

# แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

## โรงเรียนสวงวนหญิง จังหวัดสุพรรณบุรี

### 1. กรณีมัลแวร์ หรือไวรัสคอมพิวเตอร์ระบาด

1.1 กรณีที่มีมัลแวร์ หรือไวรัสคอมพิวเตอร์เข้าสู่ระบบเจ้าหน้าที่งานระบบเครือข่าย เทคโนโลยีและเว็บไซต์โรงเรียน ดำเนินการจัดการกับมัลแวร์ หรือไวรัสคอมพิวเตอร์ไม่ให้แพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย

1.2 วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

1.3 ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

1.4 กรณีเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ไม่สามารถใช้งานได้ตามปกติ เจ้าหน้าที่งานระบบเครือข่ายเทคโนโลยีและเว็บไซต์โรงเรียน จะนำเครื่องคอมพิวเตอร์สำรอง เพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง

1.5 สนับสนุนให้ครู บุคลากร และนักเรียนเก็บข้อมูลและสารสนเทศไว้ในระบบคลาวด์คอมพิวเตอร์ ( Cloud Computing ) เป็นการสำรองข้อมูล และไม่ติดมัลแวร์

1.6 ปรับปรุงโปรแกรมป้องกันมัลแวร์ให้ทันสมัยอยู่เสมอ

### 2. กรณีถูกล้วงข้อมูล

2.1 กรณีที่มีผู้บุกรุก ผู้ดูแลระบบจะวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก Log File และตรวจสอบการตั้งค่าของ Firewall และหยุดยั้งการบุกรุกนั้น

2.2 โรงเรียนมีระบบพิสูจน์ตัวตน AUTHEN และ LOG FILE จะสามารถตรวจสอบได้ว่ามาจากจุดใด

2.3 มีการสำรองข้อมูลเครื่องแม่ข่าย (Server) สัปดาห์ละ 1 ครั้ง เมื่อเกิดเหตุการณ์ที่ทำให้เครื่องแม่ข่ายเสียหาย จึงสามารถกู้คืนข้อมูลได้

### 3. กรณีเครือข่ายอินเทอร์เน็ตล่มเหลว

3.1 เมื่อสัญญาณอินเทอร์เน็ตล่มเหลว เจ้าหน้าที่งานระบบเครือข่ายฯ ตรวจสอบระบบ และแก้ไขตามกรณีต่าง ๆ ดังนี้

- กรณีที่สัญญาณอินเทอร์เน็ตล้มเหลว เนื่องจากสัญญาณของผู้ให้บริการบางแห่ง ล่ม ให้กลับไปใช้สัญญาณอินเทอร์เน็ตจากผู้ให้บริการอื่น ๆ และแจ้งไปยังเจ้าหน้าที่ผู้ให้บริการสัญญาณอินเทอร์เน็ตโดยเร่งด่วน
- กรณีที่สัญญาณอินเทอร์เน็ตจากผู้ให้บริการทุกค่ายล่ม ให้ใช้เครือข่ายอินเทอร์เน็ตของโรงเรียน และแจ้งไปยังเจ้าหน้าที่ผู้ให้บริการสัญญาณอินเทอร์เน็ตโดยเร่งด่วน
- กรณีที่เกิดจากอุปกรณ์ หรือสายแลนเสียหาย เจ้าหน้าที่งานระบบเครือข่ายฯ ตรวจสอบและดำเนินการซ่อม

3.2 เจ้าหน้าที่งานระบบเครือข่ายฯ ตรวจสอบสัญญาณอินเทอร์เน็ตให้สามารถใช้ได้ตามปกติ

#### 4. กรณีเครื่องคอมพิวเตอร์เสียหาย

4.1 กรณีเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเสียหาย ให้ดำเนินการแจ้งซ่อมไปยังงานระบบเครือข่ายเทคโนโลยีและเว็บไซต์โรงเรียน โดยการเขียนในแบบฟอร์มของระบบการซ่อม เจ้าหน้าที่จะทำการตรวจสอบ และซ่อมตามลำดับ และความจำเป็นเร่งด่วน

4.2 กรณีที่มีความจำเป็นเร่งด่วน สามารถโทรศัพท์แจ้งเจ้าหน้าที่ เพื่อดำเนินการตรวจสอบ และซ่อมต่อไป

4.3 กรณีที่ไม่สามารถซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงได้ในทันที ให้นำเครื่องคอมพิวเตอร์สำรองมาใช้ในการปฏิบัติงานก่อน แล้วจึงดำเนินการซ่อมตามระบบต่อไป

4.4 ถ้าเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงนั้นไม่สามารถซ่อมได้ เจ้าหน้าที่จะทำการส่งต่อให้ศูนย์ซ่อมภายนอก ดำเนินการต่อไป

4.5 นำข้อมูลและสารสนเทศที่ได้สำรองไว้ในระบบคลาวด์คอมพิวเตอร์ ( Cloud Computing ) มาใช้ในการปฏิบัติงาน

4.6 เมื่อดำเนินการซ่อมสำเร็จแล้ว เจ้าหน้าที่งานระบบเครือข่ายฯ ทำการส่งคืนอุปกรณ์และบันทึกในแบบฟอร์มการแจ้งซ่อม แล้วรายงานผู้บังคับบัญชาต่อไป

#### 5. กรณีไฟฟ้าขัดข้อง

5.1 เมื่อกระแสไฟฟ้าขัดข้องเครื่องสำรองไฟฟ้าที่เครื่องแม่ข่าย (SERVER) และอุปกรณ์ที่สำคัญจะทำงานทันที เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง และไม่ทำให้อุปกรณ์ที่สำคัญเกิดความเสียหาย

5.2 เจ้าหน้าที่ไฟฟ้าของโรงเรียนตรวจสอบความขัดข้องว่าเกิดจากจุดใด และทำการแก้ไข หากความขัดข้องเกิดจากระบบไฟฟ้าภายนอก เจ้าหน้าที่ทำการแจ้งการไฟฟ้า เบอร์โทรศัพท์ 0-3540-8824 เพื่อทำการแก้ไขต่อไป

5.3 เจ้าหน้าที่ไฟฟ้าแจ้งเรื่องให้งานประชาสัมพันธ์ เพื่อแจ้งข่าวให้ครู บุคลากร และนักเรียน ทราบผ่านทางสื่อสังคมออนไลน์ เพื่อให้ทำการปิดเครื่องใช้ไฟฟ้า เครื่องคอมพิวเตอร์ เครื่องปรับอากาศ เพื่อป้องกันความเสียหายของอุปกรณ์ต่าง ๆ

5.4 เจ้าหน้าที่งานระบบเครือข่ายเทคโนโลยีและเว็บไซต์โรงเรียน ตรวจสอบการทำงานของ เครื่องสำรองไฟฟ้าในอุปกรณ์สำคัญ ภาคเรียนละ 1 ครั้ง

## 6. กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

6.1 แจ้งผู้บังคับบัญชาทราบ

6.2 ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่น เพื่อให้สามารถปฏิบัติงานแทนได้

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการงานระบบเครือข่าย เทคโนโลยีและเว็บไซต์โรงเรียน เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ