เอกสารแนบท้ายประกาศ

แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ
(IT Contingency Plan)
ของ สำนักงานเศรษฐกิจการเกษตร

คำนำ

ระบบข้อมูลสารสนเทศ ถือเป็นสินทรัพย์ที่มีความสำคัญต่อการดำเนินงานของสำนักงานเศรษฐกิจการเกษตร จำเป็นต้องได้รับการดูแลรักษา เพื่อให้เกิดความมั่นคงปลอดภัยด้านสารสนเทศ สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างต่อเนื่อง และมีประสิทธิภาพสูงสุด สำนักงานเศรษฐกิจการเกษตรได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศ ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยจากภายในมากระทบ ทำให้ระบบฐานข้อมูลและสารสนเทศ เกิดการชะงักงันหรือไม่สามารถปฏิบัติงานได้อย่างเป็นปกติ รวมทั้งระบบอุปกรณ์เสียหายได้

ดังนั้นจึงได้มีการจัดทำแผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการปฏิบัติ ดูแล รักษา และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ ของสำนักงานเศรษฐกิจการเกษตร ได้อย่างทันท่วงทีและมีประสิทธิภาพ

สารบัญ

แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ
(IT Contingency Plan)

๑. หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการปฏิบัติงานราชการ ทั้งในส่วนของการบริหารจัดการการจัดเก็บและรวบรวมข้อมูล รวมไปถึงการประมวลผลระบบงานที่สำคัญ เพื่อสนับสนุนการปฏิบัติงานให้มีประสิทธิภาพและสามารถนำข้อมูลไปใช้ในการวางแผนพัฒนาหน่วยงาน ตลอดจนนำข้อมูลไปใช้ในการวิเคราะห์ เพื่อการบริหารงานของผู้บังคับบัญชาระดับสูง สำนักงานเศรษฐกิจการเกษตรได้ดำเนินงานด้านระบบเทคโนโลยีสารสนเทศและมีการพัฒนาระบบมาอย่างต่อเนื่อง ซึ่งจากการนำระบบเทคโนโลยีที่ทันสมัยดังกล่าวมาใช้ในการปฏิบัติงาน ทำให้มีความเสี่ยงในด้านระบบฐานข้อมูลสารสนเทศเกิดขึ้น เช่น ความเสี่ยงที่เกิดจากการปฏิบัติงาน ความเสี่ยงจากโปรแกรมคอมพิวเตอร์ ความเสี่ยงจากไวรัสคอมพิวเตอร์

ดังนั้นจึงได้จัดทำแผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ (IT Contingency Plan) เพื่อให้สำนักงานเศรษฐกิจการเกษตรได้ใช้เป็นแนวทางในการดำเนินการป้องกันหรือลดผลกระทบจากความเสียหายที่อาจจะเกิดขึ้น

๒. นิยามศัพท์

(๑) หน่วยงาน หมายความว่า สำนักเศรษฐกิจการเกษตร ทั้งนี้ให้หมายรวมถึงหน่วยงานในสังกัดและกำกับ

(๒) ศูนย์ หมายความว่า ศูนย์สารสนเทศการเกษตร

(๓) ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) หมายความว่า เลขาธิการสำนักงานเศรษฐกิจการเกษตร

(๔) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) หมายความว่า รองเลขาธิการสำนักงานเศรษฐกิจการเกษตรที่ได้รับมอบหมายจากเลขาธิการสำนักงานเศรษฐกิจการเกษตรให้เป็นผู้รับผิดชอบด้านเทคโนโลยีสารสนเทศของหน่วยงาน

(๕) ผู้ใช้งาน หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ/ชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน

(๖) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๗) สินทรัพย์ หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับหน่วยงาน

(๘) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

(๙) ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๑๐) ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนการบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

(๑๑) การบริหารความเสี่ยง หมายถึง การบริหารจัดการและการเก็บรวบรวมข้อมูลอย่างเป็นระบบเพื่อไม่ให้ข้อมูลที่จัดเก็บเกิดการสูญหายอันเนื่องมาจากภัยพิบัติที่เกิดขึ้น

(๑๒) ภัยพิบัติ หมายถึง ภัยที่เกิดจากธรรมชาติและจากการกระทำของมนุษย์ที่มีระดับความรุนแรงและผลกระทบที่ต่างกันไป

๓. วัตถุประสงค์

(๑) เพื่อเตรียมความพร้อมและสามารถรองรับสถานการณ์หรือภัยพิบัติฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

(๒) เพื่อให้มีแผนบริหารความเสี่ยงและแผนแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศที่สามารถควบคุมและลดผลกระทบจากความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๓) เพื่อเป็นแนวทางในการกำกับดูแลตรวจสอบการบริหารจัดการข้อมูลสารสนเทศ รวมทั้งเป็นการเผยแพร่ความรู้เกี่ยวกับการบริหารความเสี่ยงและการแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศให้ผู้ที่เกี่ยวข้องได้นำไปใช้ประโยชน์

(๔) เพื่อให้การดำเนินงานเป็นไปตามกิจกรรมที่กำหนดไว้

(๕) เพื่อให้เกิดการรับรู้ตระหนักและเข้าใจถึงความเสี่ยงที่อาจเกิดขึ้นและหาวิธีการจัดการที่เหมาะสมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๔. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๔.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน สามารถจำแนกได้เป็น ๒ กลุ่มหลัก ๆ ได้แก่

ภัยพิบัติจากภายนอก

(๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้นอุณหภูมิ แผ่นดินไหว ฯลฯ

(๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

(๓) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

(๔) ระบบกระแสไฟฟ้าขัดข้อง

(๕) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

(๖) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

(๑) ระบบแม่ข่ายหลักระบบฐานข้อมูลหลักเสียหายหรือข้อมูลถูกทำลาย

(๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในหน่วยงาน

(๓) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน

๔.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อหน่วยงานมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัยจัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่าง ๆ (Security Log Management System) เพื่อนำมาสรุปเป็นข้อมูลต่อไป

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (๕ คะแนน)			คะแนนรวม	จัดเรียงลำดับ
	ต่อระบบงาน	ต่อพันธกิจตามกฎหมาย	ต่อประชาชน		
ไฟไหม้	๕	๕	๕	๑๕	๑
โดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์	๕	๓	๕	๑๓	๒
กระแสไฟฟ้าขัดข้อง / หม้อไฟระเบิด	๕	๑	๕	๑๑	๓
น้ำท่วม	๔	๒	๔	๑๐	๔
แผ่นดินไหว	๔	๑	๕	๑๐	๔
การชุมนุม/เหตุการณ์ความไม่สงบ	๒	๓	๔	๙	๕

๕. แนวทางการป้องกันและเตรียมการเบื้องต้น

๕.๑ การประกาศแผน (Activation)

หน่วยงานมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการศูนย์สารสนเทศการเกษตรจะทำการแจ้งให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) ของหน่วยงานทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

๕.๒ กระบวนการดำเนินงาน (Procedure)

ส่วนเทคโนโลยีสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติงานกับเหตุการณ์ที่ผิดปกติในหน่วยงาน โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้นทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุก เพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่าง ๆ ที่มีความสำคัญ ต้องมีการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๕.๓ การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน ทั้งการไฟฟ้า สถานีดับเพลิง และสถานีตำรวจที่ใกล้ที่สุด มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

๕.๔ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของส่วนเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ต้องมีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็น ในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้โดยเตรียมอุปกรณ์ ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- เทปสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม Antivirus/Spyware
- ระบบสำรองไฟฉุกเฉิน
- อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๕.๕ การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์จากผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ หน่วยงานต้องมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

๕.๖ การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ตเพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยหน่วยงานต้องกำหนดนโยบายป้องกันไวรัสและซอฟต์แวร์ประสงค์ร้าย (Virus and Malicious software Protection Policy)

๕.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

(๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

(๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๓) เมื่อเกิดกระแสกระแสไฟฟ้าขัดข้อง ให้ผู้ใช้งานรีบบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๕.๘ การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๑) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้เจ้าหน้าที่ของส่วนเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไปเจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

(๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

(๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของหน่วยงานและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

(๔) มีเจ้าหน้าที่ดูแลระบบเครือข่ายทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของหน่วยงาน เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

(๕) การดำเนินการตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๕.๙ การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็นกรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ ดังนี้

(๑) เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ

(๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

(๓) ควรทราบตำแหน่งวาล์วถังก๊าซน้ำประปาและสะพานไฟฟ้า

(๔) ไม่วางของหนักไว้บนชั้นหลังตู้หรือที่สูง

(๕) ผูกหรือยึดติดอุปกรณ์หรือเครื่องใช้ไฟฟ้าที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

(๖) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจนและเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

๖. การเตรียมความพร้อม

๖.๑ การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุไฟไหม้

การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุไฟไหม้ เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ห้องควบคุมระบบ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้น เพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

(๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

(๒) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่ายเพื่อการควบคุมเพลิงในเบื้องต้น

(๓) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๖.๒ การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุกระแสไฟฟ้าขัดข้อง/หม้อไฟระเบิด

การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุกระแสไฟฟ้าขัดข้อง/หม้อไฟระเบิด เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้น เพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

(๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากกระแสไฟฟ้าขัดข้อง/หม้อไฟระเบิด

(๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้า โดยประมาณ ๓๐-๖๐ นาที

(๓) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

(๔) เมื่อเกิดกระแสกระแสไฟฟ้าขัดข้อง ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ทำค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

(๕) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

๖.๓ การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุน้ำท่วม

การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุน้ำท่วม เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้น เพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

(๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม

(๒) มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

(๓) ให้มีการสำรองฐานข้อมูล เดือนละ ๑ ครั้งเป็นอย่างน้อย

๖.๔ การเตรียมความพร้อมรับสถานการณ์ เมื่อโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์

การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดกรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๑) กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย และการป้องกันความเสียหาย

(๒) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องจำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่าย ต้องให้เจ้าหน้าที่ของส่วนเทคโนโลยีสารสนเทศผู้ดูแลระบบเครือข่ายเป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้าออกมีการติดตั้งระบบ Access Control โดยใช้ Key Card และติดตั้งกล้องโทรทัศน์วงจรปิด เพื่อป้องกันการโจรกรรม

(๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยต้องมีการเปิดใช้งาน Firewall ตลอดเวลา

(๔) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

(๕) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

(๖) อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือนเป็นอย่างน้อย (Update Patch)

(๗) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของหน่วยงานเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

(๘) มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ต หรือใช้งานระบบเครือข่ายตามอำนาจหน้าที่และความรับผิดชอบ

(๙) ให้เจ้าหน้าที่ส่วนเทคโนโลยีสารสนเทศแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

๖.๕ การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดแผ่นดินไหว

การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดแผ่นดินไหว ให้เริ่มตั้งแต่ปัจจุบัน เพื่อติดตามสถานการณ์รวบรวมข้อมูลข่าวสารและประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัยที่เกิดขึ้นได้

(๑) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก ได้แก่

(ก) กรมอุตุนิยมวิทยา : www.tmd.go.th

(ข) ศูนย์เตือนภัยพิบัติแห่งชาติ : www.ndwc.thaigov.go.th

(ค) กรมทรัพยากรธรณี : www.dmr.go.th

(ง) กรมป้องกันและบรรเทาสาธารณภัย : www.disaster.go.th

(๒) การเตรียมคน สถานที่อพยพ และวัสดุอุปกรณ์

(ก) ประสานการเตรียมงานกับหน่วยกู้ภัย เพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน

(ข) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุอุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม

(ค) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรของหน่วยงาน

(ง) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

(จ) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

(๓) การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

(ก) สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบ เพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตาม ระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

(ข) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไขหรือรื้อถอน เพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

(๔) การปฏิบัติขั้นเตรียมการ

(ก) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม

(ข) การสำรวจและจัดทำบัญชีเป้าหมายพื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญภัย

(ค) อบรมให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่มแก่เจ้าหน้าที่บุคลากรในหน่วยงาน

(ง) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๖.๖ การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุชุมนุมประท้วงและก่อจลาจล

การเตรียมความพร้อมรับสถานการณ์ เมื่อเกิดเหตุชุมนุมประท้วงและก่อจลาจล เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

(๑) ดำเนินการหาข่าวจากแหล่งต่าง ๆ ที่เชื่อถือได้

(๒) จัดเตรียมกำลังเจ้าหน้าที่วัสดุอุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

(๓) ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ให้อยู่ในสภาพที่พร้อมใช้งาน

(๔) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๖.๗ การซักซ้อมเพื่อเตรียมการป้องกัน

ควรมีการซักซ้อมกระบวนการแก้ไขปัญหา อย่างน้อยปีละ ๑ ครั้ง

๗. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

๗.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้รับผิดชอบ ได้แก่

- เลขาธิการสำนักงานเศรษฐกิจการเกษตร (Chief Executive Officer: CEO)
- รองเลขาธิการสำนักงานเศรษฐกิจการเกษตร (Department Chief Information Officer: DCIO)
- ผู้อำนวยการศูนย์สารสนเทศการเกษตร (Information Security Manager)

๗.๒ ระดับปฏิบัติ

รับผิดชอบในการตรวจสอบและแก้ไขปัญหาตามภารกิจงานต่างๆ

(ก) ทีมบริหารจัดการการกู้คืนระบบ จัดการและประสานงานการกู้คืนต่าง ๆ

ผู้รับผิดชอบ ได้แก่

๑. นางสาวอรฉัตร รัตนรัตน์	เบอร์โทรศัพท์ติดต่อ	๐๘ ๘๘๙๘ ๘๐๔๗
๒. นางสาวพัชรนันท์ เสมพืช	เบอร์โทรศัพท์ติดต่อ	๐๘ ๖๙๖๔ ๑๖๒๙
๓. นายจิรพงษ์ สิทธิฤทธิ์	เบอร์โทรศัพท์ติดต่อ	๐๙ ๗๐๕๓ ๘๗๕๑
๔. นายรัฐพล ไชยถวิล	เบอร์โทรศัพท์ติดต่อ	๐๙ ๑๐๗๑ ๙๘๐๙

(ข) ทีมกู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ

ผู้รับผิดชอบ ได้แก่

๑. นางสาวอรฉัตร รัตนรัตน์	เบอร์โทรศัพท์ติดต่อ	๐๘ ๘๘๙๘ ๘๐๔๗
๒. นางสาวพัชรนันท์ เสมพืช	เบอร์โทรศัพท์ติดต่อ	๐๘ ๖๙๖๔ ๑๖๒๙
๓. นายจิรพงษ์ สิทธิฤทธิ์	เบอร์โทรศัพท์ติดต่อ	๐๙ ๗๐๕๓ ๘๗๕๑
๔. นายรัฐพล ไชยถวิล	เบอร์โทรศัพท์ติดต่อ	๐๙ ๑๐๗๑ ๙๘๐๙

(ค) ทีมกู้คืนแอปพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน

ผู้รับผิดชอบ ได้แก่

๑. นายสุชาติ ผุแปง	เบอร์โทรศัพท์ติดต่อ	๐๘ ๑๘๒๐ ๐๔๕๑
๒. นางสาวพนิดา ฮั้วประเสริฐ	เบอร์โทรศัพท์ติดต่อ	๐๙ ๐๔๔๑ ๔๒๑๙
๓. นางสาวสุมาลยา งานดี	เบอร์โทรศัพท์ติดต่อ	๐๘ ๑๖๑๒ ๒๙๖๑
๔. นายณัฏชา ตาเที่ยง	เบอร์โทรศัพท์ติดต่อ	๐๙ ๐๙๐๑ ๑๙๒๖

(ง) ทีมประเมินความเสียหาย ทีมให้ข้อมูลความเสียหายทั้งด้านฮาร์ดแวร์, ซอฟต์แวร์, ระบบเครือข่าย เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน

ผู้รับผิดชอบ ได้แก่

๑. นางสาวอรฉัตร รัตนรัตน์	เบอร์โทรศัพท์ติดต่อ	๐๘ ๘๘๙๘ ๘๐๔๗
๒. นางสาวพัชรนันท์ เสมพืช	เบอร์โทรศัพท์ติดต่อ	๐๘ ๖๙๖๔ ๑๖๒๙
๓. นายจิรพงษ์ สิทธิฤทธิ์	เบอร์โทรศัพท์ติดต่อ	๐๙ ๗๐๕๓ ๘๗๕๑
๔. นายรัฐพล ไชยถวิล	เบอร์โทรศัพท์ติดต่อ	๐๙ ๑๐๗๑ ๙๘๐๙

(จ) ทีมอาคารสถานที่/ความปลอดภัย/ไฟฟ้า/ประปา ทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร และระบบเครื่องปรับอากาศให้พร้อมใช้งาน

ผู้รับผิดชอบ ได้แก่

๑. นายสุชาติ ผุแปง	เบอร์โทรศัพท์ติดต่อ	๐๘ ๑๘๒๐ ๐๔๕๑
๒. นายปิยะพงษ์ วงศ์มโนพณิช	เบอร์โทรศัพท์ติดต่อ	๐๖ ๕๙๙๖ ๙๙๑๔
๓. นางสาวพรทิพย์ พ่วงรอด	เบอร์โทรศัพท์ติดต่อ	๐๘ ๓๖๑๕ ๓๙๔๗
๔. นายจิรพงษ์ สิทธิฤทธิ์	เบอร์โทรศัพท์ติดต่อ	๐๙ ๗๐๕๓ ๘๗๕๑

(ฉ) ทีมการจัดการทั่วไป/ประสานงานองค์กรภายนอก ทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทำงาน

ผู้รับผิดชอบ ได้แก่

๑. นางสาวอรฉัตร รัตนรัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘ ๘๘๙๘ ๘๐๔๗
๒. นางสาวพัชรนันท์ เสมพืช เบอร์โทรศัพท์ติดต่อ ๐๘ ๖๙๖๔ ๑๖๒๙
๓. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๔. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙

(ช) ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ส่วนเทคโนโลยีสารสนเทศได้จัดหาไว้

ผู้รับผิดชอบ ได้แก่

๑. นายปิยะพงษ์ วงศ์มโนพณิช เบอร์โทรศัพท์ติดต่อ ๐๖ ๕๙๙๖ ๙๙๑๔
๒. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๓. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙
๔. นายสุวัตร โกษาวัง เบอร์โทรศัพท์ติดต่อ ๐๙ ๙๒๘๗ ๔๗๗๐

(ซ) ทีมแก้ไขปัญหาเบื้องต้น กรณีกระแสไฟฟ้าขัดข้อง/หม้อไฟระเบิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่

ผู้รับผิดชอบ ได้แก่

๑. นายปิยะพงษ์ วงศ์มโนพณิช เบอร์โทรศัพท์ติดต่อ ๐๖ ๕๙๙๖ ๙๙๑๔
๒. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๓. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙
๔. นายสุวัตร โกษาวัง เบอร์โทรศัพท์ติดต่อ ๐๙ ๙๒๘๗ ๔๗๗๐

(ฌ) ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วม ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ

ผู้รับผิดชอบ ได้แก่

๑. นายปิยะพงษ์ วงศ์มโนพณิช เบอร์โทรศัพท์ติดต่อ ๐๖ ๕๙๙๖ ๙๙๑๔
๒. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๓. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙
๔. นายสุวัตร โกษาวัง เบอร์โทรศัพท์ติดต่อ ๐๙ ๙๒๘๗ ๔๗๗๐

(ญ) ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบหรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย

ผู้รับผิดชอบ ได้แก่

๑. นางสาวอรฉัตร รัตนรัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘ ๘๘๙๘ ๘๐๔๗
๒. นางสาวพัชรนันท์ เสมพืช เบอร์โทรศัพท์ติดต่อ ๐๘ ๖๙๖๔ ๑๖๒๙
๓. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๔. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙

(ฎ) ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูลและฟื้นฟูระบบหรือข้อมูลจากความเสียหาย ให้กลับมาใช้งานให้ได้ทันทีและครบถ้วนสมบูรณ์

ผู้รับผิดชอบ ได้แก่

๑. นางสาวอรฉัตร รัตนรัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘ ๘๘๙๘ ๘๐๔๗
๒. นางสาวพัชรนันท์ เสมพืช เบอร์โทรศัพท์ติดต่อ ๐๘ ๖๙๖๔ ๑๖๒๙
๓. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๔. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙

(ฏ) ทีมแก้ไขปัญหาเนื่องจากแผ่นดินไหว ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ หลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบอาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศการเกษตรเพื่อสั่งการต่อไป

ผู้รับผิดชอบ ได้แก่

๑. นายปิยะพงษ์ วงศ์มโนพณิช เบอร์โทรศัพท์ติดต่อ ๐๖ ๕๙๙๖ ๙๙๑๔
๒. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๓. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙
๔. นายสุวัตร โกษาวัง เบอร์โทรศัพท์ติดต่อ ๐๙ ๙๒๘๗ ๔๗๗๐

(ฐ) ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่ที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศการเกษตร เพื่อทราบและสั่งการต่อไป

ผู้รับผิดชอบ ได้แก่

๑. นายปิยะพงษ์ วงศ์มโนพณิช เบอร์โทรศัพท์ติดต่อ ๐๖ ๕๙๙๖ ๙๙๑๔
๒. นายจิรพงษ์ สิทธิฤทธิ์ เบอร์โทรศัพท์ติดต่อ ๐๙ ๗๐๕๓ ๘๗๕๑
๓. นายรัฐพล ไชยถวิล เบอร์โทรศัพท์ติดต่อ ๐๙ ๑๐๗๑ ๙๘๐๙
๔. นายสุวัตร โกษาวัง เบอร์โทรศัพท์ติดต่อ ๐๙ ๙๒๘๗ ๔๗๗๐

๘. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๘.๑ กรณีจากไฟไหม้

(๑) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

(๒) แจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศและผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

(๓) เจ้าหน้าที่รับผิดชอบต้องใช้อุปกรณ์ที่ส่วนเทคโนโลยีสารสนเทศได้จัดหาไว้ดำเนินการดับเพลิงและจัดการขนย้ายอุปกรณ์ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัย

(๔) แจ้งสถานีดับเพลิงที่ใกล้ที่สุด เพื่อดำเนินการต่อไป

(๕) ผู้รับผิดชอบดำเนินการรายงานผู้อำนวยการศูนย์สารสนเทศการเกษตร เพื่อทราบและสั่งการต่อไป

(๖) ผู้รับผิดชอบจะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ และผู้อำนวยการศูนย์สารสนเทศการเกษตรทราบ

๘.๒ กรณีกระแสไฟฟ้าขัดข้อง/หม้อไฟระเบิด

(๑) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้น โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ จากนั้นผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

(๒) แจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศและผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

(๓) ผู้รับผิดชอบดำเนินการรายงานผู้อำนวยการศูนย์สารสนเทศการเกษตร เพื่อทราบและสั่งการต่อไป

(๔) ผู้รับผิดชอบจะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ และผู้อำนวยการศูนย์สารสนเทศการเกษตรทราบ

๘.๓ กรณีน้ำท่วม

(๑) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ จากนั้นตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญไปยังพื้นที่ปลอดภัย พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

(๒) แจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศและผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

(๓) ผู้รับผิดชอบดำเนินการรายงานผู้อำนวยการศูนย์สารสนเทศการเกษตร เพื่อทราบและสั่งการต่อไป

(๔) ผู้รับผิดชอบจะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศและผู้อำนวยการศูนย์สารสนเทศการเกษตรทราบ

๘.๔ กรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์

(๑) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้น มิให้เกิดความเสียหายแก่ระบบเครือข่าย พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

(๒) แจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศและผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงานให้เข้าควบคุมสถานการณ์เพื่อระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

(๓) ในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์

<u>ขั้นตอนควบคุมสถานการณ์</u>

(ก) ตรวจสอบภัยคุกคามเพื่อแก้ไขปัญหา

(ข) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

(ค) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อหน่วยงานเป็นหลัก

<u>ขั้นตอนวิเคราะห์การถูกโจมตี</u>

(ก) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System File) และไฟล์อื่น ๆ

(ข) วิเคราะห์ล็อคไฟล์ (Log file) ตรวจสอบโปรแกรมหรือข้อมูลที่ผู้บุกรุกทิ้งไว้

(ค) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

(ง) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

<u>ขั้นตอนกู้คืนระบบคอมพิวเตอร์</u>

(ก) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่

(ข) งดใช้เซอร์วิสที่ไม่จำเป็น

(ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

(ง) อุดช่องโหว่ในระบบเครือข่าย

(จ) เปลี่ยนแปลงรหัสผ่านใหม่หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

(๔) ผู้รับผิดชอบดำเนินการรายงานผู้อำนวยการศูนย์สารสนเทศการเกษตร เพื่อทราบและสั่งการต่อไป

(๕) ผู้รับผิดชอบจะต้องดำเนินการเข้าตรวจสอบระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหายเพื่อแจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ และผู้อำนวยการศูนย์สารสนเทศการเกษตรทราบ

๘.๕ กรณีแผ่นดินไหว

(๑) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบระบบ

(๒) แจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศและผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย

(๓) ผู้รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้า เพื่อป้องกันเหตุเพลิงไหม้

(๔) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควร

(๕) ขั้นตอนการปฏิบัติกรณีเกิดแผ่นดินไหว

(ก) ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน

(ข) ถ้าอยู่ในอาคาร ให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจาก หน้าต่าง/ประตู/กำแพงด้านนอก/ชั้นวางของ/สิ่งที่อาจล้มหรือหล่นได้

(ค) ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้

(ง) อย่าตื่นตกใจหากกระแสไฟฟ้าขัดข้องหรือสัญญาณเตือนภัยดังขึ้น

(จ) ห้ามใช้ลิฟท์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น

(๖) เมื่อแผ่นดินไหวสงบลง

(ก) ตรวจสอบโครงสร้างอาคาร ท่อน้ำ ท่อก๊าซ กระแสไฟฟ้าและหากพบความเสียหาย ให้ปิดระบบการทำงานทั้งหมดทันที

(ข) หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

(๗) เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ และผู้อำนวยการศูนย์สารสนเทศการเกษตร เพื่อทราบและสั่งการต่อไป

(๘) ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยี สารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์สารสนเทศการเกษตรทราบ

๘.๖ กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

(๑) ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบระบบ

(๒) แจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศและผู้มีหน้าที่รับผิดชอบทราบ เพื่อดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงานให้เข้าควบคุมสถานการณ์ และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย

(๓) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควร

(๔) ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อจลาจล

(ก) แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ ดูแลความเรียบร้อย และความปลอดภัยต่อชีวิต และทรัพย์สินของผู้ปฏิบัติงานและของหน่วยงาน

(ข) เพิ่มจำนวนเจ้าหน้าที่รักษาความปลอดภัยเป็นสองเท่า

(ค) ปิดประตูทั้ง ๒ ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาในหน่วยงาน

(ง) กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมสถานการณ์ได้ หรือมีการทำลายทรัพย์สินของสำนักงานเศรษฐกิจการเกษตร ให้แจ้งไปยังสถานีตำรวจนครบาล หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้ผู้อำนวยการศูนย์สารสนเทศการเกษตรเพื่อทราบ

(จ) เมื่อพบวัตถุต้องสงสัยให้แจ้ง เจ้าหน้าที่รักษาความปลอดภัยหรือเจ้าหน้าที่รับผิดชอบทราบทันที

(๕) เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง เจ้าหน้าที่รับผิดชอบดำเนินการสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุม และผู้อำนวยการศูนย์สารสนเทศการเกษตร เพื่อทราบและสั่งการต่อไป

(๖) ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศประเมินความเสียหาย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการส่วนเทคโนโลยีสารสนเทศทราบ

๙. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้ผู้อำนวยการศูนย์สารสนเทศการเกษตรทราบ เพื่อนำเสนอรายงานสรุปให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) เป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงทีในกรณีที่เกิดภัยพิบัติต่อไป