



แผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ
(Data Backup and IT Disaster Recovery Plan)

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ



บันทึกข้อความ

ทสส.ทอ.
เลขรับ ๕๕๑๑
วันที่ ๒๗ ก.ย. ๖๔
เวลา ๑๕๓๕.

ส่วนราชการ... คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ ทสส.ทอ. (เลขานุการฯ โทร.๒-๐๖๕๐)
ที่ ๖/๖๔ วันที่ ๒๗ ก.ย.๖๔

เรื่อง ขออนุมัติใช้แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทสส.ทอ. พ.ศ.๒๕๖๔
และแผนที่เกี่ยวข้อง

เรียน จก.ทสส.ทอ.

๑. ตามระเบียบ ทอ.ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ กำหนดให้ คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ มีหน้าที่จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วย และจัดทำแผนที่เกี่ยวข้องตามความเหมาะสม นั้น

๒. คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.ได้ดำเนินการทบทวนและปรับปรุงแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ.ให้ครอบคลุมประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบัน และได้จัดทำแผนที่เกี่ยวข้องเรียบร้อยแล้ว ดังนี้

๒.๑ แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทสส.ทอ. พ.ศ.๒๕๖๔

๒.๒ แผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ

๒.๓ แผนเผชิญเหตุจากภัยพิบัติระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓. เพื่อให้การดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.เป็นไปด้วยความเรียบร้อย เห็นสมควรอนุมัติใช้แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทสส.ทอ. พ.ศ.๒๕๖๔ และแผนที่เกี่ยวข้อง ตามข้อ ๒ รายละเอียดตามแนบ

จึงเรียนมาเพื่ออนุมัติตามข้อ ๓

พล.อ.ต.

ผอ.สบค.ทสส.ทอ.

ประธาน คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.

- อนุมัติตามข้อ ๓

• พล.อ.ท.

จก.ทสส.ทอ.

๒๗ ก.ย.๖๔



สารบัญ

	หน้า
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. ขอบเขตการดำเนินงาน	๑
๔. การสำรองข้อมูลระบบสารสนเทศ	๑
๕. ขั้นตอนการสำรองข้อมูล	๓
๖. การจัดเตรียมอุปกรณ์ที่จำเป็น	๓
๗. การฟื้นฟูระบบสารสนเทศ	๓
๘. ขั้นตอนการฟื้นฟูระบบสารสนเทศ	๓
๙. ระยะเวลาในการกู้คืนข้อมูล	๔
๑๐. การกำหนดผู้รับผิดชอบ	๔
๑๑. ผังกระบวนการฟื้นฟูระบบสารสนเทศ	
๑๑.๑ กรณีกระแสไฟฟ้าขัดข้อง	๕
๑๑.๒ กรณีมีการปรับปรุงแก้ไข เคลื่อนย้าย หรือเปลี่ยนแปลงระบบ	๖
๑๑.๓ กรณีเครื่องคอมพิวเตอร์แม่ข่ายโดนภัยคุกคามจากมัลแวร์	๗
๑๑.๔ กรณีอุปกรณ์ (Hardware) เกิดความเสียหาย	๘
๑๑.๕ กรณีซอฟต์แวร์ (Software) เกิดความเสียหาย	๘
๑๒. การติดตามและรายงานผล	๑๐
บรรณานุกรม	๑๑



แผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ (Data Backup and IT Disaster Recovery Plan)

๑. หลักการและเหตุผล

ในปัจจุบัน ทสส.ทอ.ได้นำระบบสารสนเทศมาช่วยสนับสนุนการดำเนินงานของหน่วยงานให้เป็นอย่างดีและมีประสิทธิภาพ ความเสี่ยงสำคัญที่อาจจะส่งผลกระทบต่อการทำงานคือระบบสารสนเทศหยุดชะงักซึ่งเกิดจากปัจจัยอันได้แก่ ปัญหาการเสื่อมสภาพของอุปกรณ์คอมพิวเตอร์ เกิดข้อขัดข้องของกระแสไฟฟ้า เกิดปัญหาภัยคุกคามทางไซเบอร์ เกิดภัยธรรมชาติ เป็นต้น ซึ่งอาจสร้างความเสียหายหรือส่งผลกระทบต่อทำให้ระบบสารสนเทศหยุดชะงักได้ แผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ (Data Backup and IT Disaster Recovery Plan) ฉบับนี้ จัดทำขึ้นเพื่อให้ผู้ดูแลระบบสารสนเทศของ ทสส.ทอ. ซึ่งมีหน้าที่ดูแลงานทางด้านการสำรองข้อมูลและการกู้คืนข้อมูลเว็บไซต์ (Web Hosting) ของหน่วย นำไปเป็นกรอบแนวทางดำเนินการสำรองข้อมูลและฟื้นฟูระบบงานที่อยู่ในความรับผิดชอบ ลดความเสี่ยงจากสิ่งที่เกิดขึ้นกับข้อมูลในกรณีที่ฮาร์ดแวร์หรือซอฟต์แวร์เสียหาย คอมพิวเตอร์ถูกมัลแวร์คุกคามทำลายข้อมูล มีผู้ลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยไม่ตั้งใจ ทั้งนี้ เพื่อให้สามารถนำข้อมูลกลับมาใช้งานได้ใหม่ภายในระยะเวลาที่กำหนด เพื่อให้การดำเนินงานของหน่วยเป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ

๒. วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมด้านการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศของหน่วย
๒. เพื่อให้มีแผนนำไปปฏิบัติเมื่อเกิดข้อขัดข้องต่อระบบสารสนเทศของหน่วย
๓. เพื่อลดผลกระทบจากการหยุดชะงักในการให้บริการ
๔. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้ปฏิบัติงาน ในการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศของหน่วย

๓. ขอบเขตการดำเนินงาน

แผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ (Data Backup and IT Disaster Recovery Plan) ฉบับนี้มีผลบังคับใช้เพื่อให้ผู้ดูแลฐานข้อมูลและระบบงานในความรับผิดชอบของ ทสส.ทอ.ดำเนินการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศที่ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์แม่ข่ายของ ทสส.ทอ. และภายในเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่ติดตั้ง ณ ศูนย์ข้อมูลกองทัพอากาศ ที่มีสิทธิ์ในการบริหารจัดการเท่านั้น

๔. การสำรองข้อมูลระบบสารสนเทศ

- ๔.๑ ข้อมูลระบบสารสนเทศของ ทสส.ทอ.
 - ๔.๑.๑ ระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายของ ทสส.ทอ.
 - ๔.๑.๒ ระบบแจกจ่ายหมายเลขไอพี (DHCP)
 - ๔.๑.๓ ระบบพัฒนาและทดสอบโปรแกรม
- ๔.๒ ระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ณ ศูนย์ข้อมูลกองทัพอากาศ
 - ๔.๒.๑ เว็บไซต์ของ ทสส.ทอ.
 - ๔.๒.๒ ระบบเพื่อการบริหารงานของ ทสส.ทอ.
 - ๔.๒.๒.๑ ระบบรายงานสถานภาพอุปกรณ์ (Eict Report)
 - ๔.๒.๒.๒ ระบบติดตามงาน (Work Flow)
 - ๔.๒.๒.๓ ระบบประชุม (DICT Meeting)



- ๔.๒.๓ ระบบเพื่อการบริหารงานในศูนย์ปฏิบัติการกองทัพอากาศ
 - ๔.๒.๓.๑ ระบบบันทึกการปฏิบัติงาน (AFOC Staff)
 - ๔.๒.๓.๒ ระบบตรวจสอบการใช้งานระบบ (EM Report)
 - ๔.๒.๓.๓ ระบบติดตามงาน (T Ord)
- ๔.๒.๔ ระบบไปรษณีย์อิเล็กทรอนิกส์สำหรับศูนย์ปฏิบัติการกองทัพอากาศ (AFOC Mail)
- ๔.๓ ซอฟต์แวร์ระบบสารสนเทศของ ทสส.ทอ.
 - ๔.๓.๑ ระบบแจกจ่ายหมายเลขไอพี (DHCP) ประกอบด้วย
 - ๔.๓.๑.๑ ระบบปฏิบัติการ (OS) Windows Server 2016 64 bit
 - ๔.๓.๑.๒ ระบบบริหารจัดการหมายเลขไอพี (DHCP)
 - ๔.๓.๒ ระบบพัฒนาและทดสอบโปรแกรม ประกอบด้วย
 - ๔.๓.๒.๑ ระบบปฏิบัติการ (OS) Windows Server 2016 64 bit
 - ๔.๓.๒.๒ โปรแกรมบริหารจัดการเว็บไซต์ (Web -Server)
 - ๔.๓.๒.๓ โปรแกรมบริหารจัดการฐานข้อมูล MySQL
 - ๔.๓.๓ เว็บไซต์ของ ทสส.ทอ. ประกอบด้วย
 - ๔.๓.๓.๑ ระบบปฏิบัติการ Linux
 - ๔.๓.๓.๒ โปรแกรมบริหารจัดการเว็บไซต์ Joomla 3.7
 - ๔.๓.๓.๓ โปรแกรมบริหารจัดการฐานข้อมูล MySQL
 - ๔.๓.๔ ระบบเพื่อการบริหารงานของ ทสส.ทอ. ประกอบด้วย
 - ๔.๓.๔.๑ ระบบปฏิบัติการ (OS) Windows Server 2012 64 bit
 - ๔.๓.๔.๒ โปรแกรมบริหารจัดการเว็บไซต์ XAMPP
 - ๔.๓.๔.๓ โปรแกรมบริหารจัดการฐานข้อมูล phpMyAdmin
 - ๔.๓.๕ ระบบเพื่อการบริหารงานในศูนย์ปฏิบัติการกองทัพอากาศ ประกอบด้วย
 - ๔.๓.๕.๑ ระบบปฏิบัติการ (OS) Windows Server 2012 64 bit
 - ๔.๓.๕.๒ โปรแกรมบริหารจัดการเว็บไซต์ XAMPP
 - ๔.๓.๕.๓ โปรแกรมบริหารจัดการฐานข้อมูล phpMyAdmin
 - ๔.๓.๖ ระบบไปรษณีย์อิเล็กทรอนิกส์สำหรับศูนย์ปฏิบัติการกองทัพอากาศ ประกอบด้วย
 - ๔.๓.๖.๑ ระบบปฏิบัติการ (OS) Windows Server 2016 64 bit
 - ๔.๓.๖.๒ โปรแกรมบริหารจัดการบัญชีผู้ใช้ (Active Directory)
 - ๔.๓.๖.๓ โปรแกรมระบบไปรษณีย์อิเล็กทรอนิกส์ Microsoft Exchange 2016
- ๔.๔ สื่อการสำรองข้อมูล
 - ๔.๔.๑ พื้นที่จัดเก็บข้อมูลบนคอมพิวเตอร์แม่ข่าย
 - ๔.๔.๒ ฮาร์ดดิสก์แบบภายนอก (External Hard Disk)



๕. ขั้นตอนการสำรองข้อมูล

๕.๑ ระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายของ ทสส.ทอ. จะทำการสำรองข้อมูลทุกเดือน หรือเมื่อมีการปรับปรุงระบบ โดยใช้พื้นที่จัดเก็บบน External Hard Disk

๕.๒ ระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ณ ศูนย์ข้อมูลกองทัพอากาศ สำรองข้อมูลโปรแกรมที่ติดตั้งเก็บไว้ในพื้นที่จัดเก็บข้อมูลของผู้ดูแลระบบ และทำการสำรองข้อมูลทุกวันศุกร์ โดยใช้พื้นที่จัดเก็บบนเครื่องแม่ข่าย และ External Hard Disk

๖. การจัดเตรียมอุปกรณ์ที่จำเป็น

เพื่อเตรียมความพร้อมในการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ ควรมีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็น ดังนี้

- ๖.๑ แผ่น boot disk
- ๖.๒ แผ่นติดตั้งระบบปฏิบัติการ
- ๖.๓ แผ่นติดตั้งโปรแกรม หรือระบบงานที่สำคัญ
- ๖.๔ สื่อบันทึกการสำรองข้อมูลและระบบงานที่สำคัญ
- ๖.๕ แผ่นโปรแกรม antivirus/spyware
- ๖.๖ แผ่น driver อุปกรณ์ต่าง ๆ
- ๖.๗ เครื่องคอมพิวเตอร์สำรอง
- ๖.๘ อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๗. การฟื้นฟูระบบสารสนเทศ

๗.๑ สภาพปกติของระบบสารสนเทศ

โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับ การให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้คืนระบบให้กลับมาใช้งานได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการฟื้นฟูระบบสารสนเทศเป็นวิธีการที่ทำให้ระบบการทำงานของระบบสารสนเทศและระบบฐานข้อมูล กลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน

๗.๒ ลักษณะความล้มเหลว

ต่อไปนี้จะแสดงถึงความล้มเหลวของระบบงานสารสนเทศของ ทสส.ทอ. ที่จำเป็นต้องดำเนินการตามกระบวนการกู้คืนข้อมูลเพื่อให้สามารถใช้งานระบบงานฯ ได้ตามปกติ

๗.๒.๑ ระบบงานสารสนเทศของ ทสส.ทอ. ไม่สามารถให้บริการได้ เนื่องจากข้อขัดข้องหรือสาเหตุใดก็ตาม

๗.๒.๒ ระบบงานสารสนเทศของ ทสส.ทอ. มีการทำงานที่ผิดปกติ เนื่องจากข้อขัดข้องหรือสาเหตุใดก็ตาม และมีความจำเป็นต้องหยุดให้บริการเพื่อแก้ไขปัญหา

๘. ขั้นตอนการฟื้นฟูระบบสารสนเทศ

๘.๑ ระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายของ ทสส.ทอ. ไม่สามารถให้บริการได้ ให้ผู้ดูแลระบบทำการหาสาเหตุที่ระบบไม่สามารถให้บริการได้ เมื่อทราบถึงสาเหตุให้ทำการแก้ไขตามขั้นตอนที่กำหนดไว้ตามคู่มือ หากไม่สามารถดำเนินการแก้ไขได้ จำเป็นต้องนำข้อมูลที่เก็บสำรองไว้ มา Restore ข้อมูลเข้าสู่เครื่องคอมพิวเตอร์ที่จัดเตรียมไว้



๘.๒ ระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ณ ศูนย์ข้อมูลกองทัพอากาศ ไม่สามารถให้บริการได้ ให้ตรวจสอบสาเหตุข้อขัดข้องของการให้บริการและดำเนินการแก้ไขเบื้องต้น หากไม่สามารถแก้ไขได้ และมีความจำเป็นต้องนำข้อมูลที่สำรองไว้ นำมา Restore ข้อมูลเข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายเสมือนใหม่ โดยมีรายละเอียดดังนี้

๘.๒.๑ ประธานผู้ดูแลระบบบริหารจัดการเครื่องแม่ข่ายเสมือน ศูนย์ข้อมูลกองทัพอากาศ ทำการกู้คืนข้อมูลสถานะเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่ทำงานได้ปกติครั้งล่าสุดก่อน ตามด้วยการ Restore ข้อมูลของฐานข้อมูลของระบบที่ได้ทำการ Backup ไว้ครั้งล่าสุด

๘.๒.๒ ในกรณีที่ไม่สามารถกู้คืนสถานะเครื่องแม่ข่ายเสมือนครั้งล่าสุดได้ ให้ทำการติดตั้งระบบใหม่ และนำข้อมูลโปรแกรมของระบบงานที่ผู้ดูแลระบบจัดเก็บไว้ไปติดตั้ง ตามด้วยการ Restore ข้อมูลของฐานข้อมูลของระบบที่ได้ทำการ Backup ไว้ครั้งล่าสุด

๙. ระยะเวลาในการกู้คืนข้อมูล

๙.๑ ในกรณีระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายของ ทสส.ทอ. ไม่สามารถให้บริการได้ ระยะเวลาที่ใช้ตั้งแต่การเริ่มต้นกู้คืนข้อมูลจนกระทั่งระบบสารสนเทศสามารถให้บริการได้ตามปกติ นั้น ต้องอยู่ในเวลาไม่เกิน ๘ ชั่วโมง

๙.๒ ในกรณีระบบสารสนเทศภายในเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ณ ศูนย์ข้อมูลกองทัพอากาศ ไม่สามารถใช้งานได้ ระยะเวลาที่ใช้ตั้งแต่การเริ่มต้นกู้คืนข้อมูลจนกระทั่งระบบสารสนเทศสามารถกลับมาให้บริการได้ตามปกติ นั้น ต้องอยู่ในเวลาไม่เกิน ๓ ชั่วโมง

๑๐. การกำหนดผู้รับผิดชอบ

กำหนดผู้รับผิดชอบและมอบหมายหน้าที่ ดังนี้

๑๐.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑๐.๑.๑ ประธาน คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.

๑๐.๑.๒ ผู้อำนวยการ กทส.สนผ.ทสส.ทอ.

๑๐.๒ ระดับปฏิบัติ

รับผิดชอบดูแลบำรุงรักษา ระบบคอมพิวเตอร์ ระบบเครือข่ายและความปลอดภัยของฐานข้อมูล กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน และติดตามการปฏิบัติในการสำรองข้อมูล และฟื้นฟูระบบสารสนเทศ ได้แก่

๑๐.๒.๑ นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.

๑๐.๒.๒ หน.ผทส.กทส.สนผ.ทสส.ทอ.

๑๐.๒.๓ ผู้รับผิดชอบดูแลระบบสารสนเทศและฐานข้อมูลของ นขต.ทสส.ทอ.



๑๑. ผังกระบวนการฟื้นฟูระบบสารสนเทศ

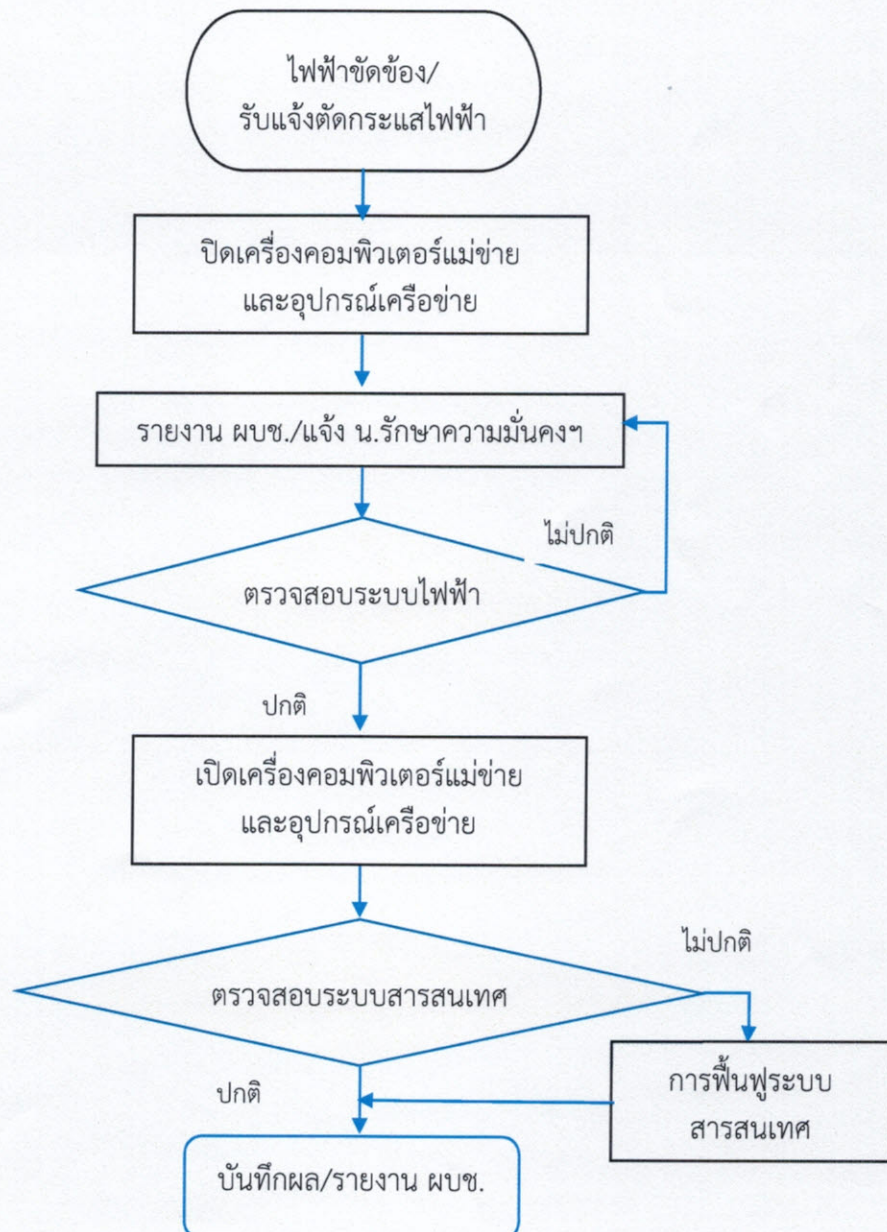
๑๑.๑ กรณีกระแสไฟฟ้าขัดข้อง

๑๑.๑.๑ เมื่อเกิดไฟฟ้าดับ/ไฟฟ้าทก หรือได้รับแจ้งการตัดกระแสไฟฟ้า ให้รีบปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายทั้งหมด เพื่อป้องกันการเกิดไฟกระชากทำให้อุปกรณ์เสียหาย

๑๑.๑.๒ เมื่อไฟฟ้ากลับมาใช้งานปกติ ให้เปิดใช้งานอุปกรณ์เครือข่าย และเครื่องแม่ข่ายทั้งหมดให้กลับมาทำงานตามปกติ

๑๑.๑.๓ ตรวจสอบข้อขัดข้อง ความเสียหายที่เกิดขึ้น หากมีข้อขัดข้องให้พิจารณาปฏิบัติตามแผนการฟื้นฟูระบบสารสนเทศต่อไป

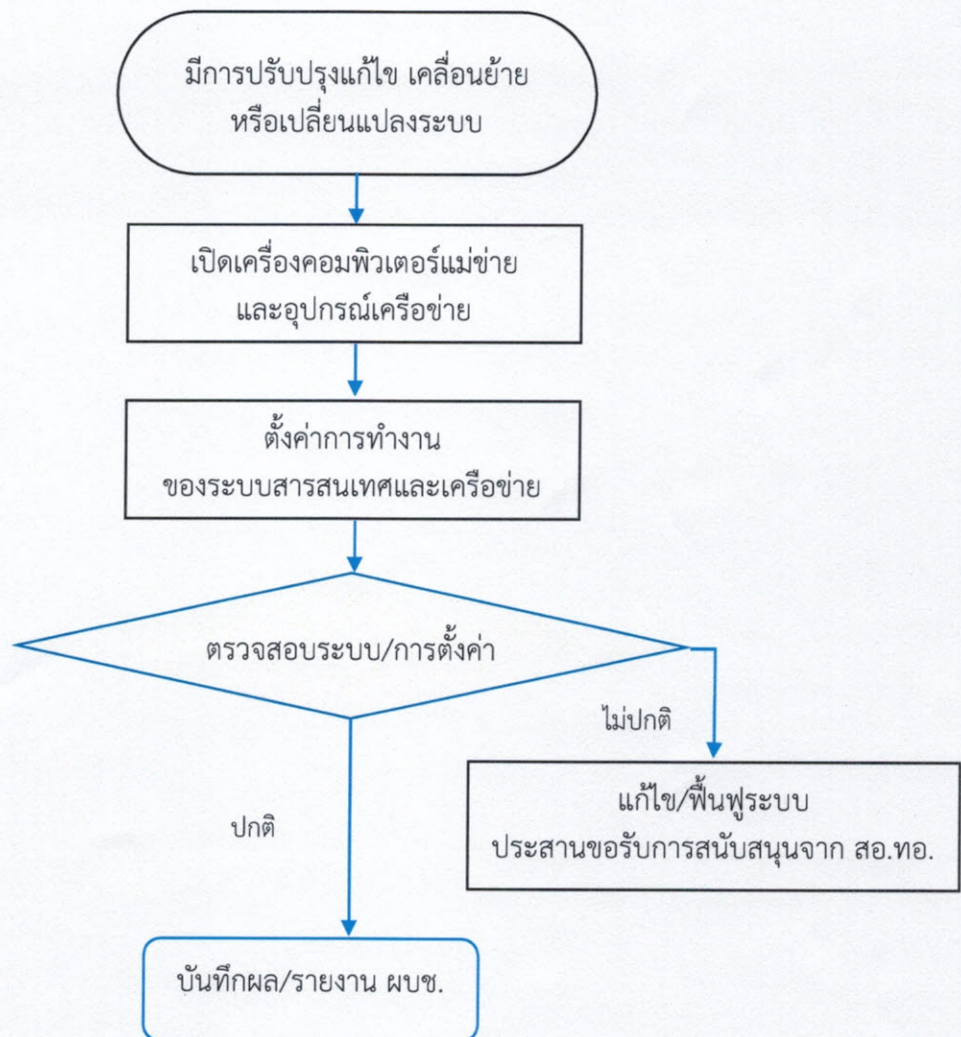
กระบวนการฟื้นฟูระบบสารสนเทศ กรณีกระแสไฟฟ้าขัดข้อง





- ๑๑.๒ กรณีมีการปรับปรุงแก้ไข เคลื่อนย้าย หรือเปลี่ยนแปลงระบบ
- ๑๑.๒.๑ ตรวจสอบการติดตั้ง หรือตั้งค่าการทำงานของอุปกรณ์เครือข่าย/ระบบสารสนเทศให้ถูกต้อง
- ๑๑.๒.๒ เปิดการทำงานของอุปกรณ์ และระบบสารสนเทศที่หยุดให้บริการ
- ๑๑.๒.๓ ตรวจสอบข้อขัดข้อง ความถูกต้องของการทำงานของอุปกรณ์ หากมีข้อขัดข้องให้ทำการตรวจสอบแก้ไข
- ๑๑.๒.๔ กรณีที่แก้ไขไม่ได้ให้ทำการกู้คืน (Restore) สถานะ/การตั้งค่าล่าสุดที่ระบบทำงานได้ปกติหรือติดต่อขอรับการสนับสนุนเจ้าหน้าที่จาก สอ.ทอ.ต่อไป

กระบวนการฟื้นฟูระบบสารสนเทศ กรณีการปรับปรุงแก้ไข เคลื่อนย้าย หรือเปลี่ยนแปลงระบบ





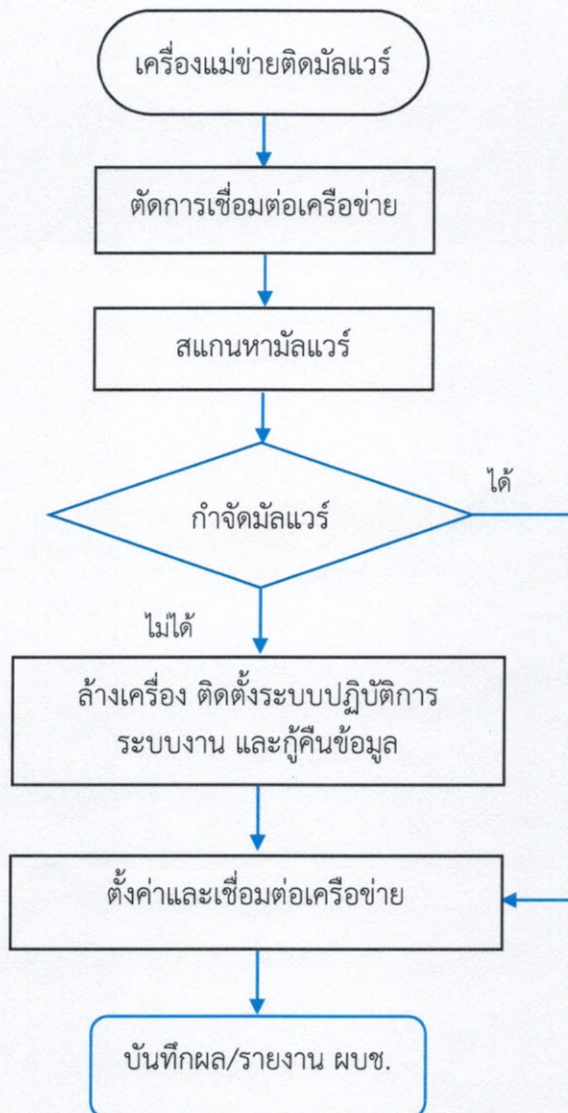
๑๑.๓ กรณีเครื่องคอมพิวเตอร์แม่ข่ายโดนภัยคุกคามจากมัลแวร์

๑๑.๓.๑ กรณีเกิดการขัดข้องเนื่องจากถูกมัลแวร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังอุปกรณ์อื่น ๆ ในระบบเครือข่าย ให้ทำการดึงสายสัญญาณเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว

๑๑.๓.๒ ทำการสแกน และกำจัดมัลแวร์โดยใช้ซอฟต์แวร์ป้องกันมัลแวร์

๑๑.๓.๓ หากไม่สามารถแก้ไขปัญหาด้วยซอฟต์แวร์ป้องกันมัลแวร์ได้ ให้ดำเนินการล้างเครื่องคอมพิวเตอร์ แล้วติดตั้งระบบปฏิบัติการ ระบบงาน และโปรแกรมป้องกันไวรัสใหม่ จากนั้นกู้คืนข้อมูลจากฐานข้อมูลที่ได้สำรองไว้ รวมทั้งตั้งค่าและตรวจสอบการทำงานให้กลับคืนสู่สภาพปกติ

กระบวนการฟื้นฟูระบบสารสนเทศ กรณีเครื่องคอมพิวเตอร์แม่ข่ายโดนภัยคุกคามจากมัลแวร์





๑๑.๔ กรณีอุปกรณ์ (Hardware) เกิดความเสียหาย

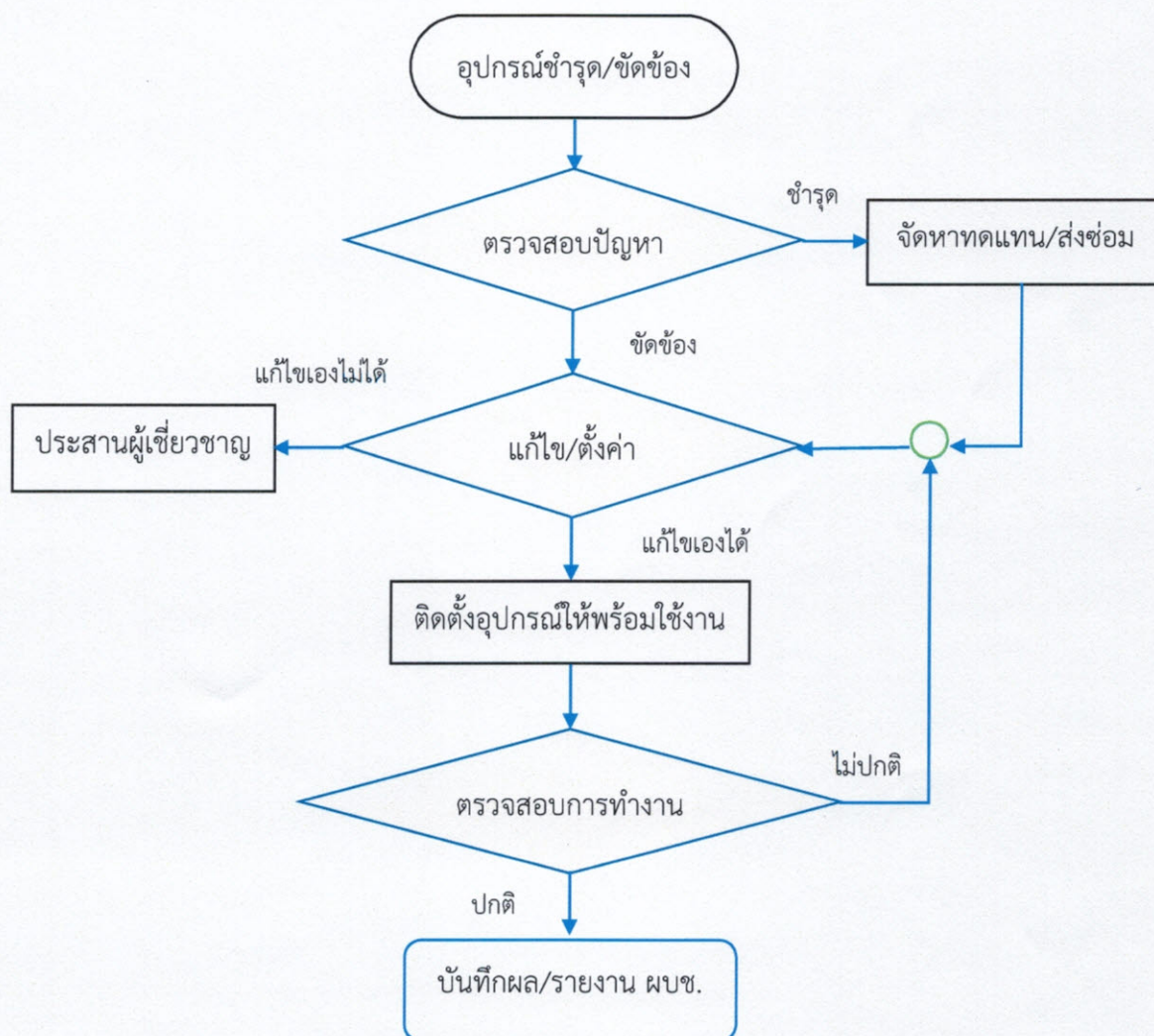
๑๑.๔.๑ ดำเนินการตรวจสอบอุปกรณ์ที่เสียหายและซ่อมแซม หากไม่สามารถซ่อมได้ ให้ประสานขอรับการสนับสนุนอุปกรณ์ทดแทนจาก สอ.ทอ. และดำเนินการส่งซ่อมอุปกรณ์ที่ชำรุดตามสายงานพัสดุ

๑๑.๔.๒ หากจำเป็นต้องตั้งค่าการทำงานหรือติดตั้งซอฟต์แวร์ ให้ดำเนินการให้พร้อมใช้งานในกรณีที่ไม่สามารถทำได้ด้วยตนเอง ให้ประสานขอรับการสนับสนุนเจ้าหน้าที่เทคนิคจาก สอ.ทอ.

๑๑.๔.๓ นำอุปกรณ์ที่ผ่านการซ่อมแซม หรืออุปกรณ์ทดแทนมาติดตั้ง

๑๑.๔.๔ ตรวจสอบความถูกต้องของการทำงาน

กระบวนการฟื้นฟูระบบสารสนเทศ กรณีอุปกรณ์ (Hardware) เกิดความเสียหาย





๑๑.๕ กรณีซอฟต์แวร์ (Software) เกิดความเสียหาย

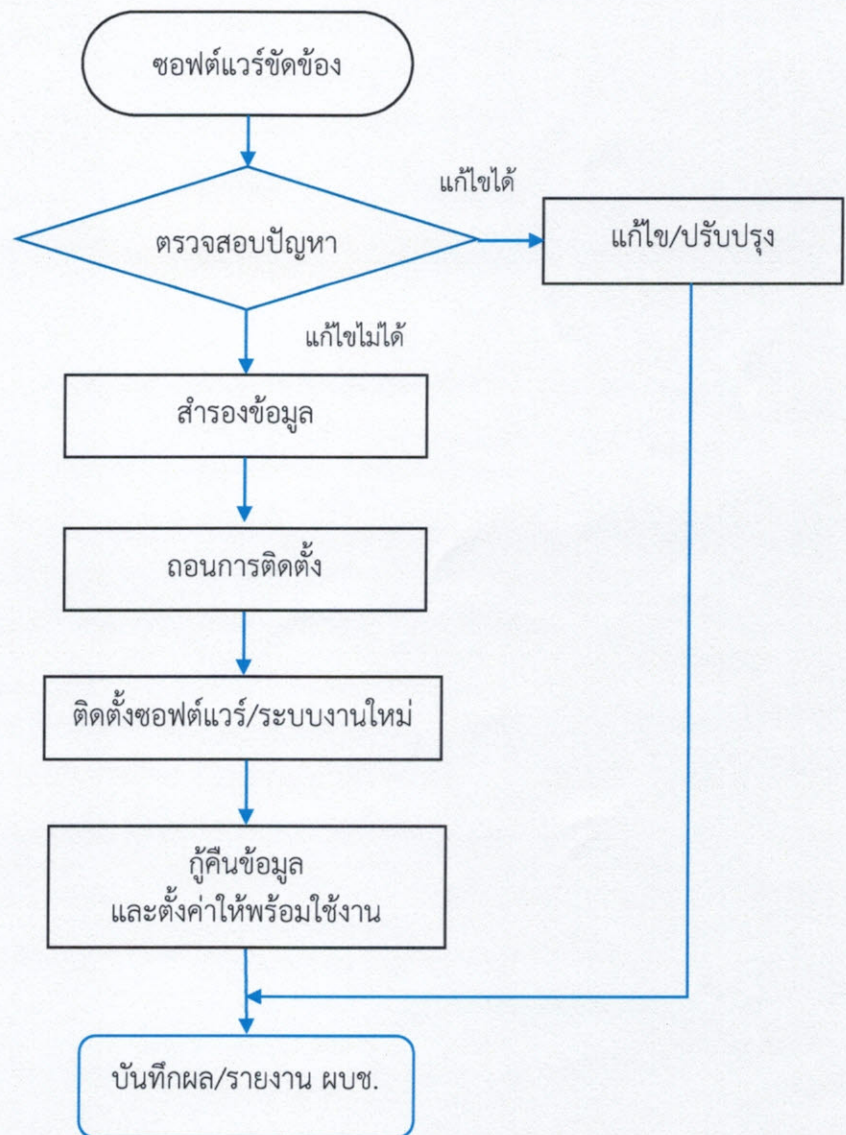
๑๑.๕.๑ ดำเนินการตรวจสอบสาเหตุและแก้ไขข้อขัดข้องซอฟต์แวร์เบื้องต้น โดยใช้ฟังก์ชันการซ่อมแซม (Repair) จากแผ่นติดตั้งซอฟต์แวร์

๑๑.๕.๒ หากไม่สามารถแก้ไขได้ ให้ดำเนินการสำรองข้อมูล (Backup) ในส่วนที่เกี่ยวข้องกับซอฟต์แวร์นั้น ๆ จากพื้นที่จัดเก็บข้อมูลของซอฟต์แวร์ดังกล่าว

๑๑.๕.๓ ดำเนินการถอนการติดตั้ง (Uninstall) และทำการติดตั้ง (Install)

๑๑.๕.๔ กู้คืน (Restore) ข้อมูลที่ได้สำรองไว้ และตั้งค่าให้พร้อมใช้งาน

กระบวนการฟื้นฟูระบบสารสนเทศ กรณีซอฟต์แวร์ (Software) เกิดความเสียหาย





๑๒. การติดตามและรายงานผล

กำหนดให้ผู้รับผิดชอบระบบสารสนเทศของ ทสส.ทอ. ร่วมกับ น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ. รายงานผลการดำเนินงานหรือการตรวจสอบความเสียหายของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เมื่อเกิดข้อขัดข้องกับระบบสารสนเทศและระบบฐานข้อมูลของหน่วย เพื่อนำเสนอรายงานสรุปให้ คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ. เพื่อที่จะนำมาปรับปรุงพัฒนาแผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น

แผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ (Data Backup and IT Disaster Recovery Plan) ฉบับนี้ ได้ผ่านการพิจารณาจาก คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ. เพื่อให้เจ้าหน้าที่มีความพร้อมในการปฏิบัติและแก้ไขปัญหาข้อขัดข้อง ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารต่อไป

พล.อ.ต.

(ธีระ เกาะประเสริฐ)

ประธานกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.

๒๗ ก.ย. ๖๔



บรรณานุกรม

- กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ. (๒๕๖๔). แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทสส.ทอ.: กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ.
- กองทัพอากาศ. (๒๕๖๓). ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓.: กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ.

