคคลที่เกี่ยวข้อง เพื่อให้มีความรู้ความเข้าใจในหน้าที่ที่ต้องปฏิบัติในแผนกู้คืนระบบสารสนเทศ เมื่อประสบเหตุการณ์ที่ส่งผลให้ระบบสารสนเทศหยุดชะงัก จากนั้นจะมีการฝึกซ้อมเพื่อทบทวนและเตรียมความพร้อมในการรับมือกับเหตุการณ์ที่ส่งผลให้ ระบบสารสนเทศหยุดชะงัก จะทำการซักซ้อมปีละ ๑ ครั้ง หรือตามความเหมาะสม ขั้นตอน สุดท้ายคือ ทบทวน/ปรับปรุงแผนกู้คืนระบบสารสนเทศปีละ ๑ ครั้ง หรือตามความเหมาะสม เพื่อให้แผนกู้คืนระบบสารสนเทศมีประสิทธิภาพ ทั้งนี้ภายในแผนกู้คืนระบบสารสนเทศจะระบุขั้นตอนการปฏิบัติ เครื่องมือที่ใช้ในการกู้คืน งบประมาณ ระยะเวลาในการการกู้คืนอย่างชัดเจน และจะมั่นใจได้ว่าจะ สามารถกู้คืนระบบสารสนเทศให้กลับมาใช้ในการดำเนินงานขององค์กรต่อไปได้

๓. วัตถุประสงค์

๑. จัดทำแผนกู้คืนระบบสารสนเทศเพื่อใช้ในองค์กร เพื่อนำไปปฏิบัติต่อไป
๒. ลดความเสียหายอันเกิดจากระบบสารสนเทศหยุดชะงัก
๓. นำแผนกู้คืนระบบสารสนเทศไปซักซ้อมปีละ ๑ ครั้ง หรือตามความเหมาะสม

๔.ประโยชน์

การจัดทำแผนกู้คืนระบบสารสนเทศ เมื่อต้องประสบปัญหาที่ส่งผลให้ระบบสารสนเทศหยุดชะงัก ซึ่งองค์กรจะได้รับประโยชน์จากโครงงานดังนี้

๑. องค์กรสามารถใช้ระบบสารสนเทศได้อย่างต่อเนื่องหากต้องประสบกับเหตุการณ์ที่ส่งผลให้ระบบสารสนเทศหยุดชะงัก
๒. องค์กรสามารถมั่นใจได้ว่าระบบสารสนเทศจะสามารถกลับมาใช้งานได้อย่างสมบูรณ์ ภายในระยะเวลาที่กำหนด
๓. รักษาความมั่นคงปลอดภัยของข้อมูล
๔. บุคคลที่เกี่ยวข้องมีความรู้ความเข้าใจในแผนกู้คืนระบบสารสนเทศ ซึ่งส่งผลให้ระบบสารสนเทศกลับมา ใช้งานได้ตามระยะเวลาที่กำหนด

๕. ขั้นตอนและระยะเวลา

๑. ศึกษาความเป็นไปได้
๒. ทำการประเมินความเสี่ยง
๓. ทำการวิเคราะห์ผลกระทบต่อองค์กร
๔. พัฒนาแผนกู้คืน
๕. จัดฝึกอบรม
๖. ทดสอบการกู้คืน
๗. การตรวจสอบแผนกู้คืน
๘. แผนการปรับปรุงและดูแลรักษาแผนกู้คืน

๖.ทฤษฎี

การจัดทำแผนกู้คืนระบบสารสนเทศเมื่อต้องประสบเหตุการณ์ ไม่คาดคิดของฮาร์ดแวร์และภัยธรรมชาติอันได้แก่ อัคคีภัย อุทกภัยและแผ่นดินไหว หรือภัยที่เกิดจากมนุษย์อันได้แก่เหตุการณ์ ทาง การเมือง การก่อจลาจลและการประท้วงหยุดงาน ซึ่งจะเป็นมาตรการเชิงป้องกันและระงับความเสียหายที่ อาจจะเกิดขึ้น แก่ระบบสารสนเทศของบริษัทเพื่อลดความเสียหายให้เหลือน้อยที่สุดเพื่อสร้างความต่อเนื่อง ให้กับโรงพยาบาล ดังนั้นเพื่อให้เกิดความรู้ ความเข้าใจในการวางแผนดังกล่าว จึงได้เสนอรายละเอียด และ ทฤษฎีที่เกี่ยวข้อง โดยครอบคลุมหัวข้อต่างๆ

๗.ระบบเครือข่ายและการเก็บข้อมูล

การเก็บข้อมูลเพื่อหาองค์ประกอบที่สำคัญที่ทำให้องค์กรขาดความต่อเนื่องในการให้บริการของโรงพยาบาลนั้น จะทำให้ทราบถึงปัญหาที่แท้จริงและสามารถมองเห็นองค์ประกอบที่อาจ ส่งผลให้การให้บริการผู้ป่วยขาดความต่อเนื่องหรือมีการหยุดชะงักองค์ประกอบที่มีส่วนสำคัญทำให้ความ ต่อเนื่องของการให้บริการขาดหายไป

ที่ติดต่อประสานงานกรณีระบบมีปัญหา

บริษัท, บริการ	เบอร์ติดต่อ ชื่อ	รายละเอียด
๑.TPS ระบบเครือข่าย	๑. ทีม Admin ๐๘๕-[redacted] ๒. k.โจ้ ๐๙๒-[redacted] ๓. k.เจี๊ยบ ๐๙๕-[redacted] cs@thepractical.co.th	ระบบเครือข่าย Router , Core Switch, Firewall รวมถึงการปรับปรุง network ต่างๆ การเพิ่มเครื่องแม่ข่าย การแก้ไข firewall - เมื่อระบบมีปัญหาให้อีเมลไปเปิดเคส
๒. CAT internet	๑. มาบตาพุดในเวลา ๐๘๑-[redacted] ๒. call center ๑๓๒๒ ๓. พัทยา ๒๔ ชั่วโมง ๐๘๑-๓๕๐-๒๑๒๖ ๔. ช่างน้อย ๐๘๑-[redacted]	Bandwidth ๕๐๐/๕๐๐ Mbps แบบ Business ๘ ip EDNO๐๓๗๑๔๙๘๙ [redacted] ค่าบริการ ๑๕,๙๐๐ ค่าเช่า router ๒,๑๐๐ บาท / เดือน จ่ายรวม VAT = ๑๙,๒๖๐ บาท / เดือน
๓. TOT internet	๑. ช่าง ๐๓๘-๖๘๙๑๕๑-๒ ๒. มาบตาพุด ๐๓๘-๖๘๓๗๗๗ ๓. คุณพรศิริ ๐๘๑-๖๒๗๑๙๖๐ ๔. พี่สมพงษ์ ๐๘๑-๔๕๙๘๐๐๘ ๕. พี่แซม ๐๙๖-๒๓๗๙๔๓๕	เลขวงจร : [redacted] เดิม ๕๐/๒๐ Mbps user : [redacted] Pass : [redacted] ๐๗/๐๕/๒๕๖๑ ได้ up เป็น ๓๐๐/๑๐๐ Mbps ค่าบริการ ๓,๗๔๕ บาท / เดือน
๔. BMS Hosxp	๐๒-๔๒๗๙๙๙๑ กด ๑ ๐๘๑-๘๑๑๘๑๗๓ ๐๘๑-๘๙๙๕๓๙๑ ๐๘๙-๙๒๔๖๒๐๗ bms.callcenter๙@gmail.com	เรื่องเกี่ยวกับ hosxp, datacenter แจ้งรหัสโรงพยาบาล ๑๐๘๒๗

๘.แผนกู้คืนระบบ

การจัดทำแผนและขั้นตอนปฏิบัติสำหรับการกู้คืนระบบจัดทำแผนและขั้นตอนปฏิบัติ สำหรับการกู้คืนระบบ ซึ่งแสดงถึงแผนงานต่างๆทีเกี่ยวข้องทั้งหมดและขั้นตอนทั้งหมด ดังนี้

- การสั่งการให้นำแผนกู้คืนมาใช้เมื่อผู้บริหารสารสนเทศได้รับทราบ ให้ดำเนินติดต่อและแต่งตั้ง ผู้จัดทำแผนโครงการกู้คืนโดยเร็วโดยลำดับการแต่งตั้งให้เริ่มต้นจากผู้รับผิดชอบหลัก หากผู้รับผิดชอบหลักไม่ สามารถเข้าประจำการได้ ให้เลื่อนเป็นผู้ที่สามารถดำเนินการแทนคนถัดไปกระบวนการในการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัยตามระดับความรุนแรงเหตุการณ์ภัย พิบัติเป็นเหตุการณ์ที่มีระดับความรุนแรง การรับแจ้งเหตุการณ์ประเภทนี้จะรับแจ้งทางเจ้าหน้าที่รักษาความปลอดภัยและกลุ่มงานสารเทคโนโลยีสารสนเทศทางการแพทย์ แล้วจะมีการประสานงานเพื่อ

ดำเนินการต่อไป ในกรณีที่เหตุการณ์ที่เกิดขึ้นนั้นมีผลทำให้เกิดการหยุดชะงักของระบบคอมพิวเตอร์ เหตุการณ์ดังกล่าวจะ พิจารณาเป็นเป็นเหตุการณ์ด้านความมั่นคงและความปลอดภัยด้วย

- การประเมินความเสียหายเกิดขึ้นประเมินความเสียหายที่เกิดขึ้นภายหลังจาก เหตุการณ์บรรเทาหรือสงบลงแล้ว ทีมประเมินความเสียหายจะต้องร่วมกันทำการสำรวจความ เสียหายที่เกิดขึ้นทีมประเมินความเสียหายร่วมกันประเมินความเสียหาย กำหนดแนวทางและ ระยะเวลาการแก้ไข

ขั้นตอนปฏิบัติในการจัดซื้อจัดจ้างผู้บริหารสารสนเทศ (หรือผู้แทน) สั่งการให้ ดำเนินการจัดซื้อโดยวิธีพิเศษ (โดยจะต้องมีคำสั่งจากผู้บริหารให้อำนาจแก่ฝ่ายจัดซื้อจัดจ้าง เพื่อให้สามารถดำเนินการได้เมื่อมีเหตุการณ์ภัยพิบัติเกิดขึ้น)

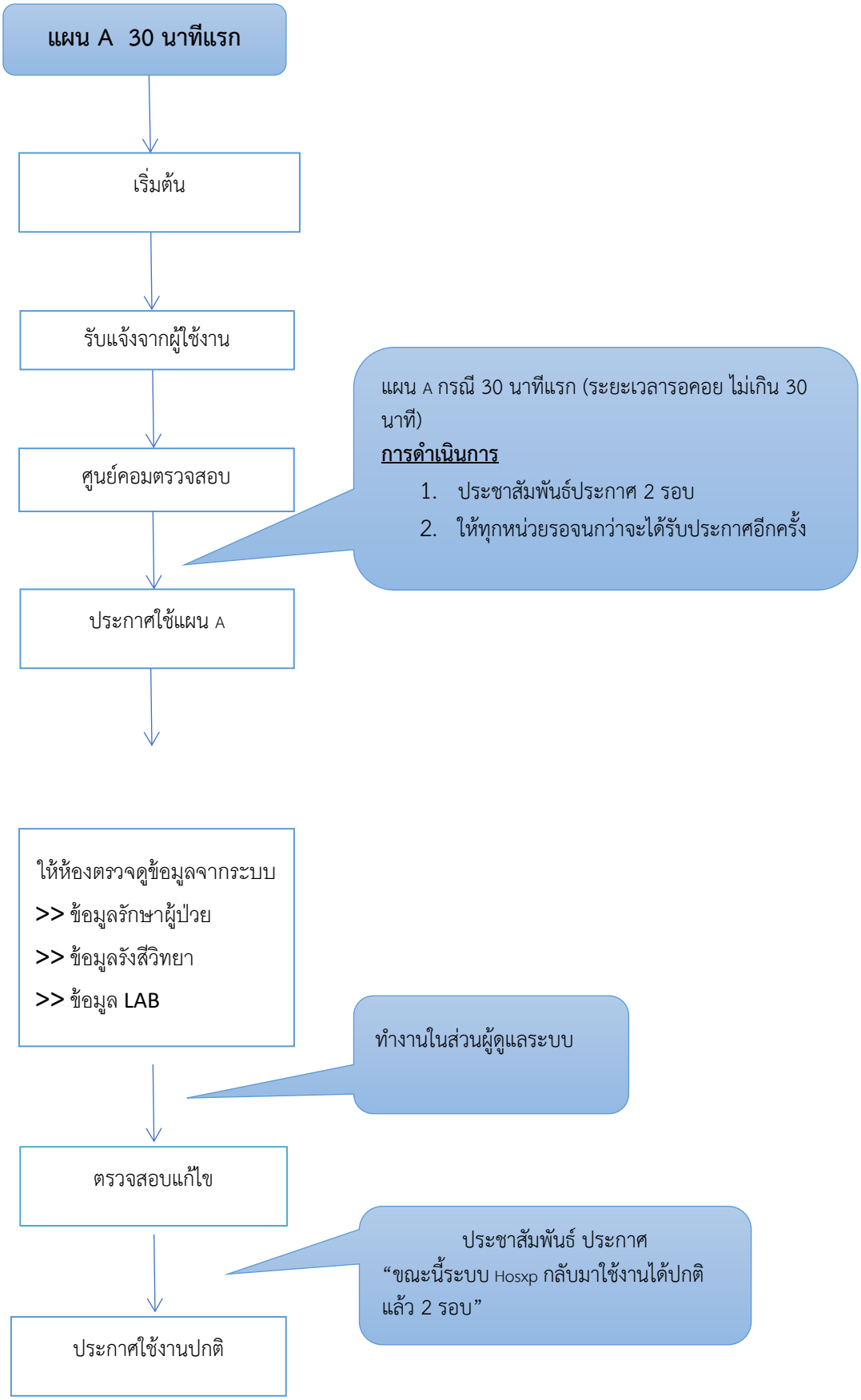
ขั้นตอนการกู้คืนระบบสารสนเทศในการปฏิบัติการกู้คืนระบบ เมื่อเกิดเหตุที่ทำ ให้ระบบงานสำคัญเกิดการหยุดชะงักและจำเป็นต้องกู้คืน เพื่อให้ระบบสามารถใช้งานต่อได้การ รวมระบบเซิร์ฟเวอร์เข้ากันด้วยกันการให้บริการต่อกระบวนการธุรกิจเป็นหลักเช่น ระบบ เทคโนโลยีสารสนเทศที่ใช้สนับสนุนกระบวนการรักษา ระบบเทคโนโลยีสารสนเทศที่ใช้สนับสนุน หน่วยงาน เป็นต้น จากนั้นกำหนดระยะเวลาในการกู้คืนในแต่ละระบบโดยการน า RTO มาใช้ใน การกำหนด และขั้นตอนต่อไปคือการกำหนดความถี่ในการสำรองข้อมูลและการส่งสื่อบันทึก ข้อมูลไปเก็บอยู่ในสถานที่ปลอดภัยภายนอกองค์กรโดยใช้ RPO ในการกำหนด ในการจัดทำ แผนกู้คืนโดยพื้นฐานแล้วคือการกำหนดขั้นตอนปฏิบัติจัดทำเอกสารที่ชัดเจน ง่ายต่อการทำความเข้าใจกับผู้ปฏิบัติ RPO (Recovery Point Objective) คือ การระบุเวลาที่ต้องการ ย้อนกลับไปเพื่อกู้คืน ข้อมูล โดยทั่วไปแล้วก็คือข้อมูลที่ได้สำรองไว้ครั้งล่าสุด เพื่อข้อมูลที่ กู้คืนกลับมามีความใกล้เคียงกับข้อมูลในปัจจุบันมากที่สุด เท่าที่สามารถจะทำได้ และ RPO ยัง แสดงให้เห็นถึงจำนวนข้อมูลที่จะต้องจัดทำเพิ่มเติมขึ้นมาหลังจากกู้คืนข้อมูลกลับมาแล้ว RTO (Recovery Time Objective) คือ ระยะเวลาที่ใช้ในการกู้คืนระบบหรือ การ กล่าวถึงความสามารถขององค์ที่สามารถดำเนินกิจการได้โดยไม่มีระบบเทคโนโลยีสารสนเทศ แต่เนื่องจาก มี Dr-site อยู่แล้วจึงไม่ต้องรวมระยะเวลาในการสั่งซื้ออุปกรณ์ใหม่

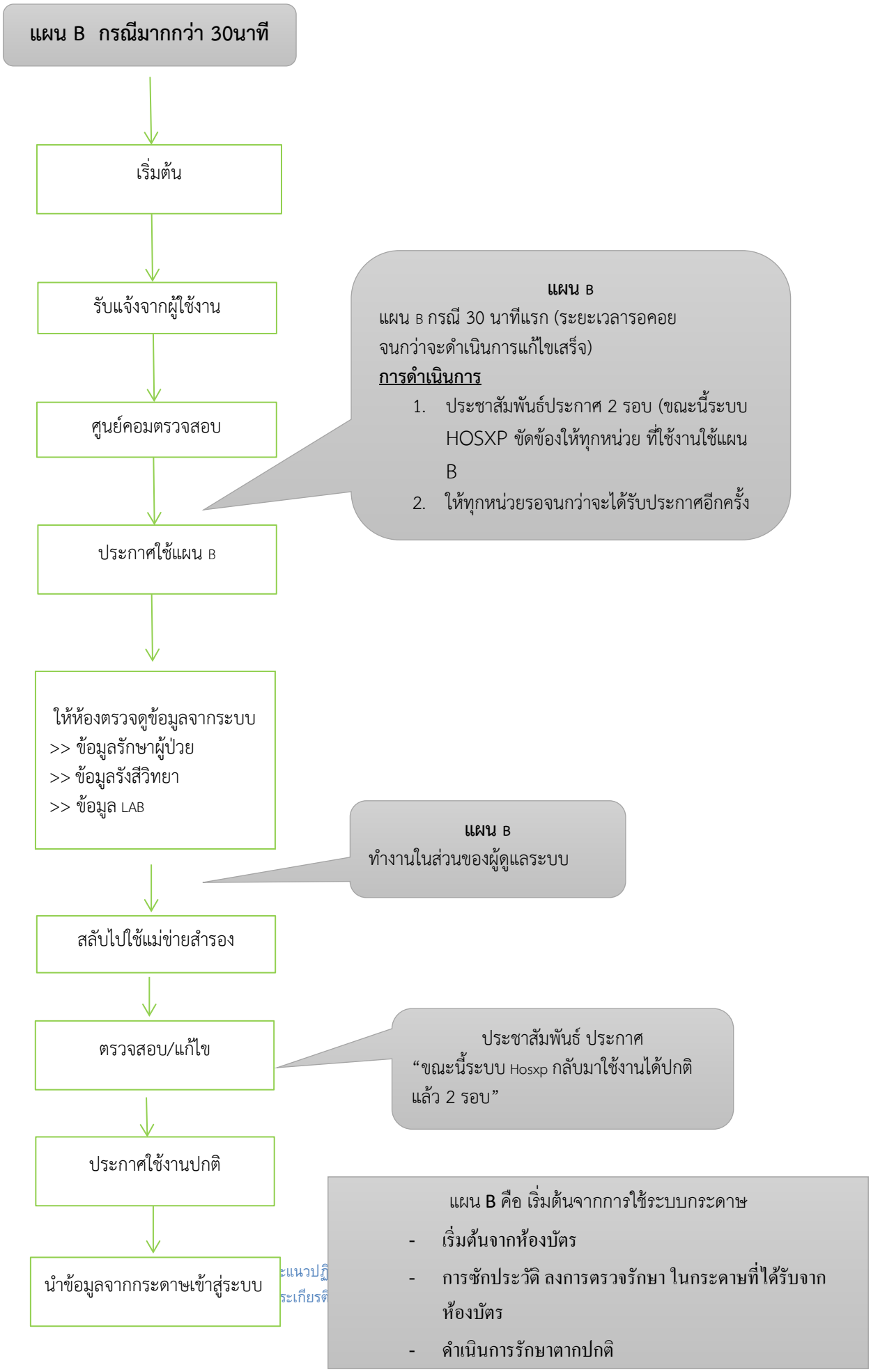
Total RTO = (MAX) ระยะเวลากู้คืนข้อมูล NRO (Network Recovery Objective) คือ ระยะเวลาในการกู้คืนระบบเครือข่าย ซึ่งต้อง ระลึกอยู่เสมอว่าเครื่องคอมพิวเตอร์ของเจ้าหน้าที่นั้นจะใช้บริการที่เซิร์ฟเวอร์เปิดให้บริการผ่าน ระบบเครือข่าย ถึงแม้ Server จะสามารถกู้คืนกลับมาให้บริการได้แล้วก็ตามแต่ก็ไม่มีประโยชน์ อันใดหากเจ้าหน้าที่หรือผู้รับผิดชอบต่องานต่างๆในองค์กรนั้นไม่สามารถเข้าถึงหรือไม่สามารถ ใช้บริการนั้นได้ ทั้งนี้จะหมายรวมถึงเหตุอันเกิดขึ้นได้กับระบบเครือข่ายทั้งหมด เช่น การไม่ สามารถเชื่อมต่อกับ ได้ IP address ของเครื่องคอมพิวเตอร์ซ้ำซ้อนกัน หรือไม่สามารถเชื่อมต่อ กับ ISP ได้ ปัญหาเหล่านี้จะถูกนำเข้ามาประเมินและวิเคราะห์ด้วย และการกู้คืนระบบเครือข่าย ไม่จำเป็นต้องจัดซื้ออุปกรณ์ใหม่ เพื่อให้บริการด้านเครือข่ายกับผู้ใช้งานระบบ หลังจากกำหนด แนวความคิดในการสร้างแผนกู้คืนระบบดังข้างต้นแล้วจึงนำแนวคิดดังกล่าวมาออกแบบให้กับแผนกู้คืนของ โรงพยาบาลฯ โดยเรียงความสำคัญ ๒ กระบวนการดังนี้ ๗.๔.๕.๑ กระบวนการกู้คืนเซิร์ฟเวอร์และข้อมูลผู้ป่วย

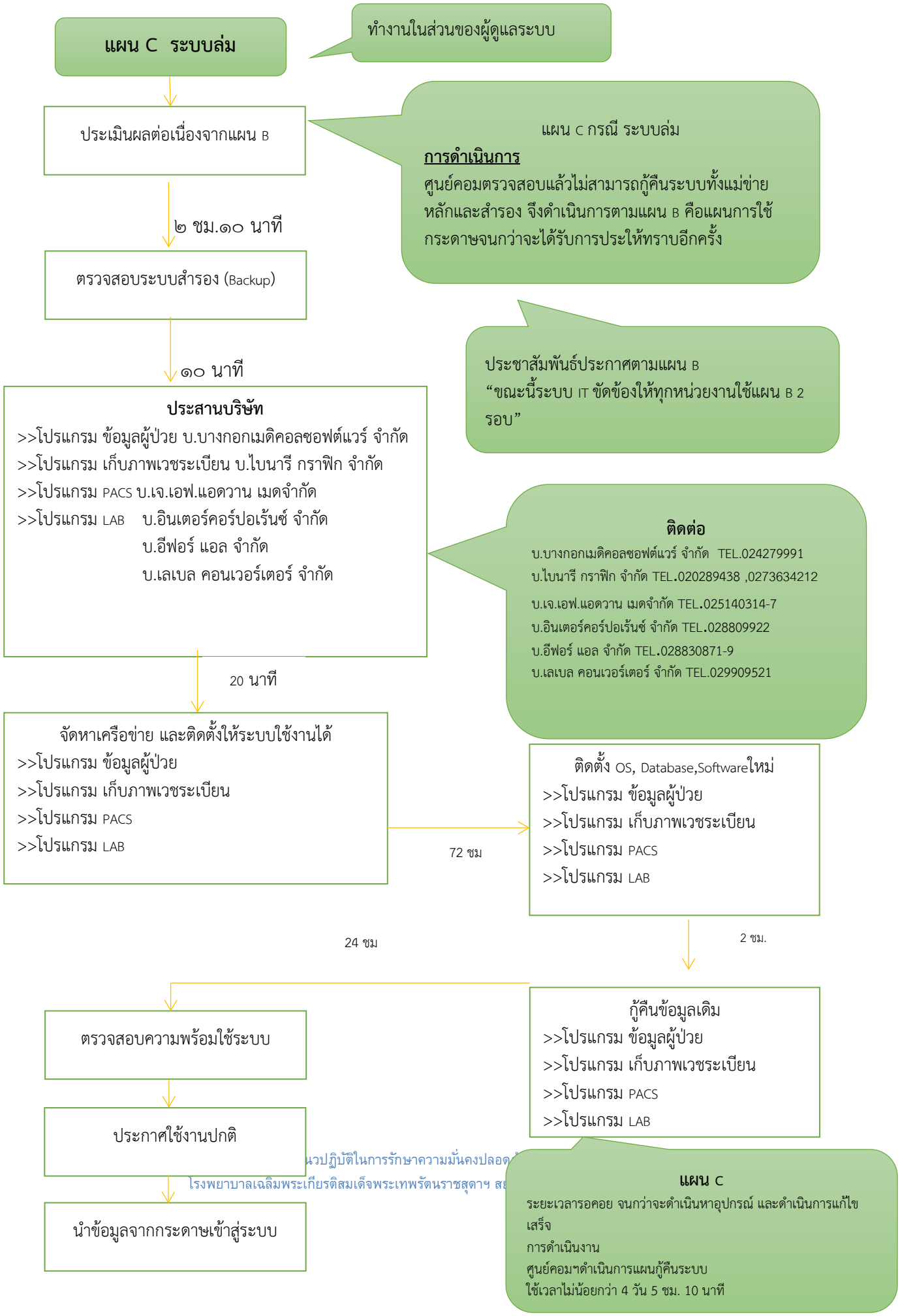
สิ่งสำคัญของการจัดทำแผนกู้คืนระบบสารสนเทศกรณีเหตุฉุกเฉินในรูปแบบต่างๆ

นั่นก็คือ การสำรองข้อมูลหากขั้นตอนการสำรองข้อมูลหรือกระบวนการสำรองข้อมูลมีปัญหาอันส่งผล กระทบให้เกิดความไม่สมบูรณ์ครบถ้วนของข้อมูลแล้วนั้น อาจส่งผลให้การดำเนินการตามแผนกู้คืนระบบ สารสนเทศ ล้มเหลว ได้ เพราะการสำรองข้อมูลถือเป็นหัวใจสำคัญสำหรับแผนกู้คืนระบบสารสนเทศ ดังนั้น เพื่อเพิ่มประสิทธิภาพการทำงานในด้านต่างๆ ต้องออกแบบการสำรองข้อมูลหรือการจัดการกับข้อมูลขององค์กรให้ดีที่สุด ทางโรงพยาบาลได้ออกแบบการสำรองข้อมูลได้ดังต่อไปนี้ จัดลำดับความสำคัญของข้อมูล ที่เกี่ยวข้องกับแผนกู้คืนระบบสารสนเทศทั้งหมด เพื่อให้องค์กร

หรือบุคลากรที่มีหน้าที่เกี่ยวข้องกับการ สำรองข้อมูลได้ตระหนักถึงความสำคัญของข้อมูลที่จะดำเนินการสำรองข้อมูลและจัดเก็บไว้อย่างเหมาะสม


แผน A 30 นาทีแรก
เริ่มต้น
รับแจ้งจากผู้ใช้งาน
ศูนย์คอมตรวจสอบ
ประกาศใช้แผน A
แผน A กรณี 30 นาทีแรก (ระยะเวลารอคอย ไม่เกิน 30 นาที)
การดำเนินการ
1. ประชาสัมพันธ์ประกาศ 2 รอบ
2. ให้ทุกหน่วยรอจนกว่าจะได้รับประกาศอีกครั้ง
ให้ห้องตรวจดูข้อมูลจากระบบ
>> ข้อมูลรักษาผู้ป่วย
>> ข้อมูลรังสีวิทยา
>> ข้อมูล LAB
ทำงานในส่วนผู้ดูแลระบบ
ตรวจสอบแก้ไข
ประชาสัมพันธ์ ประกาศ
“ขณะนี้ระบบ Hosxp กลับมาใช้งานได้ปกติแล้ว 2 รอบ”
ประกาศใช้งานปกติ


แผน B กรณีมากกว่า 30นาที
เริ่มต้น
รับแจ้งจากผู้ใช้งาน
ศูนย์คอมตรวจสอบ
ประกาศใช้แผน B
ให้ห้องตรวจดูข้อมูลจากระบบ
>> ข้อมูลรักษาผู้ป่วย
>> ข้อมูลรังสีวิทยา
>> ข้อมูล LAB
สลับไปใช้แม่ข่ายสำรอง
ตรวจสอบ/แก้ไข
ประกาศใช้งานปกติ
นำข้อมูลจากกระดาษเข้าสู่ระบบ
แผน B
แผน B กรณี 30 นาทีแรก (ระยะเวลารอคอย จนกว่าจะดำเนินการแก้ไขเสร็จ)
การดำเนินการ
1. ประชาสัมพันธ์ประกาศ 2 รอบ (ขณะนี้ระบบ HOSXP ขัดข้องให้ทุกหน่วย ที่ใช้งานใช้แผน B
2. ให้ทุกหน่วยรอจนกว่าจะได้รับประกาศอีกครั้ง
แผน B
ทำงานในส่วนของผู้ดูแลระบบ
ประชาสัมพันธ์ ประกาศ
“ขณะนี้ระบบ Hosxp กลับมาใช้งานได้ปกติแล้ว 2 รอบ”
แผน B คือ เริ่มต้นจากการใช้ระบบกระดาษ
- เริ่มต้นจากห้องบัตร
- การซักประวัติ ลงการตรวจรักษา ในกระดาษที่ได้รับจากห้องบัตร
- ดำเนินการรักษาตากปกติ


แผน C ระบบล่ม
ทำงานในส่วนของผู้ดูแลระบบ
ประเมินผลต่อเนื่องจากแผน B
แผน C กรณี ระบบล่ม
การดำเนินการ
ศูนย์คอมตรวจสอบแล้วไม่สามารถกู้คืนระบบทั้งแม่ข่าย หลักและสำรอง จึงดำเนินการตามแผน B คือแผนการใช้กระดาษจนกว่าจะได้รับการประให้ทราบอีกครั้ง
๒ ชม.๑๐ นาที
ตรวจสอบระบบสำรอง (Backup)
๑๐ นาที
ประชาสัมพันธ์ประกาศตามแผน B
“ขณะนี้ระบบ IT ขัดข้องให้ทุกหน่วยงานใช้แผน B 2 รอบ”
ประสานบริษัท
>>โปรแกรม ข้อมูลผู้ป่วย บ.บางกอกเมดิคอลซอฟต์แวร์ จำกัด
>>โปรแกรม เก็บภาพเวชระเบียน บ.ไบนารี กราฟิก จำกัด
>>โปรแกรม PACS บ.เจ.เอฟ.แอดวาน เมดจำกัด
>>โปรแกรม LAB บ.อินเตอร์คอร์ปอเร้นซ์ จำกัด
บ.อีฟอร์ แอล จำกัด
บ.เลเบล คอนเวอร์เตอร์ จำกัด
ติดต่อ
บ.บางกอกเมดิคอลซอฟต์แวร์ จำกัด TEL.024279991
บ.ไบนารี กราฟิก จำกัด TEL.020289438 ,0273634212
บ.เจ.เอฟ.แอดวาน เมดจำกัด TEL.025140314-7
บ.อินเตอร์คอร์ปอเร้นซ์ จำกัด TEL.028809922
บ.อีฟอร์ แอล จำกัด TEL.028830871-9
บ.เลเบล คอนเวอร์เตอร์ จำกัด TEL.029909521
20 นาที
จัดหาเครือข่าย และติดตั้งให้ระบบใช้งานได้
>>โปรแกรม ข้อมูลผู้ป่วย
>>โปรแกรม เก็บภาพเวชระเบียน
>>โปรแกรม PACS
>>โปรแกรม LAB
72 ชม
ติดตั้ง OS, Database,Softwareใหม่
>>โปรแกรม ข้อมูลผู้ป่วย
>>โปรแกรม เก็บภาพเวชระเบียน
>>โปรแกรม PACS
>>โปรแกรม LAB
2 ชม.
24 ชม
ตรวจสอบความพร้อมใช้ระบบ
ประกาศใช้งานปกติ
นำข้อมูลจากกระดาษเข้าสู่ระบบ
กู้คืนข้อมูลเดิม
>>โปรแกรม ข้อมูลผู้ป่วย
>>โปรแกรม เก็บภาพเวชระเบียน
>>โปรแกรม PACS
>>โปรแกรม LAB
แผน C
ระยะเวลารอคอย จนกว่าจะดำเนินหาอุปกรณ์ และดำเนินการแก้ไขเสร็จ
การดำเนินงาน
ศูนย์คอมฯดำเนินการแผนกู้คืนระบบ
ใช้เวลาไม่น้อยกว่า 4 วัน 5 ชม. 10 นาที

๙. ลำดับของผู้มีอำนาจในการสั่งการใช้แผน

ผู้มีอำนาจตามตารางจะทำหน้าที่เป็นหัวหน้าทีมสร้างความต่อเนื่องทางธุรกิจซึ่งเป็นผู้มีอำนาจ สูงสุดในการสั่งการใช้แผนฉบับนี้ ถ้าผู้ที่อยู่ในตำแหน่งสูงสุดในตารางไม่สามารถเข้าประจำการได้ เช่น เนื่องจากบาดเจ็บทุพพลภาพ หรือไม่อยู่ในพื้นที่ ให้เลื่อนมายังผู้ที่อยู่ในลำดับถัดไปให้เป็นผู้มีอำนาจสั่ง การ

ลำดับ	ชื่อ-นามสกุล	ตำแหน่ง
๑	นพ.สุกิจ บรรจงกิจ	ผู้อำนวยการโรงพยาบาล
๒	นพ.สมชาย แพรพิรุณ	รองผู้อำนวยการด้านพัฒนาระบบบริการและสนับสนุนบริการสุขภาพ
๓	ส.อ.นนทกานต์ มากพูล	หัวหน้างานเทคโนโลยีสารสนเทศ

๑.๔ การกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศ

การกำหนดโครงสร้างทีมทำงานและหน้าที่ความรับผิดชอบ จากโครงสร้างของทีมสร้างความต่อเนื่องทางธุรกิจ แผนกู้คืนระบบสารสนเทศของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง นั้นได้กำหนดหน้าที่ความ รับผิดชอบไว้อย่างชัดเจนในแต่ละหน่วย ซึ่งในแต่ละหน่วยนั้นจะประกอบด้วยบุคลากรในหลายๆ ฝ่ายที่มีความเกี่ยวข้องกับกระบวนการสำคัญทางธุรกิจของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง ซึ่งบุคลากรที่มีหน้าที่รับผิดชอบใน แต่ละหน่วยนั้นจะต้องทุ่มเทการทำงานปฏิบัติหน้าที่ในส่วนของตนเอง เพื่อให้องค์กรบรรลุวัตถุประสงค์ ที่ได้กำหนดเอาไว้

ตำแหน่ง	ผู้รับผิดชอบหลัก (Primary)	ผู้ที่สามารถดำเนินการแทน (Secondary)
รองผู้อำนวยการด้านพัฒนาระบบบริการและสนับสนุนบริการสุขภาพ	นพ.สมชาย แพรพิรุณ	ส.อ.นนทกานต์ มากพูล
หัวหน้าทีมงานด้านคอมพิวเตอร์	ส.อ.นนทกานต์ มากพูล	นายนรงฤทธิ์ งามยิ่ง
ทีมจัดระบบและอุปกรณ์	นางสาวพิมชนก น้อยมุข	นายวิชชา อินทรารักษ์
ทีมธุรการและตรวจสอบข้อมูล	นางสาวกุลิสรา โทแก้ว	นายวิชชา อินทรารักษ์

บันทึกข้อความ

ส่วนราชการ โรงพยาบาลเฉลิมพระเกียรติ สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง
กลุ่มงานพัฒนาระบบบริการสุขภาพและสนับสนุนบริการ งานเทคโนโลยีสารสนเทศ
ที่ รย ๐๐๓๓.๓(๖)/- **วันที่** ๑๘ ธันวาคม ๒๕๖๖
เรื่อง การเผยแพร่ข้อมูลนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เรียน ผู้อำนวยการโรงพยาบาลเฉลิมพระเกียรติ สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารีและหัวหน้าฝ่ายงานทุกหน่วยงาน

ตามที่โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง ได้ออกคำสั่งแต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ลงวันที่ ๒๙ พฤศจิกายน พ.ศ. ๒๕๖๖ เพื่อให้เจ้าหน้าที่ของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง ถือปฏิบัติอย่างเคร่งครัด โดยกำหนดต้องมีการทบทวนนโยบาย ปีละ ๑ ครั้ง

เพื่อให้นโยบายดังกล่าวฯ เป็นไปอย่างเรียบร้อย งานเทคโนโลยีสารสนเทศจึงเห็นสมควรให้มีการเผยแพร่ข้อมูลนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง โดยสามารถ Download นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้ที่ https://hrh.moph.go.th/ หัวข้อ ข่าวประชาสัมพันธ์

จึงเรียนมาเพื่อโปรดทราบ

(ส.อ.นนทกานต์ มากพูล)
หัวหน้ากลุ่มงานสารสนเทศทางการแพทย์

คำสั่ง โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง
ที่ ๒๒๗ /๒๕๖๖
เรื่อง แต่งตั้งคณะทำงานบริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง
ประจำโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

.....

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบาย และแผนปฏิบัติ การว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ข้อที่ ๑ การกำกับดูแล การรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) ประกอบกับปีงบประมาณ ๒๕๖๗ กระทรวงสาธารณสุขมีนโยบายบัตรประชาชนบัตรเดียวรักษาทุกที่ โดยมีวัตถุประสงค์เพื่ออำนวย ความสะดวก ให้ประชาชน สามารถเข้ารับบริการที่โรงพยาบาลทุกแห่งทุกเครือข่ายได้ด้วยบัตรประชาชน เพียงใบเดียว ดังนั้น เพื่อขับเคลื่อนนโยบายดังกล่าวจึงจำเป็นต้องสนับสนุนให้โรงพยาบาลทุกแห่งเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกันได้อย่างมีประสิทธิภาพ และยกระดับด้านความมั่นคงปลอดภัยสารสนเทศให้มีความสามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบหรือก่อให้เกิดความเสี่ยงต่อการให้บริการได้ซึ่งจะเป็นอุปสรรคต่อการบรรลุเป้าประสงค์ของนโยบายบัตรประชาชนบัตรเดียวรักษาทุกที่

ฉะนั้น เพื่อสนับสนุนการดำเนินงานให้บรรลุเป้าหมายนโยบายดังกล่าว ผู้อำนวยการโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง จึงแต่งตั้งคณะทำงานบริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง โดยมีองค์ประกอบ หน้าที่และอำนาจ ดังนี้

๑. องค์ประกอบ

๑.๑ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง	ประธานคณะทำงาน
๑.๒ รองผู้อำนวยการฯ ด้านพัฒนาระบบบริการฯ	คณะทำงาน
๑.๓ รองผู้อำนวยการฯ ด้านปฐมภูมิ	คณะทำงาน
๑.๔ รองผู้อำนวยการฯ ฝ่ายการแพทย์๒	คณะทำงาน
๑.๕ รองผู้อำนวยการฯ ด้านการพยาบาล	คณะทำงาน
๑.๖ หัวหน้ากลุ่มงานยุทธศาสตร์และแผนงานโครงการ	คณะทำงาน
๑.๗ หัวหน้ากลุ่มงานประกันสุขภาพ	คณะทำงาน
๑.๘ หัวหน้ากลุ่มงานสารสนเทศทางการแพทย์	คณะทำงานและเลขานุการ
๑.๙ เจ้าหน้าที่งานสารสนเทศทางการแพทย์	คณะทำงานและผู้ช่วยเลขานุการ

๒. หน้าที่และอำนาจ

๒.๑ ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานต่างๆ

(๒.๒) สนับสนุน....

๒.๒ สนับสนุนหน่วยงานต่างๆ ในการควบคุมและสอบสวนเหตุการณ์ไม่พึงประสงค์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และพิจารณายกระดับการตอบโต้ แก่ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง สำนักงานสาธารณสุขจังหวัดระยอง

๒.๓ เสนอแนะเป้าหมายและแนวทางการรักษาความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล รวมถึงควบคุมกำกับดูแลการบริหารจัดการความเสี่ยง การปฏิบัติตามนโยบาย และสนับสนุนการดำเนินการตามมาตรฐานที่กำหนดโดยสำนักงานปลัดกระทรวงสาธารณสุข

๒.๔ กำกับติดตามการจัดทำแผนงาน โครงการ และงบประมาณเพื่อการรักษาความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

๒.๕ สรุปรายงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาลครอบคลุมในประเด็น ประสิทธิภาพ ประสิทธิผล การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การลดความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ และกลไกในการควบคุมให้เกิดความเสี่ยงน้อยสุด

๒.๖ ดำเนินการตอบโต้สถานการณ์และประเมินความเสี่ยงสถานการณ์ภัยคุกคามทางไซเบอร์ของโรงพยาบาล

๒.๗ ปฏิบัติภารกิจอื่นตามที่กำหนดหรือตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๙ พฤศจิกายน พ.ศ. ๒๕๖๖

(นายสุกิจ บรรจงกิจ)
ผู้อำนวยการโรงพยาบาลเฉลิมพระเกียรติ
สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

คำสั่ง โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง
ที่ ๒๒๕ /๒๕๖๖
เรื่อง แต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง
ประจำโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

.....

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ข้อ ๑ การกำกับดูแล การรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) ข้อ ๑.๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่า ที่ปฏิบัติหน้าที่เสมือน CISOของหน่วยงาน ประกอบกับปีงบประมาณ ๒๕๖๗ กระทรวงสาธารณสุขมีนโยบายบัตรประชาชนบัตรเดียวรักษาทุกที่ โดยมีวัตถุประสงค์เพื่ออำนวยความสะดวกให้ประชาชน สามารถเข้ารับบริการที่โรงพยาบาลทุกแห่ง ทุกเครือข่าย ได้ด้วยบัตรประชาชนเพียงใบเดียว ดังนั้น เพื่อขับเคลื่อนนโยบายดังกล่าวจึงจำเป็นต้องสนับสนุนให้โรงพยาบาลในจังหวัดเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกันได้อย่างมีประสิทธิภาพ และยกระดับด้านความมั่นคงปลอดภัยสารสนเทศให้มีความสามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบหรือก่อให้เกิดความเสี่ยงต่อการให้บริการได้ซึ่งจะเป็นอุปสรรคต่อการบรรลุเป้าประสงค์ ของนโยบายบัตรประชาชนบัตรเดียวรักษาทุกที่ นั้น

ฉะนั้น เพื่อสนับสนุนการดำเนินงานให้บรรลุเป้าหมายนโนยายดังกล่าว ผู้อำนวยการโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง จึงมีคำสั่งดังต่อไปนี้

๑. แต่งตั้ง นายแพทย์ศุภชัย เอี่ยมกุลวรพงษ์ ตำแหน่ง นายแพทย์เชี่ยวชาญ เป็นผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง โรงพยาบาลโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

๒. หน้าที่และอำนาจ

๒.๑ ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานต่างๆ

๒.๒ สนับสนุนหน่วยงานต่างๆ ในการควบคุมและสอบสวนเหตุการณ์ไม่พึงประสงค์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และพิจารณายกระดับการตอบโต้ แก่ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง สำนักงานสาธารณสุขจังหวัดระยอง

๒.๓ เสนอแนะเป้าหมายและแนวทางการรักษาความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล รวมถึงควบคุมกำกับดูแลการบริหารจัดการความเสี่ยง การปฏิบัติตามนโยบาย และสนับสนุนการดำเนินการตามมาตรฐานที่กำหนดโดยสำนักงานปลัดกระทรวงสาธารณสุข

๒.๔ กำกับติดตามการจัดทำแผนงาน โครงการ และงบประมาณเพื่อการรักษาความปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

๒.๕ สรุปรายงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาล ครอบคลุมในประเด็น ประสิทธิภาพ ประสิทธิผล การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การลดความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ และกลไกในการควบคุมให้เกิดความเสี่ยงน้อยสุด

(๒.๖) ปฏิบัติภารกิจ.....

๒.๖ ปฏิบัติภารกิจอื่นตามที่กำหนดหรือตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๙ พฤศจิกายน พ.ศ. ๒๕๖๖

(นายสุกิจ บรรจงกิจ)
ผู้อำนวยการโรงพยาบาลเฉลิมพระเกียรติ
สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๑. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี ที่จะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ ทรัพยากรต่างๆ อย่างเหมาะสม มีประสิทธิภาพมากขึ้น และลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร

ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งเป็นความไม่แน่นอนทีอาจจะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างทีกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบทีเกิดขึ้น จัดลำดับความสำคัญของความเสี่ยง กำหนดแนวทางในการจัดการความเสี่ยง และต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อเป็นแนวทำงานทีใช้ตรวจสอบและ ประเมินความเสียงด้านเทคโนโลยีสารสนเทศด้วยการคาดการณ์ล่วงหน้า ในกรณีทีความเสียงเกิดขึ้นจริง สามารถนำแนวทำงานจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการได้

๒. วัตถุประสงค์ของแผนบริหารความเสี่ยง

๑. เพื่อให้ผู้บริหารและผู้ปฏิบัติงาน เข้าใจหลักการและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒. เพื่อให้การจัดการภายในกลุ่มงานสารสนเทศทางการแพทย์ข้อมูลมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัว ให้ทันต่อการเปลียนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่รวมทั้งลดโอกาสทีจะก่อให้เกิดความเสียหายทีไม่ ต้องการกับระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้ผู้ปฏิบัติงานได้รับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยง

๔. เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๕. เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับองค์กร

๖. เพื่อเป็นแนวทำงานการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความ เข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในโรงพยาบาล

๗. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับ การดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทำงานในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

๓. เป้าหมาย

๑. ผู้บริหารและผู้ปฏิบัติงานมีความรู้ความเข้าใจเรื่องการบริหารความเสี่ยง เพื่อนำไปใช้ในการดำเนินงานตามยุทธศาสตร์ และแผนปฏิบัติงานประจำปีให้บรรลุตามวัตถุประสงค์และเป้าหมายที่ กำหนดไว้

๒. ผู้บริหารและผู้ปฏิบัติงานสามารถระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยง และ จัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๓. สามารถนำแผนบริหารความเสี่ยงไปใช้ในการบริหารงานที่รับผิดชอบ

๔. เพื่อพัฒนาความสามารถของบุคลากรและกระบวนการดำเนินงานภายในองค์กรอย่างต่อเนื่อง

๕. ความรับผิดชอบต่อความเสี่ยงและการบริหารความเสี่ยงถูกกำหนดขึ้นอย่างเหมาะสมทั่วทั้งองค์กร

๖. การบริหารความเสี่ยงได้รับการปลูกฝังให้เป็นวัฒนธรรมขององค์กร

๔. ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้นและทำให้องค์กรสามารถจัดการ กับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย

ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

๑. เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยง และผู้บริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพ และประสิทธิผลมากยิ่งขึ้น

๒. สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร การบริหารความเสี่ยงจะเป็น แหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ ซึ่งรวมถึงการบริหารความเสี่ยง ซึ่งตั้งอยู่บนสมมุติฐานในการตอบสนองต่อเป้าหมายและภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้

๓. ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วนซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล

๔. เป็นเครื่องมือที่สำคัญในการบริหารงาน การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่า ความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของโรงพยาบาลเป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์ รวมทั้งเพิ่มมูลค่าแก่องค์กร

๕. ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์ วัตถุประสงค์ของ องค์กร และระดับความเสี่ยงอย่างชัดเจน

๖. ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากร เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล การจัดสรร ทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรมและการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูงย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

๕. นิยามความเสี่ยง

๕.๑ ความเสียง (Risk)

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลด โอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กรทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงินและการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ลักษณะของความเสี่ยง สามารถแบ่งออกได้เป็น ๓ ส่วน ดังนี้

๑. ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง

๒. เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน หรือ นโยบาย

๓. ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณ์เสี่ยง

๕.๒ การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้วทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้ จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และ ต่ำ

๕.๓ การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลงหรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ใน ระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทำงานหลัก คือ การยอมรับ การลด/ควบคุมการยกเลิกและการโอนย้ายหรือแบ่งความเสี่ยง

๕.๔ การควบคุม (Control) หมายถึง นโยบายแนวทำงานหรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลด ความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การ ควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะและการควบคุมเพื่อการแก้ไข

๕.๕ ทรัพย์สิน (Asset) หมายถึง ทรัพย์สินต่างๆ ขององค์กรแบ่งเป็น ๕ หมวด ได้แก่ หมวดข้อมูล หมวด บุคลากร หมวดฮาร์ดแวร์ หมวดซอฟต์แวร์ และหมวดบริการ

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยง ตาม มาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission) มีดังนี้

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
๒. การระบุความเสี่ยงต่างๆ (Event Identification)
๓. การประเมินความเสี่ยง (Risk Assessment)
๔. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
๕. กิจกรรมการบริหารความเสี่ยง (Control Activities)
๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
๗. การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

ทั้งนี้ ในการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลฯ ได้มีผู้เชี่ยวชาญด้านการตรวจประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑. การวิเคราะห์ความเสี่ยงและกระบวนการบริหารความเสี่ยง (Risk Analysis)

กระบวนการบริหารความเสี่ยงเป็นกระบวนการที่ใช้ในการระบุวิเคราะห์ ประเมิน และจัดลำดับความ เสียงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ในการดำเนินงานขององค์กรรวมทั้งการจัดทำแผนบริหารจัดการ ความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยให้อยู่ในระดับที่อมรับได้ ซึ่งงาน เทคโนโลยีสารสนเทศ มีขั้นตอนหรือกระบวนการบริหารความเสี่ยง ๖ ขั้นตอนหลัก ดังนี้

๑.๑ การระบุความเสี่ยง (Risk identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยง โดยต้องคำนึงถึงความเสี่ยงที่มีสาเหตุมาจากปัจจัยทั้งภายในและภายนอก ปัจจัยเหล่านี้มีผลกระทบต่อวัตถุประสงค์และเป้าหมายของ องค์กร หรือผลการปฏิบัติงานทั้งในระดับองค์กรและระดับกิจกรรม ในการระบุปัจจัยเสี่ยงจะต้องพิจารณาว่ามี เหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงานที่อาจเกิดความผิดพลาดความเสียหายและไม่บรรลุวัตถุประสงค์ที่กำหนด รวมทั้งมีทรัพย์สินใดที่จำเป็นต้องได้รับการดูแลป้องกันรักษา ดังนั้นจึงจำเป็นต้องเข้าใจใน ความหมายของ “ความเสี่ยง (Risk)” “ปัจจัยเสี่ยง (Risk Factor)” และ “ประเภทความเสี่ยง” ก่อนที่จะ ดำเนินการระบุความเสี่ยงได้อย่างเหมาะสม

- ความเสี่ยง (Risk)

หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุ เป้าหมายตามภารกิจหลักขององค์กรและเป้าหมายตามแผนปฏิบัติงาน

- ปัจจัยเสี่ยง (Risk Factor)

หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุ ได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควร เป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง โดยปัจจัย เสี่ยงแบ่งได้ ๒ ด้าน ดังนี้

๑. ปัจจัยเสี่ยงภายนอก คือ ความเสี่ยงที่ไม่สามารถควบคุมการเกิดได้โดยองค์กร เช่น เศรษฐกิจ สังคม การเมือง กฎหมาย คู่แข่ง เทคโนโลยี ภัยธรรมชาติ สิ่งแวดล้อม

๒. ปัจจัยเสี่ยงภายใน คือ ความสี่ยงที่สามารถควบคุมได้โดยองค์กร เช่น กฎระเบียบข้อบังคับภายในองค์กร วัฒนธรรมองค์กร นโยบายการบริหารและการจัดการ ความรู้/ความสามารถของบุคลากร กระบวนการทำงาน ข้อมูล/ระบบสารสนเทศ เครื่องมือ/อุปกรณ์

๑.๓ ประเภทความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของโรงพยาบาลแพร่สามารถแยกประเภทความเสี่ยงเป็น ๕ ประเภท ดังนี้

- **ความเสี่ยงด้านความมั่นคงปลอดภัยของทรัพยากรในระบบเทคโนโลยีสารสนเทศ**
- Hardware ,Software ,Network , Data

-ความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศอาจทำให้เกิดความบกพร่องในการดูแลรักษา ผู้ป่วย เป็นความเสี่ยงทีอาจเกิดขึ้นจากระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อการรักษาผู้ป่วย ทำให้ข้อมูลผิดพลาดไม่ถูกต้องตรงกัน ข้อมูลที่สำคัญไม่อยู่ระบบ ข้อมูลที่จำเป็นและสำคัญไปถึงผู้ป่วยหรือผู้ให้บริการล่าช้า จนทำให้เกิดความบกพร่องในการดูแลรักษาผู้ป่วย เช่น ข้อมูลผู้ป่วยคนหนึ่งไปอยู่กับผู้ป่วยคนหนึ่ง , ข้อมูลไม่ครบถ้วน ขาดหาย , ข้อมูลไปถึงผู้ป่วยล่าช้า , การใช้ Default values ที่ผิดพลาด , ข้อมูลในคอมพิวเตอร์กับในกระดาษไม่ตรงกัน , การแก้ไขข้อมูลหลังจากมีผู้ได้รับข้อมูลนั้นไปแล้ว เป็นต้น

-ความเสี่ยงด้านความเป็นส่วนตัวของผู้ป่วย เป็นความเสียงที่อาจเกิดขึ้นจากการดำเนินการการ จัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยี สารสนเทศของโรงพยาบาลแพร่ หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลแพร่เกินกว่าอำนาจหน้าทีของตนเองทีมีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ความเสี่ยงจากผู้ปฏิบัติงานเป็นความเสียงทีอาจเกิดขึ้นจาก การดำเนินการการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้า สู่ระบบเทคโนโลยีสารสนเทศ หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และ อาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

- **ความเสียงด้านภัยหรือสถานการณ์ฉุกเฉิน** เป็นความเสี่ยงทีอาจเกิดจากภัยพิบัติตามธรรมชาติ หรือสถานการณ์ร้ายแรงทีก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

- **ความเสียงด้านการบริหารจัดการ** เป็นความเสียงจากแนวนโยบายในการบริหารจัดการทีอาจ ส่งผลกระทบต่อการดำเนินการด้านเทคโนโลยีสารสนเทศ

๒. การจัดการความเสี่ยง (Risk management)

นโยบายของกลุ่มงานเทคโนโลยีสารสนเทศทางการแพทย์ โรงพยาบาลฯ ระดับความเสี่ยงคงเหลือที่ยอมรับได้ กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูงตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็น

๒.๑. หลีกเลี่ยงความเสี่ยง (Risk Avoidance = RA) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบันโรงพยาบาลฯ มีการสำรองข้อมูลเพียง ๑ ชุดและจัดเป็นความ เสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล ๒ ชุด และแยกเก็บในสถานที่ต่างกัน การบริหารจัดการการเชื่อมโยงสู่เครือข่ายผ่านโมเด็ม ถ้าเป็น การยากต่อการควบคุมหรือบริหารจัดการ องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ใช้บริการและแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของ ไวรัสอย่างหนัก องค์กรอาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น

๒.๒ การโอนย้ายความเสี่ยง (Risk Transfer = RF) เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่าย ไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังขาย (Maintenance service) เป็นต้น

๒.๓ การยอมรับความเสี่ยง (Risk acceptance = RC) เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ id/ password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การให้มีใช้ชีวมาตร (biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่าโรงพยาบาล อาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร

๒.๔ การลดความเสี่ยง (Loss Reduction = LR) ได้แก่ การมีมาตรการควบคุมมากชนิดขึ้น หรือชนิดที่เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (biometrics) เพื่อใช้ในการพิสูจน์ตัวจริงนอกเหนือไปจากการใช้ id/ password ที่มีอยู่เดิม

๒.ด้านการควบคุมระบบเทคโนโลยีสารสนเทศ

๒.๑ กำหนดสิทธิการเข้าถึงข้อมูลตามลำดับชั้นความลับเป็นลายลักษณ์อักษรชัดเจน

มาตรการรักษาความปลอดภัย

มาตรการรักษาความปลอดภัยของข้อมูลผู้รับบริการ โรงพยาบาล*เฉลิมพระเกียรติสมเด็จพระเทพ*รัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง โดยกำหนดให้มีมาตรการรักษาความปลอดภัยของฐานข้อมูลผู้รับบริการ โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง จึงออกประกาศไว้ ดังต่อไปนี้

๑. ให้บุคคลที่ได้รับรหัสผู้ใช้งานและรหัสผ่าน เพื่อเข้าใช้ฐานข้อมูลของโรงพยาบาล ต้องรับผิดชอบ เก็บรักษารหัสผู้ใช้งานและรหัสผ่านไว้เป็นความลับ และปกป้องมิให้บุคคลอื่นใช้รหัสผู้ใช้งาน และรหัสผ่าน เช่น ต้องไม่เขียนรหัสผ่าน หรือจดบันทึกไว้ที่มองเห็นได้

๒. ห้ามมิให้ผู้ได้รับรหัสผู้ใช้งานและรหัสผ่าน บอกหรือกระทำการใดๆที่ประสงค์ต่อผล เพื่อให้บุคคลอื่นทราบรหัสผ่านของตน

๓. ผู้ได้รับรหัสผู้ใช้งานและรหัสผ่าน ต้องเปลี่ยนรหัสผ่านทุก ๑ เดือน หรือเปลี่ยนรหัสผ่านทันที เมื่อมีข้อสงสัยว่ารหัสผู้ใช้งานและรหัสผ่านถูกเปิดเผย ทำให้ผู้อื่นนำไปใช้งานได้ การตั้งรหัสผ่านเพื่อเข้าใช้งานจะกลับมาใช้รหัสผ่านเดิมได้ ต้องมีการเปลี่ยนรหัสผ่านเป็นรหัสผ่านอื่นๆ ที่ไม่ซ้ำกันมาแล้วไม่น้อยกว่า ๓ ครั้ง

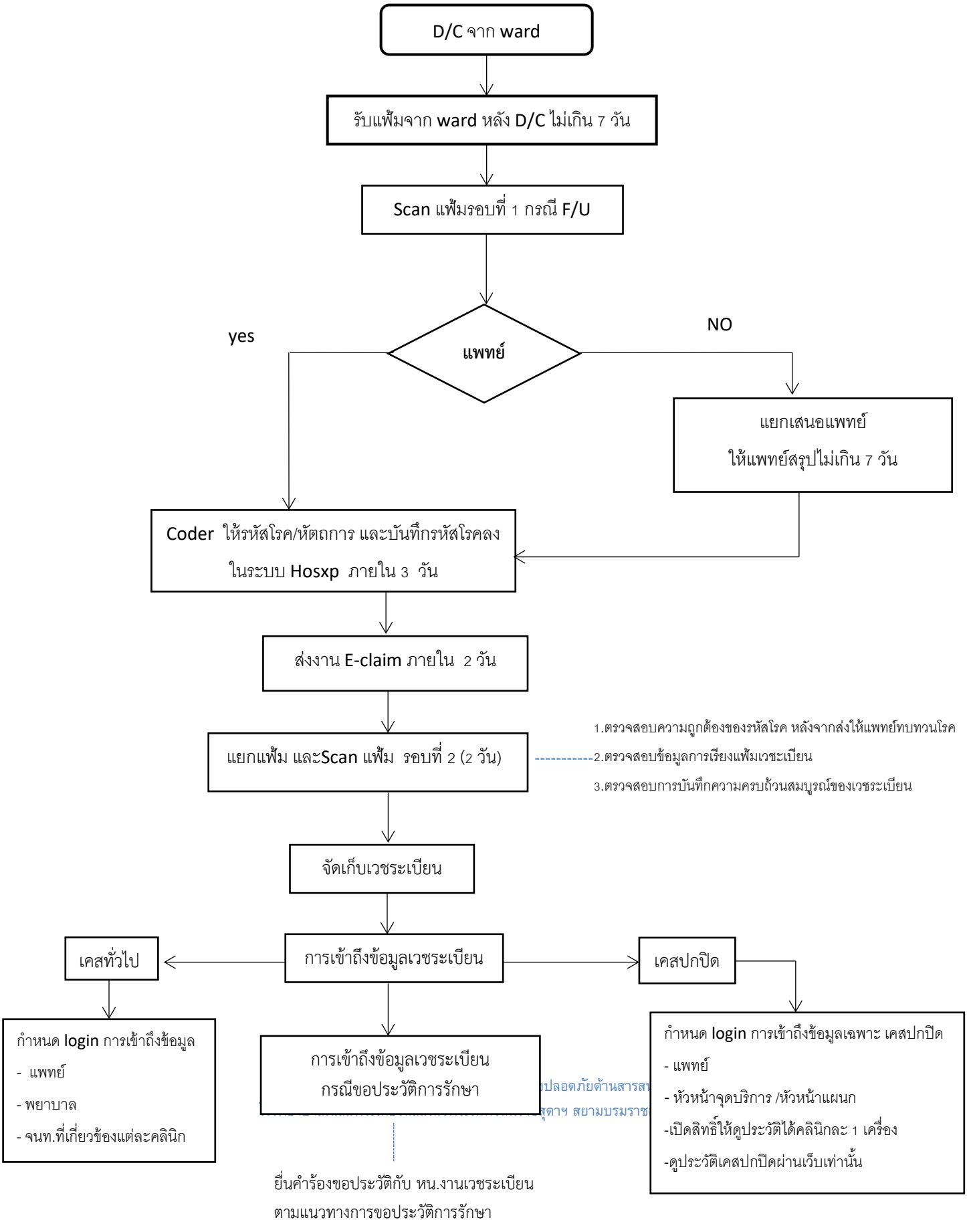
๔. ในการเข้าใช้ฐานข้อมูลผู้รับบริการของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง ให้เข้าใช้ได้ตามหน้าที่รับผิดชอบ และที่ได้รับมอบหมายจากทางโรงพยาบาลเท่านั้น

๕. กรณีตรวจพบว่าผู้ได้รับรับรหัสผู้ใช้งานและรหัสผ่าน มีการเข้าใช้งานฐานข้อมูลผู้รับบริการของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯสยามบรมราชกุมารี ระยองที่ไม่เหมาะสม คณะกรรมการสารสนเทศขอสงวนสิทธิการใช้งานของรหัสผู้ใช้ และรหัสผ่านทันที แล้วจึงแจ้งให้ทราบภายหลัง ทั้งนี้ เพื่อให้เป็นไปตามนโยบายการรักษาความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

๖. ห้ามมิให้เข้าใช้ฐานข้อมูลผู้รับบริการ เพื่อประโยชน์ทางธุรกิจ หรือเรื่องอื่นที่ไม่เกี่ยวกับทางราชการ ทั้งนี้เพื่อให้เป็นไปตามเจตนารมณ์ของ พรบ.ข้อมูลข่าวสาร

๗. ความรับผิดและปัญหาที่อาจจะเกิดขึ้นจากการไม่ปฏิบัติตามประกาศนี้ หรือจากการนำรหัสผู้ใช้งานและรหัสผ่านไปให้บุคคลอื่นใช้งาน ผู้ที่มีชื่อเป็นเจ้าของรหัสผู้ใช้งานและรหัสผ่านนั้นๆ จะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

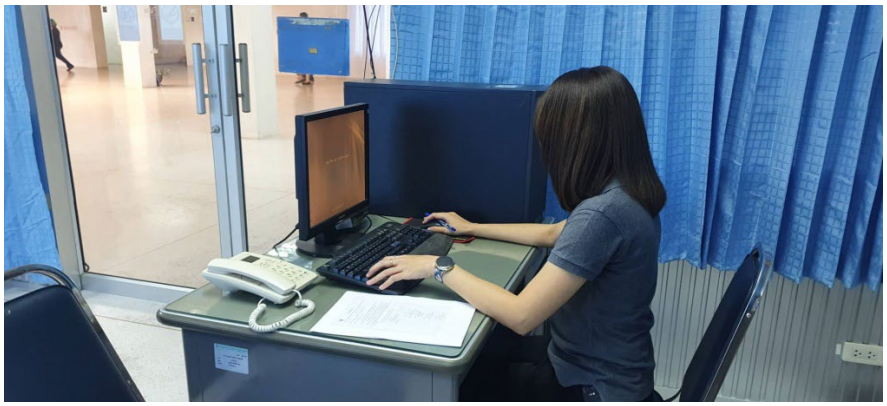
Flow chart ระบบเวชระเบียนผู้ป่วยใน หลังจำหน่าย



๒.๒ ห้องปฏิบัติงานหรือห้องควบคุมระบบเครือข่ายเป็นพื้นที่เฉพาะบุคคลที่ได้รับอนุญาตและต้องมีการแบ่งพื้นที่เป็นสัดส่วนชัดเจน เช่น

๒.๒.๑ ส่วนปฏิบัติงาน (Operation Zone)

โต๊ะสำหรับเจ้าหน้าที่ผู้ปฏิบัติงานในห้องปฏิบัติการ



๒.๒.๒ ส่วนของเครื่องแม่ข่าย (Server Zone)

Rack สำหรับ Server Zone

๒.๒.๓ ส่วนเครื่องสำรองไฟ (UPS Zone)

- มีเครื่องสำรองไฟฟ้า UPS ขนาด 3 Kva จำนวน 4 ชุด สามารถสำรองไฟฟ้าได้มากกว่า 30 นาที

๒.๓ สถานที่จัดเก็บอุปกรณ์เกี่ยวกับสารสนเทศมีการล็อคกุญแจเมื่อไม่มีการใช้งาน

สถานที่ในการเก็บอุปกรณ์และเครื่องมือทางด้านสารสนเทศจะล๊อคกุญแจททุกครั้งหลังใช้งานเสร็จ

๒.๔ มีกฎข้อบังคับการปฏิบัติตนของเจ้าหน้าที่ขณะปฏิบัติงานและมีสัญลักษณ์การแจ้งเตือน ที่เห็นชัดเจน เช่น ห้ามสูบบุหรี่ ห้ามนำอาหารและเครื่องดื่ม เข้ามารับประทาน

๒.๕ UPS (เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ) มีเพียงพอและอยู่ในสถานะพร้อมใช้งาน เพื่อป้องกันอุปกรณ์และข้อมูลสารสนเทศเสียหาย กรณีไฟฟ้าดับหรือไฟฟ้าตก

- มีเครื่องสำรองไฟฟ้า UPS ขนาด 3 Kva จำนวน 4 ชุด สามารถสำรองไฟฟ้าได้มากกว่า 30 นาที

ระบบไฟฟ้าสำรอง

สามารถผลิตกระแสไฟฟ้าได้ 24 ชั่วโมง สามารถจ่ายกระแสไฟฟ้าได้ภายใน 10 วินาทีโดยสำรองน้ำมันเชื้อเพลิงไว้ใช้ได้ 24 ชั่วโมง ครอบคลุมการบริการผู้ป่วย และสามารถจัดหาน้ำมันเชื้อเพลิงจากสถานีบริการน้ำมันที่ใกล้ที่สุดซึ่งห่างจากโรงพยาบาล 1 กิโลเมตร

เครื่อง Generator

มีเครื่อง *Generator* ที่สามารถจ่ายกระแสไฟฟ้าได้ภายใน 10 วินาที สามารถผลิตกระแสไฟฟ้าได้ 24 ชั่วโมง

๒.๖ มีแผนและการตรวจสอบ บำรุงรักษาสายไฟฟ้า สายสื่อสาร สายเคเบิล อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สำรองไฟฟ้า อุปกรณ์สำรองข้อมูล ภายในห้องปฏิบัติการ

แนวทางการปฏิบัติ

แผนการตรวจสอบ อุปกรณ์เครือข่าย อุปกรณ์คอมพิวเตอร์ อุปกรณ์สำรองไฟฟ้า อุปกรณ์สำรองข้อมูล โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง ดูแลและบำรุงรักษาอุปกรณ์เครือข่ายในโรงพยาบาล

แผนการตรวจสอบดูแลและบำรุงรักษาอุปกรณ์เครือข่าย อุปกรณ์คอมพิวเตอร์ อุปกรณ์สำรองไฟฟ้า โรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง 2567

การดำเนินการ / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ษ.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
1.ทำความสะอาดตู้ Rack Network ทุกตึก												
2.ตรวจสอบและเปลี่ยนแบตเตอรี่ UPS สำหรับระบบเครือข่าย												
3.ตรวจสอบการทำงานของ Switch ทุกตึก												
4.ตรวจสอบและบำรุงรักษาเครื่องสำรองไฟฟ้าและเครื่องคอมพิวเตอร์												
5.ตรวจสอบและบำรุงรักษาเครื่องแม่ข่ายและระบบเครือข่าย												

๓.แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศของผู้ใช้งาน

๑. การเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์ของโรงพยาบาล ดังนี้

๑.๑ ข้อมูลหน่วยงาน (General information) ประกอบด้วย ประวัติความเป็นมา วิสัยทัศน์ พันธกิจ ค่านิยม MOPH โครงสร้างหน่วยงาน ทำเนียบผู้บริหาร อำนาจหน้าที่ ยุทธศาสตร์ แผนปฏิบัติราชการ แผนงาน โครงการ และงบประมาณรายจ่ายประจำปี รายละเอียดช่องทางการติดต่อสื่อสาร หมายเลข โทรศัพท์ หมายเลขโทรสาร แผนที่ตั้งหน่วยงาน ไปรษณีย์อิเล็กทรอนิกส์ (email address)

๑.๒ คลังความรู้ (Knowledge) เช่น ข่าวสารความรู้สุขภาพในรูปแบบ Info Graphic บทความ ผลงานวิจัย ข้อมูลสถิติต่างๆ โดยอ้างอิงถึงแหล่งที่มาและวัน เวลา กำกับเพื่อประโยชน์ใน การนำข้อมูลไปใช้ต่อ (ถ้ามี)

๑.๓ รายชื่อเว็บไซต์หน่วยงานที่เกี่ยวข้อง (Web Link) เช่น กลุ่มงาน/งานต่างๆ ใน โรงพยาบาล หน่วยงานภายนอก หรือเว็บไซต์อื่นๆ ที่สนใจ

๑.๔ คู่มือสำหรับประชาชน (Service information) ข้อมูลการบริการตามภารกิจของ หน่วยงาน โดยแสดงขั้นตอนการให้บริการต่างๆ แก่ประชาชนพร้อมอธิบายขั้นตอนการบริการอย่างชัดเจนทั้งนี้ ควรระบุ ระยะเวลาในแต่ละขั้นตอนของการบริการนั้นๆ

๑.๕ ข่าวประชาสัมพันธ์ ข่าวสารทั่วไป ภาพข่าวกิจกรรม เรื่องแจ้งเตือน รวมถึงข่าว ประกาศของ หน่วยงาน เช่น ประกาศรับสมัครงาน ประกาศจัดซื้อจัดจ้าง ผลการจัดซื้อจัดจ้าง

๑.๖ แสดงสถิติการเข้าใช้บริการเว็บไซต์

๒. วิธีการและขั้นตอนการเผยแพร่ข้อมูลต่อสาธารณะผ่านเว็บไซต์หน่วยงาน ให้ดำเนินการดังนี้

๒.๑ หัวหน้าหน่วยงาน มอบหมายหรือกำหนดเจ้าหน้าที่ปฏิบัติงานบริหารจัดการเว็บไซต์ ของ หน่วยงาน

๒.๒ เจ้าหน้าที่ผู้ได้รับมอบหมาย ได้รับสิทธิ์ เข้าสู่ระบบบริหารจัดการ ดำเนินการนำข้อมูล ข่าวสารขึ้นเว็บไซต์

๒.๓ การนำข้อมูลข่าวสาร ต้องเป็นข้อมูลปัจจุบัน ถูกต้องและครบถ้วน ระบุแหล่งที่มา หรือ เจ้าของข้อมูล ช่วงวันที่ของข้อมูลข่าวสาร วันที่เผยแพร่ ประเภท (นามสกุล) ไฟล์ ขนาดไฟล์โดยมีลำดับการ ปฏิบัติอย่างน้อยดังนี้

(๑) เจ้าหน้าที่เสนอข้อมูลข่าวสาร ที่ประสงค์จะนำขึ้นเผยแพร่บนเว็บไซต์ ให้ ดำเนินการขออนุมัติ เสนอผู้อำนวยการโรงพยาบาล พิจารณาอนุญาต ด้วยแบบฟอร์มการขอเผยแพร่ข้อมูลผ่าน เว็บไซต์ของ หน่วยงาน

(๒) หัวหน้าหน่วยงาน มอบหมายเจ้าหน้าที่ผู้รับผิดชอบ บริหารจัดการระบบ เว็บไซต์ (Web Master) ของโรงพยาบาล อนุมัติสิทธิการเข้าใช้งาน (Username และ Password) เข้าสู่ ระบบบริหารจัดการ ดำเนินการนำข้อมูลข่าวสารขึ้นเว็บไซต์ในหมวดหมู่ที่ถูกต้อง

(๓) เจ้าหน้าที่ Web Master มีหน้าที่ตรวจสอบความเป็นปัจจุบันของข้อมูลทุก รายการที่เผยแพร่ บนเว็บไซต์ของหน่วยงาน หากพบว่าครบระยะเวลาการเผยแพร่ ให้นำรายการนั้นลงจาก เว็บไซต์

(๔) เจ้าหน้าที่ Web Master มีหน้าที่ตรวจสอบความครบถ้วนของรายการข้อมูล ข่าวสารตาม มาตรฐานเว็บไซต์ของหน่วยงานภาครัฐ (Government Website Standard version ๒.๐) ของ สำนักงาน

รัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) และตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ ๒๕๔๐ ตามมาตร ๒ มาตรา ๙ และข้อมูลข่าวสารอื่นที่คณะกรรมการข้อมูลข่าวสารของราชการกำหนด

(๕) เจ้าหน้าที่ web Master มีหน้าที่ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ อย่างเคร่งครัด เพื่อป้องกันไม่ให้เกิดความเสียหายและลดโอกาสที่จะ เกิดความเสียหายแก่ทางราชการ

(๖) ส่งเสริมการเพิ่มพูนความรู้แลทักษะการบริหารจัดการเว็บไซต์ การรักษาความ มั่นคงปลอดภัยสารสนเทศ (Cyber Security) ให้แก่เจ้าหน้าที่อย่างต่อเนื่อง ทั้งการฝึกอบรม (Training) การ แลกเปลี่ยนเรียนรู้ระหว่างผู้ปฏิบัติงาน (Knowledge Management)

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

๓.๑ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ครอบคลุมในเรื่องต่อไปนี้

(๑) จัดทำแบบฟอร์มการขอใช้ระบบสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๓) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษ หากซ้ำให้เพิ่มอักษรตัวแรกของนามสกุล หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือความต้องการในการใช้งานระบบ

(๖) มีการระบุ ตำแหน่ง หน่วยงานที่สังกัด

(๗) มีการจัดเก็บข้อมูลการขออนุมัติเข้าใช้ข้อมูลระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓.๒ การทบทวนสิทธิการเข้าใช้งาน ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้ระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๔. มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management)

เป็นการกำหนดสิทธิและขอบเขตในการเข้าใช้งานระบบและเข้าถึงข้อมูลของผู้ใช้งานระบบ (users) ตามบทบาทและหน้าที่รับผิดชอบเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูล สารสนเทศ การเข้าถึงข้อมูล ดังนี้

๔.๑ มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password user) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๕) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๖) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๗) ไม่จดหรือบันทึกรหสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๘) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๙) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๐) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๑) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๒) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๔) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป

๕. การกำหนดสิทธิการใช้งานระบบของผู้ใช้งาน(user responsibilities)

๕.๑ การกำหนดสิทธิในการใช้ระบบของผู้ใช้งาน โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความ รับผิดชอบและตามความจำเป็นในการใช้งาน

(๓) การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๕.๒ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยง การใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งาน ควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้ รหัสผ่านยากต่อการเดา

(๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับ ความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและ ระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัส ผู้ใช้งานตามปกติ

๕.๓ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๖. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๕) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง

๔.การเข้าถึงระบบเครือข่าย

๔. การเข้าถึงระบบเครือข่าย

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๔.๑ กำหนดสิทธิผู้ใช้งานเฉพาะบริการที่ได้รับสิทธิเท่านั้น

การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศของสำนักงานปลัดกระทรวงสาธารณะสุข

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๔.๒ หน่วยงานกำหนดข้อปฏิบัติการเข้าถึงให้ผู้ใช้งานทราบ

การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งาน ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) ทุกครั้ง

(๒) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมี วิธีการยืนยันตัวบุคคล (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้ รหัสผ่าน (password) หรือการใช้สมาร์ทการ์ด เป็นต้น

(๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน อย่างน้อย ๑ วิธี

(๔) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

๔.๓ หน่วยงานมีการควบคุมการเชื่อมต่อ VPN FTP หรือ Telnet กับระบบเครือข่ายหลักหลัก อย่างรัดกุม

การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการ เข้าถึง ดังนี้

(๑) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(๒) มีการควบคุมการใช้งานอย่างเหมาะสม

(๓) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔.๔ ผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับการเข้าถึงบริการผ่านช่องทาง ดังนี้

การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการ เข้าถึงทางกายภาพและทางเครือข่าย

(๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็น ลายลักษณ์อักษร

๔.๕ มีข้อกำหนดการยืนยันตำวบุคคลก่อนอนุญาตให้ผู้ใช้งานเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน

การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๕. การเข้าถึงระบบปฏิบัติการ

๕. การเข้าถึงระบบปฏิบัติการ

๕.๑ หน่วยงานกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติ

๕.๑.๑ จัดทำทะเบียนระบบงานของระบบปฏิบัติการ โดยกำหนดกลุ่มผู้ใช้งาน และสิทธิของกลุ่มผู้ใช้งาน

๕.๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงระบบปฏิบัติการ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดเสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- บันทึกข้อมูล
- แก้ไขข้อมูล
- ลบข้อมูล
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจสิทธิ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบปฏิบัติการของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๕.๒ หน่วยงานกำหนดให้ผู้ใช้งานแสดงข้อมูลในการยืนยันตัวตนของผู้ใช้งาน

๕.๒.๑ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ครอบคลุมในเรื่องต่อไปนี้

(๑) จัดทำฟอร์มการขอชื่อผู้ใช้และรหัสผ่าน เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

(๒) มีการระบุชื่อ นามสกุล ของผู้ใช้งาน

(๓) มีการระบุหมายเลขใบประกอบวิชาชีพ และหมายเลขบัตรประชาชน

(๔) มีการระบุตำแหน่ง หน่วยงานที่ปฏิบัติงาน

๕.๒.๒ มีการทบทวนสิทธิการเข้าใช้งาน ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้ระบบปฏิบัติการ และปรับปรุงบัญชีผู้ใช้ ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น ลาออก, เปลี่ยนตำแหน่ง, โอน, ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

แบบฟอร์ม การขอชื่อผู้ใช้และรหัสผ่านเพื่อใช้ระบบงานเทคโนโลยีสารสนเทศ

ส่วนที่ 1 สำหรับผู้ขอใช้บริการ

คำนำหน้า ❒ นาย ❒ นาง ❒ นางสาว

ชื่อ(ไทย).....นามสกุล(ไทย).....

First Name(English)..... Last Name(English).....

วัน/เดือน/ปี เกิด .....

เลขใบประกอบวิชาชีพ(ถ้ามี).....

หมายเลขบัตรประจำตัวประชาชน 13 หลัก

❒-❒❒❒❒-❒❒❒❒❒-❒❒-❒

ตำแหน่ง .....

หน่วยงานที่ปฏิบัติงานปัจจุบัน .....

กรณีย้าย โปรดระบุ โรงพยาบาลที่ย้ายมา .....

ระบบงานที่ขอใช้

❒ HOSxP

❒ เวชระเบียน กรณีมีความประสงค์ขอดูเวชระเบียนผ่านระบบ Intranet จำเป็นต้องยืนยันผู้ใช้งานผ่าน E-mail โปรด ระบุ.....

❒ อื่น ๆ โปรดระบุ.....

ข้าพเจ้าขอรับรองว่าข้อมูลข้างต้นเป็นความจริงทุกประการและจะปฏิบัติตามระเบียนข้อกำหนดและนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทุกประการ

ลงชื่อ.....(ผู้ขอใช้บริการ)

(.....)

ตำแหน่ง.....

วันที่.....

ส่วนที่ 2 สำหรับเจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ

ได้ดำเนินการสร้างผู้ใช้งานและรหัสผ่านเพื่อใช้งานระบบสารสนเทศของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯสยามบรมราชกุมารี ระยอง และแจ้งผู้ขอรับบริการเรียบร้อยแล้ว

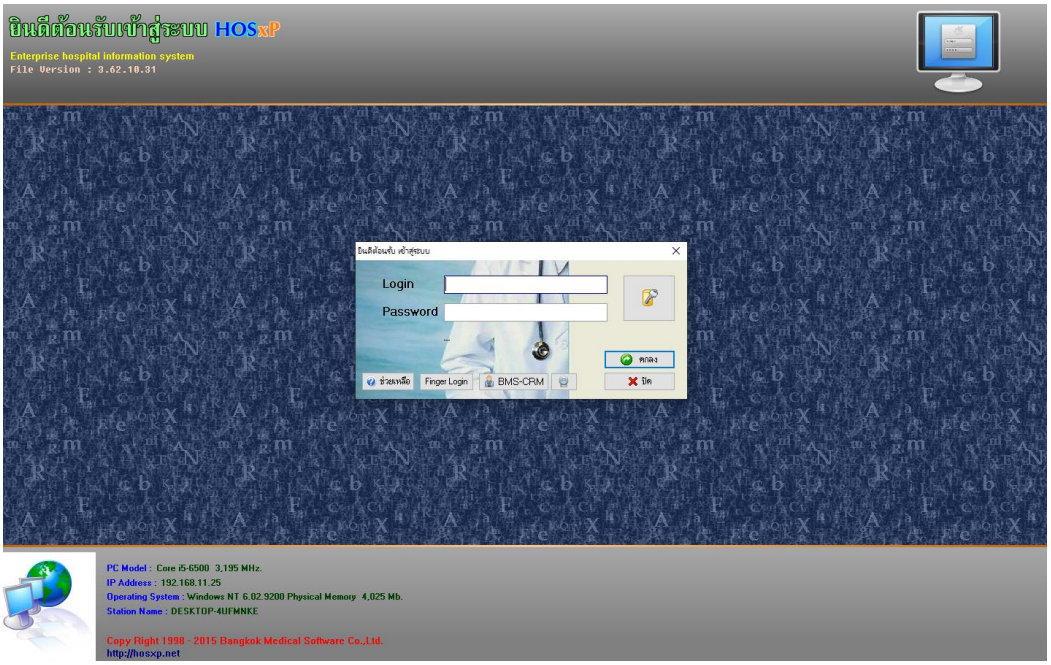
ลงชื่อ.....(ผู้ดำเนินการ) ลงชื่อ.....(หัวหน้างาน)

(.....) (.....)

วันที่..... วันที่.....

๕.๓ หน่วยงานมีการกำหนดรหัสผ่านที่สามารถทำงานอัตโนมัติได้

ก่อนการเข้าใช้งานระบบปฏิบัติการทุกครั้ง ผู้ใช้งานจะต้องทำการกรอกข้อมูล Username และ Password ในการเข้าใช้งานทุกครั้ง หากไม่มีการใช้งานติดต่อกันเกิน ๑๐ นาที ระบบจะทำการ Logout ให้โดยอัตโนมัติ



๕.๔ หน่วยงานมีการจำกัดหรือควบคุมการใช้งานโปรแกรมอรรถประโยชน์

เจ้าหน้าดูแลระบบสารสนเทศ หรือผู้ที่ได้รับมอบหมาย จะทำหน้าที่ติดตั้ง และตรวจสอบโปรแกรมอรรถประโยชน์ต่าง ๆ ที่ผู้ใช้ลงโปรแกรมเพิ่มเอง โดยเจ้าหน้าดูแลระบบสารสนเทศ จะทำการลบทุก ๆ สิ้นเดือน เพื่อเป็นการบำรุงรักษาเครื่องคอมพิวเตอร์

๕.๕ หน่วยงานจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมต่าง ๆ

มีการกำหนดเวลาในการใช้งานระบบสารสนเทศ หากไม่มีการใช้งานติดต่อกันเกิน ๑๐ นาที ระบบจะทำการ Logout ให้โดยอัตโนมัติ

๖. การเข้าถึง Application และสารสนเทศ

๖. การเข้าถึง Application และสารสนเทศ

๖.๑ หน่วยงานกำหนดแนวปฏิบัติ ในการเข้าถึงสารสนเทศ Application ต่าง ๆ ของผู้ใช้งาน

การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัด หรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุนการเข้าใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการ เข้าถึง หรือเข้าใช้งาน ที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๖.๒ ข้อจำกัดที่กำหนดเป็นไปตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานปลัดกระทรวงสาธารณะสุข ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึง ผลกระทบและระดับความสำคัญต่อหน่วยงาน
- มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ
- มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๓ หน่วยงานมีข้อกำหนดในการควบคุมคอมพิวเตอร์พกพา (Notebook) เข้าถึงสารสนเทศของหน่วยงาน

การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม ในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยง ของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๖.๔ หน่วยงานกำหนดมาตรการเพื่อป้องกันความเสี่ยงจากการใช้คอมพิวเตอร์พกพา (Notebook) และโทรศัพท์เคลื่อนที่

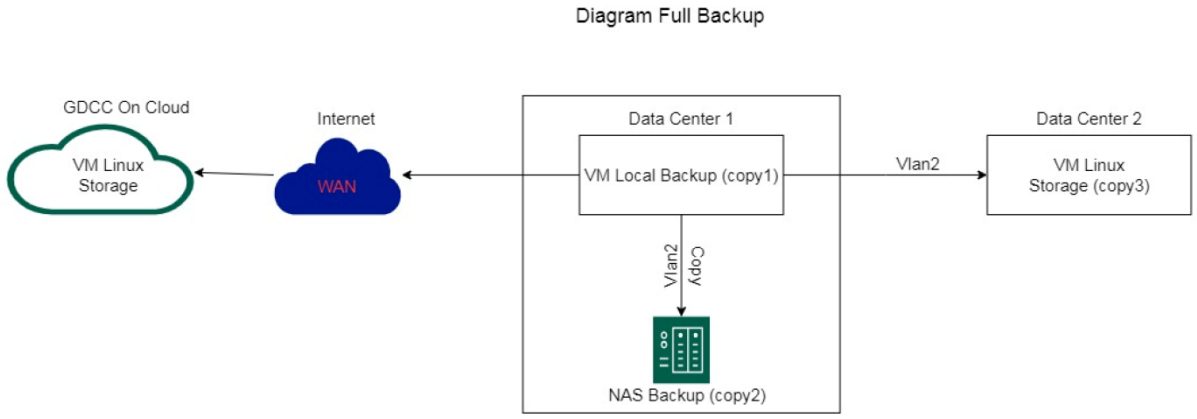
การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

๗. การจัดระบบสำรองฉุกเฉิน

๗.๑ หน่วยงานมีแนวปฏิบัติหรือหลักเกณฑ์ในการสำรองข้อมูลและกู้คืนระบบอย่างชัดเจน

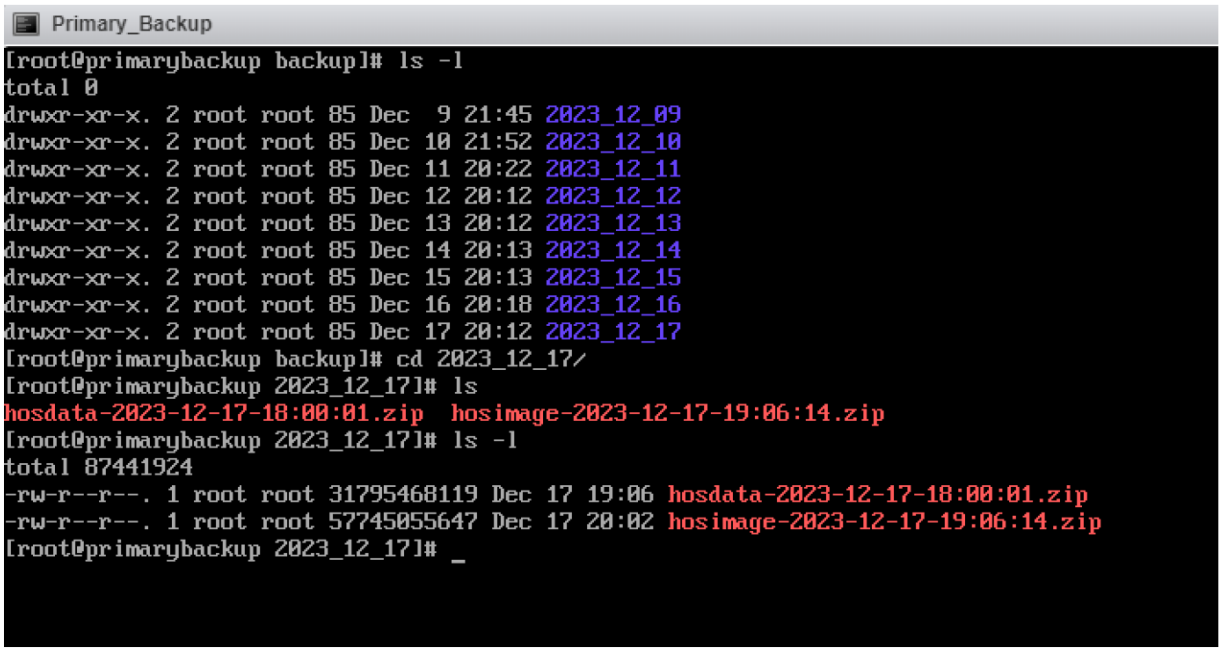
แนวทางในการสำรองข้อมูล ระบบ HIS ของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง มีระบบสำรองข้อมูลอัตโนมัติทุกวันแบบ ZIP โดยเริ่มแบ็คอัพเวลา ๐๑:๓๐ น. จะสำรองข้อมูลเสร็จประมาณ ๑๐:๐๐ น. ของทุกวัน และระบบสำรองข้อมูลบน VM สำรองระดับ OS โดยใช้ Veeam Backup & Replication สำรองข้อมูลทุกๆ ๔ ชั่วโมงสำหรับระบบ HIS ระบบอื่นๆสำรองข้อมูลทุกๆ ๒๔ ชั่วโมง หลังจากสำรองข้อมูลเสร็จสิ้นจะทำสำเนาข้อมูลเก็บแบ็คอัพไว้ ๒ ชุด โดยเก็บไว้บนเครื่องที่แบ็คอัพ ๑ ชุด และ NAS อีก ๑ ชุด โดยเก็บข้อมูลแบ็คอัพย้อนหลังไว้อย่างน้อย ๑๔ วัน และ ระบบ HIS ของโรงพยาบาลยังมีระบบ SERVER สำรองโดยระบบจะ REPICATE ข้อมูลจาก SERVER หลักไปยัง SERVER สำรองแบบ REALTIME พร้อมทั้ง REPICATE ข้อมูลไปยังระบบ CLOUD ของ GDCC

๑.สำรองข้อมูลรายวันในรูปแบบ ZIP ไฟล์

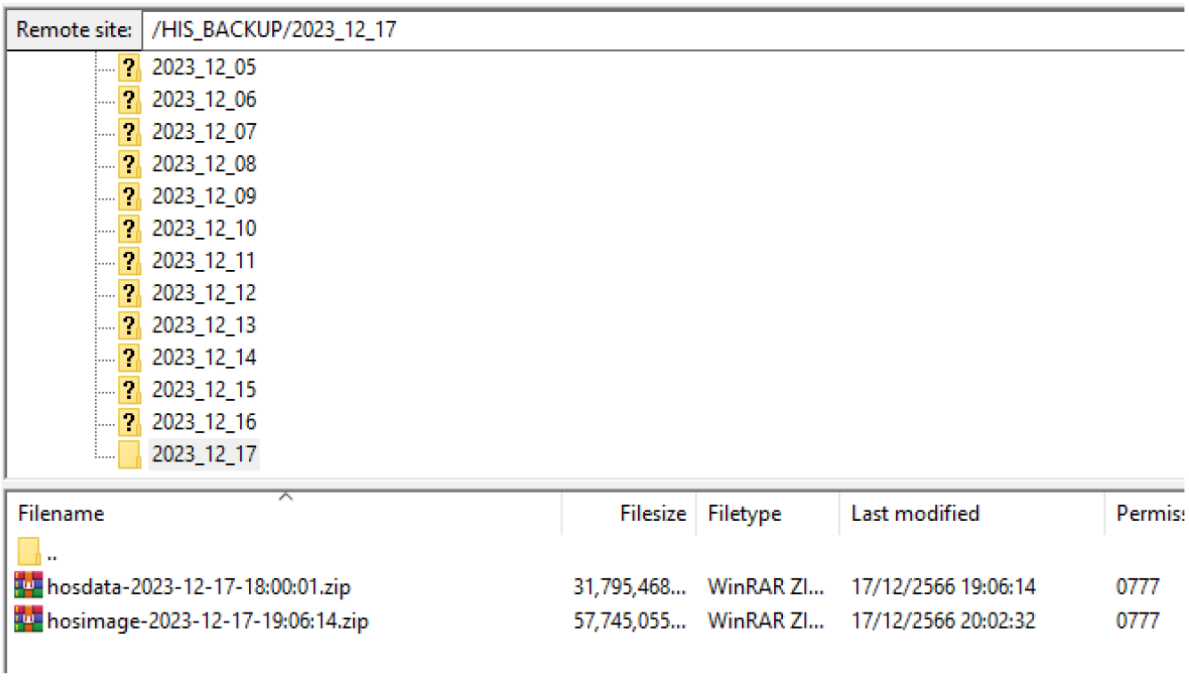


ระบบสำรองข้อมูลโดยการตั้งเวลาสั่งให้สคริปท์ทำงานโดยสคริปท์จะทำการต่อเน็ตเวิร์คอัตโนมัติและทำการสำรองข้อมูลมาเก็บไว้ที่ Local Backup หลังจากนั้นสคริปท์จะ Copy Backup ไปยัง Nas Backup ที่อยู่ใน Data center เดียวกัน , Copy ไปยัง Linux Storage ที่ Data center 2 , Copy ไปยัง Linux Storage ของ คลาวด์กลางภาครัฐ GDCC On Cloud หลังจากนั้นสคริปท์จะสั่งตัด Network อัตโนมัติ

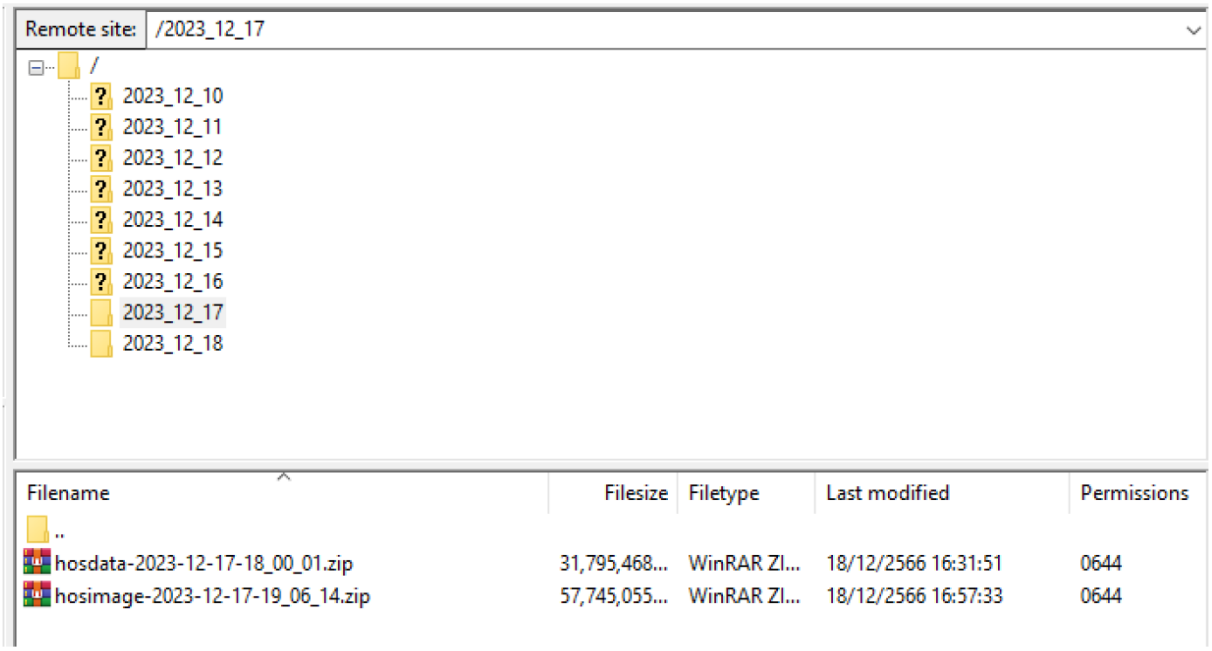
Vm Local Backup Copy1 (Data Center1)



Nas Backup Copy2 (Data Center1)



VM Storage Copy3 (Data Center2)



๒.สำรองข้อมูลระดับ VM ทุก ๔ ชั่วโมงในระบบ HIS และทุกๆ ๒๔ ชั่วโมงสำหรับระบบอื่นๆ

Backup job: HOSXP_MASTER
Created by WIN-8SELLUEVQ8L\Administrator at 20/1/2566 6:06.

18 ธันวาคม 2566 0:15:15

Success	1	**Start time**	0:15:15	**Total size**	1024 GB	**Backup size**	4.8 GB
Warning	0	**End time**	0:17:52	**Data read**	10 GB	**Dedupe**	1.0x
Error	0	**Duration**	0:02:37	**Transferred**	4.8 GB	**Compression**	2.1x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
HOSXP_MASTER	Success	0:15:33	0:17:47	1024 GB	10 GB	4.8 GB	0:02:14	

Backup job: HOSXP_MASTER
Created by WIN-8SELLUEVQ8L\Administrator at 20/1/2566 6:06.

17 ธันวาคม 2566 20:15:05

Success	1	**Start time**	20:15:05	**Total size**	1024 GB	**Backup size**	16.5 GB
Warning	0	**End time**	20:20:06	**Data read**	31.8 GB	**Dedupe**	1.0x
Error	0	**Duration**	0:05:01	**Transferred**	16.4 GB	**Compression**	2.0x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
HOSXP_MASTER	Success	20:15:23	20:20:01	1024 GB	31.8 GB	16.4 GB	0:04:38	

Backup job: HOSXP_MASTER
Created by WIN-8SELLUEVQ8L\Administrator at 20/1/2566 6:06.

17 ธันวาคม 2566 16:15:22

Success	1	**Start time**	16:15:22	**Total size**	1024 GB	**Backup size**	1.7 GB
Warning	0	**End time**	16:16:51	**Data read**	4 GB	**Dedupe**	1.0x
Error	0	**Duration**	0:01:29	**Transferred**	1.7 GB	**Compression**	2.3x

Details

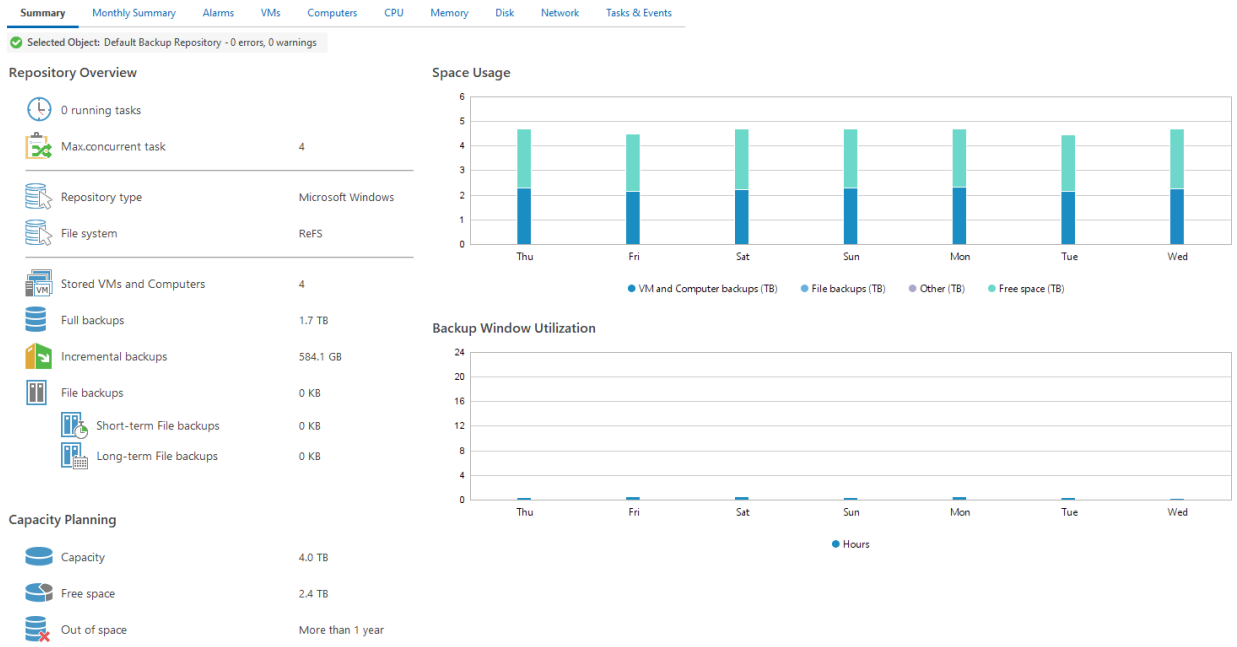
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
HOSXP_MASTER	Success	16:15:40	16:16:45	1024 GB	4 GB	1.7 GB	0:01:05	

Backup job: HOSXP_MASTER
Created by WIN-8SELLUEVQ8L\Administrator at 20/1/2566 6:06.

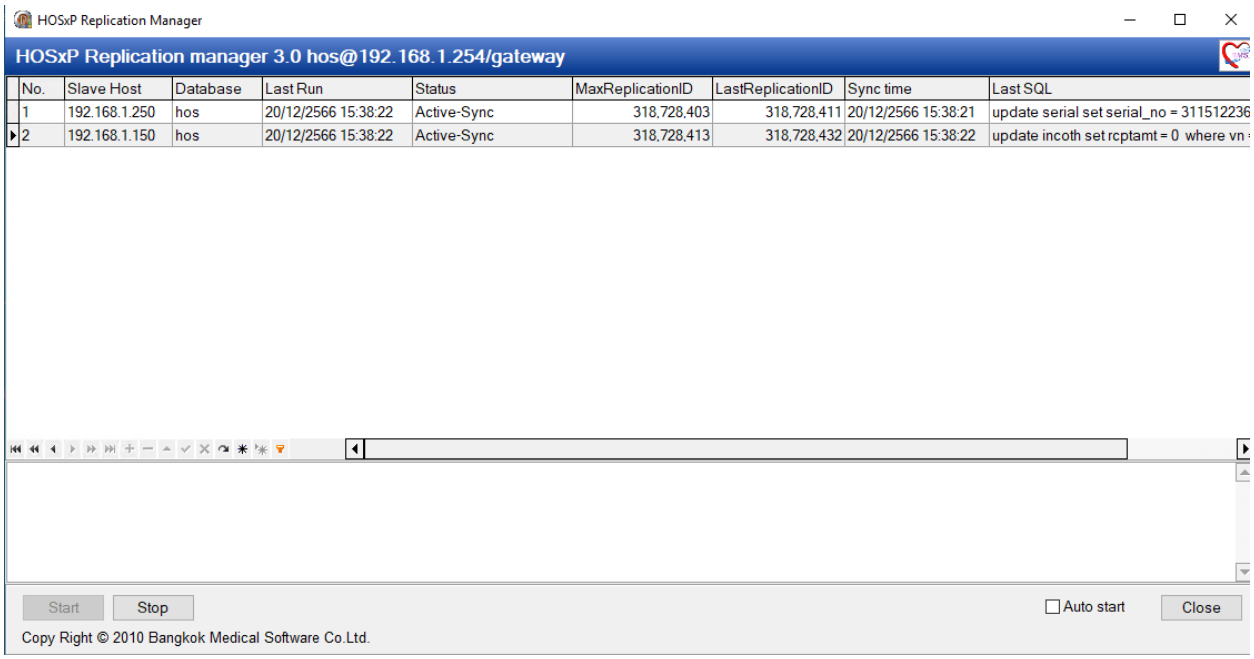
17 ธันวาคม 2566 13:24:06

Success	1	**Start time**	13:24:06	**Total size**	1024 GB	**Backup size**	5.3 GB
Warning	0	**End time**	13:26:49	**Data read**	11 GB	**Dedupe**	1.0x
Error	0	**Duration**	0:02:43	**Transferred**	5.3 GB	**Compression**	2.1x

๓.สรุปรายงานภาพรวมในการสำรองข้อมูล



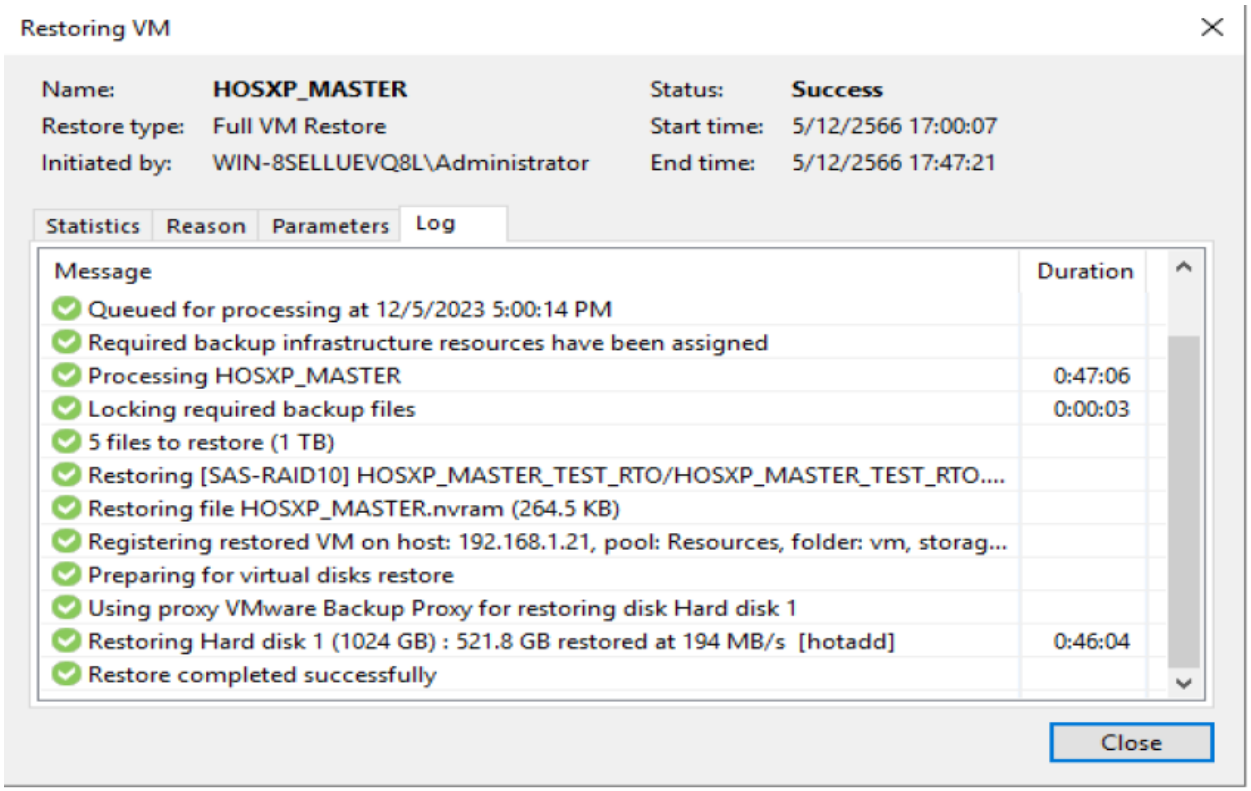
การ REPICATE ข้อมูลแบบ REALTIME ด้วยเครื่องมือของ HOSXp



แนวทางในการกู้คืน ระบบ HIS ของโรงพยาบาลเฉลิมพระเกียรติสมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี ระยอง

กรณีที่ ๑ SERVER หลักไม่สามารถใช้งานได้มีแนวทางในการกู้ระบบคือสลับไปใช้ SERVER สำรองชั่วคราว โดยเปลี่ยนไอพีของเครื่อง SERVER สำรองเป็นไอพีของเครื่อง SERVER หลักโดยขั้นตอนนี้จะใช้เวลาไม่เกิน ๑๕ นาที ระบบจะกลับมาทำงานได้ปกติระหว่างนี้ก็ทำการแก้ไขปัญหาเครื่อง SERVER หลัก หลังจากแก้ไขปัญหาเสร็จสิ้นจะทำการสลับไอพีกลับไปใช้ SERVER หลักเหมือนเดิม

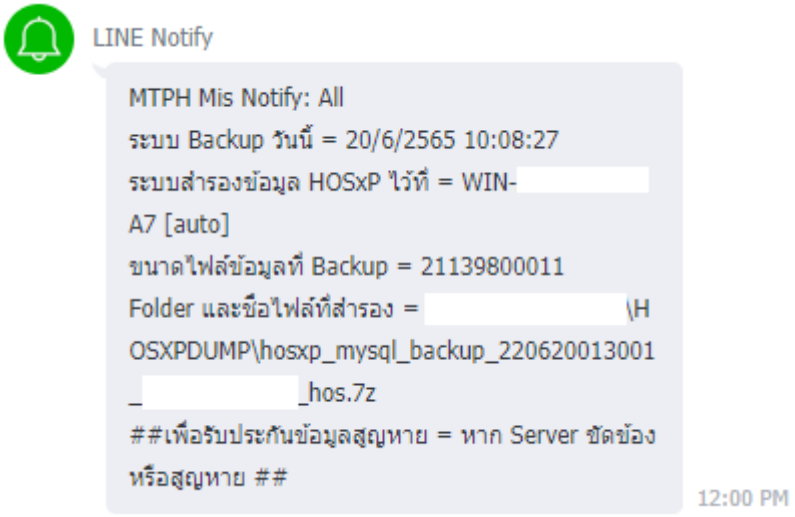
กรณีที่ ๒ ข้อมูลได้รับความเสียหายหรือสูญหายทั้ง SERVER หลักและสำรอง จะต้องทำการกู้ระบบโดยการ RESTORE ข้อมูลจาก BACKUP ที่สำรองด้วยระบบ VM ที่สำรองระดับ OS ไปยังเครื่องสำรองที่เตรียมไว้ในกรณีฉุกเฉินใช้เวลา Restore ประมาณไม่เกิน ๖๐ นาที
ตัวอย่างการทดสอบ Restore ผ่าน Veeam Backup & Replication



จากการทดสอบ Restore ใช้เวลาประมาณ 46 นาที

๗.๒ ทุกระบบที่จัดทำการสำรองข้อมูลและกู้คืนระบบมีรายงานผลการสำรองข้อมูลและกู้คืนระบบ

เมื่อระบบแบ็คอัพข้อมูลเสร็จสิ้นจะบันทึกประวัติการแบ็คอัพไว้ในฐานข้อมูลพร้อมกับแจ้งผลการแบ็คอัพผ่านระบบ Line Notify ไปยังผู้ดูแลระบบ



๗.๓ หน่วยงานมีการจัดทำแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ด้านระบบสารสนเทศ (BCP)

แนวทางการจัดการ

๑. ความเสี่ยงที่เกิดจากบุคลากรของสำนักงาน

ให้ความรู้แก่เจ้าหน้าที่ในหน่วยงานในการใช้งานคอมพิวเตอร์อย่างถูกต้องทั้งด้าน Software และ Hardware รวมถึงความรู้เรื่องการระบาดของไวรัสคอมพิวเตอร์ชนิดใหม่ๆ สม่ำเสมอ เพื่อลดความเสี่ยง

๒. ความเสี่ยงที่เกิดจากไวรัสคอมพิวเตอร์

๒.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่เครื่องแม่ข่ายและลูกข่าย
- อัพเดตฐานข้อมูลไวรัสสม่ำเสมอ
- ใช้โปรแกรมตรวจหาไวรัสในเครื่องอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๒.๒ ระมัดระวังการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ เช่น Thumb drive, CD-ROM

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลทุกครั้ง ก่อนเปิดใช้งาน
- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก หรือน่าสงสัย
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๒.๓ ระมัดระวังในการใช้งาน E-mail โปรแกรมสนทนา และ Social network และการดาวน์โหลดไฟล์จากอินเทอร์เน็ต

- ไม่ควรเปิดไฟล์ที่ไม่ทราบแหล่งที่มา และลบทันทีที่พบเห็น
- ไม่ควรเปิดไฟล์ที่ไม่รู้จักที่แนบมากับโปรแกรมสนทนาต่างๆ รวมถึงไฟล์จาก เว็บไซต์ Social network
- ควรระมัดระวัง E-mail ที่ถามข้อมูลส่วนบุคคล
- ไม่ควรเปิดเว็บไซต์ที่ ที่มากับ E-mail ที่ไม่ทราบแหล่งที่มา

- ไม่ควรเปิดเว็บไซต์ที่ไม่เหมาะสม เช่นเว็บไซต์ลามก เว็บไซต์ขายของออนไลน์ที่น่าสงสัย
- ไม่ควรดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ
- ไม่ดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ

๒.๔ มีการสำรองข้อมูล (Backup) เพื่อป้องกันความเสียหายที่จะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ หรือมีการเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีแนวทางทำระบบ Auto Backup

๓. ความเสี่ยงที่เกิดจากปัญหาไฟฟ้าดับไฟกระชาก

๓.๑ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลระบบคอมพิวเตอร์ทั้งคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๓.๒ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟให้พร้อมใช้งานเสมอ

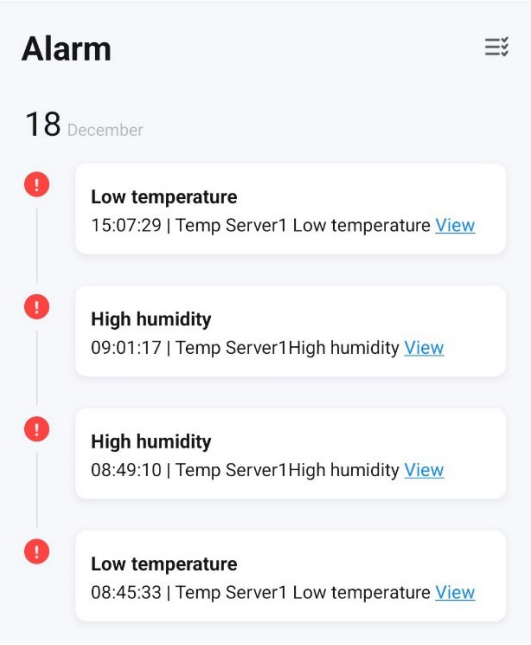
๓.๓ เมื่อเกิดไฟฟ้าดับให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๓.๔ ติดตั้งระบบป้องกันไฟกระชาก และไฟเกิน เพื่อป้องกันความเสียหายกับอุปกรณ์คอมพิวเตอร์และระบบสื่อสารผ่านอินเทอร์เน็ต

๔. ความเสี่ยงจากภัยธรรมชาติและอัคคีภัย

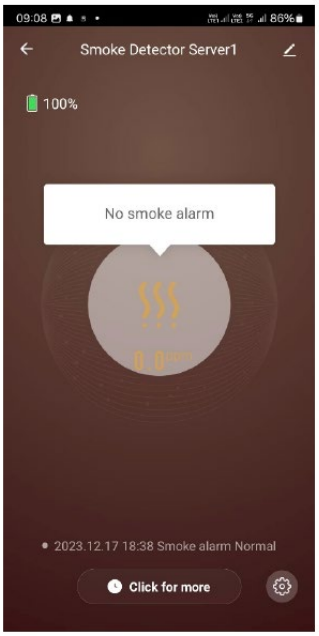
๔.๑ การป้องกันอุทกภัย อุณหภูมิและความชื้น

พื้นอาคารสำนักงานมีลักษณะยกสูงจึงปลอดภัยจากอุทกภัย แต่คอมพิวเตอร์แม่ข่ายต้องเปิดใช้งานตลอดเวลาจึงมีความเสี่ยงจากอุณหภูมิและความชื้นที่ไม่เหมาะสม ซึ่งส่งผลต่ออายุการใช้งาน ของอุปกรณ์คอมพิวเตอร์แม่ข่ายจึงเปิดเครื่องปรับอากาศตลอด ๒๔ ชั่วโมง และมี ระบบเฝ้าระวังมอนิเตอร์อุณหภูมิและความชื้น เมื่ออุณหภูมิหรือความชื้นเกินที่ตั้งไว้ระบบจะแจ้งเตือนผ่านแอพไปยังผู้ดูแลระบบ



๕.๒ การป้องกันอัคคีภัย

- จัดทำแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิงและการหนีไฟ
- มีระบบป้องกันไฟไหม้ โดยติดตั้งอุปกรณ์ตรวจจับควัน และอุปกรณ์ดับเพลิงทุกชั้น เพื่อการควบคุมเพลิงในเบื้องต้น



ข้อมูล *Smoke Detector*

๗.๔ หน่วยงานจัดให้มีการซักซ้อมแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ด้านสารสนเทศ

๑. หน่วยงานมีการทดสอบสลับการใช้เครื่อง SERVER หลักกับ SERVER สำรอง เพื่อมั่นใจได้ว่าข้อมูลทั้ง ๒ SERVER มีข้อมูลที่ตรงกัน

๒. หน่วยงานมีการทดสอบ RESTORE ข้อมูล BACKUP ทุกวันศุกร์เพื่อให้มั่นใจได้ว่าข้อมูลที่ BACKUP สมบูรณ์และใช้งานได้หากเกิดภาวะฉุกเฉิน

๗.๕ หน่วยงานจัดให้มีการทดสอบระบบสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งาน

๑.หน่วยงานมีการตรวจเช็คสถานะการทำงานของระบบสำรองไฟฟ้าทุกวัน

๒.หน่วยงานมีการทดสอบการทำงานของระบบสำรองไฟฟ้าทุกเดื