รายงานองค์ความรู้ที่มีการจัดการ
เพื่อให้เกิดวิธีปฏิบัติที่เป็นเลิศ

กระบวนการด้านระบบสารสนเทศ

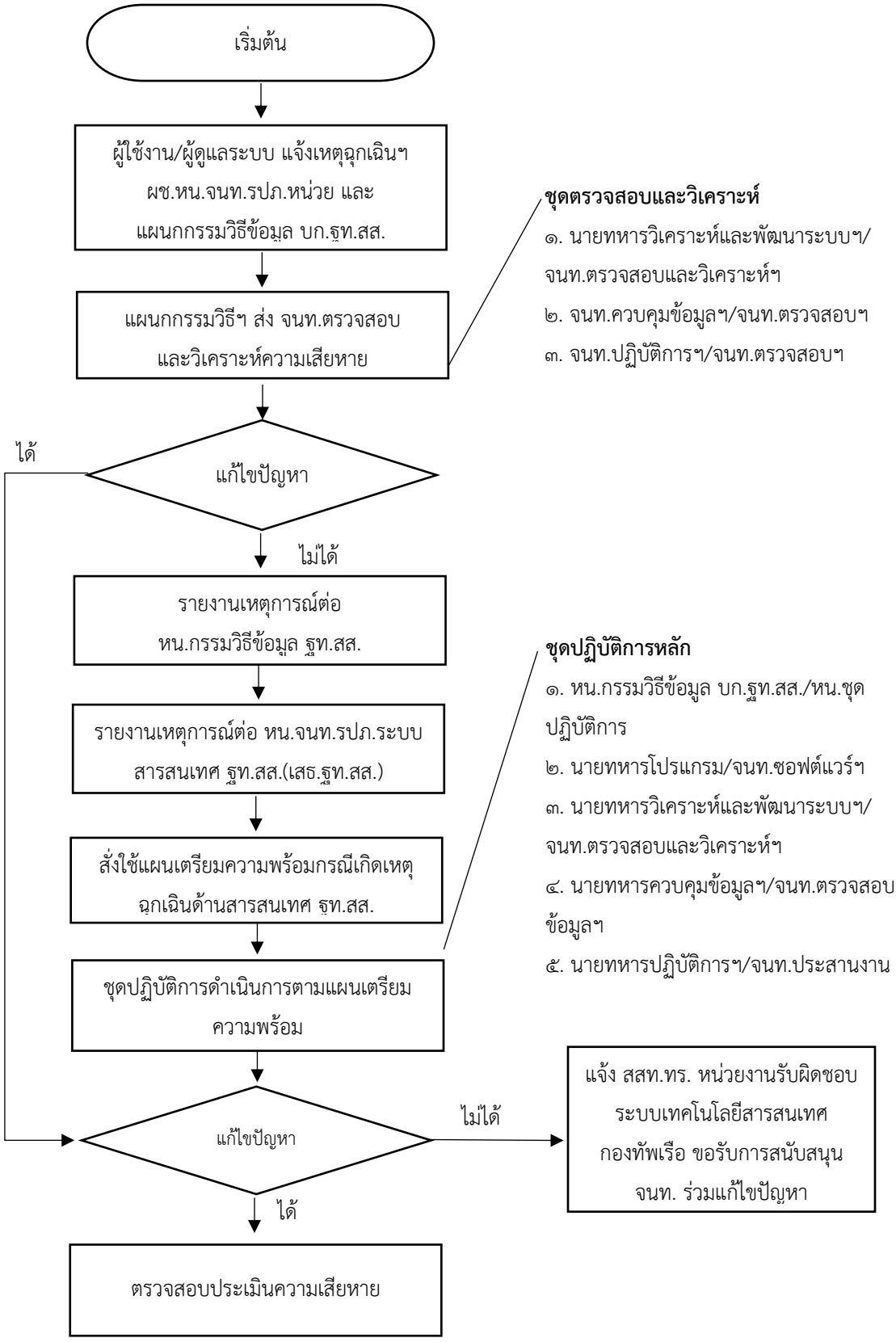
เพื่อสนับสนุนกรณีเกิดอัคคีภัยในเขตท่าเรือจุกเสม็ด กทส.ฐท.สส.

จัดทำโดย

แผนกกรรมวิธีข้อมูล บก.ฐท.สส.

ประจำปีงบประมาณ ๒๕๖๗

๑. ผังการปฏิบัติด้านระบบสารสนเทศ เพื่อสนับสนุนกรณีเกิดอัคคีภัยในเขตท่าเรือจุกเสม็ด กทส.ฐท.สส.



๒. โครงสร้าง/สายการบังคับบัญชาด้านการรักษาความปลอดภัยระบบสารสนเทศ ฐท.สส.

๓. การจัดชุดปฏิบัติการในด้านระบบสารสนเทศ เพื่อสนับสนุนกรณีเกิดอัคคีภัยในเขตท่าเรือจุกเสม็ด กทส.ฐท.สส.

หน.ชุดปฏิบัติการ
(หน.กรรมวิธีข้อมูล บก.ฐท.สส.)

ชุดตรวจสอบและวิเคราะห์ความเสียหาย	**ชุดแก้ไขสถานการณ์หลัก**	**ชุดแก้ไขสถานการณ์ร่วม**
๑.นายทหารวิเคราะห์และพัฒนาระบบ/หน.ชุด ๒.จนท.ควบคุมข้อมูลฯ ๓.จนท.ปฏิบัติการ ฯ	๑.หน.แผนกกรรมวิธีข้อมูล บก.ฐท.สส./หน.ชุด ๒.นายทหารโปรแกรมฯ ๓.นายทหารวิเคราะห์ฯ ๔.นายทหารควบคุมข้อมูลฯ ๕.นายทหารปฏิบัติการฯ ๖.จนท.ควบคุมข้อมูลฯ ๗.จนท.ปฏิบัติการฯ	๑.หน.แผนกสารสนเทศทางการแพทย์ รพ.อาภากรเกียรติวงศ์ ฐท.สส./หน.ชุด ๒.หน.มว.กรรมวิธีข้อมูลและสถิติ กรง.ฐท.สส./รอง หน.ชุด ๓.จนท.แผนกสารสนเทศทางการแพทย์ฯและ จนท.มว.กรรมวิธีข้อมูลและสถิติฯ

๔. มาตรการด้านระบบสารสนเทศ เพื่อสนับสนุนกรณีเกิดอัคคีภัยในเขตท่าเรือจุกเสม็ด กทส.ฐท.สส.

๑. ผู้สั่งการในที่เกิดเหตุ : หน.กรรมวีข้อมูล บก.ฐท.สส./หน.ชุดปฏิบัติการ

๒. การตรวจสอบและและสรุปหาสาเหตุเบื้องต้น

๒.๑ สัญญาณเตือนอัคคีภัยทำงาน

๒.๒ รับแจ้งว่าไฟไหม้อาคาร

๓. การรายงานเหตุ

๓.๑ รายงานการตรวจสอบ และสรุปหาสาเหตุเบื้องต้นให้ หน.จนท.รปภ.ระบบสารสนเทศ ฐท.สส./ผู้บริหารเทคโนโลยีสารสนเทศของ ฐท.สส.(CIO) หรือผู้บังคับบัญชาของ ฐท.สส. ทราบในโอกาสแรก

๓.๒ วิเคราะห์สาเหตุและเสนอแนะหนทางการแก้ไขปัญหา

๓.๓ รายงานยการปฏิบัติทั้งหมดในการแก้ไขปัญหาให้ผู้บังคับบัญชาทราบ

๔. ขั้นตอนการปฏิบัติ

๔.๑ แจ้งนายทหารเวรประจำวัน ฐท.สส.

๔.๒ ขณะเกิดเหตุให้ปฏิบัติตามแผนเผชิญเหตุของ ฐท.สส. (การป้องกันและระงับอัคคีภัย)

๔.๓ หลังเกิดเหตุให้ตรวจสอบและประเมินความเสียหาย ที่เกิดกับระบบสารสนเทศ

๔.๔ เข้าตรวจสอบอุปกรณ์ทั้งหมด ถ้าไม่เสียหาย ดำเนินการกู้คืนระบบทั้งหมดกลับมาใช้งานตามปกติ

๔.๕ ในกรณีที่เกิดความเสียหายจนไม่สามารถให้บริการได้ ทำการสำรองข้อมูล ปิดระบบทั้งหมด

๕. มาตรการหรือแนวทางการปฏิบัติด้านระบบสารสนเทศ เพื่อสนับสนุนกรณีเกิดอัคคีภัยในเขตท่าเรือจุกเสม็ด กทส.ฐท.สส.

เพื่อให้การป้องกันและแก้ไขตลอดจนการจัดการกับระบบสารสนเทศและระบบเครือข่ายเป็นไปอย่างมีประสิทธิภาพในกรณีที่เกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติฉุกเฉินขึ้น จึงกำหนดมาตรการหรือแนวทางการปฏิบัติ ดังนี้

๑. การตรวจสอบและสรุปสาเหตุเบื้องต้น โดยการสังเกตอาการหรือเหตุผิดปกติ มี ๒ องค์ประกอบ คือ

๑.๑ ทางกายภาพ สภาพอันผิดปกติ เช่น กลิ่น อุณหภูมิ ไฟฟ้าดับ เสียง อาการสั่น

๑.๒ การทำงานของระบบ เช่น ไม่สามารถเข้าระบบงานได้ ระบบทำงานผิดพลาดมีข้อความแจ้งเหตุอันผิดปกติ

๒. การแจ้งเหตุ

๒.๑ แจ้งเหตุกรณีเร่งด่วน ให้ประสานแจ้งผู้เกี่ยวข้องโดยตรง เช่น หน.จนท.รปภ. ระบบสารสนเทศ ฐท.สส. หรือนายทหารเวรประจำวัน ฐท.สส.

๒.๒ แจ้งเหตุกรณีปกติ ให้สรุปสาเหตุและจัดทำรายงานแจ้งไปยังผู้ที่เกี่ยวข้อง หรือแจ้ง จนท.รปภ. ระบบสารสนเทศ ฐท.สส. เพื่อรายงานผู้บังคับบัญชาทราบตามลำดับต่อไป

๓. การประเมินการปฏิบัติ

ให้เจ้าหน้าที่ ณ ที่เกิดเหตุ ประเมินสถานการณ์ที่เกิดขึ้นแล้ว แจ้ง หน.จนท.รปภ.ระบบสารสนเทศ ฐท.สส. เพื่อทำการป้องกันและแก้ไขปัญหาจากภัยพิบัติฉุกเฉินต่อไป

๔. แนงทางการปฏิบัติ

๔.๑ เป้าหมายการปฏิบัติ

๔.๑.๑ หน่วยงานที่เกี่ยวข้องสามารถสนับสนันและประสานการปฏิบัติด้านระบบสารสนเทศอย่างเป็นระบบและรวดเร็ว

๔.๑.๒ สามารถป้องกันและลดความเสียหายที่อาจเกิดขึ้น ทั้งที่เป็นผลที่เกิดจากเหตุการณ์ภัยพิบัติฉุกเฉินโดยตรงและผลกระทบที่ตามมาได้อย่างทันท่วงที

๔.๒ หลักการปฏิบัติ

๔.๒.๑ ความรวดเร็วในการแก้ปัญหา การประเมินสถานการณ์ในกรณีที่เกิดเหตุภัยพิบัติฉุกเฉินในเขตพื้นที่รับผิดชอบ ให้พิจารณาเหตุการณ์ว่าภัยฉุกเฉินประเภทใดและรายงานให้ ฐท.สส. ทราบทันที

๔.๒.๒ การสั่งการ เพื่อแก้ปัญหาให้หน่วยงานและบุคคลที่เกี่ยวข้องกับการปฏิบัติดำเนินการภายใต้คำสั่งของ ฐท.สส. หรือ ผู้บริหารเทคโนโลยีสารสนเทศ ฐท.สส. (CIO) หรือผู้ที่ได้รับมอบหมาย (แล้วแต่กรณี)

๔.๒.๓ ในกรณี ฐท.สส. พิจารณาเห็นว่าเหตุการณ์ที่เกิดขึ้นเกินขีดความสามารถในการดำเนินการให้ประสานขอรับการสนับสนุนจากหน่วยงานอื่นที่เกี่ยวข้องหรือขอรับการสนับสนุนจากหน่วยงานอื่นที่เกี่ยวข้องหรือขอรับการสนับสนุน จนท.สสท.ทร. เข้าร่วมปฏิบัติการตามความจำเป็นและเหมาะสม

๔.๒.๔ ในกรณีที่ปรากฏว่าภัยที่เกิดขึ้นจากระบบเทคโนโลยี ให้ถือว่าการรักษาข้อมูลสารสนเทศเพื่อการบริหารเป็นสิ่งที่สำคัญที่สุด หากจำเป็นให้ทำการขนย้ายวัสดุอุปกรณ์และระบบฐานข้อมูลสารสนเทศออกจากบริเวณเกิดภัยพิบัติฉุกเฉินทันที

๔.๒.๕ ความสม่ำเสมอในการตรวจสอบระบบ โดยใช้โปรแกรมป้องกันมัลแวร์ และ Firewall

๔.๒.๖ ต้องใช้วัสดุอุปกรณ์ที่ได้มาตรฐานและกำหนดมาตรฐานในการควบคุมดูแล ในกรณีที่มีการเก็บรักษาข้อมูลสารสนเทศที่อาจก่อให้เกิดผลกระทบต่อการดำเนินงานด้านระบบสารสนเทศ

๕. ขั้นตอนการปฏิบัติการ/และการป้องกันฉุกเฉินด้านสารสนเทศ

๕.๑ การฟื้นฟู

๕.๑.๑ หน่วยงานที่ประสบภัยพิบัติฉุกเฉิน ประเมินค่าความเสียหาย

๕.๑.๒ ปรับปรุงแก้ไขให้สถานการณ์คืนสู่สภาพปกติ กู้ข้อมูลคืนในกรณีที่เห็นว่าสามารถดำเนินการได้เอง

๕.๑.๓ กรณีที่ไม่สามารถดำเนินการได้ ให้รายงานความเสียหาย ประมาณการค่าความเสียหายให้ ฐท.สส. ทราบ เพื่อขอสนับสนุนงบประมาณต่อไป

๕.๒ แนวทางปฏิบัติการบำรุงรักษาทั่วไปเพื่อป้องกันภัยพิบัติฉุกเฉินด้านสารสนเทศ

๕.๒.๑ มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้ โดยผู้ดูแลเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบต่อพ่วง รวมถึงการมีการรับประกันความเสียหายจากผู้ขายและมีการดูแลอย่างถูกต้องและต่อเนื่อง

๕.๒.๒ ปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

๕.๒.๓ ทำความสะอาดเครื่องคอมพิวเตอร์อยู่เสมอ และมีการตรวจสอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

๕.๒.๔ ใช้คำสั่งของระบบปฏิบัติการในการบำรุงรักษาเครื่องเป็นประจำ

๕.๒.๕ การฝึกอบรมผู้ดูแลระบบและผู้ใช้งานให้มีความรู้ความเข้าใจในระบบงาน รวมถึงการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ

๕.๒.๖ การจัดเตรียมอุปกรณ์ที่จำเป็นในการเตรียมความพร้อมรับภัยพิบัติฉุกเฉินที่จะเกิดขึ้นต่อระบบสารสนเทศ ดังนี้

๕.๒.๖.๑ แผ่น Startup ระบบปฏิบัติการ

๕.๒.๖.๒ แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานต่าง ๆ

๕.๒.๖.๓ แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

๕.๒.๖.๔ แผ่นโปรแกรมป้องกันโปรแกรมประสงค์ร้าย

๕.๒.๖.๕ แผ่น Driver อุปกรณ์ต่าง ๆ

๕.๒.๖.๖ ระบบสำรองไฟฉุกเฉิน

๕.๒.๖.๗ อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๖. การสำรองข้อมูลและการกู้คืนข้อมูล

๖.๑ การสำรองข้อมูล (Back Up) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ให้ทำการสำรองข้อมูลไว้ใน External Hard disk , USB Flash Drive , DVD/CD หรือติดตั้งระบบ Backup อื่น ๆ เพื่อให้มีความพร้อมในการใช้งานและป้องกันข้อมูลสูญหายของข้อมูลในระบบสารสนเทศ โดยให้ทำการสำรองข้อมูลไว้ดังนี้

๖.๑.๑ การ Backup ข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายให้ Backup ไว้ที่เครื่องคอมพิวเตอร์แม่ข่ายสำรองข้อมูล (Backup Server) ที่เวลา ๑๖๐๐ ของทุกวัน

๖.๑.๒ การ Backup ข้อมูลของหน่วยงาน ให้เจ้าหน้าที่ประจำเครื่องนั้น ๆ ทำการ Backup ข้อมูลลงใน External Hard disk หรือสื่อบันทึกข้อมูลทุกสัปดาห์ และหากเป็นการสำรองข้อมูลที่มีชั้นความลับ จะต้องมีมาตรการควบคุมการเข้าถึงข้อมูล เช่น การใส่รหัสผ่าน การเข้ารหัส เป็นต้น

๖.๑.๓ ลงคำสั่งแต่งตั้งเจ้าหน้าที่รับผิดชอบงานรักษาความปลอดภัยระบบสารสนเทศไว้อย่างชัดเจนเป็นลายลักษณ์อักษร

๖.๑.๔ กำหนดให้มีการทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบว่าข้อมูลและโปรแกรมต่าง ๆ ที่สำรองไว้มีความถูกต้องครบถ้วน และสามารถใช้งานได้จริง

๖.๑.๔ จัดเก็บข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัยและติดป้ายแสดงไว้อย่างชัดเจน

๗. การตรวจสอบการเข้าสู่ระบบ

๗.๑ กำหนดสิทธิให้แก่ผู้ใช้งาน

๗.๑.๑ กำหนดสิทธิการเข้าถึงระบบสารสนเทศ เช่น กำหนดสิทธิในการเข้าใช้ระบบให้แก่ผู้ใช้งานให้เหมาะกับหน้าที่และความรับผิดชอบ

๗.๑.๒ กำหนดระยะเวลาการใช้งานของ User และ Password และต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๗.๑.๓ กำหนดให้มีการเปลี่ยนแปลงรหัสผ่านอย่างรอบคอบและมีชั้นความลับ

๗.๑.๔ ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น จะต้องขออนุญาตจากผู้มีอำนาจหน้าที่เพื่อให้การอนุมัติทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นในการเข้าใช้งาน

๗.๒ ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

๗.๒.๑ กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากล ไม่ควรต่ำกว่า ๘ ตัว

๗.๒.๒ องค์ประกอบของรหัสผ่านจะต้องมีตัวเลข (0-9) ตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่ (A-Z) ตัวพิมพ์เล็ก (a-z) และควรใช้อักขระพิเศษประกอบด้วย เช่น @ ; < > # เป็นต้น

๗.๒.๓ สำหรับผู้ใช้งานทั่วไปควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุก ๖ เดือน ส่วนผู้ดูแลระบบควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

๗.๒.๔ ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรจะกำหนดรหัสผ่านใหม่ซ้ำรหัสเดิม และควรคาดเดาได้ยาก

๗.๒.๕ ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ไม่เปิดเผยรหัสผ่านให้แก่ผู้อื่น หรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตนเองหรือไม่ใช้รหัสผ่านร่วมกับผู้อื่น ทั้งในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที