แผนการจัดการหรือแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

พ.ศ. ๒๕๖๓

โดย

ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์
กรมประชาสัมพันธ์

คำนำ

ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์ ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่มีความสำคัญยิ่งต่อการบริหารระบบราชการ จำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา ดังนั้น เพื่อลดความเสี่ยงต่าง ๆ อันอาจจะเกิดขึ้นกับระบบสารสนเทศ จึงได้จัดทำแผนการจัดการหรือแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการบำรุงรักษาและป้องกันแก้ไขปัญหาอันอาจส่งผลกระทบต่อข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ โปรแกรมระบบฐานข้อมูลระบบเครือข่ายสารสนเทศของกรมประชาสัมพันธ์

ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์
กรมประชาสัมพันธ์

สารบัญ

ภาคผนวก

แผนการจัดการหรือแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๑. หลักการและเหตุผล

กรมประชาสัมพันธ์ ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานและให้บริการประชาชนได้รับความสะดวก ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตีจากผู้ไม่หวังดี (Hacker) จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการดำเนินงานของกรมประชาสัมพันธ์ เพื่อป้องกันและแก้ไขปัญหาดังกล่าว โดยศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์ ได้เล็งเห็นความจำเป็นที่จะต้องมีแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของหน่วยงานต่าง ๆ ของกรมประชาสัมพันธ์

๓. เป้าหมาย

๓.๑ **ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database and Software)** เช่น ระบบเว็บไซต์หลักกรมประชาสัมพันธ์, ระบบถังรวมสื่อประชาสัมพันธ์, ฐานข้อมูลระบบรายงานผลการดำเนินงานตามแผนยุทธศาสตร์และแผนปฏิบัติราชการขององค์การ (PMS), ฐานข้อมูลเพื่อการบริหารจัดการภายใน (Back Office) ได้แก่ ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์, ระบบป้องกันไวรัสและการถูกโจมตีผ่านระบบเครือข่าย (Anti Virus), โปรแกรมระบบปฏิบัติการการบริหารจัดการเครือข่าย (Network Software) เป็นต้น

๓.๒ **อุปกรณ์คอมพิวเตอร์ (Hardware)** เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเน็ตเวิร์ค (Network Server), เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server), เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server), เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์องค์การ (Web Server), ระบบป้องกันการจู่โจมจากผู้ไม่ประสงค์ดี (Firewall), เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook), เครื่องสแกนเนอร์ (Scanner), เครื่องพิมพ์ (Printer), อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS), อุปกรณ์กระจายสัญญาณเครือข่าย (Switch), อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access Point) เป็นต้น

๔. <u>การประเมินสถานการณ์ความเสี่ยง</u>

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ โดยศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์ พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

๔.๑ เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรมสัมมนา ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด

๔.๒ ถูกโจมตีจากผู้ไม่หวังดี (Hacker) เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

๑) ติดตั้ง Firewall ทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องให้บริการ (server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย

๒) แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ต รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่าง ๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๔.๓ **เกิดจากระบบไฟฟ้าขัดข้อง** หรือความเสียหายจากเพลิงไหม้ โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บ และสำรองข้อมูลไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุม ป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่าง ๆ ในอาคารและทำป้ายบอกจุดติดตั้งเพื่อดับเพลิง

๔.๔ **เกิดจากโจรกรรม** การขโมยอุปกรณ์คอมพิวเตอร์ ในส่วนของห้องคอมพิวเตอร์แม่ข่ายได้กำหนดห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ เป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ติดตั้งเครื่องอ่านบัตรแบบแม่เหล็กและเครื่องอ่านลายนิ้วมือ เพื่อป้องกันไม่ให้บุคคลภายนอกเข้ามาในหน่วยงานโดยไม่ได้รับอนุญาต นอกจากนี้ได้มีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม บริเวณศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ และห้องคอมพิวเตอร์หลัก อีกด้วย

๕. <u>การเตรียมการเบื้องต้น</u>

๕.๑ **การสำรองข้อมูล (Back up)** เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีแนวทาง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูลไว้ในเทปบันทึกข้อมูล ตัวอย่างขั้นตอนการ Backup แสดงในภาคผนวก ก.

๕.๒ **การป้องกันไวรัสคอมพิวเตอร์** มีการติดตั้งซอฟแวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ โดยมีวิธีการดังนี้

๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัส
- อัพเดตข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่าง ๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยวันละ ๑ ช่วงเวลา

๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกหรือข้อมูลจากแหล่งต่างๆ เช่น แผ่นซีดี แฟลชไดร์ฟ ลิงก์จากอินเทอร์เน็ต เป็นต้น
- สแกนหาไวรัสจากสื่อบันทึกข้อมูลหรือจากแหล่งข้อมูล ก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลก ๆ ที่ไม่รู้จักหรือน่าสงสัย
  เช่น .pif, .exe, .com, .scr, .cmd, .bat, .hta, .reg, .vbs, .wsc, .wsf, .wsh
- ไม่ใช้สื่อบันทึกข้อมูลหรือลิงก์ข้อมูลที่ไม่ทราบแหล่งที่มา

๓) ใช้ความระมัดระวังในการเปิด E-mail
- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๔) ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่าง ๆ เช่น Line, FB MSN
- ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลดไฟล์ จาก Website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่าง ๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๕.๓ **การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง** เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ

๕.๔ **มีระบบป้องกันไฟไหม้** แบบไพโรเจนภายในห้องคอมพิวเตอร์หลัก และมีอุปกรณ์ดับเพลิงติดตั้งในทุกชั้นของอาคาร เพื่อการควบคุมเพลิงในเบื้องต้น พร้อมมีมาตรการในการป้องกันอัคคีภัย

๕.๕ **การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์** เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

๑) มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย และติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก มีการติดตั้งสายยูและกุญแจล็อก

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Security Cache เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์การและกลั่นกรองข้อมูลที่มาทาง Website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์การ เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๕) การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่าง ๆ ทั้งในส่วนกลาง และส่วนภูมิภาค ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ความรับผิดชอบ

๖) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับที่ ๒) จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๕.๖ **การจัดเตรียมอุปกรณ์ที่จำเป็น** ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

๑) แผ่นไฟล์ข้อมูลติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ ไฟล์ข้อมูลติดตั้งระบบงานที่สำคัญ

๒) เทปสำรองข้อมูลและระบบงานที่สำคัญ

๓) แผ่นโปรแกรม Antivirus/Spyware

๔) แผ่น Driver อุปกรณ์ต่าง ๆ

๕) ระบบสำรองไฟฉุกเฉิน

๖) อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๖. <u>การกำหนดผู้รับผิดชอบ</u>

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ โดยมีการจัดองค์การปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน

๖.๑ **ระดับนโยบาย** รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

๑) รองอธิบดีกรมประชาสัมพันธ์ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ประจำกรมประชาสัมพันธ์ (DCIO)

นางสุดฤทัย เลิศเกษม รองอธิบดีกรมประชาสัมพันธ์

๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์

นายเสมอ นิ่มเงิน ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศฯ

๖.๒ ระดับปฏิบัติ

๑) รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวนวางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ

นายพลี อุดมพรมนตรี	หัวหน้ากลุ่มพัฒนาระบบสารสนเทศการบริหาร
นายอนุสรณ์ อัครนิติ	หัวหน้ากลุ่มพัฒนาเทคนิคและเชื่อมโยงเครือข่าย
นางสาวศิริกาญจน์ บุญล้อ	หัวหน้ากลุ่มพัฒนาระบบสารสนเทศการประชาสัมพันธ์
นางณัฐกาญจน์ ตันเจริญ	หัวหน้าฝ่ายบริหารทั่วไป

โดยมีหน้าที่ ดังต่อไปนี้

- วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศฯ
- มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการระงับเหตุฉุกเฉิน จะมาถึงที่เกิดเหตุ
- อำนาจสั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ
- ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ท่านผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่
- ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น
- รายงานให้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว
- กำหนดอัตราเจ้าหน้าที่ วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต
- ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๒) รับผิดชอบดูแลบำรุงรักษา ระบบเครื่องแม่ข่าย ระบบเครือข่ายและระบบความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่าง ๆ ของระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งการสำเนาฐานข้อมูล

นายฑีภากรณ์ สำเภา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
นายจิรศักดิ์ โตรัตน์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
นายรังสรรค์ จันทร์เหล่าหลวง	นายช่างไฟฟ้าชำนาญงาน
นายเชษฐ์ สิงโต	นักวิชาการคอมพิวเตอร์

นายวิทวัส แก้วเวหา นักวิชาการคอมพิวเตอร์

นายอภิสิทธิ์ ดิษบรรจง นักวิชาการคอมพิวเตอร์

โดยมีหน้าที่ ดังต่อไปนี้

- กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง
- พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่น ๆ มาช่วย
- ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน
- ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด
- หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุอุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ประธานศูนย์ฯ ทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่
  - ทำการตรวจสอบระบบ Firewall
  - ทำการตรวจสอบ Virus, Worm, Spy ware
  - ทำการตรวจสอบ UPS
  - ทำการตรวจสอบ Transaction log files
  - ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
  - ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
  - ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
  - ทำการตรวจสอบค่า Configuration ของระบบ
- เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว
- ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทคู่สัญญาในการกู้และฟื้นคืนระบบ
- ทำการสำรองข้อมูลทุกวัน วันอาทิตย์-วันศุกร์ ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันเสาร์ทำการสำรองข้อมูลทั้งระบบ
- ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรมรายการฮาร์ดแวร์สำรอง สำเนาคู่มือ
- นำระบบสำรองข้อมูลออกมา Recovery เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๓) รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลสารสนเทศการบริหาร รวมทั้งการทำสำเนาฐานข้อมูล

นางสาวสโรชา ชามทอง	นักวิชาการคอมพิวเตอร์ชำนาญการ
นางสาวภิญญา แซ่แต้	นักวิชาการคอมพิวเตอร์ชำนาญการ
นายพุทธรัฐ ศิลาพันธ์	นักวิชาการคอมพิวเตอร์

โดยมีหน้าที่ดังต่อไปนี้

- เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว
- ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทคู่สัญญาในการกู้ระบบ
- ทำการสำรองข้อมูลทุกวัน วันอาทิตย์-วันศุกร์ ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันเสาร์ทำการสำรองข้อมูลทั้งระบบ
- ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรมรายการฮาร์ดแวร์สำรอง สำเนาคู่มือ
- นำระบบสำรองข้อมูลออกมา Recovery เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๔) รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลสารสนเทศการประชาสัมพันธ์ รวมทั้งการทำสำเนาฐานข้อมูล

นายณเรนธร จาดพันธุ์อินทร์	นักวิชาการคอมพิวเตอร์ชำนาญการ
นางสาวบัวชมพู เพิกสวน	นักวิชาการคอมพิวเตอร์
นางสาวพัชรินทร์ เสาวรส	นักวิชาการคอมพิวเตอร์
นางสาวกันต์ แว่นจง	นักวิชาการคอมพิวเตอร์

โดยมีหน้าที่ดังต่อไปนี้

- เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว
- ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทคู่สัญญาในการกู้ระบบ
- ทำการสำรองข้อมูลทุกวัน วันอาทิตย์-วันศุกร์ ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันเสาร์ทำการสำรองข้อมูลทั้งระบบ

- ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรมรายการฮาร์ดแวร์สำรอง สำเนาคู่มือ
- นำระบบสำรองข้อมูลออกมา Recovery เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๕) รับผิดชอบในการรักษาความปลอดภัยทั่วไป

นางสุนียา เจนร่วมจิต	เจ้าพนักงานธุรการชำนาญงาน
นางสุภาพร อรรถปักษ์	เจ้าพนักงานธุรการชำนาญงาน
นางสาวรัสรินทร์ ธนวิชญ์วรภัทร์	เจ้าพนักงานธุรการปฏิบัติงาน
นางสาวธิดาพร บุญกว้าง	เจ้าพนักงานธุรการปฏิบัติงาน

โดยมีหน้าที่ดังต่อไปนี้

- แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว
- ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัยระบบสารสนเทศนำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

๗. <u>มาตรการความปลอดภัยด้วยรหัสผ่าน</u>

มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศ ไม่สามารถเข้าถึง แก้ไข เปลี่ยนแปลง ข้อมูล หรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง โดย

๗.๑ กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้าในระบบได้ตามความรับผิดชอบ (Access) โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละระดับฐานข้อมูล ดังนี้

๑) บุคคลที่สามารถเรียกดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถแก้ไข ปรับปรุงข้อมูลได้

๒) บุคคลที่สามารถเรียกดูข้อมูลและแก้ไข ปรับปรุงข้อมูลในส่วนที่ผู้ใช้รับผิดชอบต่อความถูกต้องของข้อมูลในฐานข้อมูลนั้น

๓) บุคคลที่สามารถเรียกดู แก้ไข ปรับปรุงข้อมูลระดับฐานข้อมูล ในกรณีที่ผู้ใช้มีข้อผิดพลาดในการปรับปรุงข้อมูล ผู้รับผิดชอบของหน่วยงานเจ้าของหน่วยงานเป็นผู้ดูแล แก้ไข ข้อมูลในส่วนนี้ ซึ่งการเข้าใช้ฐานข้อมูลในแต่ละระบบจะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูล ตามหน้าที่ความรับผิดชอบของผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูล โดยมีการกำหนด Log in และ Password ในการ

เข้าถึงข้อมูลและผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงและเปลี่ยนแปลงแก้ไขข้อมูลได้ ผู้ใช้ระบบทั่วไปที่ผู้บังคับบัญชาที่เป็นหน่วยงานเจ้าของระบบ เป็นผู้อนุมัติให้ดำเนินการได้ โดยจะแบ่งเป็นการดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถเปลี่ยนแปลงแก้ไขได้ และการที่สามารถปรับปรุงข้อมูลได้ ทั้งนี้ เพื่อเป็นการรักษาความปลอดภัยของฐานข้อมูล

๗.๒ กำหนดระยะเวลาการใช้งานระบบสารสนเทศของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้

๗.๓ การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๖ ตัวอักษร และควรใช้ ตัวเลข อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ ๖ เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

๘. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๘.๑ กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว

๓) ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสาย ในชั้นนั้นออกให้หมด

๘.๒ กรณีเครื่องบริการ (Server) และอุปกรณ์เครือข่าย

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๕) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗) ผู้ดูแลระบบต้องรีบรายงานบังคับบัญชาตามลำดับชั้นจนถึงผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์ทราบโดยเร็ว

๘.๓ กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

๑) ติดตั้งโปรแกรม Anti-virus

๒) ใช้งานโปรแกรม Anti-virus

๘.๔ กรณีเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งานไม่ได้ ให้แจ้งผู้ดูแลระบบสารสนเทศหรือผู้ที่ได้รับมอบหมายในการสนับสนุนด้านเทคนิคของแต่ละหน่วยงาน

๘.๕ กรณีเมนบอร์ดหรือฮาร์ดดิสก์

กรณีเมนบอร์ดเสียหาย

๑) ทำการจัดหาเมนบอร์ด Main board หรือ Mother board มาเปลี่ยน (อาจใช้วิธีในการจัดหามาก่อนแล้วจัดซื้อตามในตอนหลัง) จากนั้นถอดเมนบอร์ดเดิมที่ชำรุดออกแล้วติดตั้งเมนบอร์ดใหม่แทน แล้วทำการเปิดระบบใช้งานตามปกติ

กรณีฮาร์ดดิสก์เสียหาย

๑) จัดหาฮาร์ดดิสก์มาเปลี่ยน

๒) ติดตั้งระบบปฏิบัติการ และระบบเครือข่าย

๓) นำ Backup ที่ได้จัดทำไว้มาทำ Recovery เพื่อนำข้อมูลเดิมกลับมาใช้เหมือนเดิม

๔) ทำการรันเครื่องทำงานตามเดิม

๘.๖ กรณีเกิดอัคคีภัย ตัวอย่างขั้นตอนการ Backup แสดงในภาคผนวก ข.

๙. <u>แผนกู้ระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม</u>

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติ ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕) นำ BACKUP TAPE / DVD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบ (ผู้ดูแลระบบ และทีมงานจากบริษัทฯ ที่จัดจ้างบำรุงรักษาระบบสารสนเทศ) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๖) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูล และระบบอื่น ๆ ที่เกี่ยวข้อง

๑๐.<u>การติดตามและรายงานผล</u>

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และรายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้

๑๑. <u>ผู้เสนอ</u>

ลงชื่อ.....ผู้เสนอ

(นายเสมอ นิ่มเงิน)

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์

กรมประชาสัมพันธ์

๑๒. <u>ผู้เห็นชอบ</u>

ลงชื่อ.....ผู้เห็นชอบ

(นางสุดฤทัย เลิศเกษม)

รองอธิบดีกรมประชาสัมพันธ์

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

ประจำกรมประชาสัมพันธ์ (DCIO)

๑๓. <u>ผู้อนุมัติ</u>

พลโท.....ผู้อนุมัติ

(สรรเสริญ แก้วกำเนิด)

อธิบดีกรมประชาสัมพันธ์

ภาคผนวก ก.

<u>การสำรองและกู้คืนข้อมูล</u>

(Backup and Recovery)

๑. แนวทางปฏิบัติในการสำรองข้อมูลและระบบงาน

จัดทำแผนสำรองข้อมูลและระบบงาน

๑.๑ จัดทำทะเบียนข้อมูลและระบบงานทั้งหมดของกรมพร้อมจัดลำดับความสำคัญ

๑.๒ กำหนดผู้รับผิดชอบในการดำเนินการสำรองข้อมูลและระบบงาน

๑.๓ กำหนดรายละเอียดของรายการข้อมูลที่ต้องดำเนินการสำรอง ขั้นตอนและความถี่

๑.๔ ดำเนินการสำรองข้อมูลและระบบตามที่กำหนดไว้ พร้อมกับการตรวจสอบความสมบูรณ์ของการสำรองแต่ละครั้ง

๑.๕ นำสื่อที่ได้สำรองข้อมูลและระบบงานเก็บในสถานที่ที่กำหนดไว้

๑.๖ รายงานผลการปฏิบัติงานตามสายงานการบังคับบัญชา

๒. แนวทางปฏิบัติในการกู้คืนข้อมูลและระบบงาน

จัดทำแผนกู้คืนข้อมูลและระบบงาน

๒.๑ กำหนดผู้รับผิดชอบในการดำเนินการกู้คืนข้อมูลและระบบงาน

๒.๒ ทดสอบการกู้คืนข้อมูลและระบบงานตามแผน

๒.๓ ตรวจสอบทะเบียนข้อมูลและระบบงาน

๒.๔ นำสื่อสำรองข้อมูลและระบบงานจากสถานที่เก็บ

๒.๕ ดำเนินการกู้คืนข้อมูลและระบบงาน

๒.๖ ตรวจสอบความสมบูรณ์ของข้อมูลและระบบที่ได้จากการกู้คืน

๒.๗ ทดสอบการปฏิบัติงานตามคู่มือข้อมูลและระบบงานที่กู้คืนแต่ละระบบหรือทั้งหมด

๒.๘ รายงานผลการปฏิบัติงานตามสายงานการบังคับบัญชา

ภาคผนวก ข.

หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัย

เพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติของบุคลากรในศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ ดังนี้

๑. ไม่กระทำการใด ๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๒. ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

๓. ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบดูทางออกฉุกเฉินไม่ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางออกจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉินทั้งสองทาง เพื่อให้ไปถึงทางหนีฉุกเฉินได้ ถึงแม้ว่าไฟจะดับหรือปกคลุมไปด้วยควัน

๔. เมื่อเกิดเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้จากนั้นหนีจากอาคารแล้วโทรศัพท์แจ้งหน่วยดับเพลิง โทร ๑๙๙ ทันที หรือแจ้ง ๑๖๖๙

๕. เมื่อได้ยินเสียงสัญญาณเตือนไฟไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

๖. ถ้าเพลิงไหม้ในห้องทำงานให้หนีออกมาแล้วปิดประตูห้องทันที รีบแจ้งฝ่ายอาคารและสถานที่เพื่อโทรศัพท์แจ้งหน่วยดับเพลิงต่อไป

๗. ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อย ๆ เปิดประตู แล้วหนีไปยังทางหนีไฟฉุกเฉินที่อยู่ใกล้ที่สุด

๘. ถ้าเพลิงไหม้อยู่บริเวณใกล้ ๆ ประตู ประตูจะมีความร้อน ห้ามเปิดประตูเด็ดขาด ให้รีบโทรศัพท์เรียกหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งถูกเพลิงไหม้ หาผ้าเช็ดตัวเปียก ๆ ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๙. เมื่อต้องเผชิญกับควันไฟที่ปกคลุม ให้ใช้วิธีคลานหนีไปทางฉุกเฉินเพราะอากาศบริสุทธิ์จะอยู่ด้านล่าง (เหนือพื้นห้อง) นำกุญแจห้องทำงานไปด้วยหากหมดหนทางหนีจะได้สามารถกลับเข้าห้องได้

๑๐. ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ จะมีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับสูงมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากที่จะหลีกเลี่ยงได้ ก็คือผลกระทบต่าง ๆ ที่เกิดขึ้นจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์หรือการสูญหายของข้อมูลที่สำคัญ รวมถึงการสูญเสียเวลา จากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ซึ่งประกอบด้วย

๑. ไฟฟ้าตก (Sag หรือ Brownout)

ไฟฟ้าตก คือ สภาวะที่แรงดันไฟฟ้าลดต่ำลงจากปกติในช่วงเวลาสั้น ๆ ซึ่งเป็นปัญหาทางไฟฟ้าที่พบบ่อยที่สุด

สาเหตุ เกิดจากการเปิดสวิทช์อุปกรณ์บางชนิดที่ต้องการใช้กระแสไฟฟ้ามากในการติดเครื่อง เมื่อเทียบกับการทำงานในภาวะปกติ ส่งผลให้แรงดันไฟฟ้าในสายส่งการไฟฟ้าฯ ลดต่ำลง

๒. ไฟฟ้าดับ (Blackout)

ไฟฟ้าดับ คือ เกิดจากความต้องการกระแสไฟฟ้าจากสายส่งการไฟฟ้าฯ ที่มาเกินไป, เกิดไฟฟ้าลัดวงจรในสายส่ง, พายุฟ้าคะนอง, แผ่นดินไหล

สาเหตุ ปัญหาที่เกิดขึ้นกับสายส่งการไฟฟ้าฯ เช่น เสาไฟฟ้าล้ม หรือหม้อแปลงระเบิด ฯลฯ ซึ่งส่งผลให้ไม่สามารถจ่ายไฟจากการไฟฟ้าได้

ผลกระทบ การทำงานของ RAM หยุดชะงักทันที ทำให้ข้อมูลปัจจุบันสูญหายได้รวมถึงการบันทึกข้อมูลของตารางการจัดการแฟ้ม (FAT) สูญหายได้ มีผลให้ข้อมูลที่เก็บไว้ทั้งหมดสูญหายได้

๓. ไฟฟ้ากระชาก (Spike)

ไฟฟ้ากระชาก คือ สภาวะที่แรงดันไฟฟ้าเพิ่มสูงขึ้นอย่างกระทันหัน โดยสามารถเข้าไปยังอุปกรณ์ไฟฟ้า ได้ทั้งจากสายส่งการไฟฟ้าฯ เครือข่ายสื่อสาร และสายโทรศัพท์

สาเหตุ เกิดจากฟ้าผ่าในบริเวณใกล้เคียง หรืออาจเกิดจากสายส่งการไฟฟ้าฯ ที่หยุดการทำงานไปและกลับมาทำงานใหม่อย่างกระทันหัน

ผลกระทบ สร้างความเสียหายหรือทำลายชิ้นส่วนอุปกรณ์อิเล็กทรอนิกส์ของอุปกรณ์ไฟฟ้าได้ รวมถึงข้อมูลเกิดการสูญหาย

๔. ไฟฟ้าเกิน (Surge)

ไฟฟ้าเกิน คือ สภาวะที่มีแรงดันไฟฟ้าไหลมามากเกินในช่วงเวลาสั้น (๑/๒๐ วินาที)

สาเหตุ เกิดจากการใช้อุปกรณ์ไฟฟ้าที่มีมอเตอร์กินไฟมาก เช่น เครื่องปรับอากาศ หรืออุปกรณ์ไฟฟ้าอื่น ๆ ที่มีลักษณะใกล้เคียงกัน ฯลฯ เนื่องจากอุปกรณ์เหล่านี้เมื่อหยุดทำงาน แรงดันไฟฟ้าส่วนหนึ่งที่เหลืออยู่ในมอเตอร์ จะไหลกลับเข้าไปในสายส่งการไฟฟ้าฯ ทำให้เกิดแรงดันไฟฟ้าสูงเกิน

ผลกระทบ ทำให้ชิ้นส่วนอุปกรณ์ภายในเสื่อมสภาพเร็วกว่าปกติหรือเสียหายได้ รวมถึงหน่วยความจำของคอมพิวเตอร์สูญหายและคลาดเคลื่อน, Power Supply เสียหาย และการทำงานของระบบสื่อสารผิดพลาด

๕. สัญญาณรบกวน (Noise)

สัญญาณรบกวน คือ สัญญาณรบกวนที่เกิดจากสนามแม่เหล็กไฟฟ้า (EMI) และสัญญาณคลื่นความถี่วิทยุ (RFI) ซึ่ง ๒ สัญญาณเหล่านี้จะไปรบกวนสัญญาณคลื่นไซน์ (Sine Wave) ของสายส่งการไฟฟ้าฯ

สาเหตุ เกิดขึ้นได้จากปรากฏการณ์ทางธรรมชาติ (เช่น ฟ้าผ่า), การเปิด-ปิดสวิทช์อุปกรณ์ไฟฟ้า, เครื่องส่งวิทยุ เป็นต้น โดยสัญญาณรบกวนอาจเกิดขึ้นเป็นระยะ ๆ หรืออาจเกิดอย่างสม่ำเสมอก็ได้

ผลกระทบ ทำให้การประมวลผลของโปรแกรมและแฟ้มข้อมูลทำงานผิดพลาดและเกิดข้อบกพร่อง

ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ ได้มีการป้องกันปัญหาจากกระแสไฟฟ้าดังกล่าวโดยการติดตั้งเครื่องสำรองไฟฟ้า โดยการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply: UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC)

หลักปฏิบัติของบุคลากร

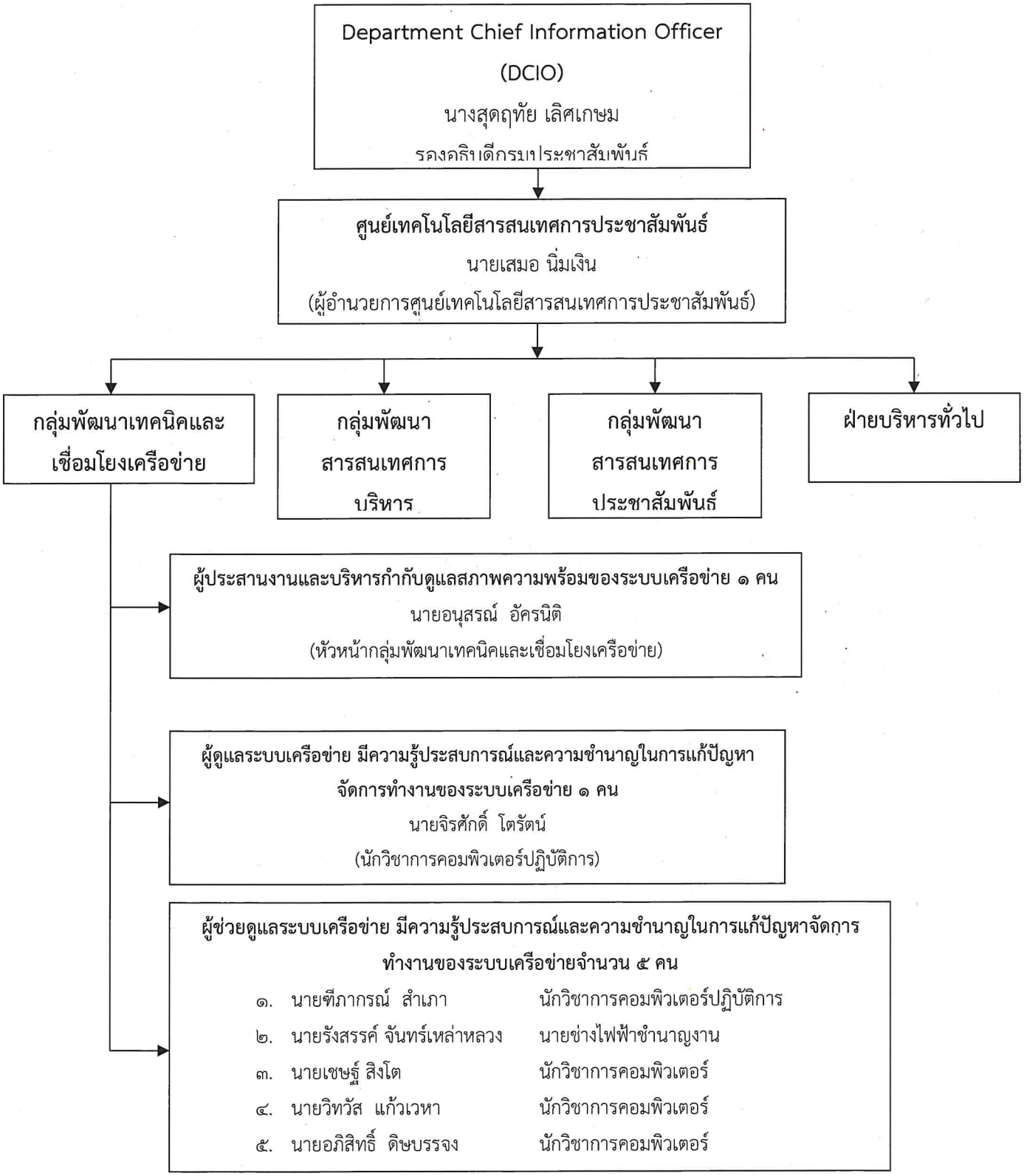
เพื่อป้องกันมิให้เกิดความเสียหายอันเกิดจากกระแสไฟฟ้า และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดปัญหาจากกระแสไฟฟ้า จึงกำหนดหลักปฏิบัติของบุคลากรในสังกัดของศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์ดังนี้

๑. เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์ทั้งเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล

๒. เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safely) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กรมประชาสัมพันธ์

ภาคผนวก ค.

<u>แผนผังสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน</u>



ติดต่อศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์
โทร ๐๒-๖๑๘-๒๓๒๓ ต่อ ๑๐๑๕
e-mail : itsupport@prd.go.th