



# IT CONTINGENCY PLAN



## คำนำ

การบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Infrastructure) ของกรมพินิจและคุ้มครองเด็กและเยาวชน เริ่มทวีความซับซ้อนมากยิ่งขึ้น เนื่องจากการพัฒนาระบบใหม่ๆ เพื่อให้ตอบสนองและรองรับภารกิจได้อย่างต่อเนื่อง รวมถึงการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในกรม และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ ซึ่งมีประโยชน์ต่อการวางแผนพัฒนาองค์การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น กรมพินิจและคุ้มครองเด็กและเยาวชนจำเป็นต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา และจัดทำแผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ และต้องทบทวนอย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือต่อเหตุฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น และเป็นกรอบแนวทางในการดูแลรักษา และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนได้

เพื่อให้กรมพินิจและคุ้มครองเด็กและเยาวชน มีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยมีความพร้อมใช้ข้อมูลได้อย่างเต็มประสิทธิภาพตลอดเวลา และนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กร ตลอดจนเลือกใช้วิธีที่เหมาะสมในการบริหารจัดการความเสี่ยงที่ได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และการดำเนินงานของกรมพินิจและคุ้มครองเด็กและเยาวชน ให้อยู่ในระดับที่สามารถรองรับได้ จึงจำเป็นต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เป็นกรอบแนวทางในการดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงที่อาจนำไปสู่ผลเสียหรือความเสียหายได้ทั้งทางตรงและทางอ้อม

ศูนย์เทคโนโลยีสารสนเทศ  
กรมพินิจและคุ้มครองเด็กและเยาวชน  
สิงหาคม ๒๕๖๕

-๗-  
สารบัญ

หน้า

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| คำนำ.....                                                               | ก  |
| สารบัญ.....                                                             | ข  |
| สารบัญแผนภูมิ/ตาราง.....                                                | ค  |
| <b>แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ</b>                            |    |
| ๑. หลักการและเหตุผล.....                                                | ๑  |
| ๒. วัตถุประสงค์.....                                                    | ๒  |
| ๓. นิยามศัพท์เฉพาะ.....                                                 | ๒  |
| ๔. การประเมินความเสี่ยง.....                                            | ๕  |
| ๕. แนวทางการจัดการภัยพิบัติ.....                                        | ๗  |
| ๖. มาตรการความปลอดภัยด้วยรหัสผ่าน.....                                  | ๒๐ |
| ๗. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ.....                           | ๒๑ |
| ๘. หลักปฏิบัติในการป้องกันอัคคีภัย.....                                 | ๒๒ |
| ๙. การกำหนดผู้รับผิดชอบ.....                                            | ๒๒ |
| ๑๐. แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติ.....                            | ๒๓ |
| ๑๑. การติดตามและรายงานผล.....                                           | ๒๔ |
| <b>แผนการควบคุมการเข้าถึงระบบเครือข่าย</b>                              |    |
| ๑. การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย.....                     | ๒๕ |
| ๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย.....                          | ๒๕ |
| ๓. การบริหารจัดการการเข้าถึงเครือข่าย.....                              | ๒๖ |
| ๔. การบริหารจัดการระบบคอมพิวเตอร์.....                                  | ๒๗ |
| ๕. การบริหารจัดการการบันทึกและตรวจสอบ.....                              | ๒๘ |
| ๖. การควบคุมการใช้งานระบบจากภายนอกกรมพินิจและคุ้มครองเด็กและเยาวชน..... | ๒๘ |
| ๗. การพิสูจน์ตัวตน.....                                                 | ๒๘ |
| ๘. ผู้รับผิดชอบการจัดทำแผน.....                                         | ๒๙ |





## สารบัญแผนภูมิ หรือ ตาราง

### หน้า

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย.....                                    | ๘  |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีการป้องกันไวรัสส่มเหลว.....                                         | ๙  |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีไฟฟ้าขัดข้อง.....                                                   | ๑๐ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีไฟไหม้.....                                                         | ๑๑ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีโจรกรรม .....                                                       | ๑๔ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีการเชื่อมโยงเครือข่ายล้มเหลวชั้น ๖ - ๗.....                         | ๑๕ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีการเชื่อมโยงเครือข่ายล้มเหลวต่างจังหวัด.....                        | ๑๖ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีการป้องกันผู้บุกรุกล้มเหลว.....                                     | ๑๗ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีแผ่นดินไหว.....                                                     | ๑๘ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง.....                                     | ๑๙ |
| แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์กรณีบุคลากรภายในศูนย์เทคโนโลยีสารสนเทศ<br>ไม่สามารถมาปฏิบัติงานได้..... | ๑๙ |
| ตารางบุคลากรที่ดูแลรับผิดชอบระบบสารสนเทศ.....                                                               | ๒๓ |
| แผนการจัดทำระบบบริหารความเสี่ยง.....                                                                        | ๒๔ |
| แบบฟอร์มติดตามความเสี่ยง .....                                                                              | ๒๕ |



**แผนรองรับสถานการณ์ฉุกเฉิน  
ที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)  
ของกรมพินิจและคุ้มครองเด็กและเยาวชน**

**๑. หลักการและเหตุผล**

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ จึงจำเป็นต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติฯ เพื่อให้มีความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน เป็นไปอย่างยั่งยืนตามรายละเอียด เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน พ.ศ.๒๕๖๕ โดยกรมพินิจและคุ้มครองเด็กและเยาวชน ต้องมีระบบสารสนเทศและระบบสำรองข้อมูลเพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ และต้องจัดทำระบบเทคโนโลยีสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา และจัดทำแผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ และต้องทบทวนอย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือต่อเหตุฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น และเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชนได้

เพื่อให้สามารถนำแผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของกรมพินิจและคุ้มครองเด็กและเยาวชน มาช่วยในการบริหารงานและการตัดสินใจด้านต่างๆ ตลอดจนมีการใช้ทรัพยากรอย่างเหมาะสมและมีประสิทธิภาพ ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งโปรแกรมระบบสารสนเทศตามภารกิจหลัก และภารกิจสนับสนุน ที่ได้พัฒนาขึ้นมาเพื่อช่วยเพิ่มประสิทธิภาพในการปฏิบัติงาน และบริการประชาชนให้ได้รับความสะดวกมากยิ่งขึ้น ภายใต้สถานการณ์ดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารล้วนแต่มีความเสี่ยงซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินการหรือเป้าหมายขององค์กร ขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตีจากบุคคล จากไวรัสคอมพิวเตอร์ เครื่องของบุคลากร ปัญหาไฟฟ้า อัดคัสภัย หรือจากปัจจัยภายในและภายนอกต่างๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการปฏิบัติงานของกรมพินิจและคุ้มครองเด็กและเยาวชน และเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ว่าด้วยการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ จึงจำเป็นต้องมีการปรับปรุงแผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของกรมพินิจและคุ้มครองเด็กและเยาวชน

/๒. วัตถุประสงค์...

## ๒. วัตถุประสงค์

๒.๑ เพื่อใช้เป็นแนวทางในการดำเนินการ การกำกับดูแล การตรวจสอบการบริหารจัดการ และดูแลรักษาระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศให้มีความเสถียรภาพ มีความพร้อมสำหรับการใช้งาน และเฝ้าระวังความเสี่ยงใหม่ๆ ที่อาจเกิดขึ้นได้ตลอดเวลา

๒.๒ เพื่อลดความเสียหายที่อาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันทั่วทั้งที่

๒.๔ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับการดำเนินงานของศูนย์เทคโนโลยีสารสนเทศ ให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบ และมีความต่อเนื่อง

๒.๕ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๕๙

๒.๖ สร้างกรอบและแนวทางในการดำเนินงานให้แก่บุคลากรในองค์กร เพื่อให้สามารถบริหารจัดการความไม่แน่นอนที่จะเกิดขึ้นกับองค์กรได้อย่างมีระบบและมีประสิทธิภาพ

## ๓. นิยามศัพท์เฉพาะ

ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม

ศูนย์เทคโนโลยีสารสนเทศ หมายถึง ศูนย์เทคโนโลยีสารสนเทศ กรมพินิจและคุ้มครองเด็กและเยาวชน เครื่องแม่ข่าย หรือ Server คือ เครื่องหรือโปรแกรมคอมพิวเตอร์ซึ่งทำงานให้บริการในระบบเครือข่ายแก่ลูกข่าย (ซึ่งให้บริการผู้ใช้อีกทีหนึ่ง)

เครื่องลูกข่าย (Client) คือ ระบบหรือแอปพลิเคชันที่สามารถเชื่อมต่อเข้ากับระบบคอมพิวเตอร์อื่นที่เรียกว่าเซิร์ฟเวอร์ได้

ตู้ RACK คือ ตู้สำหรับเก็บอุปกรณ์ Server Computer และ อุปกรณ์ Network ต่างๆ รวมถึงสายสัญญาณ (Network Cable) เอาไว้ข้างในเพื่อความสะดวกในการจัดเก็บอุปกรณ์และการบริหารจัดการสายสัญญาณ

โปรแกรม Anti-Virus คือ โปรแกรมประเภทหนึ่งที่ช่วยป้องกัน ตรวจสอบ และกำจัดไวรัสก่อนที่จะไวรัสนั้นจะเข้ามาทำลายโปรแกรมหรือข้อมูลในเครื่องคอมพิวเตอร์

ระบบ IPS คือ ระบบตรวจสอบและตอบโต้การบุกรุก IPS (Intrusion Prevention System) คือ Software หรือ hardware ที่ได้รับการออกแบบมาเพื่อให้ตรวจสอบการบุกรุก มีคุณสมบัติพิเศษ ในการจับจ้องกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยไม่จำเป็นต้องอาศัยโปรแกรมหรือ hardware ตัวอื่นๆ

ไวรัสคอมพิวเตอร์ (Computer Virus) คือ ชุดคำสั่งหรือโปรแกรมคอมพิวเตอร์ที่พัฒนาขึ้นมาเพื่อก่อความเสียหายระบบคอมพิวเตอร์ ไม่ว่าจะเป็นข้อมูลชุดคำสั่ง หรืออุปกรณ์ต่าง ๆ เช่น แผ่นดิสก์ ฮาร์ดดิสก์ หรือหน่วยความจำคอมพิวเตอร์ โดยสามารถแพร่กระจายเข้าเครื่องคอมพิวเตอร์ผ่านทางแผ่นบันทึกข้อมูลหรือระบบเครือข่าย

/อุปกรณ์...



**อุปกรณ์เครือข่าย** คือ อุปกรณ์ที่นำมาใช้ในเครือข่ายทำหน้าที่จัดการเกี่ยวกับการรับ-ส่งข้อมูลในเครือข่าย หรือใช้สำหรับทวนสัญญาณเพื่อให้การรับ-ส่งข้อมูลได้ดี และส่งในระยะที่ไกลมากขึ้น หรือใช้สำหรับขยายเครือข่ายให้มีขนาดใหญ่ขึ้น

**Access Control** คือ ระบบควบคุมกำหนดสิทธิการเข้า-ออก

**Access Point** คือ อุปกรณ์ที่มีหน้าที่ในการกระจายสัญญาณ Wi-Fi เป็นหลัก ซึ่งนิยมนำไปวางกระจายตามจุดต่างๆ ให้รัศมีของสัญญาณ Wi-Fi ครอบคลุม เพื่อให้อุปกรณ์ที่รองรับ Wi-Fi เชื่อมต่อเข้ามาอยู่ในวง LAN เดียวกัน

**Application logs** คือ การบันทึกการทำงานของโปรแกรมนั้นๆ

**Authentication** คือ ระบบการยืนยันตัวตนที่เมื่อเราจะเข้าใช้งานในเว็บไซต์ แอปพลิเคชัน หรืออะไรก็ตามบนโลกออนไลน์ พุดง่าย ๆ ก็คือ การ Log in นั้นเองเช่น การเข้าสู่ระบบ Email, การเข้าสู่ระบบ Internet Banking และการเข้าสู่ระบบ social media ต่างๆ เพื่อเป็นการยืนยันตัวตนว่าเราคือคน ๆ นี้และกำลังจะใช้บริการต่างๆ ในฐานะคนนี้ พร้อมทั้งทำการตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบนั้นมีสิทธิ์ใช้ได้และเป็นเจ้าของข้อมูลเหล่านั้นจริงๆ โดยการยืนยันนั้นก็จะมีการใส่ Username และ Password ไม่ว่าจะเป็นแบบที่เรากำหนดตัวเองหรือแบบที่ระบบกำหนดมาให้เราใช้ตาม มันมีชื่อเรียกสั้นๆ ว่า AuthN

**Backup** คือ การสำรองข้อมูล เป็นการคัดลอกแฟ้มข้อมูลเพื่อทำสำเนา เพื่อหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย โดยสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้ทันที

**Chief Information Officer (CIO)** คือ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกรมพินิจและคุ้มครองเด็กและเยาวชน

**Cloud หรือ Cloud Computing** คือ เป็นระบบคอมพิวเตอร์ที่พร้อมรองรับการทำงานของผู้ใช้งานในทุกๆ ด้านไม่ว่าจะเป็นระบบเครือข่าย การจัดเก็บข้อมูล การทดสอบระบบหรือติดตั้งฐานข้อมูล หรือการใช้งานซอฟต์แวร์เฉพาะด้านในธุรกิจต่างๆ โดยที่ผู้ใช้งานไม่ต้องติดตั้งระบบทั้งฮาร์ดแวร์และซอฟต์แวร์ไว้ที่สำนักงานให้ยุ่งยาก แต่สามารถใช้งานในสิ่งที่ต้องการได้ด้วยการเชื่อมต่อกับระบบ Cloud Computing ผ่านอินเทอร์เน็ต

**Command line** คือ ข้อความที่พิมพ์ลงบนจอภาพ เพื่อเป็นคำสั่งให้ เครื่องคอมพิวเตอร์ทำงาน โดยปกติใช้หมายถึงคำสั่งที่อยู่พิมพ์หลัง A> B> หรือ C> เช่น A>COPY

**Core Switch** คือ อุปกรณ์ที่ใช้เป็นศูนย์กลางในการเชื่อมต่อไปยัง server และ router/gateway เพื่อให้ผู้ใช้งานเข้าถึง corporate application และ cloud-based application ได้

**Cracker** คือ การก่ออาชญากรรมทางโลกไซเบอร์ มีลักษณะคล้ายกับแฮกเกอร์แต่แตกต่างกันตรงความคิดและเจตนา แฮกเกอร์ คือผู้ที่นำความรู้ในการแฮกไปใช้ในทางที่มีประโยชน์ ส่วนแครกเกอร์ คือผู้ที่นำความรู้ในการแฮกไปใช้ในการทำความผิด เช่น การขโมยข้อมูล การทำลายข้อมูล หรือแม้กระทั่งการครอบครองคอมพิวเตอร์คนอื่น

**Database Server** คือ เซิร์ฟเวอร์ที่มีไว้เพื่อรันระบบที่เป็นฐานข้อมูล DBMS (Database Management System) เช่น MSQL, MySQL เป็นต้น โดยภายในเซิร์ฟเวอร์ ที่มีทั้งฐานข้อมูลและตัวจัดการ ฐานข้อมูล ตัวจัดการฐานข้อมูลในที่นี้หมายถึง มีการแบ่งปัน การประมวลผล

**Default** คือ ค่าค่าหนึ่งที่กำหนดไว้ในโปรแกรมสำเร็จ (ทุกโปรแกรม) ให้เป็นค่าที่ใช้ในตอนเริ่มต้นโปรแกรม ทุกครั้งที่เรียกโปรแกรมนั้นใช้

**DR Site (Disaster Recovery Site)** คือ ไซต์สำรองสำหรับแก้ไขปัญหาระบบสารสนเทศที่เกิดขึ้นจากภัยพิบัติต่างๆ ให้สามารถทำงานได้อย่างต่อเนื่อง





**Firewall** คือ ระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ไม่ให้ถูกโจมตีจากผู้ไม่หวังดี หรือการสื่อสารที่ไม่ได้รับอนุญาต

**FTP** คือ แอปพลิเคชันซอฟต์แวร์ที่เปิดใช้งานการถ่ายโอนไฟล์จากอุปกรณ์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง

**Government Data Center and Cloud service (GDCC)** คือ บริการระบบคลาวด์กลาง ภาครัฐหรือเป็นบริการของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) ซึ่งดำเนินการร่วมกับบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ในการ รวมศูนย์การให้บริการเครื่องคอมพิวเตอร์เสมือนสำหรับหน่วยงานภาครัฐ

**Generator** คือ เครื่องกำเนิดไฟฟ้า หรือ เครื่องปั่นไฟ

**Hacker** คือ บุคคลผู้ที่เป็นอาชญากร มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูล ในคอมพิวเตอร์ โดยเจาะผ่านระบบรักษาความปลอดภัย ของคอมพิวเตอร์ได้

**IP Address** คือ หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอล แบบ TCP/IP สามารถบอกได้ว่าเครื่องคอมพิวเตอร์ตั้งอยู่ที่ไหน ซึ่งสามารถระบุได้ผ่าน ip address และ ip จะไม่ซ้ำกัน

**Local Area Network (LAN) หรือ ข่ายงานบริเวณระยะใกล้** คือ การเชื่อมโยงเครือข่ายคอมพิวเตอร์ ถึงกันทั้งหมดโดยอาศัยสื่อกลาง มีการแบ่งแยกเครือข่ายออกเป็น ๓ รูปแบบการเชื่อมโยงคือ การเชื่อมโยง ภายในพื้นที่ระยะใกล้หรือ แลน (LAN) การเชื่อมโยงเครือข่ายระดับเมืองหรือแมน (MAN) และการเชื่อมโยง ระยะไกลหรือแวน (WAN) Log

**Main Board** คือ อุปกรณ์ที่สำคัญรองมาจากซีพียู เมนบอร์ดทำหน้าที่ควบคุม ดูแลและจัดการการทำงานของอุปกรณ์ชนิดต่างๆ ในเครื่องคอมพิวเตอร์

**Malware** คือ โปรแกรมชนิดหนึ่งที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อคอมพิวเตอร์ ซึ่งในปัจจุบัน Malware ถูกแบ่งประเภทออกได้มากมายหลากหลายประเภทตามลักษณะพิเศษของแต่ละชนิดเช่น Computer Virus, Worms, Trojan house, Spyware เป็นต้น

**MPLS** คือ เป็นบริการวางจรรยาบรรณข้อมูลความเร็วสูงสำหรับเชื่อมโยงเครือข่ายองค์กรเข้าหากันด้วย เทคโนโลยีของ MPLS ช่วยเพิ่มความคล่องตัวในการติดต่อสื่อสารระหว่างองค์กร ทำให้สามารถใช้โครงข่ายได้อย่างคุ้มค่าและเต็มประสิทธิภาพ

**Network** คือ ระบบเครือข่ายที่เชื่อมโยงคอมพิวเตอร์เข้าด้วยกันเพื่อการติดต่อสื่อสาร

**Operating system (OS)** คือ ระบบซอฟต์แวร์ที่ทำหน้าที่จัดการอุปกรณ์คอมพิวเตอร์และแหล่งซอฟต์แวร์และบริการโปรแกรมคอมพิวเตอร์ Packet filtering

**Patch** คือ โปรแกรมที่ใช้ซ่อมแซมจุดบกพร่องของโปรแกรมคอมพิวเตอร์ หรือปรับปรุงข้อมูลสำหรับ โปรแกรมให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น

**Remote access** คือ การเข้าถึงคอมพิวเตอร์หรือเครือข่ายจากระยะทางไกลผ่านระบบอินเทอร์เน็ต

**SAN Storage** คือ การเชื่อมต่ออุปกรณ์บันทึกข้อมูลเข้ากับ Server โดยตรง เพื่อช่วยให้การจัดเก็บข้อมูลมีประสิทธิภาพมากยิ่งขึ้น

**Service Set Identifier (SSID)** คือ การระบุชื่อเครือข่ายไร้สาย อุปกรณ์ไร้สายทั้งหมดบนเครือข่าย จะต้องใช้ SSID เดียวกัน

**Source Code** คือ คำสั่งหรือโค้ดในโปรแกรม ซึ่งเขียนด้วยภาษาคอมพิวเตอร์ ภาษาต่างๆ เช่น C , Java , pascal เป็นต้น มนุษย์สามารถอ่านเข้าใจได้ ซึ่งโปรแกรมเมอร์จะต้องเขียนก่อนที่โปรแกรมจะถูกแปล ไปเป็นคำสั่งภาษาเครื่อง ที่คอมพิวเตอร์สามารถเข้าใจได้



WPA หรือ Wi-Fi Protected Access (WPA) คือ มาตรฐานยอตนนิยมที่ใช้ในการตั้งค่าเครือข่าย Wi-Fi ซึ่งใช้ในการตรวจสอบสิทธิ์ผู้ใชัด้วยรหัสผ่าน และข้อมูลทั้งหมดที่ส่งระหว่างเราเตอร์และอุปกรณ์ที่ใช้ Wi-Fi จะถูกเข้ารหัสและไม่สามารถถูกดักจับโดยคนใกล้เคียง หรือเชื่อมต่อเครือข่าย Wi-Fi เดียวกัน

#### ๔. การประเมินสถานการณ์ความเสี่ยง

เนื่องจากกรมพินิจและคุ้มครองเด็กและเยาวชนมีภารกิจที่หลากหลาย เทคโนโลยีสารสนเทศ จึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสที่จะเกิดความเสียหาย รวมถึงแนวทางในการตรวจสอบและประเมิน ความเสี่ยงด้านสารสนเทศ ที่จะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยี สารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคง ปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน พบประเภทความเสี่ยงที่อาจเกิดผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

**๔.๑ ความเสี่ยงด้านเทคนิค** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและ อุปกรณ์ อาจถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ความเสี่ยงที่เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) และสร้างความเสียหายให้แก่เครื่อง คอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ถึงขั้นใช้งานไม่ได้ จึงมีการดำเนินการเชิงป้องกันไว้ดังนี้

๔.๑.๑ ติดตั้ง Firewall เพื่อป้องกันไม่ให้บุคคลอื่นที่ไม่ได้รับอนุญาตเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชนได้

๔.๑.๒ ติดตั้งระบบป้องกันไวรัส เพื่อป้องกันไวรัสคอมพิวเตอร์ที่เครื่องคอมพิวเตอร์แม่ข่าย และมีการติดตั้งซอฟต์แวร์ (Software) ป้องกันไวรัสที่เครื่องให้บริการ (Server) และเครื่องคอมพิวเตอร์ ลูกข่าย (Client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย รวมทั้งแนะนำวิธีการป้องกันและการกำจัด ไวรัสต่างๆ ให้ผู้ใช้งานได้ศึกษาสามารถดำเนินการได้อย่างถูกวิธี และเพื่อตระหนักถึงความเสี่ยงที่จะเกิดขึ้น รวมถึงการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๔.๑.๓ ติดตั้งระบบตรวจสอบและตอบโต้การบุกรุก IPS (Intrusion Prevention System) เพื่อดำเนินการตรวจสอบข้อมูลที่มีลักษณะการทำงานที่เป็นความเสี่ยงต่อระบบเครือข่าย และสั่งการป้องกัน อันตรายไม่ให้เข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ โดยระบบดังกล่าวของกรมพินิจและคุ้มครอง เด็กและเยาวชนอยู่ภายใต้การดูแลของสำนักงานปลัดกระทรวงยุติธรรม

**๔.๒ ความเสี่ยงด้านบุคคล** เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดลำดับ ความสำคัญในการเข้าถึงข้อมูลที่ไม่เหมาะสมกับการใช้งาน หรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบ สารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมพินิจและคุ้มครองเด็กและเยาวชนเกินกว่าอำนาจหน้าที่ขององค์กร และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความ เข้าใจในการใช้งานเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมาย หน้าที่และสิทธิของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด การ ถ่ายทอดความรู้ในคุณลักษณะของงานที่ชัดเจนให้ผู้รับผิดชอบงานรายใหม่ เพื่อให้บุคลากรมีความรู้ ความ เข้าใจในการใช้งานที่ถูกต้อง รวมถึงการดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ดังนี้





๔.๒.๑ ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักหรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

๔.๒.๒ ความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดลำดับความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้งานอาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

เพื่อเป็นการเสริมสร้างความรู้ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศเบื้องต้น จึงควรจัดให้เจ้าหน้าที่เข้ารับการฝึกอบรม สัมมนาให้มีความรู้ความเข้าใจในด้านการใช้งานเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด พร้อมทั้งนี้ควรจัดให้มีการสร้างความตระหนักรู้ ให้สอดคล้องด้านกฎหมาย พ.ร.บ.บริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔.๓ ความเสี่ยงที่เกิดจากระบบไฟฟ้าขัดข้องหรือความเสียหายจากเพลิงไหม้ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม ได้ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) เพื่อสำรองไฟฟ้าและจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) กรณีเกิดกระแสไฟฟ้าขัดข้อง จะทำให้ระบบเครือข่ายสามารถให้บริการได้ต่อเนื่องในระยะเวลาประมาณ ๘ ชั่วโมง ที่จะสามารถทำการจัดเก็บข้อมูลและสำรองข้อมูล (Backup) ไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงไหม้ นั้น สำนักงานปลัดกระทรวงยุติธรรม จัดให้มีระบบควบคุมป้องกันเพลิงไหม้ไว้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่างๆ ภายในอาคารกระทรวงยุติธรรม และได้มีข้อกำหนดการซักซ้อมแผนป้องกันอัคคีภัยให้กับบุคลากรที่มีส่วนเกี่ยวข้อง ปีละ ๑ ครั้ง

๔.๔ ความเสี่ยงด้านภัยพิบัติตามธรรมชาติหรือสถานการณ์ฉุกเฉินอื่น เกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความสูญเสียหรือเสียหายกับข้อมูลสารสนเทศ เช่น น้ำท่วม การชุมนุมประท้วง ความไม่สงบเรียบร้อยในบ้านเมือง โรคระบาด เป็นต้น ซึ่ง ศูนย์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดเก็บข้อมูลสำรองไว้อย่างสม่ำเสมอและต่อเนื่อง ซึ่งกรมพินิจและคุ้มครองเด็กและเยาวชนควรจะมีศูนย์สำรองระบบสารสนเทศ (Disaster Recovery Site) และจัดทำระบบสำรองข้อมูล (Backup System) ทั้งนี้ GDCC (Cloud กลางภาครัฐ) มีพื้นที่ไม่เพียงพอต่อการให้บริการของกรมพินิจและคุ้มครองเด็กและเยาวชน ควรจะมีการจัดหาศูนย์สำรองระบบสารสนเทศ (Disaster Recovery Site)

๔.๕ เกิดจากการโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์และข้อมูลในส่วนของห้องศูนย์ข้อมูลกระทรวงยุติธรรม (MOJ Data Center) จึงได้มีข้อกำหนดห้ามไม่ให้เจ้าหน้าที่และบุคลากรภายนอกที่ไม่มีส่วนเกี่ยวข้องเข้าไปในบริเวณห้องศูนย์ข้อมูลกระทรวงยุติธรรม (MOJ Data Center) ยกเว้นหากมีความจำเป็นที่ต้องเข้าไปปฏิบัติงานในห้องดังกล่าว จะต้องมีเจ้าหน้าที่กลุ่มระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และความมั่นคงปลอดภัย เป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้า-ออก ได้ติดตั้งเครื่องอ่านบัตรแบบแม่เหล็ก (Access Control) เพื่อป้องกันไม่ให้ บุคคลภายนอก และเจ้าหน้าที่ที่ไม่ได้มีส่วนเกี่ยวข้องเข้ามาในห้องศูนย์ข้อมูลกระทรวงยุติธรรม (MOJ Data Center) โดยไม่ได้รับอนุญาต และมีการติดตั้งกล้องวงจรปิดไว้ภายในบริเวณห้องศูนย์ข้อมูลกระทรวงยุติธรรม (MOJ Data Center) เพื่อป้องกันการโจรกรรม

/จากผล...





จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชน ดังกล่าวข้างต้น พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงมีความจำเป็นที่จะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน

#### ๕. แนวทางการจัดการภัยพิบัติ

**๕.๑ การสำรองข้อมูล (Backup)** เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล เพื่อให้สามารถนำข้อมูลกลับมาใช้งานได้ทันที โดยมีแนวทางดำเนินการที่ชัดเจน ซึ่งปัจจุบัน ศูนย์เทคโนโลยีสารสนเทศ ได้สำรองข้อมูลทั้งหมด (Full backup) มาใช้เพื่อเพิ่มประสิทธิภาพการทำงานให้สามารถใช้งานได้อย่างต่อเนื่อง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลแบบอัตโนมัติด้วยโปรแกรม Commvault โดยทำการกำหนดค่า วัน เวลา และเครื่องคอมพิวเตอร์แม่ข่ายที่ต้องการจะทำการสำรองข้อมูล (Policies) โดยสำรองไว้ที่อุปกรณ์จัดเก็บ เช่น อุปกรณ์บันทึกข้อมูล (Network Attached Storage : NAS) และอุปกรณ์จัดเก็บข้อมูลสำหรับเครื่องแม่ข่ายขนาดใหญ่ Storage Area Network (SAN) สามารถแบ่งการสำรองข้อมูลออกเป็น ๒ ประเภท ดังนี้

**๕.๑.๑ การสำรองฐานข้อมูล (Database)** การสำรองฐานข้อมูลหลักที่มีความสำคัญมาก จะทำการสำรองข้อมูลทุกวัน เริ่มตั้งแต่เวลา ๐๐.๐๐ น. โดยจะทำการสำรองลงในอุปกรณ์จัดเก็บข้อมูลสำหรับเครื่องแม่ข่ายขนาดใหญ่ (Storage Area Network : SAN) และอุปกรณ์บันทึกข้อมูล เช่น ระบบโครงข่ายระดับบูรณาการภาครัฐและประชาชน ระบบงานคดีครอบครัว ระบบงานคดีกำกับการปกครอง และระบบสนับสนุนการปฏิบัติงานต่างๆ ของเจ้าหน้าที่กรมพินิจและคุ้มครองเด็กและเยาวชน เป็นต้น

**๕.๑.๒ การสำรองโปรแกรมโครงสร้างและฐานข้อมูลและระบบปฏิบัติการ (OS)** การสำรองข้อมูลและระบบปฏิบัติการ (OS) จะทำการสำรองข้อมูล โดยจะเริ่มต้นในเวลา ๐๐.๐๐ น. ซึ่งจัดเก็บลงในเครื่องแม่ข่ายขนาดใหญ่ Storage Area Network (SAN) โดยมีการกำหนดระยะเวลาตรวจสอบความสมบูรณ์และพร้อมใช้ของข้อมูลที่ได้ทำการสำรองไว้ด้วยวิธีการตรวจสอบสถานะข้อผิดพลาดของข้อมูลที่ได้ทำการ backup ทุกครั้งหลังการ backup

**๕.๒ ทำการทดสอบและกู้คืนฐานข้อมูล (Database Recovery)** โดยมีแผนดำเนินการทุก ๖ เดือน

**๕.๓ จัดหาเจ้าหน้าที่ บำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์จัดเก็บข้อมูลขนาดใหญ่** เพื่อลดความเสียหายของข้อมูล

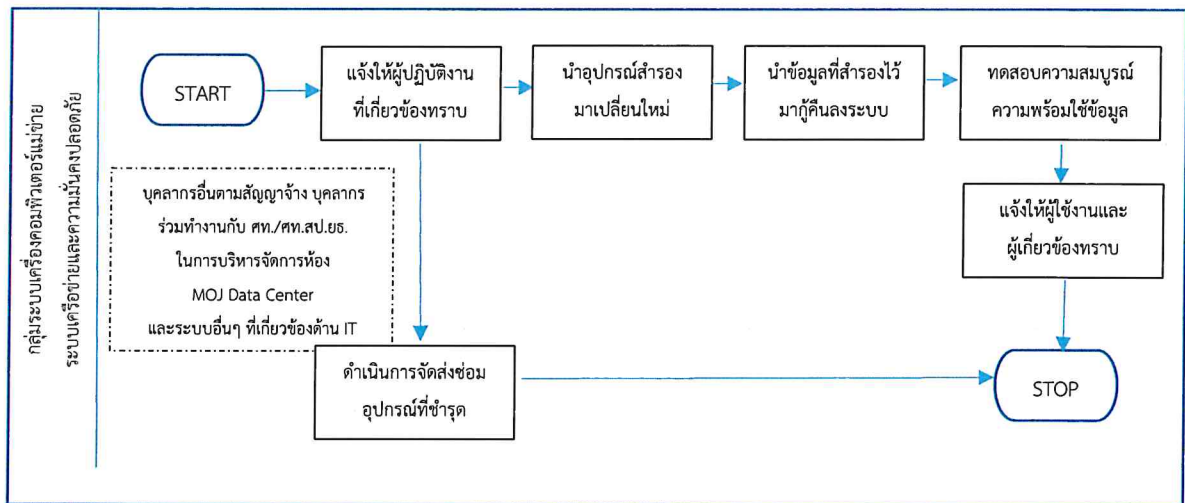
**กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย มีวิธีการดำเนินการดังนี้**

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- จัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่สำรองไว้มากู้คืนลงระบบโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งผู้ใช้งานและผู้เกี่ยวข้องทราบ

/แผนภูมิ...



### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



๕.๔ การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย ซึ่งผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้กับผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ มีวิธีการดังนี้

๕.๔.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ โดยเครื่องคอมพิวเตอร์แม่ข่าย (Server) จะทำหน้าที่โหลด patch โปรแกรมที่มีความทันสมัยและมีความสามารถในการป้องกันไวรัสที่มีประสิทธิภาพไว้ที่เครื่อง Server ก่อนแล้วจึงส่ง patch การอัปเดตไปยังเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่เชื่อมต่อกับระบบเครือข่ายและมีการเปิดใช้งานอยู่อีกครั้ง

๕.๔.๒ ใช้ความระมัดระวังในการเปิด E-mail ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มาและควรลบทิ้งทันที

๕.๔.๓ ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet ไม่ดาวน์โหลดจากเว็บไซต์ที่น่าเชื่อถือและหลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น มีการติดตามข้อมูลการแจ้งการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

๕.๔.๔ วิเคราะห์สาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด มีการตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

๕.๔.๕ กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งเหตุให้ศูนย์เทคโนโลยีสารสนเทศ ทราบ หรือกรณีมีเหตุอันทำให้อุปกรณ์คอมพิวเตอร์ไม่สามารถให้บริการเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศจะต้องประกาศให้หน่วยงานในสังกัด กรมพินิจและคุ้มครองเด็กและเยาวชนทราบ

#### กรณีการป้องกันไวรัสล้มเหลว มีวิธีการดำเนินการดังนี้

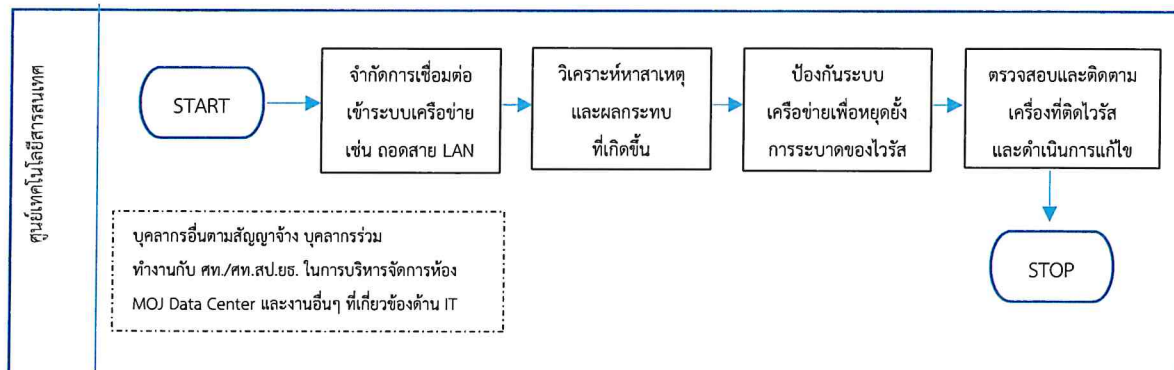
- กรณีถูกไวรัสหรือผู้บุกรุกเพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย เช่น การถอดสาย LAN
- วิเคราะห์สาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

/กรณี...



- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติให้แจ้งเหตุให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศทราบทันที หรือกรณีมีเหตุอันทำให้ศูนย์เทคโนโลยีสารสนเทศไม่สามารถให้บริการด้านเครือข่ายได้จะต้องประสานให้ผู้ใช้งานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชนทราบ

#### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีการป้องกันไวรัสสล์มเหลว



**๕.๕ การป้องกันและแก้ไขที่เกิดจากกระแสไฟฟ้าขัดข้อง/ไฟดับ** เพื่อเป็นการป้องกันและแก้ไข ปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆได้ โดยมีวิธีการดังนี้

๕.๕.๑ ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) สำรองไฟฟ้า เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) เป็นการควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบคอมพิวเตอร์ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งจะทำให้ระบบของคอมพิวเตอร์สามารถให้บริการได้ในระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๘ ชั่วโมง

๕.๕.๒ เครื่องกำเนิดไฟฟ้า (Generator) ทำงานทันทีเมื่อไฟฟ้าภายในอาคารกระทรวงยุติธรรม ขัดข้องหรือดับและมีการบำรุงรักษาเครื่องกำเนิดไฟฟ้าให้มีสภาพพร้อมใช้งานอยู่เสมอ

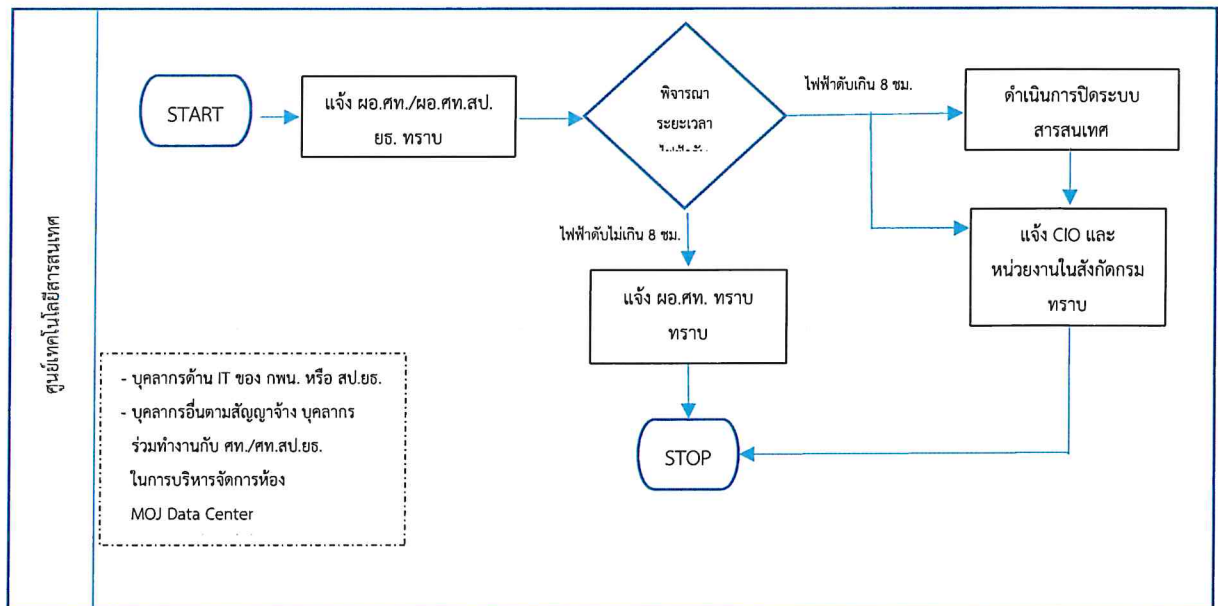
๕.๕.๓ เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้งานเร่งทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ เพื่อป้องกันการสูญหายในระดับหนึ่ง

#### กรณีไฟฟ้าขัดข้อง มีวิธีการดำเนินการดังนี้

- หากไฟฟ้ามดับทันทีจะมีระบบ SMS แจ้งเตือนไปยังผู้ดูแลระบบและส่งคำสั่งให้เครื่อง Generator ทำงานในระยะเวลาของการสำรองไฟฟ้าได้ประมาณ ๘ ชั่วโมง
- หากกระแสไฟฟ้าไม่สม่ำเสมอ ผู้ดูแลระบบต้องดำเนินการเปิดเครื่อง Generator ด้วยมือ
- หากเครื่อง Generator มีปัญหา แจ้ง ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. และบริษัทผู้รับจ้าง เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาอุปกรณ์มาทดแทนทันที

/แผนภูมิ...

### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีไฟฟ้าขัดข้อง



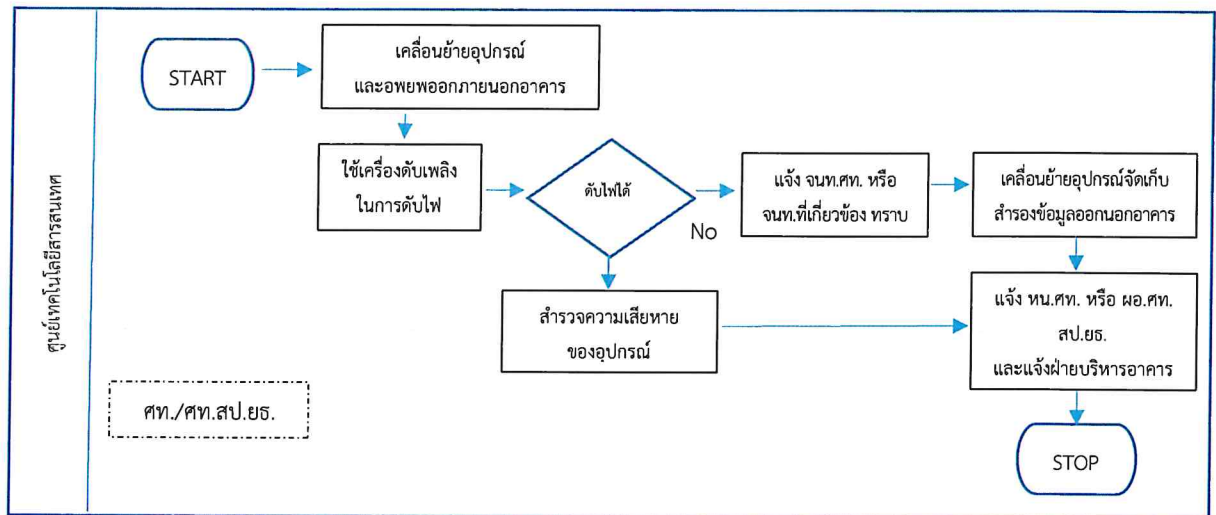
๕.๖ มีระบบป้องกันไฟไหม้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ติดตั้งเครื่องตรวจจับควันเตือนภัยเมื่อมีควันไฟ Carbon Monoxide Detector ไว้ในห้องคอมพิวเตอร์แม่ข่าย พร้อมเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์ มีการจัดทำเครื่องหมายระบุความสำคัญของอุปกรณ์ตามลำดับเพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน ซึ่งในพื้นที่ควบคุมจะมีอุปกรณ์ดับเพลิงติดตั้งในทุกอาคารเพื่อทำการควบคุมเพลิงในเบื้องต้นได้

#### กรณีไฟไหม้ มีวิธีการดำเนินการดังนี้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบอพยพออกไปภายนอกอาคารและให้ผู้ที่สามารถใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บสำรองข้อมูลออกภายนอกอาคารและแจ้งฝ่ายบริหารอาคารกระทรวงยุติธรรม โทร ๐๘ ๑๘๘๐ ๕๓๕๑ หรือเจ้าหน้าที่ฝ่ายอาคารของกรมพินิจและคุ้มครองเด็กและเยาวชน โทร ๐ ๒๑๔๑ ๕๔๕๑
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน และอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟและดับไฟอัตโนมัติ



### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีไฟไหม้



๕.๗ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล เพื่อเป็นป้องกันการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย มีวิธีการดังนี้

๕.๗.๑ มีการควบคุมการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้เจ้าหน้าที่ของ ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. เป็นผู้รับผิดชอบนำพาเข้าไป

๕.๗.๒ จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย โดย ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ได้ติดตั้งเครื่องอ่านบัตรแบบแม่เหล็ก (Access Control) เพื่อป้องกันไม่ให้เกิดบุคคลภายนอกเข้ามาในหน่วยงานโดยไม่ได้รับอนุญาต

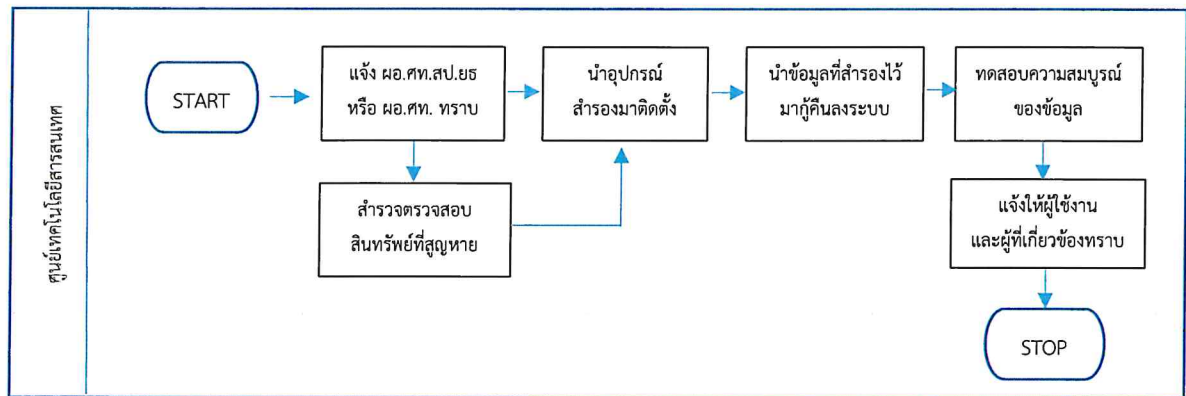
๕.๗.๓ มีการติดตั้งกล้องวงจรปิดเพื่อสามารถตรวจสอบการโจรกรรมในภายหลังได้

กรณีถูกโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย มีวิธีการดำเนินการดังนี้

- ผู้ดูแลระบบแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบโดยด่วน
- สำรวจตรวจสอบรายการสินทรัพย์ที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์มาติดตั้งทดแทน และนำข้อมูลที่สำรองไว้กู้คืนในระบบ เพื่อให้ผู้ใช้งานสามารถใช้ระบบงานได้โดยเร็ว

/แผนภูมิ...

### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีถูกโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย



๕.๘ การโจรกรรมข้อมูล/ข้อมูลรั่วไหล ซึ่งเป็นข้อมูลที่กรมพินิจและคุ้มครองเด็กและเยาวชนเป็นผู้ดูแลรับผิดชอบ ถูกโจมตีหรือคุกคามทางไซเบอร์โดยการใช้แรนซัมแวร์ (Ransomware) มีการนำข้อมูลไปเรียกค่าไถ่หรือไปจำหน่ายบนอินเทอร์เน็ต จนทำให้เกิดข้อมูลรั่วไหลมีการนำไปใช้ในทางมิชอบ เผยแพร่สู่สาธารณะซึ่งเป็นการละเมิดสิทธิส่วนบุคคลจนทำให้เกิดความเสียหายต่อเจ้าของข้อมูล เพื่อเป็นการป้องกันเหตุการณ์ดังกล่าว กรมพินิจและคุ้มครองเด็กและเยาวชนจึงได้มีการดำเนินการดังนี้

๕.๘.๑ ดำเนินการกำหนดสิทธิและรหัสผ่าน การเข้าถึงคอมพิวเตอร์ และระบบเครือข่ายภายในกรมพินิจฯ

๕.๘.๒ ประกาศใช้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้เจ้าหน้าที่ภายในกรมพินิจฯ ถือปฏิบัติโดยเคร่งครัด

๕.๘.๓ จัดหาซอฟต์แวร์ในการตรวจสอบข้อมูลที่มีลักษณะการทำงานที่เป็นความเสี่ยงต่อระบบเครือข่าย และสิ่งการป้องกันอันตรายไม่ให้เข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ และสามารถระบุตัวบุคคล/อุปกรณ์ ของผู้กระทำความผิดได้

๕.๘.๔ จัดทำ Data Inventory/Record of Processing Activity (ROPA) ตามภารกิจหลัก และภารกิจสนับสนุนของกรมพินิจฯ ให้เป็นปัจจุบันอย่างสม่ำเสมอ

๕.๘.๕ มีการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Awareness Training) เพื่อเสริมสร้างให้บุคลากรมีองค์ความรู้เท่าทันภัยไซเบอร์ และสามารถใช้งานทรัพยากรสารสนเทศได้อย่างปลอดภัย

๕.๘.๖ จัดตั้งคณะกรรมการ/คณะทำงาน ดำเนินการให้ข้อเสนอแนะ ตรวจสอบ กำกับ ติดตามและขับเคลื่อน การดำเนินงานตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และพ.ร.บ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ตลอดจนปฏิบัติตามกรอบธรรมาภิบาลข้อมูลภาครัฐ และประกาศ/แนวปฏิบัติของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

/กรณี...



### กรณีพบการโจรกรรมข้อมูล มีวิธีการดำเนินการดังนี้

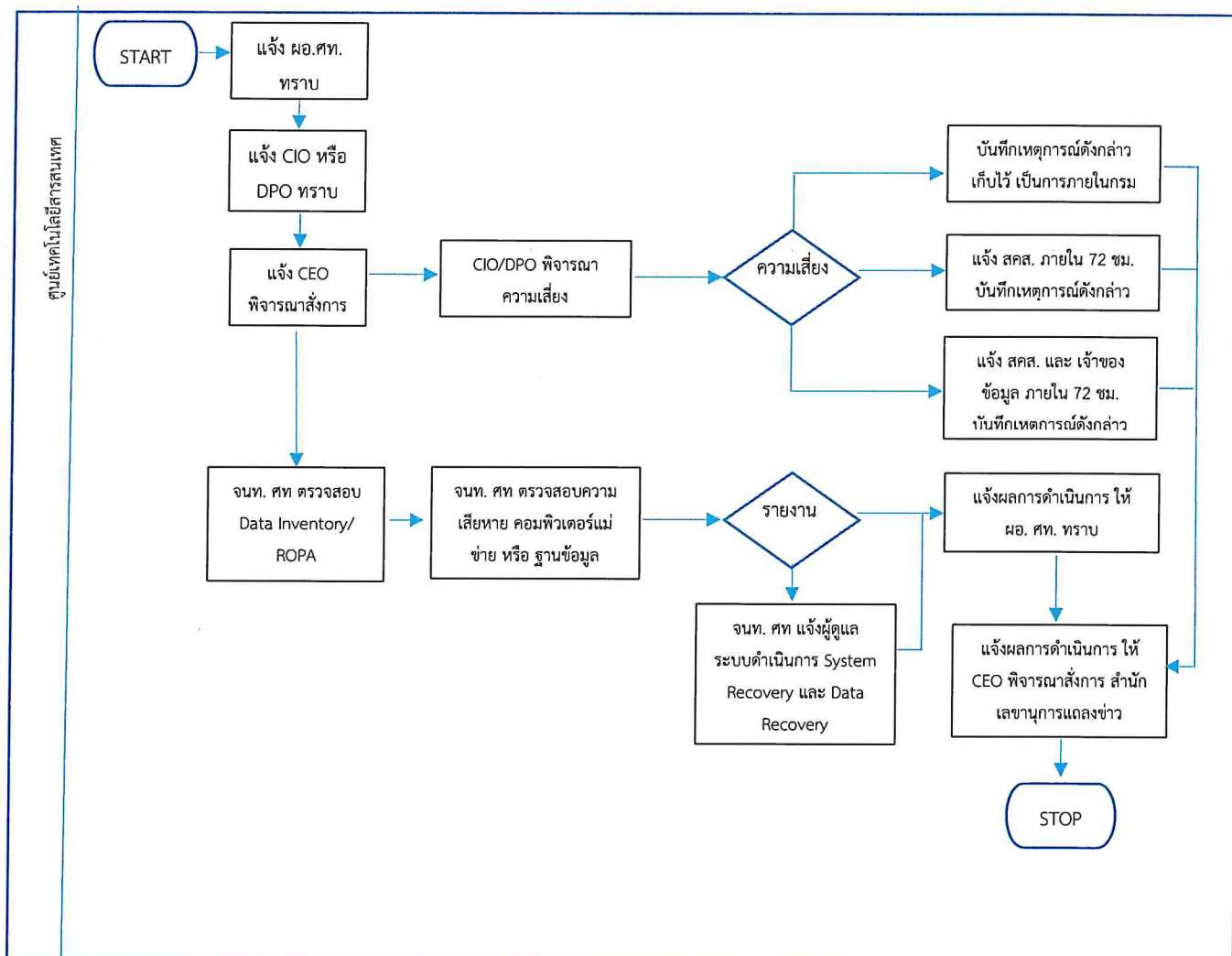
- หากเกิดการโจรกรรมข้อมูล/ข้อมูลรั่วไหล ผู้ดูแลระบบ แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบโดยด่วน
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศแจ้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) , Data Protection Officer (DPO)
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือ Data Protection Officer (DPO) แจ้งอธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อพิจารณาสั่งการให้เจ้าหน้าที่ที่เกี่ยวข้อง
  - ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือ Data Protection Officer (DPO) พิจารณาความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
    - ความเสี่ยงต่ำ ข้อมูลถูกเข้ารหัสจนไม่สามารถใช้งานได้ และมีระบบรองรับการบริการอย่างต่อเนื่อง ให้ดำเนินการบันทึกเหตุการณ์ดังกล่าวเก็บไว้ เป็นการภายในกรมพินิจฯ
    - ความเสี่ยงปานกลาง ข้อมูลไม่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ดำเนินการ แจ้งไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ ภายใน ๗๒ ชั่วโมง และดำเนินการบันทึกเหตุการณ์ดังกล่าวเก็บไว้
    - ความเสี่ยงสูง ข้อมูลไม่มีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ดำเนินการ แจ้งไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล/เจ้าของข้อมูลส่วนบุคคลทราบ ภายใน ๗๒ ชั่วโมง และดำเนินการบันทึกเหตุการณ์ดังกล่าวเก็บไว้
  - ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศแจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศดำเนินการตรวจสอบด้านเทคนิค
    - เจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศ ตรวจสอบ Data Inventory/Record of Processing Activity (ROPA) เพื่อระบุตำแหน่งที่จัดเก็บของข้อมูลส่วนบุคคล
    - เจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศ ตรวจสอบความเสียหายของอุปกรณ์แม่ข่าย หรือ ฐานข้อมูล ในกรณีถูกโจมตีหรือคุกคามทางไซเบอร์
    - กรณีพบความเสียหายของอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย หรือ ฐานข้อมูล เจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศ วิเคราะห์ปัญหา ดำเนินการแก้ไขปัญหา และแจ้งผู้ดูแลระบบที่เกี่ยวข้องดำเนินการกู้คืนข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (System Recovery) และการกู้ข้อมูล (Data Recovery) เพื่อให้ระบบสารสนเทศกลับมาใช้งานได้ตามปกติ และแจ้งผลการดำเนินการให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ
    - กรณีไม่พบความเสียหายของอุปกรณ์แม่ข่าย หรือ ฐานข้อมูล แจ้งผลการดำเนินการให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

/ผู้อำนวยการ...



- ผู้อำนวยการเทคโนโลยีสารสนเทศรายงานผลการดำเนินงาน ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือ Data Protection Officer (DPO) ทราบ
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือ Data Protection Officer (DPO) รายงานผลการดำเนินงาน ให้อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน ทราบ
- อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน สั่งการ สำนักงานเลขาธิการกรม แลงข่าวความเสียหายจากการโจรกรรมข้อมูล หรือข้อมูลรั่วไหล

### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีการโจรกรรมข้อมูล



/๕.๙ ระบบ...

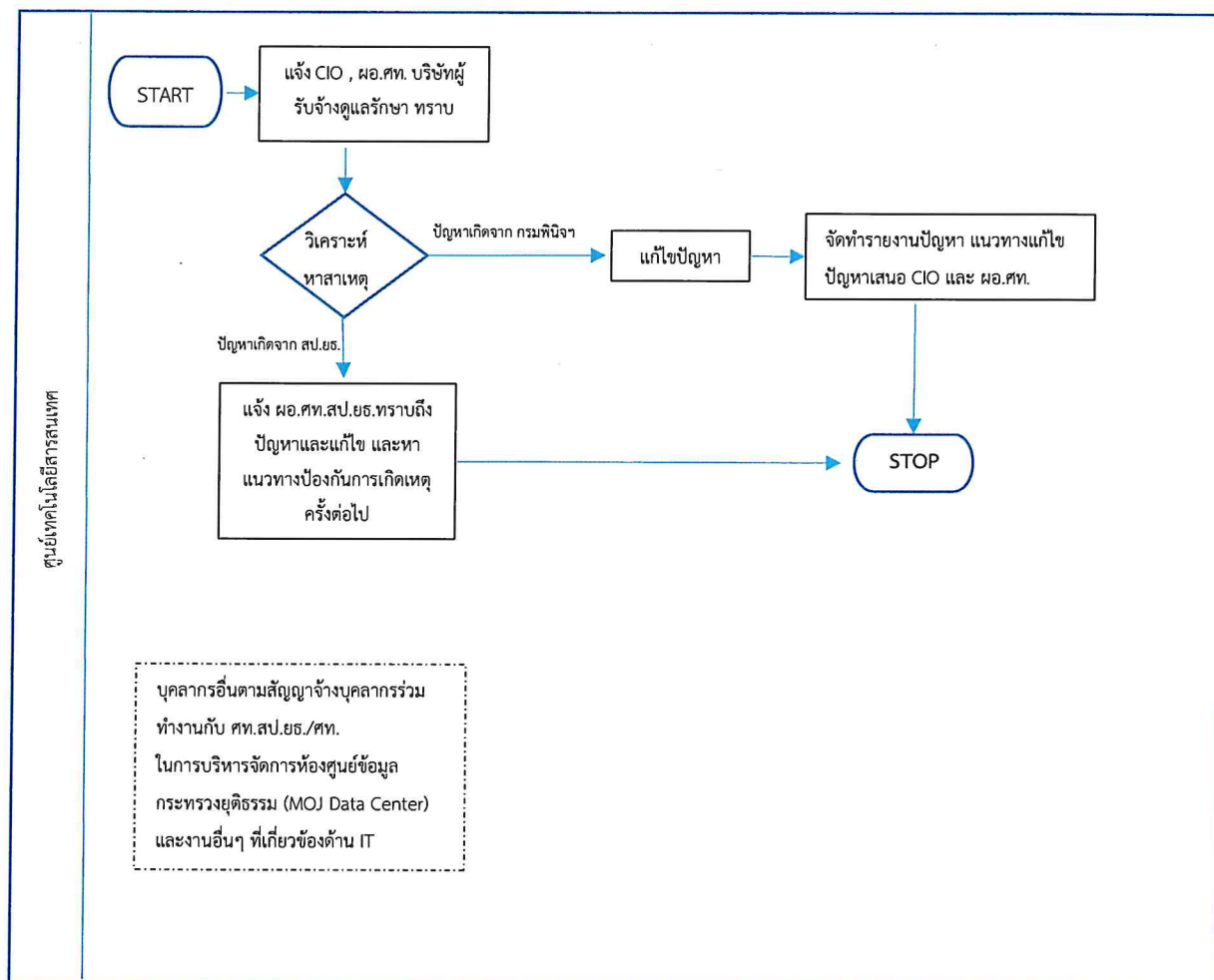


๕.๙ ระบบการสื่อสารของเครื่องแม่ข่าย ที่เชื่อมต่อบริเวณเครือข่ายเกิดความขัดข้อง ซึ่งกรมพินิจและคุ้มครองเด็กและเยาวชน ใช้ระบบเครือข่ายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม (ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ.) ดำเนินการตรวจสอบวงจรเครือข่าย วิเคราะห์และแก้ไขปัญหาให้วงจรเครือข่ายให้พร้อมใช้งานภายใน ๔ ชั่วโมง และรายงานการดำเนินงานให้ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศทราบโดยทันที

กรณีการเชื่อมโยงเครือข่ายล้มเหลว มีวิธีการดำเนินการดังนี้

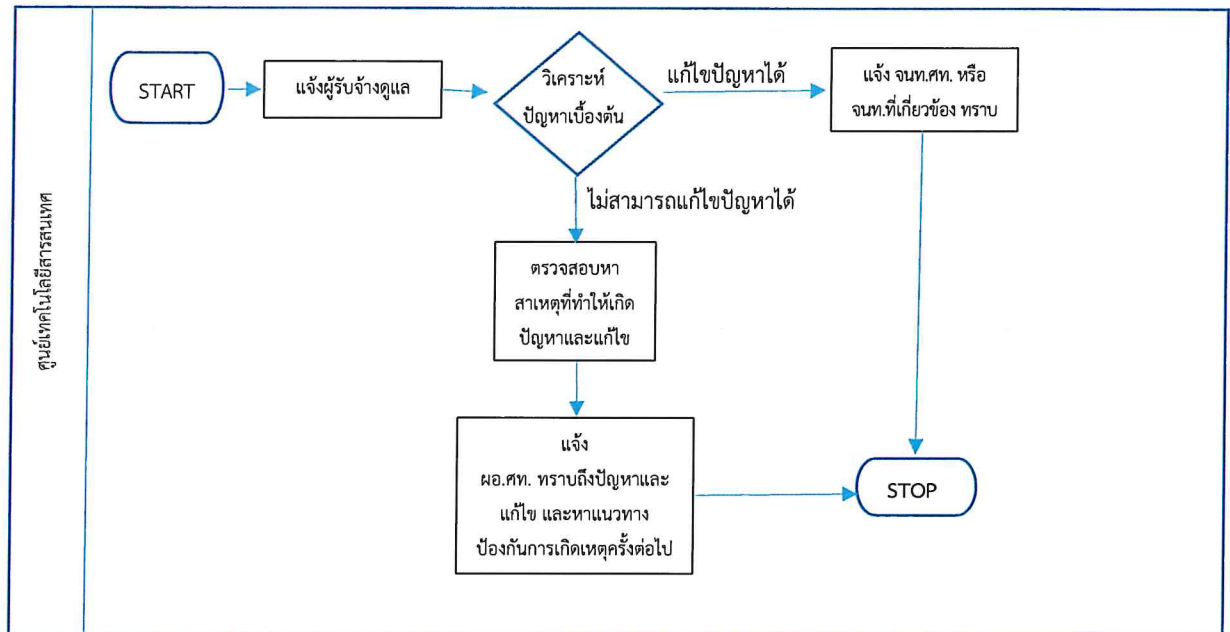
- รับดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิลขาด ให้รีบติดต่อบริษัทผู้รับจ้างบำรุงรักษา ทำการซ่อมแซมสายเคเบิลให้เสร็จโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางชั้นภายในอาคารกระทรวงยุติธรรม ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ Core Switch ที่ติดตั้งอยู่ภายในอาคารกระทรวงยุติธรรม

แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีเชื่อมโยงเครือข่ายล้มเหลว ส่วนกลางชั้น ๖-๗



/แผนภูมิ...

### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีเชื่อมโยงเครือข่ายล้มเหลว ส่วนภูมิภาค



๕.๑๐ การบุกรุกหรือการโจมตีจากภายนอก เพื่อหลีกเลี่ยงการเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศจากภายนอกที่สร้างความเสียหายหรือทำลายระบบข้อมูล ดำเนินการดังนี้

๕.๑๐.๑ สแกนหาจุดอ่อนและ Update Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยการใช้ซอฟต์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๕.๑๐.๒ ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมพินิจและคุ้มครองเด็กและเยาวชนได้

๕.๑๐.๓ ติดตั้งระบบ IPS เพื่อตรวจจับภัยคุกคามต่างๆ ที่อาจเกิดภายในระบบเครือข่าย

๕.๑๐.๔ จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตของกรมพินิจและคุ้มครองเด็กและเยาวชน เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕.๑๐.๕ ติดตั้งระบบป้องกันไวรัสให้ทันสมัยและมีการอัปเดตอย่างสม่ำเสมอ และปิด Port ที่ไม่ใช้บริการทั้งหมด

๕.๑๐.๖ การใช้งานระบบสารสนเทศจากหน่วยงานต่างๆ ทั้งในส่วนกลางและส่วนภูมิภาค ระบบเครือข่ายภายใน (Intranet) ผู้ใช้งานจะต้องมีการบันทึกชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) เพื่อระบุตัวตนก่อนเข้าใช้งานได้ตามสิทธิ และอำนาจหน้าที่ที่ได้รับมอบหมาย โดยมีการกำหนดรหัสผ่านไม่น้อยกว่า ๘ ตัวอักษร พร้อมทั้งมีอักขระพิเศษอย่างน้อย ๒ ตัวอักษร และไม่ควรกำหนดรหัสผ่านเดียวกันทุกระบบ และให้มีการเปลี่ยนรหัสผ่านทุก ๓ เดือน

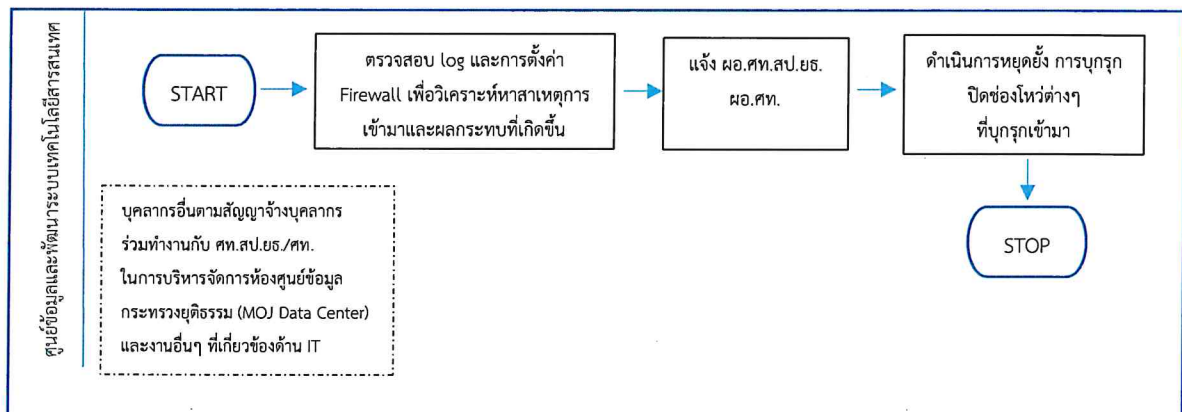
/๕.๑๐.๗ การดำเนิน...

๕.๑๐.๗ การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐, พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และพ.ร.บ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

#### กรณีการป้องกันผู้บุกรุกล้มเหลว มีวิธีการดำเนินการดังนี้

- กรณีที่มีผู้บุกรุก ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. หรือ ศูนย์เทคโนโลยีสารสนเทศ และนักวิชาการคอมพิวเตอร์ทุกคน รวมถึงเจ้าหน้าที่อื่นที่เกี่ยวข้องจะต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบของผู้บุกรุกและความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall และจากแหล่งอื่นๆ
- ผู้ดูแลระบบต้องแจ้ง ผอ.ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ./หัวหน้าศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ด้วยการปิดช่องโหว่ต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

#### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีการป้องกันผู้บุกรุกล้มเหลว



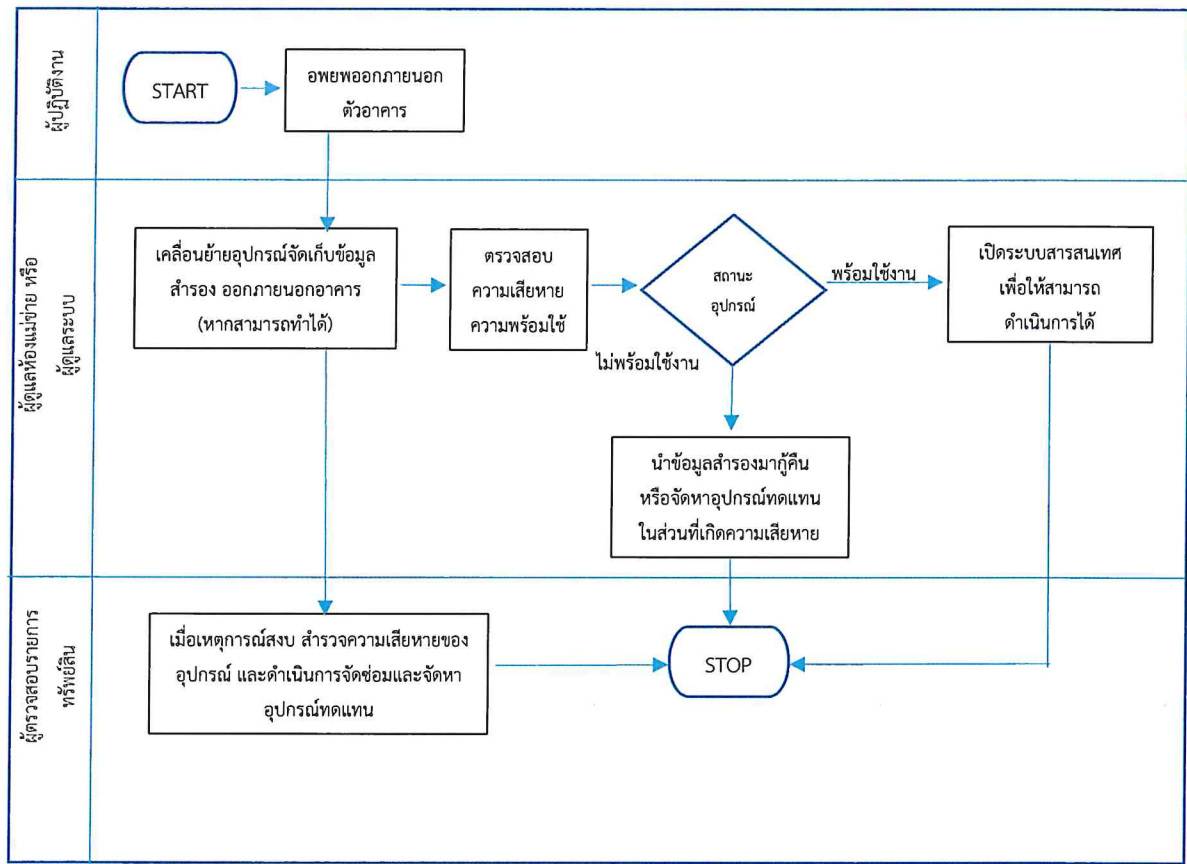
#### ๕.๑๑ กรณีแผ่นดินไหว เพื่อหลีกเลี่ยงอันตรายที่อาจเกิดขึ้นได้ ให้ปฏิบัติดังนี้

- ๕.๑๑.๑ ให้ผู้ปฏิบัติงานรีบอพยพออกภายนอกตัวอาคาร
- ๕.๑๑.๒ ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- ๕.๑๑.๓ เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

/แผนภูมิ...



### แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีแผ่นดินไหว



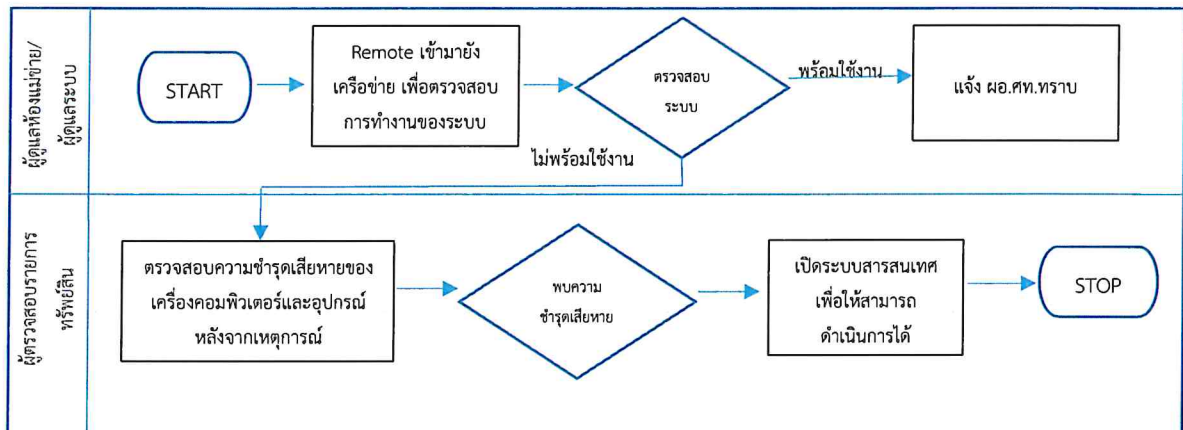
๕.๑๒ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง เพื่อหลีกเลี่ยงอันตรายที่อาจเกิดขึ้นได้ ให้ปฏิบัติดังนี้

๕.๑๒.๑ กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

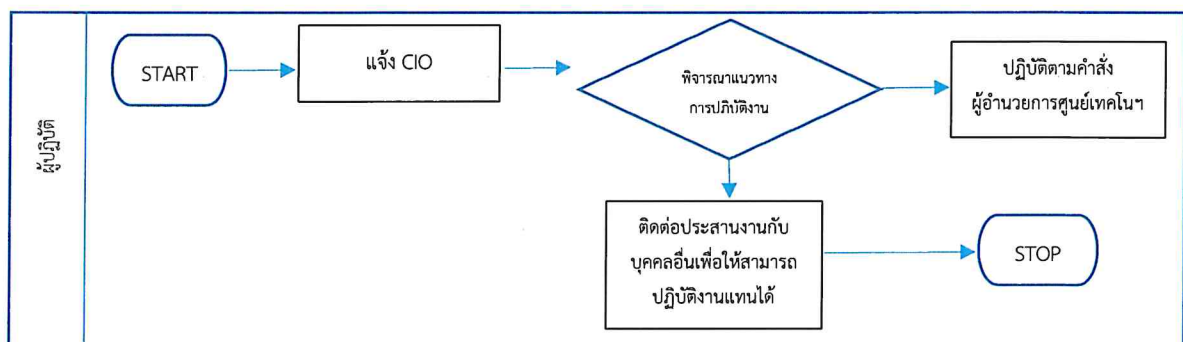
๕.๑๒.๒ หลังจากเกิดเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

/แผนภูมิ...

แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง



แผนภูมิแสดงขั้นตอนการรองรับสถานการณ์ กรณีบุคลากรภายในศูนย์เทคโนโลยีสารสนเทศ ไม่สามารถมาปฏิบัติงานได้



๕.๑๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจ ในการใช้อุปกรณ์ คอมพิวเตอร์ทั้งด้าน Hardware และ Software ทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือ หยุดทำงาน

๕.๑๓.๑ ให้ความรู้แก่บุคลากรภายในหน่วยงานผ่านเว็บไซต์ของกรมพินิจและคุ้มครองเด็ก และเยาวชน [www.djop.go.th](http://www.djop.go.th) ,จดหมายอิเล็กทรอนิกส์ (e-mail), ผ่านทาง Social Network, Group Line ของกรมพินิจและคุ้มครองเด็กและเยาวชน ระบบ e-Learning ของกรมพินิจและคุ้มครองเด็กและเยาวชน ที่ ได้จัดทำขึ้น

๕.๑๓.๒ จัดจ้างบริษัทที่มีบุคลากรซึ่งมีความรู้ความชำนาญทำหน้าที่ดูแล ให้คำปรึกษา ตรวจสอบและบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ทั้งทางด้าน Hardware และ Software โดยมีเจ้าหน้าที่ ผู้มีความรู้ ความชำนาญร่วมปฏิบัติงานกับ ศูนย์เทคโนโลยีสารสนเทศ เป็นประจำทุกวันทำการ

/๕.๑๔ การจัด...

**๕.๑๔ การจัดเตรียมอุปกรณ์ที่จำเป็น** เป็นการเตรียมความพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. หรือ ศูนย์เทคโนโลยีสารสนเทศ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

๕.๑๔.๑ แผ่น Boot Disk

๕.๑๔.๒ แผ่นติดตั้งระบบปฏิบัติการ ระบบเครือข่าย แผ่นติดตั้งระบบงานที่สำคัญ

๕.๑๔.๓ แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

๕.๑๔.๔ แผ่นโปรแกรม Anti-Virus

๕.๑๔.๕ แผ่น Driver อุปกรณ์ต่างๆ

๕.๑๔.๖ Hard Disk สำรอง

๕.๑๔.๗ ระบบสำรองไฟฟ้าฉุกเฉิน

๕.๑๔.๘ สำเนารายละเอียดการบันทึกค่าต่างๆ ในการติดตั้งอุปกรณ์ที่จำเป็น และอุปกรณ์อื่นที่เกี่ยวข้อง

## ๖. มาตรการความปลอดภัยด้วยรหัสผ่าน

การสร้างความปลอดภัยให้กับระบบสารสนเทศ มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศ ไม่สามารถเข้าถึงข้อมูล แก้ไข เปลี่ยนแปลงหรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มีใช้อำนาจหน้าที่เกี่ยวข้องของตนได้ โดย

๖.๑ กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีการลำดับชั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคลากรสามารถเข้าถึงแต่ละระดับ ดังนี้

๖.๑.๑ ผู้ดูแลระบบเครือข่ายหรือผู้ดูแลเครื่องแม่ข่ายจะต้องเป็นผู้ควบคุมรหัสผู้ใช้งานทั้งหมด โดยกำหนดรหัสผู้ใช้งานให้แก่บุคคลที่รับผิดชอบโดยตรงในแต่ละงานให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบเครือข่าย

๖.๑.๒ การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ FTP Server จะต้องระบุถึง IP Address ของผู้ใช้งาน และเพิ่มข้อมูลที่ต้องการเข้าถึง

๖.๑.๓ การกำหนดสิทธิให้แก่ผู้ใช้งานสำหรับ Database Server จะต้องกำหนดแยกเป็นรายฐานข้อมูล

๖.๒ กำหนดระยะเวลาการใช้งานระบบสารสนเทศของผู้ใช้งาน โดยผู้ใช้งานจะไม่สามารถใช้งานระบบสารสนเทศได้เมื่อพ้นระยะเวลาที่กำหนดไว้

๖.๓ การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๘ ตัวอักษร และควรใช้ตัวเลขผสมอักขระพิเศษประกอบ และสำหรับผู้ใช้งานระบบสารสนเทศควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๓ เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

/๗. ข้อปฏิบัติ...



## ๗. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

### ๗.๑ กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย ให้ดำเนินการดังนี้

๗.๑.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๗.๑.๒ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการและประสิทธิภาพของเครื่องสำรองไฟฟ้า

๗.๑.๓ ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๗.๑.๔ รับผิดชอบอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายไปไว้ในที่ปลอดภัย

๗.๑.๕ ประสานขอความช่วยเหลือให้กับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบ เครือข่ายโดยเร็วที่สุด

๗.๑.๖ กรณีที่อุปกรณ์ด้าน Hardware เสีย ให้จัดหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (Maintenance) นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗.๑.๗ ผู้ดูแลระบบต้องรีบแจ้งให้ ผอ.ศูนย์เทคโนโลยีสารสนเทศ และ ผอ.ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. รับทราบถึงปัญหาโดยเร็ว

### ๗.๒ กรณีเครื่องลูกข่าย ให้ดำเนินการดังนี้

๗.๒.๑ ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติให้ผู้ใช้งาน แจ้งเหตุขึ้นให้ ศูนย์เทคโนโลยีสารสนเทศ รับทราบ หรือกรณีมีเหตุอันทำให้ ศูนย์เทคโนโลยีสารสนเทศ ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๗.๒.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการถอดสายเชื่อมต่อระบบเครือข่าย (LAN) ออกจากเครื่องนั้นโดยเร็ว

๗.๒.๓ ในกรณีที่เกรงว่าเหตุที่จะเกิดเป็นอันตรายต่อหน่วยงานภายในอาคารที่ตั้งของเครื่องคอมพิวเตอร์ที่พบความขัดข้อง ให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด และปฏิบัติตามแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ (IT Contingency Plan)

๗.๒.๔ กรณีที่อุปกรณ์เสีย เช่น Main Board, Hard disk, ระบบปฏิบัติการและระบบเครือข่าย ให้รับหา อุปกรณ์สำรองหรือแจ้งให้บริษัทผู้รับจ้างการบำรุงรักษา (Maintenance) เพื่อนำอุปกรณ์มาเปลี่ยนโดยเร็ว ที่สุดและทำการ Recovery เพื่อนำข้อมูลเดิมกลับมาใช้โดยเร็ว

๗.๒.๕ ให้ผู้ดูแลระบบแจ้งเหตุขัดข้องนั้น ให้ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ หรือ ผอ. ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. รับทราบโดยเร็วที่สุด

### ๗.๓ กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

๗.๓.๑ ผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์ เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๗.๓.๒ ทำการ Scan Virus และฆ่าไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมด้านไวรัสที่มีอยู่ในเครื่อง

/๗.๓.๓ แจ้ง...



๗.๓.๓ แจ้งศูนย์เทคโนโลยีสารสนเทศ เพื่อตรวจสอบให้ละเอียดอีกครั้ง

#### ๘. หลักปฏิบัติในการป้องกันอัคคีภัย

เพื่อป้องกันมิให้เกิดอัคคีภัยภายในอาคารกระทรวงยุติธรรมและบุคลากรสามารถปฏิบัติตนได้อย่างถูกต้องเมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติของบุคลากรภายในกรมพินิจและคุ้มครองเด็กและเยาวชน ดังนี้

๘.๑ ไม่กระทำการใด ๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคารกระทรวงยุติธรรม

๘.๒ ควรศึกษาเรื่องตำแหน่งเส้นทางหนีไฟออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัย จากเพลิงไหม้และการหนีไฟอย่างละเอียด

๘.๓ ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉินไม่ให้ปิดตายหรือมีสิ่งกีดขวางและสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉินทั้งสองทางเพื่อให้สามารถไปถึงทางหนีไฟได้ถึงแม้จะมีมืดและมีควันปกคลุม

๘.๔ เมื่อเกิดเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพื่อเปิดสัญญาณเตือนเพลิงไหม้ จากนั้นหนีออกจากอาคารแล้วรีบโทรศัพท์แจ้งเจ้าหน้าที่รักษาความปลอดภัย (รปภ.) โทร ๐ ๒๕๑๕ ๔๐๓๙ ทันที

๘.๕ ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันทีและให้รีบแจ้ง ผอ.ศูนย์เทคโนโลยีสารสนเทศ และหน่วยงานในสังกัดกรมพินิจและคุ้มครองเด็กและเยาวชน ชั้น ๖ - ๗ เพื่อแจ้งหน่วยดับเพลิงต่อไป

๘.๖ ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตูก่อนหากประตูมีความเย็นอยู่ให้ค่อย ๆ ปิดประตูแล้วหนีไปทางหนีไฟฉุกเฉินที่อยู่ใกล้ที่สุด

๘.๗ ถ้าเพลิงไหม้อยู่บริเวณใกล้ๆ ประตูจะมีความร้อน ห้ามเปิดประตูเด็ดขาดให้รีบโทรศัพท์เรียก เจ้าหน้าที่รักษาความปลอดภัยและแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารที่ถูกเพลิงไหม้ หาผ้าเช็ดตัวเปียก ๆ ปิดทางเข้าของควัน ปิดพัดลมและเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๘.๘ ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

#### ๙. การกำหนดผู้รับผิดชอบ หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

๙.๑ ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามกำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ ได้แก่

๙.๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) แผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๙.๑.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๙.๒ ระดับปฏิบัติ รับผิดชอบในการกำกับดูแลการปฏิบัติงาน ศึกษา ทบทวนวางแผนติดตามการบริหาร ความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ได้แก่

๙.๒.๑ ผู้ดูแลระบบ คือ ฝ่ายเทคโนโลยีสารสนเทศเครือข่ายและคอมพิวเตอร์และฝ่ายพัฒนาระบบฐานข้อมูล

๙.๒.๒ กลุ่มงานสนับสนุนอื่น ประกอบด้วย

๙.๒.๒.๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม

๙.๒.๒.๒ บุคลากรอื่นตามสัญญาจ้างที่ร่วมทำงานกับศูนย์เทคโนโลยีสารสนเทศ

/บุคลากร...





บุคลากรที่ดูแลรับผิดชอบระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน  
ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการ  
ด้วยวิธีทางอิเล็กทรอนิกส์ หรือไม่สามารถเข้ามาให้บริการภายในอาคารกระทรวงยุติธรรม

| ลำดับ                                                                                         | ชื่อ - สกุล                   | ตำแหน่ง                                                                                            | เบอร์ที่ทำงาน | มือถือ       | e-mail                        |
|-----------------------------------------------------------------------------------------------|-------------------------------|----------------------------------------------------------------------------------------------------|---------------|--------------|-------------------------------|
| <b>ผู้บริหารสูงสุด (CEO: Chief Executive Officer)</b>                                         |                               |                                                                                                    |               |              |                               |
| ๑                                                                                             | พันตำรวจโท วรณพงษ์ ศรักษ์     | อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน                                                             | ๐ ๒๑๔๑ ๖๔๕๑   | ๐๖ ๕๙๒๙ ๐๐๘๑ | Wannapong.k@djop.mail.go.th   |
| <b>ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO: Chief Information Officer)</b>                    |                               |                                                                                                    |               |              |                               |
| ๑                                                                                             | นายโกมล พรหมเพ็ง              | รองอธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน                                                          | ๐ ๒๑๔๑ ๓๕๕๘   | ๐๘ ๑๙๐๙ ๑๑๓๗ | Komol.p@djop.mail.go.th       |
| <b>เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO: Data Protection Officer)</b>                      |                               |                                                                                                    |               |              |                               |
| ๑                                                                                             | นายโกมล พรหมเพ็ง              | รองอธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน                                                          | ๐ ๒๑๔๑ ๓๕๕๘   | ๐๘ ๑๙๐๙ ๑๑๓๗ | Komol.p@djop.mail.go.th       |
| <b>ศูนย์ข้อมูลและพัฒนาระบบเทคโนโลยีสารสนเทศ</b>                                               |                               |                                                                                                    |               |              |                               |
| ๑                                                                                             | นายธีรเดช ปรียานนท์           | นักวิชาการอบรมและฝึกวิชาชีพ<br>ชำนาญการ รักษาการใน<br>ตำแหน่งผู้อำนวยการศูนย์<br>เทคโนโลยีสารสนเทศ | ๐ ๒๑๔๑ ๓๕๕๕   | ๐๘ ๙๙๖๘ ๔๑๖๒ | Theeradet.p@djop.mail.go.th   |
| ๒                                                                                             | นายจิตรพล อินกุนา             | นักวิชาการคอมพิวเตอร์<br>ปฏิบัติการ                                                                | ๐ ๒๑๔๑ ๓๕๕๕   | ๐๘ ๙๖๖๔ ๖๙๙๓ | chittrapol@djop.mail.go.th    |
| ๓                                                                                             | นางสาวศิริกัญญา วัฒนวงศ์      | นักวิชาการสถิติปฏิบัติการ                                                                          | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๙ ๘๙๑๒ ๑๕๖๒ | sirinya.w@djop.mail.go.th     |
| ๔                                                                                             | นายธวัชชัย อัมฤทธิ์           | นักวิชาการคอมพิวเตอร์                                                                              | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๘ ๓๐๐๖ ๒๙๕๕ | Tawatchai.a@djop.mail.go.th   |
| ๕                                                                                             | นายอนนท์ ธรรมพรหม             | นักวิชาการคอมพิวเตอร์                                                                              | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๙ ๕๐๑๐ ๔๐๖๑ | Anon.t@djop.mail.go.th        |
| ๖                                                                                             | นางสาวศรดา ทิพย์แสง           | นักวิชาการคอมพิวเตอร์                                                                              | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๘ ๕๑๕๑ ๔๖๖๕ | Saruda.t@djop.mail.go.th      |
| ๗                                                                                             | นายประดับ วาหมงคล             | นักวิชาการคอมพิวเตอร์                                                                              | ๐ ๒๑๔๑ ๓๕๕๔   | ๐๘ ๔๗๖๐ ๖๑๑๘ | pradap.va@djop.mail.go.th     |
| ๘                                                                                             | นายวสพล รุ่งโรจน์วรกุล        | นักวิชาการคอมพิวเตอร์                                                                              | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๘ ๕๗๗๓ ๘๐๐๔ | wasapon@djop.mail.go.th       |
| ๙                                                                                             | นางสาวอรัญพร ต่อพันธ์         | นักวิชาการคอมพิวเตอร์                                                                              | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๙ ๘๑๕๕ ๕๐๖๘ | aratchaporn.t@djop.mail.go.th |
| ๑๐                                                                                            | ว่าที่ร้อยตรีชัชฎิเดช เดชผดุง | นักวิชาการคอมพิวเตอร์                                                                              | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๘ ๙๐๗๓ ๔๔๒๑ | kasidas.d@djop.mail.go.th     |
| ๑๑                                                                                            | นางสาวสวลักษณ์ ช่วยชู         | นักวิเคราะห์นโยบายและแผน                                                                           | ๐ ๒๑๔๑ ๓๕๕๖   | ๐๙ ๓๓๐๔ ๗๑๕๗ | sawarak.c@djop.mail.go.th     |
| <b>บริษัท บลูซิสเต็ม เทคโนโลยี จำกัด (จนท. MA ประจำกรมพินิจและคุ้มครองเด็กและเยาวชน)</b>      |                               |                                                                                                    |               |              |                               |
| ๑                                                                                             | นายประสิทธิ์ ปทุมสุติ         | เจ้าหน้าที่ MA                                                                                     | ๐ ๒๒๔๖ ๒๕๕๐   | ๐๙ ๘๒๔๘ ๔๕๕๕ | Prasit.bst@gmail.com          |
| ๒                                                                                             | นายโสภณ เพชรนิล               | เจ้าหน้าที่ MA                                                                                     | ๐ ๒๒๔๖ ๒๕๕๐   | ๐๙ ๒๕๔๕ ๙๗๔๕ | Soponp.bst@gmail.com          |
| <b>บริษัท Jasminw Internation Public (จนท. Network ประจำกรมพินิจและคุ้มครองเด็กและเยาวชน)</b> |                               |                                                                                                    |               |              |                               |
| ๓                                                                                             | นายณัฐวุฒิ มงคล               | เจ้าหน้าที่ Network                                                                                | ๐ ๒๑๐๐ ๓๗๐๐   | ๐๖ ๒๓๑๓ ๓๖๖๓ | nattwut.mo@jasmine.com        |

#### ๑๐. แผนการทำให้ระบบคอมพิวเตอร์กลับสู่สภาพปกติ

การกู้คืนข้อมูลเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการดังนี้

/๑๐.๑ จัดทำ...



๑๐.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทนและเปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๑๐.๒ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียให้แล้วเสร็จภายใน ๔๘ ชั่วโมง

๑๐.๓ นำอุปกรณ์ Backup Storage, Hard disk ที่จัดเก็บข้อมูลที่สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ ทีมกู้ระบบ (เจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ., เจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศ และบริษัทผู้รับจ้างการบำรุงรักษาระบบสารสนเทศ) ร่วมกันกู้ระบบ กลับมาโดยเร็ว ภายใน ๔๘ ชั่วโมง

๑๐.๔ ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่รวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน จึงมีแผนจัดทำสำรองข้อมูลเพื่อนำไปไว้อีกที่หนึ่งเพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ

#### ๑๑. การติดตามและรายงานผล

เพื่อให้เป็นระบบบริหารความเสี่ยงที่สมบูรณ์จำเป็นจะต้องติดตามผลหลังดำเนินการตามแผน และทำการสอบทานว่าแผนจัดการความเสี่ยงได้มีประสิทธิภาพดีให้คงดำเนินการต่อไปหรือแผนใดควรปรับเปลี่ยน โดยอาจกำหนดข้อมูลที่ต้องติดตาม จัดทำ Check List และกำหนดความถี่เพื่อสอบทานรายวัน รายเดือน ทุก ๓ เดือน หรือทุกปี เป็นต้น ทั้งนี้ขึ้นอยู่กับสภาพปัญหาที่เกิดขึ้น นอกจากนี้ยังได้กำหนดให้มีการประเมินและทบทวนแผนความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง เพื่อดูว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้วหรือมีความเสี่ยงใหม่เพิ่มขึ้นมาอีกหรือไม่ โดยอาจกำหนดเป็นแผนดำเนินงานรวมทั้งปี และต้องกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบทำการรายงานผลการดำเนินการหรือการตรวจสอบให้ ผอ.ศูนย์เทคโนโลยีสารสนเทศทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้

#### แผนการจัดทำระบบบริหารความเสี่ยง

| ขั้นตอนการดำเนินงาน            | ปี พ.ศ. ๒๕๖๕ |            |            |            |            |             |             |            |             |            |            |            |
|--------------------------------|--------------|------------|------------|------------|------------|-------------|-------------|------------|-------------|------------|------------|------------|
|                                | ต.ค.<br>๖๕   | พ.ย.<br>๖๕ | ธ.ค.<br>๖๕ | ม.ค.<br>๖๕ | ก.พ.<br>๖๕ | มี.ค.<br>๖๕ | เม.ย.<br>๖๕ | พ.ค.<br>๖๕ | มิ.ย.<br>๖๕ | ก.ค.<br>๖๕ | ส.ค.<br>๖๕ | ก.ย.<br>๖๕ |
| กำหนดวัตถุประสงค์              | →            |            |            |            |            |             |             |            |             |            |            |            |
| ระบุความเสี่ยง                 | →            | →          |            |            |            |             |             |            |             |            |            |            |
| ประเมินความเสี่ยง (ครั้งที่ ๑) |              |            |            | →          |            |             |             |            |             |            |            |            |
| ดำเนินการตามแผน                |              |            |            |            | →          |             |             |            |             |            |            |            |
| รายงานผลการดำเนินงาน           |              |            |            |            |            | →           |             |            |             |            |            |            |
| ประเมินความเสี่ยง (ครั้งที่ ๒) |              |            |            |            |            |             | →           |            |             |            |            |            |
| ทบทวนและปรับเปลี่ยนแผน         |              |            |            |            |            |             |             |            | →           | →          | →          |            |

ทั้งนี้ การจัดทำระบบบริหารความเสี่ยงจะต้องกระทำอย่างต่อเนื่องและสม่ำเสมอ มีการตรวจสอบและติดตามเป็นระยะๆ จึงจะเกิดประโยชน์อย่างแท้จริง

/แบบฟอร์ม...

## แบบฟอร์มติดตามความเสี่ยง

| ประเด็น<br>ความเสี่ยง | กิจกรรม/แนวทาง<br>การจัดการ<br>ความเสี่ยง | ระดับความเสี่ยง |               |                    | ผลสำเร็จของ<br>การจัดการ<br>ความเสี่ยง | ระยะเวลา<br>การ<br>ดำเนินการ | งบประมาณ<br>ที่ใช้ | ข้อเสนอแนะ<br>การแก้ไข |
|-----------------------|-------------------------------------------|-----------------|---------------|--------------------|----------------------------------------|------------------------------|--------------------|------------------------|
|                       |                                           | ผลกระทบ         | โอกาส<br>เกิด | โอกาส x<br>ผลกระทบ |                                        |                              |                    |                        |
|                       |                                           |                 |               |                    |                                        |                              |                    |                        |
|                       |                                           |                 |               |                    |                                        |                              |                    |                        |

## แผนการควบคุมการเข้าถึงระบบเครือข่าย

จากการติดตามตรวจสอบความเสี่ยงในระบบสารสนเทศกรมพินิจและคุ้มครองเด็กและเยาวชน พบว่า ความเสี่ยง ที่อาจเป็นอันตรายต่อระบบเครือข่ายคอมพิวเตอร์ซึ่งเป็นองค์ประกอบหลักในระบบสารสนเทศ คือ ปัญหาระบบเครือข่ายล่มเหลว เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของกรมพินิจและคุ้มครองเด็กและเยาวชน หรือการทำงานหยุดชะงักและทำให้สามารถตรวจสอบ ติดตาม การพิสูจน์ตัวบุคคลที่ใช้งานระบบเทคโนโลยีสารสนเทศ ของกรมพินิจและคุ้มครองเด็กและเยาวชนได้อย่างถูกต้อง จึงได้จัดทำ แผนการควบคุมปัญหาไว้ดังนี้

## ๑. การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย (Access Control)

๑.๑ สถานที่ตั้งห้อง Data Center ซึ่งมีการเก็บข้อมูลสารสนเทศที่สำคัญต้องมีการควบคุม การเข้า-ออก ที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น และ ระบบควบคุมประตูปิดเปิดอัตโนมัติต้องเป็นระบบที่ได้มาตรฐาน

๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิในการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้ งาน ของผู้ใช้งานและสอดคล้องกับหน้าที่ความรับผิดชอบ รวมทั้งให้มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๑.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น (Administrator) ที่สามารถแก้ไขเปลี่ยนแปลง สิทธิ การเข้าถึงข้อมูลและระบบข้อมูลสารสนเทศได้

๑.๔ ผู้ดูแลระบบ จัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเครือข่ายกรมพินิจ และคุ้มครองเด็กและเยาวชน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญอย่างสม่ำเสมอ

๑.๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบต่าง ๆ และการผ่านเข้าออก สถานที่ตั้งระบบเครือข่ายทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมี ปัญหาเกิดขึ้น

๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) วัตถุประสงค์ เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของกรมพินิจและคุ้มครอง เด็กและเยาวชน โดยจัดให้มีการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสม รวมถึงได้มีการ ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะต้องผ่านการพิสูจน์ตัวตน (Authentication) ก่อนใช้ งานระบบเสมอ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย โดยมีแนวปฏิบัติดังนี้

๒.๑ ผู้ใช้งาน (User) ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมพินิจและคุ้มครองเด็ก และเยาวชนจะต้องทำบันทึกเสนอหัวหน้าหน่วยงานของผู้ใช้งาน เพื่อขอความเห็นชอบและพิจารณาอนุญาต เป็นลายลักษณ์อักษร และจัดส่งบันทึกความประสงค์การใช้งานดังกล่าวไปยัง ศูนย์เทคโนโลยีสารสนเทศ ต่อไป

/๒.๒ ผู้ดูแล...



๒.๒ ผู้ดูแลระบบ (Admin) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมก่อนเข้าใช้งานระบบ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้การกำหนดสิทธิ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สายไว้เป็นหลักฐาน

๒.๔ กำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณ ของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอก อาคารกระทรวงยุติธรรมหรือบริเวณขอบเขตที่ควบคุมได้ (ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ดำเนินการ)

๒.๕ ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหล ออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น (ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ดำเนินการ)

๒.๖ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน (ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ดำเนินการ)

๒.๗ ผู้ดูแลระบบควรเปลี่ยนค่า ชื่อ login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรเลือกใช้ชื่อ login และรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้ โดยง่าย (ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ดำเนินการ)

๒.๘ ต้องกำหนดค่าใช้ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น (ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ดำเนินการ)

๒.๙ ควรมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สาย กับเครือข่ายภายใน

๒.๑๐ ควรใช้ Software หรือ Hardware ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย อย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

๓. การบริหารจัดการการเข้าถึงเครือข่าย มีการออกแบบระบบเครือข่าย ซึ่งจำเป็นต้องมีการป้องกัน และมีการจัดแบ่งระบบเครือข่ายเป็นโซน เพื่อให้เกิดความสะดวกในการควบคุมและจัดการโดยเฉพาะการติดตั้ง Firewall ทั้งนี้เพื่อให้เกิดความปลอดภัย โดยแบ่งตาม Zoning ของ Network (ศูนย์เทคโนโลยีสารสนเทศ สป.ยธ. ดำเนินการ) คือ

๓.๑ Internal zone หมายถึง ระบบเครือข่ายภายในองค์กร ซึ่งถือเป็น zone ที่มีความปลอดภัย และน่าเชื่อถือสูงสุด

๓.๒ External zone หมายถึง ระบบเครือข่ายภายนอก ซึ่งถือเป็น zone ที่มีความปลอดภัยต่ำมาก ดังนั้น จึงจำเป็นต้องมีการควบคุมในเรื่องการสื่อสารที่ต้องติดต่อกับเครือข่ายภายนอกให้มีประสิทธิภาพ

๓.๓ Demilitarized Zone (DMZ) เป็น zone พิเศษที่จะติดต่อโดยตรงทั้ง Internal และ External เช่น Mail Server, Web Server เป็นต้น

/๓.๔ จำกัด..



๓.๔ จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๓.๕ ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๓.๖ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นได้

๓.๗ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้ง บุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๓.๘ ระบบเครือข่ายทั้งหมดของกรมพินิจและคุ้มครองเด็กและเยาวชน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอก องค์กร ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall และ IPS หรือฮาร์ดแวร์อื่น รวมทั้งต้องมีความสามารถในการตรวจจับ Malware ด้วย

๓.๙ การเข้าสู่ระบบงานเครือข่ายภายในกรมพินิจและคุ้มครองเด็กและเยาวชน โดยผ่านทางอินเทอร์เน็ตจำเป็นต้อง มีการ login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๓.๑๐ IP Address ระบบเครือข่ายภายในกรมพินิจและคุ้มครองเด็กและเยาวชนจำเป็นต้องมีการป้องกันมิให้หน่วยงาน ภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อป้องกันมิให้บุคคลภายนอกล่วงรู้ข้อมูลเกี่ยวกับโครงสร้างของ ระบบเครือข่ายของกรมพินิจและคุ้มครองเด็กและเยาวชนได้โดยง่าย

๓.๑๑ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๑๒ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุญาตจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๑๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดย ศูนย์เทคโนโลยีสารสนเทศ เท่านั้น

#### ๔. การบริหารจัดการระบบคอมพิวเตอร์

๔.๑ กำหนดกลุ่มงานหรือบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการ กำหนด แก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๔.๒ มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีพบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานต่อ หน.ศูนย์เทคโนโลยีสารสนเทศ ทันที

๔.๓ เปิดให้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่ จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๔.๔ ติดตั้งตัว Update ระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างเหมาะสม เช่น web server เป็นต้น

/๔.๕ มีการ...

๔.๕ มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากแก้ไขหรือบำรุงรักษา

๔.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศ เท่านั้น

#### ๕. การบริหารจัดการการบันทึกและตรวจสอบ

๕.๑ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึก การปฏิบัติงาน ของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออก ระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall log เป็นต้น เพื่อประโยชน์ ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๕.๒ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๕.๓ มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึก เหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๕.๔ มีการเก็บบันทึกการถ่ายโอนข้อมูลของกรมพินิจฯ โดยสามารถระบุถึงชื่อผู้ใช้งาน และ อุปกรณ์ที่ใช้ในการจัดเก็บ

๖. การควบคุมการใช้งานระบบจากภายนอกกรมพินิจและคุ้มครองเด็กและเยาวชน ต้องกำหนดให้ มีการควบคุมการใช้งานระบบ เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก ดังนี้

๖.๑ การเข้าสู่ระบบระยะไกล (Remote access) เข้าสู่ระบบเครือข่ายของกรมพินิจและ คุ้มครองเด็กและเยาวชนต้องควบคุม บุคคลที่จะเข้าสู่ระบบของหน่วยงานจากระยะไกล โดยกำหนดมาตรการ การรักษาความปลอดภัยที่เพิ่มขึ้นจาก มาตรฐานการเข้าสู่ระบบภายใน

๖.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับการ อนุมัติจาก ผอ.ศูนย์เทคโนโลยีสารสนเทศ ก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และ ผู้ใช้งานต้อง ปฏิบัติตามข้อกำหนดของ ศูนย์เทคโนโลยีสารสนเทศ ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๖.๓ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความ จำเป็น ในการดำเนินงานกับองค์กรอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๖.๔ มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๖.๕ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๗. การพิสูจน์ตัวตน (Authentication) ถือเป็นกระบวนการที่มีความสำคัญและเป็นการยืนยัน ความถูกต้อง ตัวบุคคล (Identity) ของผู้ใช้งาน ซึ่งการใช้งานระบบเครือข่ายของกรมพินิจและคุ้มครองเด็กและเยาวชน นั้น ผู้ใช้งานทุกคน จะต้องผ่านการพิสูจน์ตัวตนจากระบบ Authentication โดยวิธีการแสดงชื่อผู้ใช้งาน (Username) และใส่ รหัสผ่าน (Password) ก่อนการใช้งานในระบบเครือข่ายทุกครั้ง

/๑๒. ผู้รับ...



## ๘. ผู้รับผิดชอบการจัดทำแผน

## ศูนย์เทคโนโลยีสารสนเทศ

- |                                    |                                                                                           |
|------------------------------------|-------------------------------------------------------------------------------------------|
| ๑) นายธีรเดช ปรียานนท์             | นักวิชาการอบรมและฝึกวิชาชีพชำนาญการ<br>รักษาการในตำแหน่งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ |
| ๒) นายจิตรพล อินกุนา               | นักวิชาการคอมพิวเตอร์ปฏิบัติการ                                                           |
| ๓) นางสาวศิริกัญญา วัฒนวงศ์        | นักวิชาการสถิติปฏิบัติการ                                                                 |
| ๔) นายธวัชชัย อัมฤทธิ              | นักวิชาการคอมพิวเตอร์                                                                     |
| ๕) นายอนนท์ ธรรมพรม                | นักวิชาการคอมพิวเตอร์                                                                     |
| ๖) นางสาวศรดา ทิพย์แสง             | นักวิชาการคอมพิวเตอร์                                                                     |
| ๗) นายประดับ วาหมงคล               | นักวิชาการคอมพิวเตอร์                                                                     |
| ๘) นายวสพล รุ่งโรจน์วรกุล          | นักวิชาการคอมพิวเตอร์                                                                     |
| ๙) นางสาวอริษพร ต่อพันธ์           | นักวิชาการคอมพิวเตอร์                                                                     |
| ๑๐) ว่าที่ร้อยตรี กษิต์เดช ผดุงเดช | นักวิชาการคอมพิวเตอร์                                                                     |
| ๑๑) นางสาวสวลักษณ์ ช่วยชู          | นักวิเคราะห์นโยบายและแผน                                                                  |

แผนรองรับสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของกรมพินิจและคุ้มครองเด็กและเยาวชน ฉบับนี้ได้ผ่านการพิจารณาให้ความเห็นชอบจากคณะกรรมการเทคโนโลยีสารสนเทศ กรมพินิจและคุ้มครองเด็กและเยาวชนแล้ว เพื่อให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและบุคลากรภายในกรมพินิจและคุ้มครองเด็กและเยาวชน ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ



ผู้เสนอ

(นายธีรเดช ปรียานนท์)

นักวิชาการอบรมและฝึกวิชาชีพชำนาญการ  
รักษาการในตำแหน่งผู้อำนวยการเทคโนโลยีสารสนเทศ



ผู้เห็นชอบ

(นายโกมล พรหมเพ็ง)

รองอธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน  
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

พันตำรวจโท



ผู้อนุมัติ

(วรรณพงษ์ คชรักษ์)

อธิบดีกรมพินิจและคุ้มครองเด็กและเยาวชน