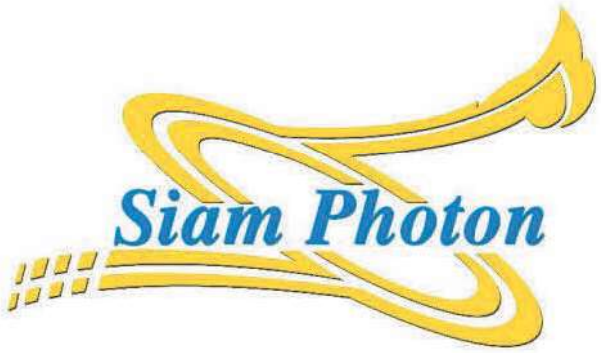

แผนรองรับสถานการณ์ฉุกเฉิน

(IT Contingency Plan)

สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน) (สซ.)

พ.ศ. ๒๕๖๘

โดย ส่วนเทคโนโลยีสารสนเทศและสื่อสาร

สารบัญ

แผนรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

บทนำ

ปัจจุบัน สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน). มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น องค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน) หรือต่อไปนี้เรียกว่า “สซ.” จึงได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของ สซ. และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของ สซ. ดังนั้น เพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

(๑) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

(๒) เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

(๓) เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

(๔) เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ สซ.

(๕) เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของ สซ.

การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของ สซ.สามารถจำแนกได้เป็น ๒ กลุ่มหลัก ๆ ได้แก่

(๑) ภัยพิบัติจากภายนอก

- ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ
- การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง
- ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ
- การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
- ไวรัสคอมพิวเตอร์

(๒) ภัยพิบัติจากภายใน

- ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย
- ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร
- เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดทำงาน

การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อ สซ. มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่าง ๆ (Security Log Management System) โดยเจ้าหน้าที่ส่วนเทคโนโลยีสารสนเทศ เพื่อนำมาสรุปเป็นข้อมูลต่อไปนี้

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน ๕ คะแนน)			คะแนนรวม	จัดเรียงลำดับ
	ต่อระบบงาน	ต่อพันธกิจ	ต่อผู้ใช้บริการ		
ไฟไหม้	๕	๕	๕	๑๕	๑
ไฟฟ้าดับ	๕	๓	๕	๑๓	๒
โดนเจาะระบบ	๕	๓	๕	๑๓	๒
น้ำท่วม / น้ำรั่ว	๔	๒	๔	๑๐	๓
พายุ	2	1	5	๘	๔
สถานการณ์ทางการเมือง	2	2	2	๖	๕

แนวทางการป้องกันและการเตรียมการเบื้องต้น

การประกาศแผน (Activation)

สซ. ต้องการประกาศใช้แผนรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน หัวหน้าส่วนเทคโนโลยีสารสนเทศและสื่อสารจะทำการแจ้งให้ CIO หรือ CEO ของ สซ. ทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

กระบวนการดำเนินงาน (Procedure)

ส่วนเทคโนโลยีสารสนเทศและสื่อสารจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติใน สซ. โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ทีเกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่าง ๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อหน่วยงานภายนอก เพื่อใช้สำหรับติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ ผู้ให้บริการเครือข่าย เป็นต้น

การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของส่วนงานเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- เทปสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม antivirus/spyware
- แผ่น driver อุปกรณ์ต่าง ๆ
- ระบบสำรองไฟฉุกเฉิน
- อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดย สซ. มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์และแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

การเตรียมความพร้อมและการดำเนินการรองรับสถาการณ์ฉุกเฉิน

(๑) การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

(๑.๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

(๑.๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๑.๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ

(๑.๔) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือน เป็นอย่างน้อย

(๒) การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุไฟไหม้ เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

(๒.๑) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เพื่อการควบคุมเพลิงเบื้องต้น

(๒.๒) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือน เป็นอย่างน้อย

(๓) การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม/น้ำรั่ว เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม/น้ำรั่ว ซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

(๓.๑) มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

(๓.๒) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือน เป็นอย่างน้อย

(๓.๓) หากเกิดเหตุน้ำท่วม/น้ำรั่ว ให้ผู้ดูแลระบบทำการปิดระบบแลเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ บริเวณอื่นที่ไม่มีผลกระทบ

(๓.๔) ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

(๓.๕) ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดการเพื่อให้สามารถดำเนินการได้

(๔) การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส

(๔.๑) ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

(๔.๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ที่ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้

(๔.๓) อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย

(๔.๔) ให้เจ้าหน้าที่ส่วนงานเทคโนโลยีสารสนเทศแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่อง สม่ำเสมอรวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

(๔.๕) กรณีถูกไวรัส เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่น ๆ ในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อระบบเครือข่าย

(๔.๖) วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

(๔.๗) ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

(๔.๘) ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการไข

(๔.๙) กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่ส่วนงานเทคโนโลยีสารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ส่วนงานเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ส่วนงานจะต้องประกาศให้ทุกหน่วยงานภายในทราบ

(๕) การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก การโจมตีระบบเครือข่าย และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๕.๑) กำหนดมาตรการควบคุมการเข้าออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ หากจำเป็นต้องเข้าไป ให้มีเจ้าหน้าที่ของส่วนงานเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน

(๕.๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

(๕.๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของ สซ. และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

(๕.๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของ สซ. เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศที่มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

(๕.๕) มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

(๕.๖) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ได้เป็นอย่างดี

(๕.๗) กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก Log และตรวจสอบการตั้งค่าของ Firewall ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้และแจ้งให้ CIO หรือ CEO ให้ทราบโดยด่วน

(๕.๘) กรณีการเชื่อมโยงเครือข่ายล้มเหลว ผู้ดูแลระบบต้องรีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

(๖) การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่ส่วนงานต่าง ๆ ภายใน สซ. ขาดทักษะความรู้ความเข้าใจในเครื่องมือและอุปกรณ์คอมพิวเตอร์ ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจด้านฮาร์ดแวร์ และซอฟต์แวร์เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

(๖.๑) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศโดยเจ้าหน้าที่ สซ. เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

(๖.๒) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานเครือข่ายคอมพิวเตอร์ จัดทำคู่มือการใช้งานระบบคอมพิวเตอร์และเครือข่าย เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

(๗) การเตรียมความพร้อมรับสถานการณ์จากอุปกรณ์จัดเก็บข้อมูลเสียหาย ผู้ดูแลระบบแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ และรีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลทดแทน และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว จากนั้น ทดสอบความสมบูรณ์ของข้อมูลและแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

(๘) การเตรียมความพร้อมรับสถานการณ์จากกรณีแผ่นดินไหว

(๘.๑) ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ผู้ดูแลระบบ

(๘.๒) ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้

(๘.๓) เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

(๙) การเตรียมความพร้อมรับสถานการณ์จากกรณีความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

(๙.๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งให้ CIO หรือ CEO ให้ทราบโดยด่วน

(๙.๒) หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุดเสียหาย ซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการแก้ไข

(๑๐) การเตรียมความพร้อมรับสถานการณ์จากกรณีโจรกรรม

(๑๐.๑) ผู้ปฏิบัติงานแจ้งให้ผู้บังคับบัญชาให้ทราบโดยด่วน

(๑๐.๒) สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

(๑๐.๓) ผู้ดูแลระบบบริบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

(๑๑) การเตรียมความพร้อมรับสถานการณ์จากกรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

(๑๑.๑) แจ้งให้ผู้บังคับบัญชาทราบ

(๑๑.๒) ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เป็นดังนี้

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงานได้แก่

(๑.๑) ผู้อำนวยการสถาบันวิจัยแสงซินโครตรอน

(๑.๒) รองผู้อำนวยการสนับสนุนเทคนิคและวิศวกรรม

(๑.๓) หัวหน้าฝ่ายพัฒนาเทคนิคและวิศวกรรม ที่ดูแลส่วนเทคโนโลยีสารสนเทศและสื่อสาร

(๒) รับผิดชอบปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ตรวจสอบรายการทรัพย์สิน และประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่ เจ้าหน้าที่ส่วนงานเทคโนโลยีสารสนเทศ