แผนเผชิญเหตุ
(IT Contingency Plan)
แผนป้องกันภัยธรรมชาติ
แผนป้องกันอัคคีภัย
ระบบเทคโนโลยีสารสนเทศและการสื่อสาร
โรงเรียนการบิน
พ.ศ.๒๕๖๗

คณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ รร.การบิน

สารบัญ

หน้า

แผนเผชิญเหตุ (IT Contingency Plan)
แผนป้องกันภัยธรรมชาติ แผนป้องกันอัคคีภัย
ระบบเทคโนโลยีสารสนเทศและการสื่อสารโรงเรียนการบิน

๑. หลักการและเหตุผล

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินการตามภารกิจของ รร.การบิน ซึ่งอาจมีปัจจัยภายนอกและปัจจัยภายในมากระทบ ทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเกิดความเสียหายได้ ดังนั้น จึงจัดทำแผนเผชิญเหตุจากภัยพิบัติระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเตรียมความพร้อมและสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารให้สามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน

๒. วัตถุประสงค์

๒.๑ เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน

๒.๒ เป็นแนวทางในการปฏิบัติหากมีภัยพิบัติเกิดขึ้น เพื่อให้ระบบสารสนเทศกลับคืนสู่สภาวะปกติสามารถปฏิบัติงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

๒.๓ สร้างความเข้าใจร่วมกันระหว่างผู้บังคับบัญชาและผู้ปฏิบัติงาน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน

๓. ระเบียบ และแผนปฏิบัติที่เกี่ยวข้อง

๓.๑ ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

๓.๒ แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทสส.ทอ.พ.ศ.๒๕๖๔

๓.๓ แผนเผชิญเหตุจากภัยพิบัติระบบสารสนเทศ ทสส.ทอ.พ.ศ.๒๕๖๔

๓.๔ ระเบียบ รร.การบิน ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๕

๓.๕ แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รร.การบิน พ.ศ.๒๕๖๕

๓.๖ แผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ รร.การบิน พ.ศ.๒๕๖๕

๓.๗ แผนบรรเทาสาธารณภัย รร.การบิน พ.ศ.๒๕๖๔

๓.๘ ระเบียบ ทอ.ว่าด้วยการป้องกันและระงับอัคคีภัย พ.ศ.๒๕๖๕

๔. ขอบเขต...

๔. ขอบเขตการดำเนินงาน

แผนเผชิญเหตุจากภัยพิบัติระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) ของ รร.การบิน ดำเนินการตามข้อกำหนดของ ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ ซึ่งได้รวมแผนป้องกันภัยธรรมชาติ แผนป้องกันอัคคีภัย ไว้ในเอกสารนี้ด้วย โดยจัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดูแลรักษา และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน มีขอบเขตการดำเนินงาน ดังนี้

๔.๑ การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติหรือสถานการณ์ฉุกเฉิน

๔.๒ การเตรียมความพร้อม

๔.๓ มาตรการในการป้องกันและการแก้ไขปัญหา

๔.๔ การกำหนดหน้าที่และผู้รับผิดชอบ

๔.๕ ผังกระบวนการแก้ไขปัญหาเมื่อเกิดภัยพิบัติหรือสถานการณ์ฉุกเฉิน

๔.๖ การติดตามและรายงานผล

๕. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติหรือสถานการณ์ฉุกเฉิน

๕.๑ การวิเคราะห์เหตุการณ์จากภัยพิบัติ

จากการวิเคราะห์และตรวจสอบความเสี่ยงในระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน พบว่า ความเสี่ยงจากภัยพิบัติหรือสถานการณ์ฉุกเฉินที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน แบ่งออกเป็น ๒ กลุ่ม ได้แก่

๕.๑.๑ ภัยพิบัติจากภายนอก

๕.๑.๑.๑ ภัยพิบัติจากธรรมชาติ เช่น วาตภัย อุทกภัย แผ่นดินไหว อาคารถล่ม

๕.๑.๑.๒ ภัยพิบัติจากอัคคีภัย

๔.๑.๑.๓ ภัยจากสถานการณ์ความไม่สงบ เช่น การชุมนุมประท้วง การจลาจล

๕.๑.๑.๔ เครื่องแม่ข่ายหรือระบบการสื่อสารของเครื่องแม่ข่ายขัดข้อง

๕.๑.๑.๕ ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๕.๑.๒ ภัยพิบัติจากภายใน

๕.๑.๒.๑ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในหน่วย

๕.๑.๒.๒ เจ้าหน้าที่หรือบุคลากรภายใน ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ หรือละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๕.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง

จากการวิเคราะห์และตรวจสอบสถานการณ์ภัยพิบัติ สามารถประเมินและกำหนดระดับความรุนแรงของเหตุการณ์ภัยพิบัติที่ส่งผลกระทบระบบงานและพันธกิจของหน่วย นำมาสรุปเป็นข้อมูล ดังนี้

ตาราง...

ตารางแสดงการประเมินสถานการณ์และกำหนดระดับความรุนแรง

ภัยพิบัติ หรือสถานการณ์ฉุกเฉิน	ค่าการประเมินสถานการณ์ (คะแนน ๑ - ๕)		คะแนนรวม	เรียงลำดับ
	โอกาส	ความรุนแรง		
๑. ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในหน่วย	๔	๕	๒๐	๑
๒. เจ้าหน้าที่หรือบุคลากรภายใน ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ หรือละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	๔	๔	๑๖	๒
๓. ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ	๓	๕	๑๕	๓
๔. ภัยพิบัติจากอัคคีภัย	๒	๕	๑๐	๔
๕. ภัยพิบัติทางธรรมชาติ	๒	๔	๘	๕
๖. เครื่องแม่ข่ายหรือระบบการสื่อสารของเครื่องแม่ข่ายขัดข้อง	๑	๕	๕	๖
๗. ภัยจากสถานการณ์ความไม่สงบ	๑	๔	๔	๗

๖. แผนเผชิญเหตุจากภัยพิบัติและภัยอื่น ๆ

๖.๑ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในหน่วย

การเตรียมความพร้อมรองรับสถานการณ์หากเกิดไวรัสคอมพิวเตอร์จากผู้ใช้ภายในหน่วย รร.การบิน ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศ ระบบฐานข้อมูลและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางดำเนินการเบื้องต้นเพื่อลดความเสียหายที่จะเกิดขึ้นกับระบบสารสนเทศของ รร.การบิน ดังนี้

๖.๑.๑ การเตรียมความพร้อม

๖.๑.๑.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๖.๑.๑.๒ ระวังภัยจากการเปิด E-mail หรือดาวน์โหลดไฟล์จากอินเทอร์เน็ต

๖.๑.๑.๓ ตรวจหาไวรัสจากสื่อบันทึกข้อมูลทุกครั้งก่อนใช้งานทุกครั้ง

๖.๑.๑.๔ ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอมหรือน่าสงสัย

๖.๑.๑.๕ ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๖.๑.๑.๖ ไฟล์ทั้งหมดที่ดาวน์โหลดในหน่วยงานต้องได้รับการตรวจหาโปรแกรมประสงค์ร้ายก่อนเปิดใช้งาน

๖.๑.๑.๗ ห้ามผู้ใช้งานทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ตโดยปราศจากการตรวจสอบจาก ศชบ.ทอ.

๖.๑.๒ มาตรการ...

๖.๑.๒ มาตรการในการป้องกัน และการแก้ไขปัญหา

๖.๑.๒.๑ เมื่อสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัส ให้เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้น ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับเครือข่าย

๖.๑.๒.๒ ตรวจหา และกำจัดไวรัส หรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

๖.๑.๒.๓ ในกรณีที่ได้รับแจ้งว่าการแพร่ระบาดอาจส่งผลกระทบต่อระบบงาน และอาจคุกคามระบบคอมพิวเตอร์ในเครือข่าย รร.การบิน ให้ปิดเครื่องคอมพิวเตอร์รายงานผู้บังคับบัญชา และแจ้ง น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน ทันที

๖.๑.๒.๔ ให้ น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน รายงานขั้นต้นต่อ ศซบ.ทอ.เพื่อการค้นหา และตรวจพิสูจน์พยานหลักฐานทางดิจิตอล (Digital Forensic)

๖.๑.๒.๕ บันทึกสถานการณ์ละเมิดคความมั่นคงปลอดภัยระบบสารสนเทศ ร่วมตรวจสอบ ค้นหา สาเหตุช่องโหว่และผลเสียหาย พร้อมแนวทางป้องกันมิให้เกิดซ้ำอีก และรายงานผู้บังคับบัญชา

๖.๒ เจ้าหน้าที่หรือบุคลากรภายใน ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์หรือละเมิดการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๖.๒.๑ การเตรียมความพร้อม

๖.๒.๑.๑ ชี้แจง และอบรมกำลังพลให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๖.๒.๑.๒ สร้างเครือข่ายให้ข่าวสารความรู้ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศเช่น ให้คำแนะนำ คำเตือน ข้อควรระวัง ประชาสัมพันธ์จากภาพ Infographic ผ่านระบบสื่อสังคมออนไลน์

๖.๒.๑.๓ เน้นย้ำให้เจ้าหน้าที่ปฏิบัติตามระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ อย่างเคร่งครัด

๖.๒.๒ มาตรการในการป้องกัน และการแก้ไขปัญหา

๖.๒.๒.๑ ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้งานสารสนเทศได้ตามปกติให้เจ้าหน้าที่ผู้นั้นรายงานผู้บังคับบัญชา และแจ้งเหตุให้ น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน ทราบ

๖.๒.๒.๒ ลดความเสียหายที่จะเกิดขึ้น โดยการหยุดใช้งาน ดึงสาย LAN ออกจากจุดเชื่อมต่อระบบเครือข่าย และปิดเครื่อง

๖.๒.๒.๓ สำรวจความเสียหายที่เกิดจากการละเมิด ให้ตรวจสอบสาเหตุและช่องโหว่โดยประสาน ศซบ.ทอ.ร่วมตรวจสอบด้วย

๖.๒.๒.๔ แต่งตั้ง...

๖.๒.๒.๔ แต่งตั้งคณะกรรมการ เพื่อดำเนินการสอบสวนหาผู้กระทำผิด และพิจารณาลงโทษ ผู้รับผิดชอบ และผู้กระทำผิดตามกรณีที่ก่อให้เกิดความเสียหายต่อระบบ หรือดำเนินการตามกระบวนการทางกฎหมายที่เกี่ยวข้อง

๖.๒.๒.๕ กำหนดมาตรการหรือระเบียบปฏิบัติเพิ่มเติม เพื่อป้องกันและขจัดความเสียหายที่จะเกิดการละเมิดซ้ำ

๖.๒.๒.๖ ให้ น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน เผยแพร่ประชาสัมพันธ์ และอบรมให้ความรู้เรื่อง การตระหนักรู้ทางด้านไซเบอร์และการใช้งานคอมพิวเตอร์ และระบบสารสนเทศ อย่างน้อย ปีละ ๒ ครั้ง

๖.๒.๒.๗ กำหนดให้มีการทดสอบความตระหนักรู้ทางด้านไซเบอร์ การใช้งานเครื่องคอมพิวเตอร์ และระบบสารสนเทศอย่างน้อย ปีละ ๒ ครั้ง เพื่อประเมินความรู้ และความเข้าใจของกำลังพล รร.การบิน

๖.๓ ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๖.๓.๑ การเตรียมความพร้อม

๖.๓.๑.๑ ติดตั้งเครื่องสำรองไฟฟ้า และปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

๖.๓.๑.๒ เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๖.๓.๑.๓ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่าง ๆ เพื่อป้องกันความเสียหายจากไฟกระชาก

๖.๓.๒ มาตรการในการป้องกัน และการแก้ไขปัญหา

๖.๓.๒.๑ ถ้าไฟฟ้าดับหรือไฟฟ้าตก หรือไฟกระชาก ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๖.๓.๒.๒ เวรรักษาการณ์แจ้งผู้ดูแลระบบงานหรือระบบเครือข่าย เพื่อดำเนินการปิดระบบอย่างปลอดภัย และรายงานให้ผู้บังคับบัญชาทราบ

๖.๓.๒.๓ ตรวจสอบสาเหตุข้อขัดข้องของระบบไฟฟ้าร่วมกับ ฝสณ.ผชย.กรก.รร.การบิน

๖.๓.๒.๔ เมื่อกระแสไฟฟ้าใช้งานได้ตามปกติ ให้ผู้ดูแลระบบตรวจสอบความเสียหายและเปิดระบบตรวจสอบความพร้อมในการปฏิบัติงาน และรายงานให้ผู้บังคับบัญชาทราบ

๖.๔ เครื่องแม่ข่าย...

๖.๔ เครื่องแม่ข่ายหรือระบบการสื่อสารของเครื่องแม่ข่ายขัดข้อง

๖.๔.๑ การเตรียมความพร้อม

๖.๔.๑.๑ กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้มี จนท.ดูแลรับผิดชอบระบบเครือข่ายเป็นผู้รับผิดชอบนำพาเข้าไป และบันทึกเหตุการณ์หรือกิจกรรม ที่เกี่ยวข้อง

๖.๔.๑.๒ มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายของหน่วยงานได้ และต้องเปิดใช้งานตลอดเวลา

๖.๔.๑.๓ มีการใช้งานเว็บไซต์ตามรูปแบบ ที่ ทสส.ทอ.กำหนดเพื่อลดความเสี่ยงในการถูกโจมตี

๖.๔.๑.๔ ปฏิบัติตามระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศอย่างเคร่งครัด จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุก และภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๖.๔.๒ มาตรการในการป้องกัน และการแก้ไขปัญหา

๖.๔.๒.๑ ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์หรือระบบเครือข่ายไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้ น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน หรือผู้ดูแลระบบสารสนเทศของหน่วยงานทราบ

๖.๔.๒.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสโจมตี เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่น ๆ ในระบบเครือข่ายให้ดึงสายเชื่อมโยงเครือข่าย (LAN) ออกจากเครื่องคอมพิวเตอร์โดยเร็ว ในกรณีที่คาดว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในอาคาร ที่ตั้งของระบบเครือข่ายเดียวกับเครื่องคอมพิวเตอร์ที่ถูกโจมตี ให้ปิดระบบเครือข่ายภายในอาคารนั้น

๖.๔.๒.๓ ปิดระบบงานและตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว และปิดอุปกรณ์อื่น ๆ ตามลำดับความสำคัญของการให้บริการ

๖.๔.๒.๔ ให้ผู้รับผิดชอบดูแลระบบสารสนเทศและเครือข่ายของ รร.การบิน ตรวจสอบและแก้ไขปัญหา ข้อขัดข้องเบื้องต้น ถ้าหากไม่สามารถดำเนินการได้ให้ประสานกับหน่วยเกี่ยวข้อง และรายงานผู้บังคับบัญชา ทราบโดยเร็ว

๖.๕ เกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

๖.๕.๑ การเตรียมความพร้อม

๖.๕.๑.๑ ติดตามสถานการณ์จากแหล่งต่าง ๆ เช่น โทรทัศน์ วิทยุ ตำรวจ และหน่วยงานที่เกี่ยวข้อง เพื่อรวบรวมข่าวสาร และประเมินสถานการณ์จากการชุมนุมประท้วงอย่างต่อเนื่อง

๖.๕.๑.๒ สำรวจและจัดเตรียมชุดปฏิบัติการ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้น เพื่อเตรียมการปฏิบัติไว้ให้พร้อม

๖.๕.๑.๓ ตรวจสอบความปลอดภัยอาคารสถานที่เพิ่มเติม เช่น ระบบรักษาความปลอดภัยในอาคาร กล้องวงจรปิด ระบบไฟฟ้า ระบบปั๊มน้ำ เป็นต้น

๖.๕.๒ มาตรการ...

๖.๕.๒ มาตรการในการป้องกัน และการแก้ไขปัญหา

๖.๕.๒.๑ เวรรักษาการณ์ ปิดประตูทุกอาคาร และควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาในพื้นที่

๖.๕.๒.๒ ปฏิบัติตามแผนที่ผู้บังคับบัญชาสั่งการ

๖.๕.๒.๓ กรณีเกิดสถานการณ์รุนแรง และป้องกันความเสียหายกับระบบสารสนเทศของหน่วยให้ผู้ดูแลระบบ Remote เข้ามาปิดระบบ

๖.๕.๒.๔ กรณีเกิดสถานการณ์ยาวนานไม่สามารถปฏิบัติงานที่หน่วยได้ จำเป็นต้องย้ายสถานที่ปฏิบัติงานชั่วคราว ให้ผู้ดูแลระบบนำข้อมูลสำรองที่จัดเก็บไว้มาติดตั้ง ณ สถานที่ที่กำหนด

๗. แผนป้องกันอัคคีภัย

๗.๑ การเตรียมความพร้อม

เพื่อรองรับสถานการณ์ฉุกเฉินจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหาย แก่ระบบสารสนเทศ และอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางดำเนินการเบื้องต้น เพื่อลดความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศของหน่วย ดังนี้

๗.๑.๑ ติดตั้งเครื่องดับเพลิงยกหิ้วให้เพียงพอในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่าย และตรวจสภาพเป็นประจำทุกเดือน

๗.๑.๒ จัดเจ้าหน้าที่เข้าร่วมฝึกอบรมหลักสูตรป้องกัน และระงับอัคคีภัยของหน่วยงาน เพื่อให้มีความรู้ ความเข้าใจ พร้อมรองรับสถานการณ์ฉุกเฉินกรณีเกิดเหตุเพลิงไหม้เป็นประจำทุกปี

๗.๑.๓ ให้สำรองข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย และแยกเก็บไว้ที่อื่นที่ปลอดภัยอีก ๑ ชุด

๗.๑.๔ หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคารให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

๗.๑.๕ หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร และโทรแจ้ง จนท.ฝ่ายดับเพลิงและกู้ภัย ผชย.กรก.รร.การบิน โทร.๑๙๒

๗.๑.๖ หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหายให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

๗.๒ มาตรการในการป้องกัน และการแก้ไขปัญหา

๗.๒.๑ ผู้ที่พบเห็นเพลิงไหม้หรือผู้ที่ปฏิบัติหน้าที่เวรรักษาการณ์ ให้รีบแจ้งเหตุไฟไหม้และแจ้งผู้เกี่ยวข้องให้ตัดระบบจ่ายไฟภายในอาคาร รวมทั้งแจ้ง จนท.ฝ่ายดับเพลิงและกู้ภัย ผชย.กรก.รร.การบิน โทร.๑๙๒ โดยใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว แล้วรีบขนย้ายอุปกรณ์ที่สำคัญไปไว้ในที่ปลอดภัย

๗.๒.๒ จนท....

๗.๒.๒ จนท.ดับเพลิงดับและกู้ภัย ผชย.กรก.รร.การบิน ประเมินสถานการณ์ว่าสามารถดับเพลิงด้วยตนเองได้หรือไม่ ถ้าไม่สามารถดับเพลิงได้ ให้รีบออกจากพื้นที่เกิดเพลิงไหม้ตามเส้นทางหนีไฟที่ปลอดภัยไปยังจุดรวมพลที่กำหนดไว้ และปฏิบัติตามแผนป้องกันและบรรเทาอัคคีภัยของ รร.การบิน โทรศัพท์แจ้ง น.นิรภัยภาคพื้น รร.การบิน โทร.๓-๗๒๐๙ น.เวร และผู้บังคับบัญชาตามลำดับชั้นทราบ เพื่อระงับเหตุ

๗.๒.๓ ปฏิบัติตามแผนป้องกันและบรรเทาอัคคีภัยของนิรภัยภาคพื้น รร.การบิน

๗.๒.๔ หลังจากเพลิงสงบแล้วให้ผู้ดูแลระบบงานตรวจสอบ และประเมินความเสียหายหรือประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบงานหรือระบบเครือข่าย เพื่อตรวจสอบและแก้ไขปัญหาข้อขัดข้อง ในกรณีที่อุปกรณ์ฮาร์ดแวร์เสียหาย ให้รีบจัดหาอุปกรณ์สำรอง หรือประสานหน่วยเกี่ยวข้องที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗.๒.๕ ดำเนินการฟื้นฟูระบบสารสนเทศ โดยใช้แผนฟื้นฟูระบบสารสนเทศของ รร.การบิน

๗.๒.๖ สรุปผลการปฏิบัติและรายงานผู้บังคับบัญชา

๘. แผนป้องกันภัยธรรมชาติ

๘.๑ การเตรียมความพร้อม

รองรับสถานการณ์ฉุกเฉินจากกรณีเกิดภัยธรรมชาติ เช่น วาตภัย อุทกภัย แผ่นดินไหว ตึกถล่ม เป็นต้น ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศ และอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางดำเนินการเบื้องต้นเพื่อลดความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศของหน่วย ดังนี้

๘.๑.๑ ติดตามสถานการณ์ข้อมูลข่าวสารเตือนภัยจากหน่วยงานของรัฐ เช่น ข้อมูลการพยากรณ์ อากาศจากกรมอุตุนิยมวิทยา (www.tmd.go.th) ศูนย์เตือนภัยพิบัติแห่งชาติ (www.ndwc.thaigov.go.th) ข้อมูลพื้นที่เสี่ยงภัยจากกรมทรัพยากรธรณี (www.dmr.go.th) หรือ กรมป้องกันและบรรเทาสาธารณภัย (www.disaster.go.th) เป็นต้น

๘.๑.๒ การสังเกตพฤติกรรมของสัตว์ เช่น สัตว์เลี้ยงในบ้าน แมลงสาบ หนู งู แสดงอาการตกใจผิดปกติ

๘.๑.๓ จัดชุดเตรียมพร้อมรองรับสถานการณ์ฉุกเฉิน จัดทำบัญชียานพาหนะ และเครื่องมือเครื่องใช้ให้ครบถ้วน พร้อมใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัยพิบัติ

๘.๑.๔ จัด จนท.เข้าร่วมการอบรมให้ความรู้การปฏิบัติเมื่อเกิดภัยธรรมชาติ และซักซ้อมการปฏิบัติ ตามแผนป้องกันและบรรเทาสาธารณภัย ปีละ ๑ ครั้ง เป็นอย่างน้อย

๘.๒ มาตรการในการป้องกัน และการแก้ไขปัญหา

เมื่อเกิดสถานการณ์ฉุกเฉินหรือภัยพิบัติจากกรณีเกิดภัยธรรมชาติ เช่น วาตภัย อุทกภัย แผ่นดินไหว ตึกถล่ม เป็นต้น ซึ่งอาจสร้างความเสียหายแก่อาคารสถานที่ หรือระบบสารสนเทศของหน่วยงาน ให้ปฏิบัติ ดังนี้

๘.๒.๑ ผู้ปฏิบัติ...

๘.๒.๑ ผู้ปฏิบัติหน้าที่เวรรักษาการณ์ ผู้ปฏิบัติหน้าที่ในอาคารหรือผู้ดูแลระบบสารสนเทศ รอฟังประกาศ สถานการณ์ฉุกเฉิน ควบคุมสติ อยู่ห่างจากประตู หน้าต่าง หรือชั้นวางของที่อาจพังหรือล้มลงได้ง่าย อย่าตื่นตกใจ และแย่งกันออกจากอาคาร ให้หาทางออกอาคารในช่องทางที่ปลอดภัยโดยเร็ว

๘.๒.๒ อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดประกายไฟ อาจเกิดอันตรายจากแก๊สรั่วได้

๘.๒.๓ หากอยู่ภายนอกอาคารให้อยู่ห่างต้นไม้ใหญ่ เสาไฟ สายไฟฟ้า หรือป้ายโฆษณา

๘.๒.๔ เมื่อสถานการณ์สงบลง ให้ชุดสำรวจอาคารสถานที่ตรวจสอบและประเมินโครงสร้างอาคาร ท่อน้ำ ก๊าซ ระบบไฟฟ้า ระบบการสื่อสาร และประสานการปฏิบัติกับหน่วยอื่น ๆ ที่เกี่ยวข้อง

๘.๒.๕ ชุดตรวจสอบและประเมินความเสียหายระบบสารสนเทศและระบบเครือข่าย ตรวจสอบและประเมินความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน

๘.๒.๖ ชุดฟื้นฟูระบบสารสนเทศ และระบบเครือข่าย ดำเนินการฟื้นฟูระบบต่าง ๆ ให้สามารถกลับมาใช้งานได้ตามปกติ ตามแผนฟื้นฟูระบบสารสนเทศของ รร.การบิน

๘.๒.๗ สรุปผลการปฏิบัติ และรายงานผู้บังคับบัญชา

๙. การกำหนดหน้าที่และผู้รับผิดชอบ

จัดเตรียมทีมงานและมอบหมายหน้าที่ เพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ รร.การบิน ดังนี้

๙.๑ ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ รร.การบิน (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจน ติดตาม กำกับดูแล ควบคุม ตรวจสอบ การปฏิบัติตามแผน ได้แก่

๙.๑.๑ ผู้บัญชาการโรงเรียนการบิน

๙.๑.๒ รองบัญชาการโรงเรียนการบิน

๙.๒ ระดับปฏิบัติ

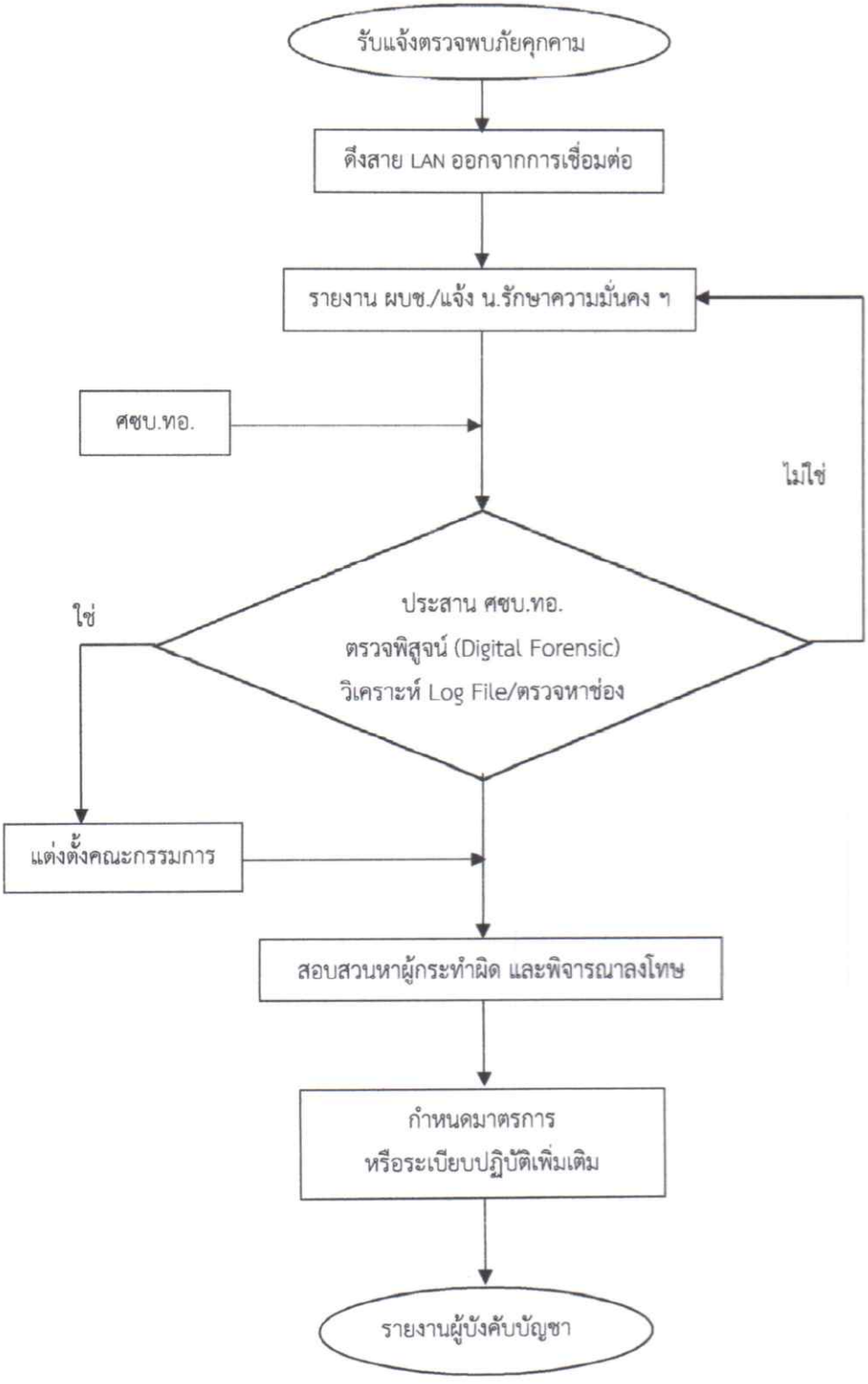
รับผิดชอบในการปฏิบัติงานด้านเทคนิคและการประสานงานในส่วนที่เกี่ยวข้อง ติดตาม กำกับดูแล ควบคุม ตรวจสอบ รับผิดชอบงาน ได้แก่

ตาราง...

ลำดับ	ทีมงาน	ภารกิจ	ผู้รับผิดชอบ	โทรศัพท์
๑	ชุดสำรวจอาคารสถานที่และดำเนินงานด้านธุรการ	ทำหน้าที่ประสานการปฏิบัติงานตามแผนแก้ไขปัญหาเบื้องต้น จัดเตรียม สถานที่สำรองสำหรับปฏิบัติงาน ตรวจสอบระบบไฟฟ้า ระบบการสื่อสาร ระบบปรับอากาศ และดำเนินงานด้านธุรการ	๑.๑ น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน/นทสส.รร.การบิน ๑.๒ นนพ.รร.การบิน ๑.๓ ผสอ.รร.การบิน ๑.๔ ผธก.บก.รร.การบิน	๓-๗๔๗๙ ๓-๗๒๐๙ ๓-๗๓๗๘ ๓-๗๔๐๓
๒	ชุดตรวจสอบและประเมินความเสียหายระบบสารสนเทศและระบบเครือข่าย	ทำหน้าที่ประเมินความเสียหายและให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน	๑.๑ นทสส.รร.การบิน ๑.๒ ผสอ.รร.การบิน	๓-๗๔๗๙ ๓-๗๓๗๘
๓	ชุดฟื้นฟูระบบสารสนเทศและระบบเครือข่าย	ทำหน้าที่ดำเนินการฟื้นฟูระบบต่าง ๆ ให้สามารถกลับมาใช้งานได้ตามปกติ	น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน และ นทสส.รร.การบิน	๓-๗๔๗๙

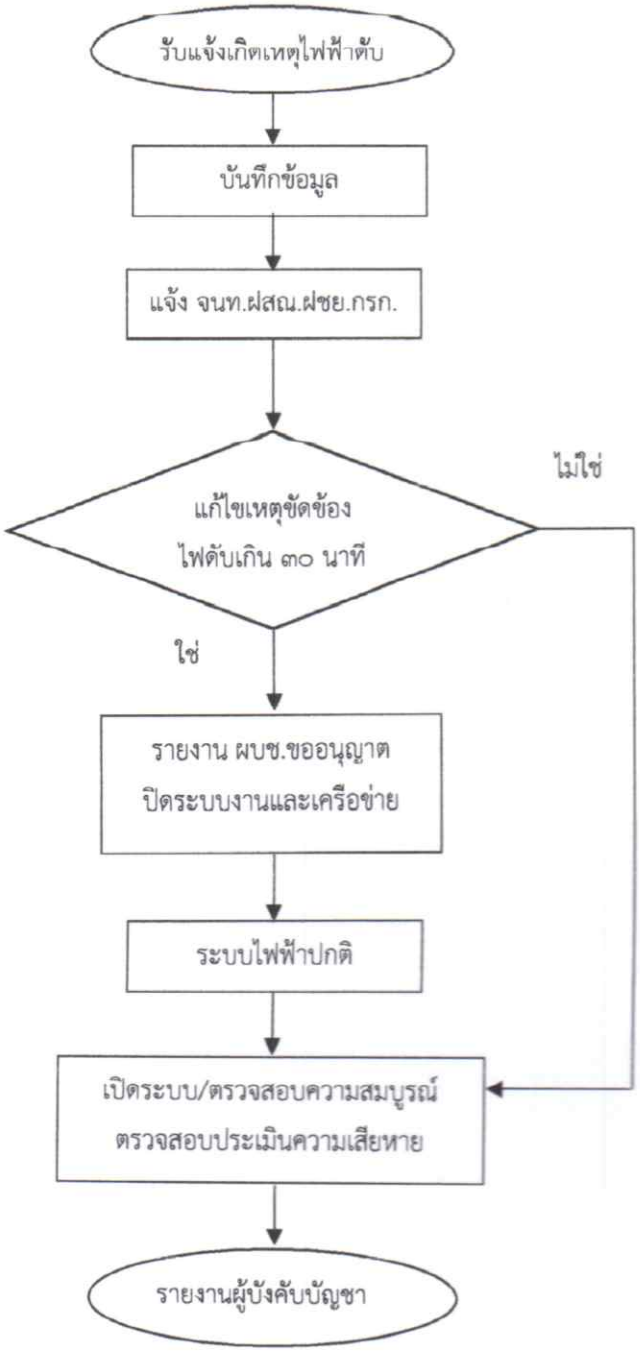
๑๐. แผนผังกระบวนการแก้ไขปัญหาเมื่อเกิดภัยพิบัติหรือสถานการณ์ฉุกเฉิน

๑๐.๑ ขั้นตอนการปฏิบัติกรณีเกิดไวรัสคอมพิวเตอร์หรือบุคลากรภายในละเมิดการรรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน



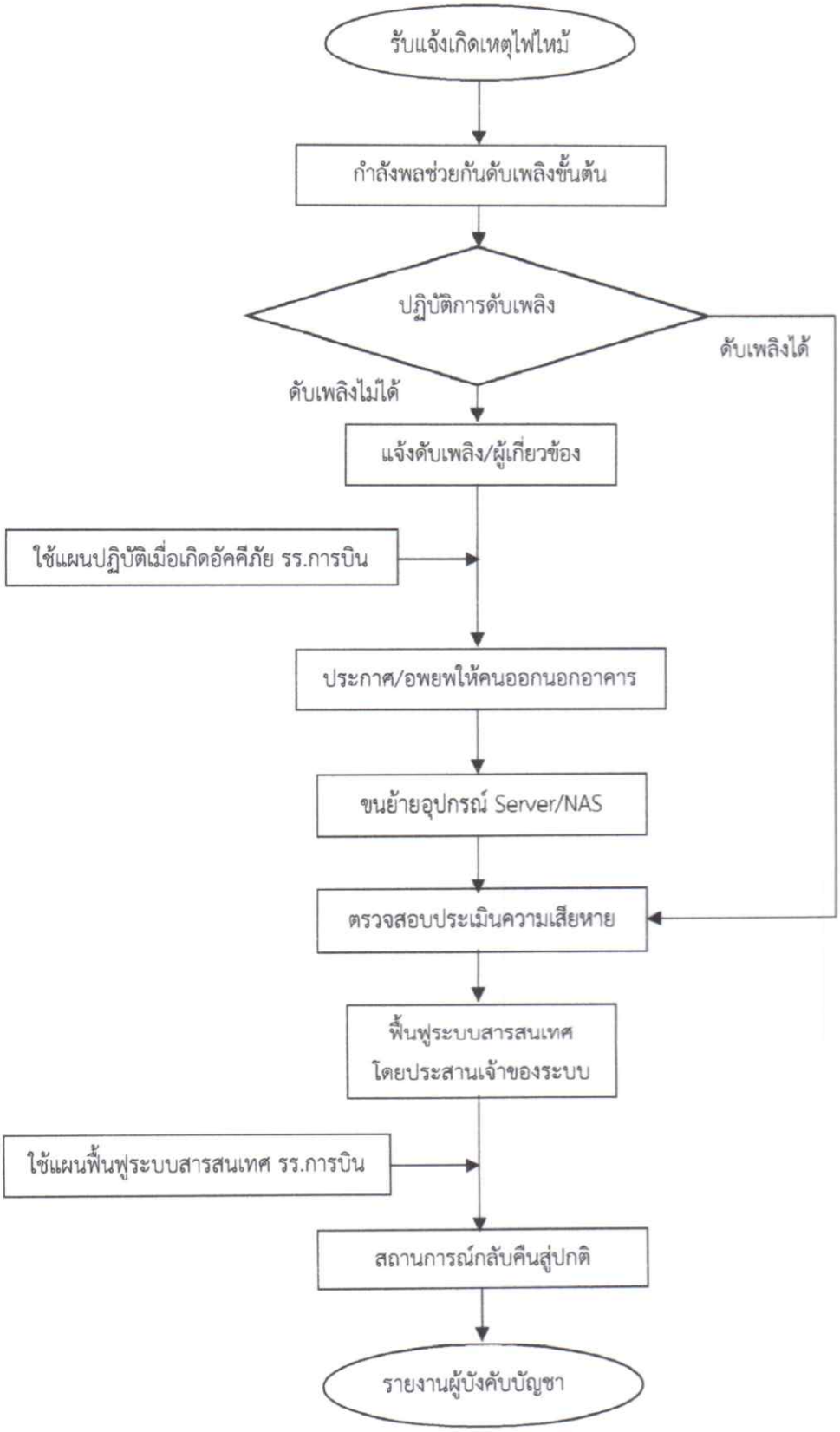
๑๐.๒ ขั้นตอน...

๑๐.๒ ขั้นตอนการปฏิบัติกรณีระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ



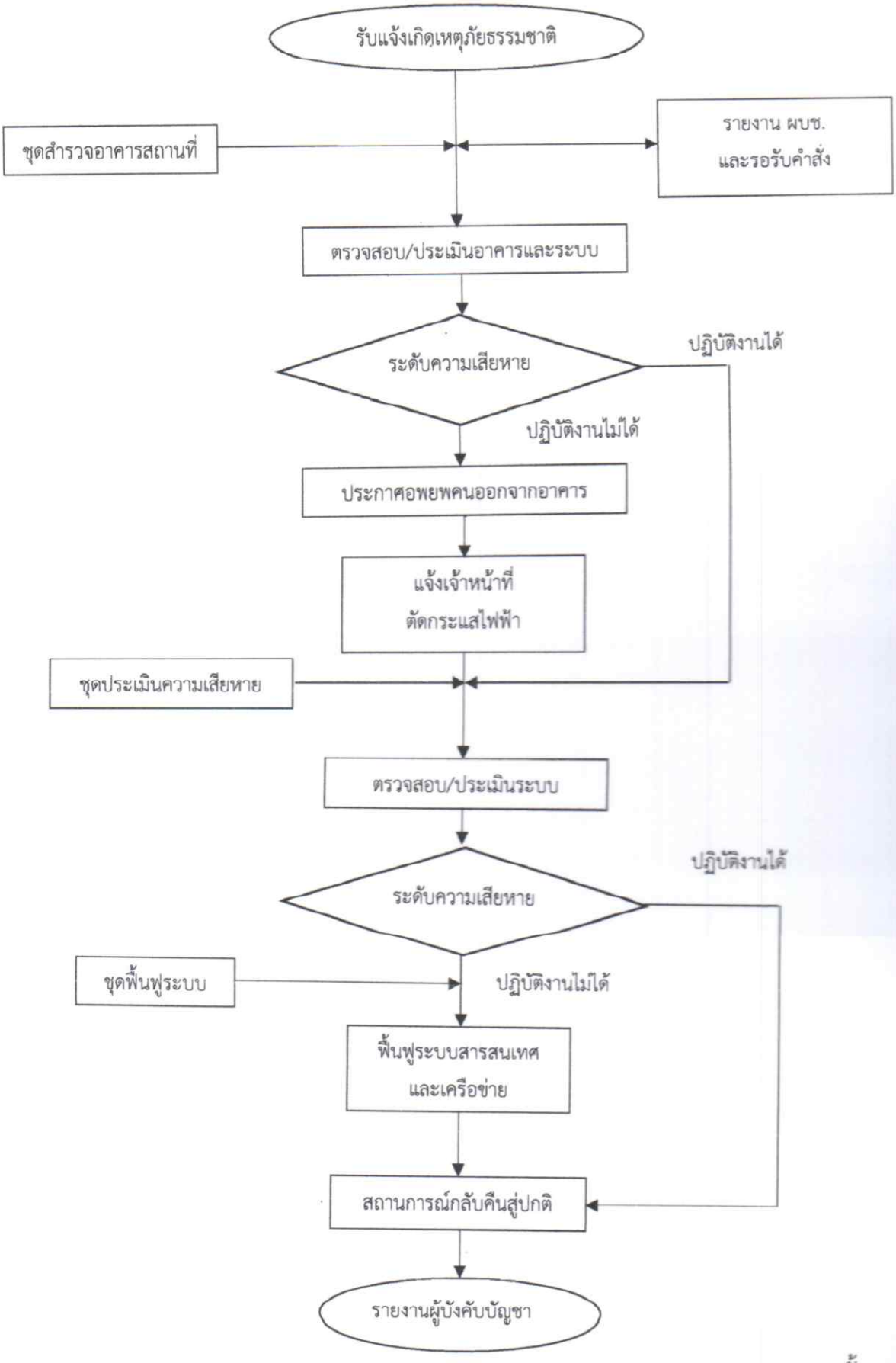
๑๐.๓ ขั้นตอน...

๑๐.๓ ขั้นตอนการปฏิบัติกรณีเกิดอัคคีภัย



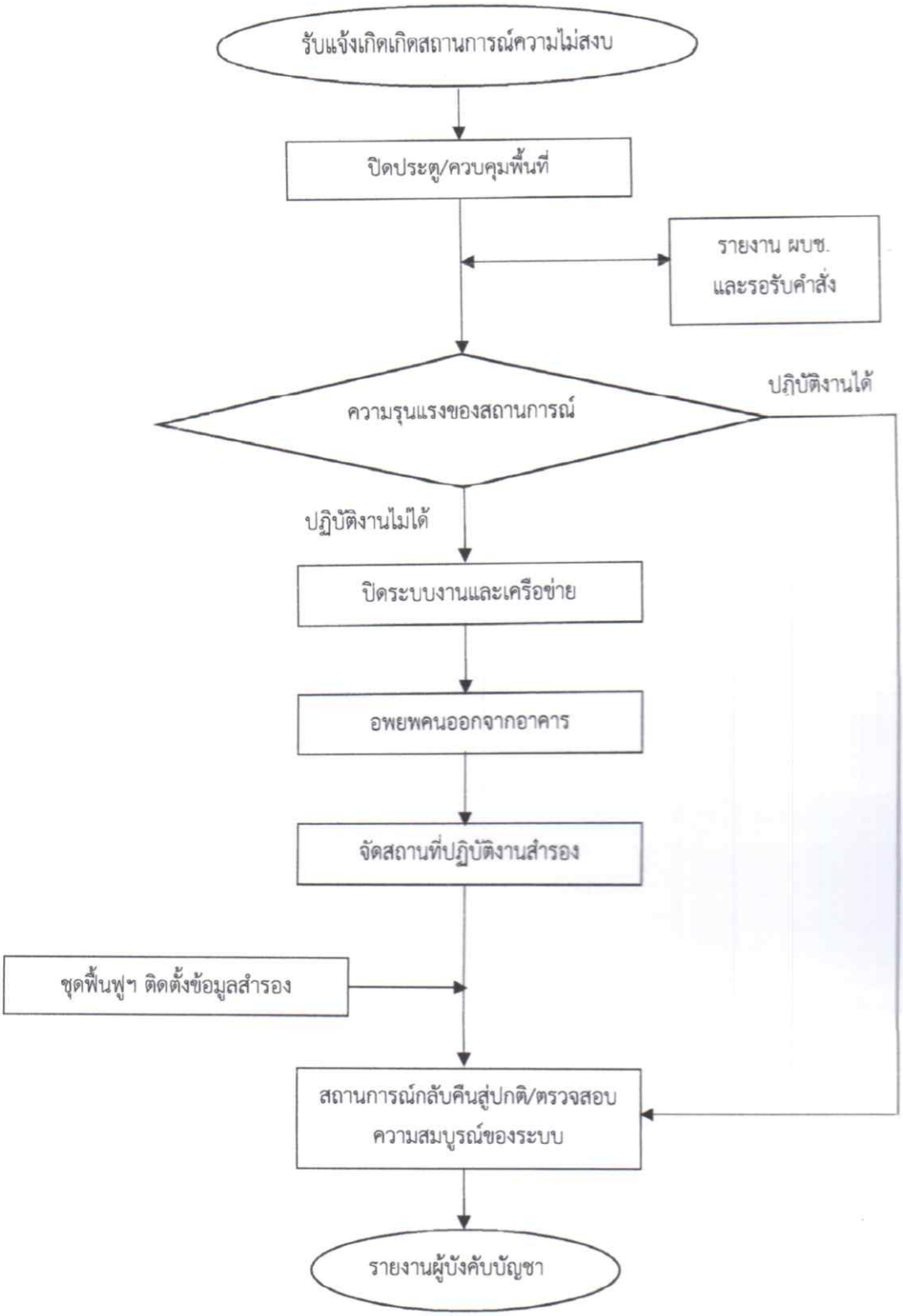
๑๐.๔ ขั้นตอน...

๑๐.๔ ขั้นตอนการปฏิบัติกรณีเกิดภัยพิบัติทางธรรมชาติ



๑๐.๕ ขั้นตอน...

๑๐.๕ ขั้นตอนการปฏิบัติกรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง



๑๑. การติดตาม...

๑๑. การติดตามและรายงานผล

กำหนดให้ผู้รับผิดชอบระบบสารสนเทศของ รร.การบิน น.รักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน รายงานผลดำเนินงานหรือการตรวจสอบความเสียหายของระบบเทคโนโลยีสารสนเทศและสื่อสาร เมื่อเกิดเหตุการณ์ฉุกเฉินจากภัยพิบัติ เพื่อนำเสนอรายงานสรุปให้คณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ รร.การบิน เพื่อที่จะนำมาปรับปรุงพัฒนาแผนเผชิญเหตุจากภัยพิบัติให้มีประสิทธิภาพมากยิ่งขึ้น

แผนเผชิญเหตุจากภัยพิบัติระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน ฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ รร.การบิน เพื่อให้เจ้าหน้าที่มีความพร้อมในการปฏิบัติและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารต่อไป

น.อ.
(ขวัญชาติ ชวนสนิท)
เสนาธิการ รร.การบิน/ผู้บริหารเทคโนโลยีสารสนเทศ (CIO)
ประธานคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน
ก.พ.๖๗