

## Business Continuity Plan (BCP) กลุ่มงานการพยาบาลผู้ป่วยอายุรกรรม โรงพยาบาลอุดรธานี

เหตุการณ์: การวางแผนเมื่อเกิดภัยคุกคามทางไซเบอร์

วันที่: 2 กันยายน พ.ศ. 2567

แผนก: หอผู้ป่วยอายุรกรรมชั้น 7

ผู้รับผิดชอบ: นางสาวสุภาภรณ์ คำสร้าง (ผู้ประสาน)

### 1. บทนำ

ภัยคุกคามทางไซเบอร์ อาจเกิดจากสาเหตุ ดังต่อไปนี้

1) การป้องกันที่ไม่เพียงพอ 2) การเตรียมความพร้อมไม่สมบูรณ์ 3) การตอบโต้ภาวะฉุกเฉินไม่ทันท่วงที ได้วิเคราะห์สาเหตุของปัญหาจากการโดนภัยคุกคามทางไซเบอร์อาจมีดังนี้:

- ขาดการป้องกันและความระมัดระวัง: การเกิดภัยคุกคามทางไซเบอร์เกิดขึ้นเนื่องจากขาดการป้องกันที่เพียงพอหรือความระมัดระวังในการรักษาความปลอดภัยของระบบคอมพิวเตอร์ภายในโรงพยาบาล อาจจะมีช่องโหว่ในระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตที่สม่ำเสมอ
- การเข้าถึงข้อมูลที่ไม่เป็นไปตามนโยบายความปลอดภัย: ผู้ไม่ประสงค์ดีอาจได้รับการเข้าถึงระบบคอมพิวเตอร์ของโรงพยาบาลและข้อมูลสำคัญโดยไม่ได้รับอนุญาต ซึ่งอาจมีปัญหาในการจัดการสิทธิ์การเข้าถึงข้อมูลและการควบคุม
- การเลือกใช้รหัสผ่านที่ไม่ปลอดภัย: การใช้รหัสผ่านที่ง่ายต่อการเดาหรือไม่ปลอดภัยอาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบได้ง่ายขึ้น การใช้รหัสผ่านที่แข็งแกร่งและการเปลี่ยนรหัสผ่านเป็นระยะๆ อาจช่วยลดความเสี่ยงในอนาคต
- ขาดการอบรมและการปรับปรุงความรู้: บุคลากรอาจขาดการอบรมและความรู้ในการรักษาความปลอดภัยของระบบคอมพิวเตอร์ การปรับปรุงความรู้และการอบรมเกี่ยวกับการป้องกัน การคุกคามทางไซเบอร์ อาจช่วยเพิ่มความเข้าใจและความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์
- การไม่ปฏิบัติตามนโยบายด้านความปลอดภัย: การไม่ปฏิบัติตามนโยบายและข้อกำหนดด้านความปลอดภัยอาจเป็นเหตุให้เกิดช่องโหว่หรือความเสี่ยงต่อการโจมตี การคุกคามทางไซเบอร์ อาจต้องพิจารณาการสร้างและปฏิบัติตามนโยบายความปลอดภัยอย่างเคร่งครัดในอนาคต
- ความเสี่ยงจากการเชื่อมต่ออินเทอร์เน็ตที่ไม่ปลอดภัย: การเชื่อมต่ออินเทอร์เน็ตที่ไม่ปลอดภัยหรือใช้บริการอินเทอร์เน็ตที่ไม่ได้รับการควบคุมอาจเสี่ยงต่อการโจมตี การคุกคามทางไซเบอร์ การใช้มาตรฐานความปลอดภัยในการเชื่อมต่ออินเทอร์เน็ตอาจช่วยลดความเสี่ยงในการโจมตีในอนาคต
- ความไม่มั่นคงในการดำเนินงานระบบ: ความไม่มั่นคงในระบบคอมพิวเตอร์และการทำงานของบุคลากรหลังจากการโจมตี การคุกคามทางไซเบอร์ อาจส่งผลให้บุคลากรไม่มั่นใจในการใช้งานระบบคอมพิวเตอร์ ซึ่งอาจส่งผลให้ลดประสิทธิภาพในการทำงานและการให้บริการลูกค้า

- ระบุแนวทางการแก้ไขปัญหา

เพื่อแก้ไขปัญหาเมื่อเกิดภัยคุกคามทางไซเบอร์ในกลุ่มงานการพยาบาลผู้ป่วยอายุรกรรม อาจทำตามแนวทางดังนี้:

- การปรับปรุงระบบความปลอดภัย: อัปเดตและปรับปรุงระบบความปลอดภัยของโรงพยาบาลเพื่อป้องกันภัยคุกคามทางไซเบอร์อนาคต การเพิ่มมาตรการความปลอดภัยเช่นการตรวจสอบระบบป้องกันไวรัสและซอฟต์แวร์ป้องกันไวรัสอัปเดตอย่างสม่ำเสมอ
- การสร้างการสำรองข้อมูล: การสร้างการสำรองข้อมูลและการกู้คืนข้อมูลที่มีประสิทธิภาพเป็นสิ่งสำคัญ เพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีเกิดการโจมตีภัยคุกคามทางไซเบอร์ หรือสูญหายของข้อมูล
- การอบรมและการเผชิญหน้ากับความเสี่ยง: จัดการความรู้และการอบรมเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ให้แก่บุคลากร เพื่อเพิ่มความเข้าใจและความตระหนักในการจัดการความเสี่ยง
- การตรวจสอบและการวิเคราะห์เชิงลึก: การตรวจสอบระบบคอมพิวเตอร์และการวิเคราะห์เชิงลึกข้อมูลเพื่อตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ และการระบุความเสี่ยงที่เป็นไปได้
- การสร้างแผนฉุกเฉิน: การสร้างแผนฉุกเฉินที่เข้มงวดและประสานงานกับหน่วยงานที่เกี่ยวข้อง เพื่อการตอบสนองที่รวดเร็วในกรณีเกิดภัยคุกคามทางไซเบอร์หรือเหตุการณ์ด้านความปลอดภัยอื่นๆ
- การส่งเสริมการใช้รหัสผ่านที่ปลอดภัย: ส่งเสริมการใช้รหัสผ่านที่ปลอดภัยและการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เพื่อป้องกันการเข้าถึงไม่มีอำนาจในระบบ

7. การประเมินและการปรับปรุง: ประเมินภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเพื่อการเรียนรู้และการปรับปรุงระบบความปลอดภัยในอนาคต การวิเคราะห์และการปรับปรุงต่อไปนี้จะช่วยลดความเสี่ยงในการโดนโจมตีในอนาคต

ในส่วนของ**อุปสรรค**ที่เกิดขึ้นในการรับมือกับภัยคุกคามทางไซเบอร์ : พบว่าเป็นอุปสรรคในการป้องกัน คือ **ขาดการควบคุมการเข้าถึง**

วิเคราะห์สาเหตุของอุปสรรค: อาจมีสาเหตุดังนี้:

1. อาจมีขาดการควบคุมการเข้าถึงข้อมูลในระบบคอมพิวเตอร์ ไม่มีการกำหนดสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสม หรือการตั้งค่าการเข้าถึงที่ไม่ถูกต้องซึ่งทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลได้โดยไม่ได้รับอนุญาต
2. ช่องโหว่ในระบบ: ระบบคอมพิวเตอร์อาจมีช่องโหว่ที่ไม่ได้รับการปรับปรุง หรืออัปเดตอย่างสม่ำเสมอซึ่งทำให้เกิดความเสี่ยงในการโจมตีและเข้าถึงข้อมูล
3. ขาดการตระหนักในความสำคัญของความปลอดภัยข้อมูล: บุคลากรอาจไม่มีความตระหนักในความสำคัญของการใช้รหัสผ่านที่ปลอดภัย เช่น การใช้รหัสผ่านที่ยากต่อการเดา หรือการไม่แบ่งแยกรหัสผ่านสำหรับการเข้าสู่ระบบที่ต่างกัน
4. การละเมิดนโยบายและคำแนะนำ: อาจมีการละเมิดนโยบายหรือคำแนะนำที่ต้องใช้รหัสผ่านที่ปลอดภัย แต่บุคลากรอาจเลือกที่จะไม่ปฏิบัติตามนโยบายนั้น เนื่องจากความสะดวกหรือข้อจำกัดในการจดจำรหัสผ่าน
5. ขาดการอบรมหรือการเข้าใจเกี่ยวกับความปลอดภัยของข้อมูล: บุคลากรอาจขาดการอบรมหรือความเข้าใจเกี่ยวกับความสำคัญของความปลอดภัยของข้อมูล ซึ่งอาจทำให้พวกเขาเลือกที่จะใช้รหัสผ่านที่ไม่ปลอดภัย
6. การไม่มีนโยบายหรือมาตรการที่เข้มงวด: หากโรงพยาบาลไม่มีนโยบายหรือมาตรการที่เข้มงวดในการตรวจสอบความปลอดภัยของรหัสผ่าน บุคลากรอาจมีแนวโน้มที่จะใช้รหัสผ่านที่ไม่ปลอดภัยโดยไม่มี การตรวจสอบหรือการให้คำแนะนำ
7. ความไม่สะดวกในการสร้างและจดจำรหัสผ่านที่แข็งแรง: บุคลากรบางส่วนไม่สะดวกในการสร้างและจดจำรหัสผ่านที่ยากต่อการเดา ซึ่งทำให้เลือกใช้รหัสผ่านที่ง่ายต่อการจดจำและใช้งาน
8. ความไม่มั่นใจในความปลอดภัยของระบบ: บุคลากรบางส่วนอาจไม่มั่นใจในความปลอดภัยของระบบ ทำให้เลือกใช้รหัสผ่านที่ไม่ปลอดภัยเพื่อความสะดวกและความง่ายในการเข้าถึงข้อมูล

**แนวทางการแก้ไขอุปสรรค ดังนี้:**

1. ปรับปรุงนโยบายความปลอดภัย: ทำการปรับปรุงนโยบายความปลอดภัยเพื่อให้มีมาตรการที่ชัดเจนและเข้มงวด เช่น กำหนดเครื่องหมายรับรองสำหรับการเข้าถึงข้อมูลที่มีความสำคัญ เป็นต้น
2. การสร้างและบริหารจัดการสิทธิ์: ทำการตรวจสอบและปรับปรุงการกำหนดสิทธิ์การเข้าถึงข้อมูล เพื่อให้แน่ใจว่าเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้
3. การประชุมและการอบรม: จัดการประชุมและการอบรมเพื่อเพิ่มความตระหนักในการรักษาความปลอดภัยของข้อมูลและสิทธิ์การเข้าถึงข้อมูลให้แก่พนักงาน
4. การใช้เทคโนโลยีเพื่อความปลอดภัย: ใช้เทคโนโลยีเพื่อช่วยในการควบคุมการเข้าถึงข้อมูลอย่างมีประสิทธิภาพ เช่น การใช้ระบบควบคุมการเข้าถึง (Access Control Systems) หรือระบบการตรวจจับการบุกรุก (Intrusion Detection Systems)
5. การตรวจสอบและการติดตาม: สร้างกระบวนการตรวจสอบและการติดตามเพื่อตรวจจับการเข้าถึงข้อมูลที่ไม่เป็นไปตามนโยบายความปลอดภัย และดำเนินการแก้ไขให้ทันที่
6. การปรับปรุงระบบคอมพิวเตอร์: ปรับปรุงระบบคอมพิวเตอร์เพื่อเพิ่มระดับความปลอดภัย เช่น การอัปเดตซอฟต์แวร์ การติดตั้งโปรแกรมป้องกันไวรัส และการปรับปรุงระบบป้องกันการเข้าถึงไม่มีอำนาจ
7. การตรวจสอบความปลอดภัยของระบบ: ทำการตรวจสอบและทดสอบความปลอดภัยของระบบอย่างสม่ำเสมอ เพื่อตรวจจับและแก้ไขช่องโหว่ที่อาจทำให้เกิดการเข้าถึงข้อมูลที่ไม่เป็นไปตามนโยบายความปลอดภัย
8. การใช้เทคโนโลยีการตรวจสอบ: การใช้เทคโนโลยีการตรวจสอบเพื่อตรวจสอบความปลอดภัยของรหัสผ่าน เช่น การใช้ขั้นตอนการสร้างรหัสผ่านที่มีความซับซ้อนและการตรวจสอบความปลอดภัยของรหัสผ่านอัตโนมัติ
9. การแนะนำและการส่งเสริมการใช้งาน: แนะนำและส่งเสริมการใช้รหัสผ่านที่ปลอดภัยในแผนก โดยให้คำแนะนำเกี่ยวกับวิธีการสร้างรหัสผ่านที่แข็งแรงและไม่สะดวกง่าย
10. การตรวจสอบและการประเมิน: ตรวจสอบและประเมินการใช้รหัสผ่านในแผนกอย่างสม่ำเสมอ เพื่อตรวจสอบว่านโยบายและมาตรการที่กำหนดไว้ได้ถูกปฏิบัติหรือไม่ และทำการปรับปรุงตามต้องการอย่างสม่ำเสมอ

ฟอร์มนี้จัดทำขึ้นเพื่อให้แต่ละแผนกในโรงพยาบาลอุตรธานีสามารถจัดทำแผนรับมือ Business Continuity Plan (BCP) กรณีเกิดภัยคุกคามทางไซเบอร์ส่งผลให้ระบบบริการไม่สามารถดำเนินได้ แผน BCP นี้จะช่วย  
ให้แต่ละแผนกสามารถดำเนินงานต่อเนื่องได้อย่างมีประสิทธิภาพ แม้จะเผชิญกับเหตุการณ์วิกฤต

## 2. รายละเอียดแผน BCP

### 2.1 ผลกระทบ

การโจมตีด้วยภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับกลุ่มงานการพยาบาลผู้ป่วยอายุรกรรมในโรงพยาบาลอุตรธานีจะมีผลกระทบที่รุนแรงต่อการให้บริการและความปลอดภัยของข้อมูลทางการแพทย์ ทำให้ข้อมูลทางการแพทย์ถูกเข้าถึงและเข้ารหัสโดยไม่ได้รับอนุญาต โรงพยาบาลจะไม่สามารถเข้าถึงข้อมูลสำคัญเพื่อการรักษาได้ ซึ่งอาจส่งผลกระทบต่อการดูแลรักษาผู้ป่วยและการตอบสนองต่อสถานการณ์ฉุกเฉินได้ นอกจากนี้ยังมีความเสี่ยงที่ข้อมูลส่วนบุคคลของผู้ป่วยอาจถูกขโมยหรือนำไปใช้ในทางที่ไม่เหมาะสม โรงพยาบาลจะต้องดำเนินการฟื้นฟูข้อมูลและระบบให้กลับสู่สภาพปกติโดยเร็วเพื่อลดผลกระทบต่อการให้บริการแก่ผู้ป่วยและป้องกันการเกิดเหตุการณ์ที่เช่นนี้เกิดขึ้นอีกในอนาคต

ผลกระทบของการถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ กลุ่มงานการพยาบาลผู้ป่วยอายุรกรรม มีดังนี้:

1. การชะลอหรือยกเลิกการนัดหมายและการรักษา: ผู้ป่วยที่มีนัดหมายหรือการรักษาในแผนกอาจต้องพบกับความไม่สะดวก เนื่องจากระบบคอมพิวเตอร์และข้อมูลทางการแพทย์ถูกเข้าถึงและเข้ารหัสไฟล์
2. ความไม่สามารถเข้าถึงข้อมูล: บุคลากรทางการแพทย์และพยาบาลอาจไม่สามารถเข้าถึงข้อมูลที่จำเป็นสำหรับการรักษาผู้ป่วยได้ ซึ่งอาจทำให้การดูแลรักษาล่าช้าหรือไม่สามารถดำเนินการได้อย่างเหมาะสม
3. ความเสียหายต่อความเชื่อมั่นของผู้ใช้บริการ : โรงพยาบาลอาจเสียชื่อเสียงและความเชื่อมั่นจากผู้ป่วยและครอบครัวของพวกเขา เนื่องจากการละเมิดความเป็นส่วนตัวและการรักษาที่ส่งผลกระทบต่อการให้บริการ
4. การสูญเสียข้อมูลสำคัญ: ข้อมูลทางการแพทย์อาจถูกสูญหายโดยถาวรหรือไม่สามารถกู้คืนได้ ซึ่งอาจมีผลกระทบต่อการรักษาและการติดตามของผู้ป่วย
5. การล้มเหลวของระบบ: ระบบคอมพิวเตอร์ของโรงพยาบาลอาจเกิดการล้มเหลวหรือทำงานได้ช้าเนื่องจากการโจมตี การคุกคามทางไซเบอร์ ซึ่งส่งผลกระทบต่อการทำงานของโรงพยาบาลทั้งหมด
6. ค่าใช้จ่ายในการฟื้นฟู: โรงพยาบาลอาจต้องใช้ค่าใช้จ่ายสูงสุดในการฟื้นฟูระบบคอมพิวเตอร์และข้อมูลที่สูญหาย รวมถึงค่าใช้จ่ายในการจ้างผู้เชี่ยวชาญทางด้านความปลอดภัยเพื่อช่วยเร่งด่วนในการแก้ไขปัญหา
7. ความไม่มั่นคงทางระบบ: ภัยคุกคามทางไซเบอร์อาจทำให้โรงพยาบาลเสี่ยงต่อการโจมตีอื่นๆ และการรั่วไหลของข้อมูลในอนาคต ทำให้ความมั่นคงของระบบเสี่ยงลดลง
8. ความเสี่ยงต่อความปลอดภัยของผู้ป่วย: ข้อมูลทางการแพทย์ที่ถูกเข้าถึงโดยไม่ได้รับอนุญาตอาจถูกนำไปใช้ในทางที่ไม่เหมาะสม ซึ่งอาจเปิดโอกาสให้เกิดความเสี่ยงต่อความปลอดภัยและความเป็นส่วนตัวของผู้ป่วย
9. ความเสียหายต่อการดำเนินงาน: โรงพยาบาลอาจต้องใช้เวลาและทรัพยากรในการฟื้นฟูระบบและข้อมูลที่สูญหาย ซึ่งอาจส่งผลกระทบต่อการดำเนินงานประจำวันของโรงพยาบาล

นอกจากนั้นภัยคุกคามทางไซเบอร์ ยังส่งผลกระทบต่อบุคลากร ดังนี้:

1. ขาดระบบการทำงาน : ภัยคุกคามทางไซเบอร์อาจทำให้ระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วนของโรงพยาบาลไม่สามารถใช้งานได้ ซึ่งอาจส่งผลให้บุคลากรไม่สามารถทำงานได้อย่างปกติ
2. การล่าช้าในการให้บริการ : ภัยคุกคามทางไซเบอร์อาจทำให้กระบวนการการทำงานของโรงพยาบาลมีความล่าช้า ซึ่งอาจส่งผลให้บุคลากรต้องทำงานเพิ่มเติมหรือทำงานในสภาพแวดล้อมที่ยุ่งเหยิง
3. ความเสียหายจากข้อมูลส่วนตัว : ภัยคุกคามทางไซเบอร์อาจทำให้ข้อมูลส่วนตัวของบุคลากรถูกเข้าถึงและเข้ารหัสไฟล์ ซึ่งอาจส่งผลให้ข้อมูลส่วนตัวถูกขโมยหรือถูกละเลย
4. ความเครียดและความกังวล : ภัยคุกคามทางไซเบอร์อาจสร้างความเครียดและความกังวลให้กับบุคลากร โดยเฉพาะกับบุคลากรที่ต้องรับผิดชอบในการดูแลระบบคอมพิวเตอร์และข้อมูล
5. การสูญเสียข้อมูลและเอกสารสำคัญ : ภัยคุกคามทางไซเบอร์อาจทำให้ข้อมูลและเอกสารสำคัญของโรงพยาบาลถูกเข้ารหัสหรือสูญหายไป ซึ่งอาจส่งผลให้บุคลากรต้องเสียเวลาในการกู้คืนข้อมูลหรือสร้างข้อมูลใหม่
6. ความไม่มั่นคงใจในระบบ : ภัยคุกคามทางไซเบอร์อาจทำให้บุคลากรไม่มั่นคงใจในระบบคอมพิวเตอร์และระบบการจัดการข้อมูลของโรงพยาบาล ซึ่งอาจส่งผลให้เกิดความไม่มั่นคงใจในการทำงาน
7. ค่าใช้จ่ายในการซ่อมแซมและกู้คืนข้อมูล : การกู้คืนข้อมูลหรือการซ่อมแซมระบบหลังจากเกิดภัยคุกคามทางไซเบอร์อาจต้องใช้งบประมาณสูง ซึ่งอาจส่งผลให้โรงพยาบาลต้องจ่ายค่าใช้จ่ายเพิ่มเติมในการซ่อมแซมระบบและการกู้คืนข้อมูล

## 2.2 กลยุทธ์

- กลยุทธ์ที่จะใช้ในการรับมือกับภัยคุกคามทางไซเบอร์ : กลยุทธ์ที่สามารถใช้ในการรับมือกับการโจมตีด้วยภัยคุกคามทางไซเบอร์ในกลุ่มงานการพยาบาลผู้ป่วยอายุรกรรม โดยเตรียมความพร้อมและการฟื้นฟูด้วย ดังนี้  
  1. สร้างแผนการปฏิบัติฉุกเฉิน : สร้างแผนการปฏิบัติที่เตรียมความพร้อมทั้งในกรณีที่เกิดภัยคุกคามทางไซเบอร์โดยรวมถึงกระบวนการและขั้นตอนการดำเนินการที่ชัดเจนสำหรับทุกกลุ่มเป้าหมาย
  2. กำหนดบทบาทและความรับผิดชอบ : กำหนดบทบาทและความรับผิดชอบของทุกคนในแผนกเพื่อการตอบสนองที่รวดเร็วและเชื่อถือได้
  3. สร้างระบบสำรองข้อมูลและการฟื้นฟู : จัดทำแผนการสำรองข้อมูลที่เข้มงวดและปฏิบัติการฟื้นฟูข้อมูลที่รวดเร็ว รวมถึงการทดสอบและประสานงานกับผู้ให้บริการสำรองข้อมูล
  4. การฝึกฝนและการอบรม : ฝึกฝนบุคลากรในการใช้และการดำเนินการตามแผนการปฏิบัติฉุกเฉินเมื่อเกิดภัยคุกคามทางไซเบอร์ รวมถึงการทดสอบสมรรถนะอย่างเป็นระยะเวลา
  5. การวิเคราะห์และการประเมิน : ทำการวิเคราะห์และประเมินแผนการปฏิบัติฉุกเฉินอย่างสม่ำเสมอเพื่อปรับปรุงและปรับใช้ตามสถานการณ์และการเรียนรู้จากการโจมตีที่เกิดขึ้นในอดีต
- แผนการปฏิบัติที่เตรียมความพร้อมในกรณีของภัยคุกคามทางไซเบอร์เพื่อรักษาบริการที่จำเป็นในกลุ่มงานการพยาบาลผู้ป่วยอายุรกรรม ดังนี้  
  1. การสำรองข้อมูลแบบเป็นระบบ : จัดทำและบำรุงรักษาการสำรองข้อมูลแบบเป็นระบบที่ตรวจสอบและอัปเดตอย่างสม่ำเสมอ ซึ่งรวมถึงข้อมูลผู้ป่วยที่สำคัญและข้อมูลอื่นๆ ที่เกี่ยวข้องกับการให้บริการทางการแพทย์
  2. การกำหนดแผนการฟื้นฟูแบบทันที : กำหนดแผนการฟื้นฟูที่ทันทีที่เกิดภัยคุกคามทางไซเบอร์ ซึ่งรวมถึงการกำหนดกระบวนการการทำงานที่จะเริ่มทำทันทีเพื่อยกเลิกผลกระทบ
  3. การฟื้นฟูข้อมูลอย่างรวดเร็ว : มีการวางแผนและสำรองข้อมูลอย่างเป็นระบบที่สามารถฟื้นฟูข้อมูลอย่างรวดเร็วโดยมีกระบวนการที่ชัดเจนและเป็นเป้าหมาย
  4. การอบรมและการทดสอบแผนการฟื้นฟู : อบรมบุคลากรในการปฏิบัติตามแผนการฟื้นฟูและทดสอบแผนการเพื่อแน่ใจว่ามีความพร้อมและสามารถทำงานได้อย่างเต็มประสิทธิภาพ
  5. การติดตามและประเมิน : ติดตามและประเมินผลของแผนการฟื้นฟูเพื่อทราบข้อบกพร่องและการปรับปรุงในการจัดการภายหลัง เพื่อให้การรักษาบริการที่จำเป็นไม่มีผลกระทบต่อผู้ป่วย
- กลยุทธ์ที่สามารถใช้ในการเตรียมความพร้อมและการฟื้นฟูด้วยเมื่อเกิดภัยคุกคามทางไซเบอร์ เพื่อลดผลกระทบต่อผู้ป่วย ญาติ และบุคลากรในกลุ่มงานการพยาบาลผู้ป่วยอายุรกรรม ดังนี้  
  1. สร้างแผนการฟื้นฟูฉุกเฉิน : สร้างแผนการฟื้นฟูฉุกเฉินที่รวมถึงกระบวนการและขั้นตอนการดำเนินงานที่ต้องทำเมื่อเกิดภัยคุกคามทางไซเบอร์เพื่อให้การฟื้นฟูเกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ
  2. สำรองข้อมูลอย่างสม่ำเสมอ : มีการสำรองข้อมูลอย่างสม่ำเสมอและเก็บไว้ในตำแหน่งที่ปลอดภัย เพื่อให้สามารถกู้คืนข้อมูลได้อย่างรวดเร็วเมื่อเกิดการโจมตี
  3. การทดสอบและประเมินการฟื้นฟู : ทดสอบและประเมินแผนการฟื้นฟูอย่างสม่ำเสมอเพื่อให้แน่ใจว่าสามารถทำงานได้ตามที่วางไว้และสามารถลดเวลาในการฟื้นฟูได้มากที่สุด
  4. การเตรียมความพร้อมเชิงเทคนิค : ตรวจสอบและปรับปรุงระบบความปลอดภัยอย่างสม่ำเสมอ เช่น อัปเดตซอฟต์แวร์ ติดตั้งโปรแกรมป้องกันไวรัสและฟรียอลล์ และมีการติดตั้งเครื่องมือตรวจจับและตอบสนองสัญญาณของการโจมตี
  5. การสื่อสารและการสนับสนุน : สร้างช่องทางสื่อสารที่มีประสิทธิภาพเพื่อแจ้งเตือนผู้ป่วย ญาติ และบุคลากรเกี่ยวกับสถานการณ์ และให้การสนับสนุนทางด้านจิตใจและอารมณ์ในขณะที่กำลังฟื้นฟูจากการโจมตี

## 2.3 แผนปฏิบัติการ

- ระบุขั้นตอนที่ชัดเจนในการรับมือกับภัยคุกคามทางไซเบอร์
- ระบุผู้รับผิดชอบสำหรับแต่ละขั้นตอน
- ระบุเวลาที่คาดว่าจะใช้ในการดำเนินการแต่ละขั้นตอน

| แผนปฏิบัติการ                                          |                                                |        |           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                    |
|--------------------------------------------------------|------------------------------------------------|--------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------|
| การตอบโต้ภาวะฉุกเฉินในการรับมือกับ ภัยคุกคามทางไซเบอร์ |                                                |        |           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |                                    |
| กลยุทธ์                                                | วัตถุประสงค์                                   | กลวิธี | ตัวชี้วัด | กิจกรรม                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | เวลาดำเนินการ           | ผู้รับผิดชอบ                       |
| 1. เข้าถึงได้ง่าย                                      | -เพื่อป้องกันการเข้าถึงข้อมูลได้ง่าย           |        | -         | 1. ปรับปรุงระบบการป้องกัน โดยใช้ซอฟต์แวร์และเครื่องมือการป้องกันที่มีประสิทธิภาพ เช่น ซอฟต์แวร์แอนตี้ไวรัส ซอฟต์แวร์ไฟร์วอลล์ และการตั้งค่าระบบป้องกันการบุกรุก<br>2. อัปเดตระบบปฏิบัติการและโปรแกรมประยุกต์อย่างสม่ำเสมอเพื่อรักษาความปลอดภัยของระบบ<br>3. การควบคุมการเข้าถึง: ให้กำหนดสิทธิ์การเข้าถึงข้อมูลอย่างเคร่งครัด และจำกัดสิทธิ์การเข้าถึงข้อมูลเฉพาะตามความจำเป็น ตามแนวปฏิบัติของการเข้าถึงระบบข้อมูลของโรงพยาบาล<br>4. อบรมบุคลากรในการระมัดระวังและการปฏิบัติตามนโยบายการใช้งานคอมพิวเตอร์อย่างปลอดภัย<br>5. นิเทศติดตามการปฏิบัติของบุคลากรในกลุ่มงานตามนโยบายการใช้คอมพิวเตอร์อย่างปลอดภัย<br>6. การใช้เทคโนโลยีการระบอดอย่างระมัดระวังเพื่อตรวจจับและป้องกันการระบาดของไวรัสและมัลแวร์<br>7. การเข้ารหัสข้อมูลที่สำคัญเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต | ตุลาคม ถึง ธันวาคม 2567 | - นางสาวไสว อินทะชูป               |
| 2. ใช้ Password ร่วมกัน                                | -เพื่อป้องกันการใช้ Password ร่วมกัน           |        | -         | 1. บุคลากรทุกคนต้องมีรหัส (password) ที่เข้าฐานข้อมูล และต้องมีการเปลี่ยนรหัสเข้าถึงข้อมูลอย่างสม่ำเสมอ<br>2. ห้ามใช้รหัสที่เข้าฐานข้อมูลของบุคคลอื่น ถ้าพบมีการใช้ฐานข้อมูลผู้อื่น จะมีการทบทวนร่วมกัน และหาแนวทางแก้ไข<br>3. การตรวจสอบและการประเมิน ตรวจสอบและประเมินผล :องการไม่ละเมิดการใช้รหัสฐานข้อมูลผู้อื่น<br>4. นำผลการตรวจสอบและประเมินมาวิเคราะห์ วางระบบการป้องกันการละเมิดการใช้รหัสฐานข้อมูลผู้อื่น                                                                                                                                                                                                                                                                                                                                                                     | ตุลาคม ถึง ธันวาคม 2567 | นางสมไสว-อินทะชูป                  |
| 3. แผน resilience                                      | เพื่อสามารถปฏิบัติงานได้ตามปกติได้อย่างรวดเร็ว |        |           | 1. หอผู้ป่วยทุกหอจัดทำแฟ้มต้นฉบับ standing order ที่อยู่ในระบบ OP serve เป็นปัจจุบัน<br>2. หอผู้ป่วยทุกหามีเอกสารสำหรับทำรับใหม่<br>3. เมื่อมีการจำหน่ายผู้ป่วย เจ้าหน้าที่ต้องให้เอกสารที่เกี่ยวข้องกับผู้ป่วย เช่น ใบรายการยา Home med, ผลตรวจพิเศษต่างๆ แบบ official เช่น ผล CT scan, echo, MRI, ultrasound เป็นต้น<br>4. มีการเก็บเอกสารสำคัญ ในเครื่อง stand alone                                                                                                                                                                                                                                                                                                                                                                                                                 | ตุลาคม ถึง ธันวาคม 2567 | - IT nurse<br>- นางสาวไสว อินทะชูป |

## 2.4 ทรัพยากร

- ระบุทรัพยากรที่จำเป็นในการดำเนินการแผน BCP : เครื่อง scan เอกสาร จำนวน 2 เครื่อง คอมพิวเตอร์ stand alone ที่มีหน่วยความจำสูง ความเร็วสูง
- ระบุแหล่งที่มาของทรัพยากร

## 2.5 การทดสอบและฝึกอบรม

- ระบุวิธีการทดสอบแผน BCP
- ระบุวิธีการฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้

## 3. เอกสารแนบ

- แผนงาน

## 4. การอนุมัติ

หัวหน้าแผนก: \_\_\_\_\_

วันที่: \_\_\_\_\_

## 5. บทสรุป

ฟอร์มนี้เป็นแนวทางสำหรับแต่ละแผนกในการจัดทำแผน BCP แผน BCP ที่ดีจะช่วยให้โรงพยาบาลอุดรธานีสามารถรับมือกับ การคุกคามทางไซเบอร์ attack และเหตุการณ์วิกฤตอื่นๆ ได้อย่างมีประสิทธิภาพ

### หมายเหตุ:

- ฟอร์มนี้สามารถปรับแต่งให้เหมาะกับแต่ละแผนกได้
- แผน BCP ควรได้รับการทบทวนและปรับปรุงเป็นประจำ

### แหล่งข้อมูล

#### คำแนะนำ

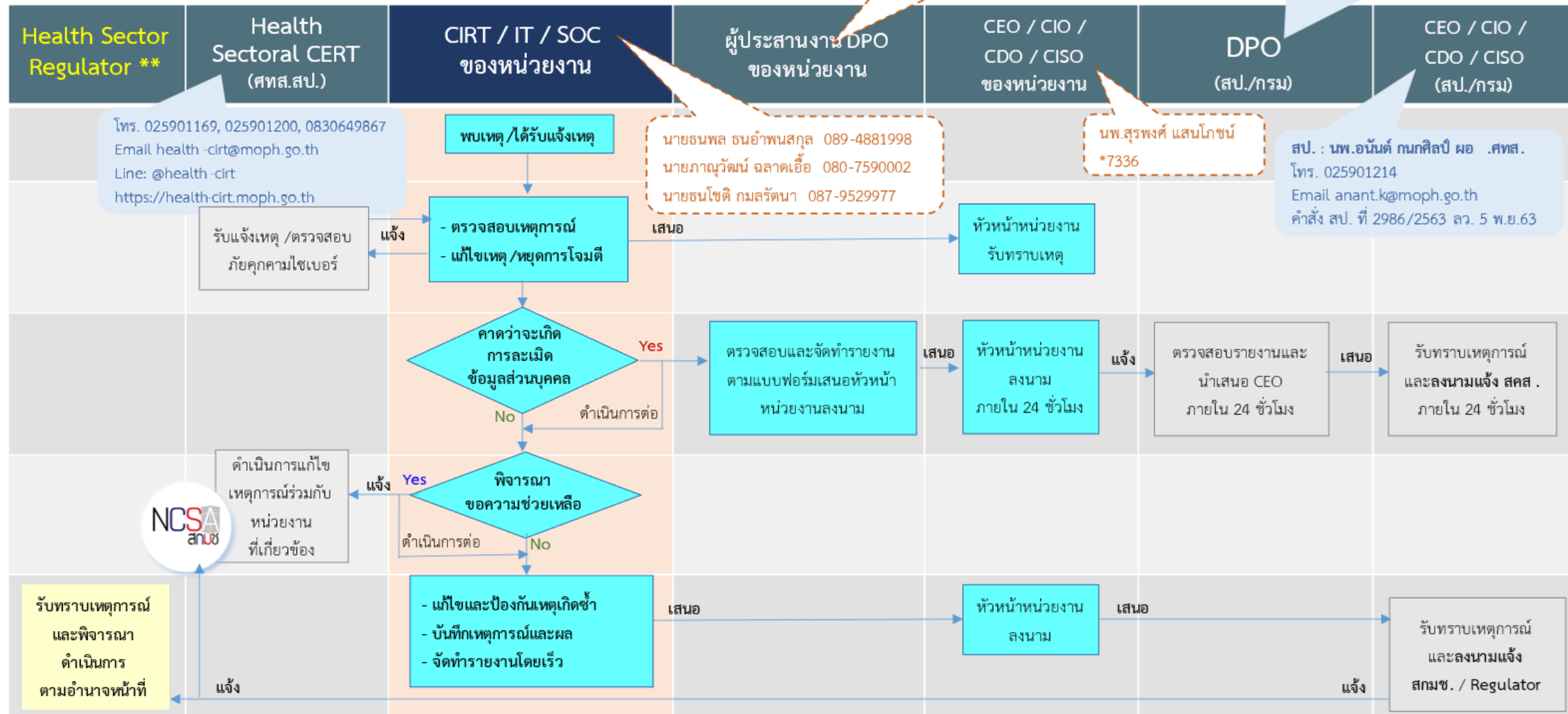
- การเข้าถึงข้อมูล ควรมีรหัสส่วนตัวของผู้ใช้ข้อมูล และปิดเป็นความลับ
- ควรจัดทำแผน BCP ร่วมกับผู้เชี่ยวชาญด้านไอที
- ควรทดสอบแผน BCP เป็นประจำ
- ควรฝึกอบรมบุคลากรให้สามารถปฏิบัติตามแผน BCP ได้



## Flow การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์ ของหน่วยงาน ..โรงพยาบาลอุดรธานี....

นายธนพล ธนอำพนสกุล  
089-4881998

สป. : คุณสุวันทนา เสมอเนตร  
โทร. 025902180 ต่อ 112  
Email dpo@moph.go.th  
คำสั่ง สป. ที่ 1189/2565 ลว. 25 พ.ค.65



\*\* Regulator ของ รพ. คือ กรมสนับสนุนบริการสุขภาพ (สบส.)

Regulator ของ ผลิตภัณฑ์สุขภาพ รวมถึงอาหาร ยา เครื่องมือแพทย์ คือ อย .

Regulator ของ หน่วยงานที่มีการดำเนินการกับข้อมูลสุขภาพ (Digital health) ยกเว้น รพ. คือ สป.(ศทส.)

- คำสั่ง สป. ที่ 1480/2565 เรื่องแต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล (ประสาน DPO ระดับจังหวัด/หน่วยงาน)

- แบบการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ดาวน์โหลดได้ที่ <https://pdpa.moph.go.th/>



สรุปประเด็นที่ควรดำเนินการ

| สรุปประเด็นที่ควรดำเนินการ                               | U<br>( / ) | S<br>( / ) | I<br>( / ) |
|----------------------------------------------------------|------------|------------|------------|
| การป้องกัน                                               | /          | /          | /          |
|                                                          |            |            |            |
|                                                          |            |            |            |
|                                                          |            |            |            |
| การเตรียมความพร้อมเพื่อรับสถานการณ์เมื่อเกิดเหตุ         | /          | /          | /          |
|                                                          |            |            |            |
|                                                          |            |            |            |
| การปฏิบัติระหว่างเกิดเหตุเพื่อให้การบริการดำเนินต่อไปได้ | /          | /          | /          |
|                                                          |            |            |            |
|                                                          |            |            |            |
| การปฏิบัติหลังระบบกลับสู่ปกติ                            | /          | /          | /          |
|                                                          |            |            |            |
|                                                          |            |            |            |
|                                                          |            |            |            |

U =ดำเนินการได้เองระดับหน่วยงาน  
S = ต้องคุยเชิงระบบเพื่อทำงานให้สอดคล้องกัน  
I = ต้องได้รับการสนับสนุนจาก IT