แผนบริหารความต่อเนื่อง
การรักษาและฟื้นฟูความเสียหาย
ที่เกิดจากภัยคุกคามทางไซเบอร์
Business Continuity Plan (BCP)
ของ
สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

โดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

มีนาคม 2567

สารบัญ

แผนบริหารความต่อเนื่อง การรักษาและฟื้นฟูความเสียหาย ที่เกิดจากภัยคุกคามทางไซเบอร์ ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ Business Continuity Plan (BCP)

แผนบริหารความต่อเนื่อง หรือเรียกว่า “Business Continuity Plan (BCP)” จัดทำขึ้นเพื่อให้ **“ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์”** สามารถนำไปใช้ในการตอบสนองและปฏิบัติงานในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ ที่เกิดจากภัยคุกคามทางไซเบอร์ โดยสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินส่งผลให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ต้องหยุดการดำเนินงาน หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง

หากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ไม่มีกระบวนการรองรับการดำเนินงานอย่างต่อเนื่องในการใช้งานเทคโนโลยีดิจิทัลอาจส่งผลกระทบต่อสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ในด้านต่าง ๆ เช่น ผลกระทบจากการดำเนินงาน ผลกระทบต่อผู้รับบริการ

ดังนั้น แผนบริหารความต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ สามารถรับมือกับเหตุการณ์ฉุกเฉินที่ไม่คาดคิดและทำให้กระบวนการการใช้งานเทคโนโลยีดิจิทัลสามารถกลับมาดำเนินการได้อย่างปกติ หรือตามระดับการให้บริการที่กำหนดได้ในระยะเวลาที่เหมาะสม ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อสำนักงานปลัดกระทรวงเกษตรและสหกรณ์

1. วัตถุประสงค์ (Objectives)

1. เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง และเป็นการเตรียมความพร้อมในการรับมือกับภาวะวิกฤตที่จะส่งผลให้การใช้งานเทคโนโลยีดิจิทัลไม่สามารถใช้งานได้
2. เพื่อให้หน่วยงานมีการเตรียมความพร้อมในการรับมือกับสภาวะวิกฤติ
3. เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ
4. เพื่อบรรเทาความเสียหายให้อยู่ระดับที่ยอมรับได้
5. เพื่อให้ประชาชน เจ้าหน้าที่ หน่วยงานรัฐวิสาหกิจ หน่วยงานภาครัฐ และผู้มีส่วนได้ส่วนเสีย (Stakeholder) มีความเชื่อมั่นในศักยภาพของหน่วยงาน แม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

2. สมมติฐานของแผนบริหารความต่อเนื่อง (BCP Assumptions)

เอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

1. เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาสำคัญต่าง ๆ แต่มิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้
2. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารในฐานะที่รับผิดชอบในการสำรองระบบสารสนเทศต่าง ๆ โดยระบบสารสนเทศสำรองมิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเหมือนกับระบบสารสนเทศหลัก
3. “บุคลากร” ที่ถูกระบุในเอกสารฉบับนี้ หมายถึง เจ้าหน้าที่และพนักงานทั้งหมดของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

3. ขอบเขตของแผนบริหารความต่อเนื่อง (Scope of BCP)

แผนบริหารความต่อเนื่อง (BCP) ฉบับนี้ใช้รับรองสถานการณ์ กรณีเกิดสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินจากภัยคุกคามทางไซเบอร์ ในส่วนที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์กำกับดูแลทั้งหมด

4. การวิเคราะห์ทรัพยากรที่สำคัญ

เพื่อให้หน่วยงานสามารถบริหารจัดการการดำเนินงานขององค์กรให้มีความต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็น และต้องระบุไว้ในแผนความต่อเนื่อง ซึ่งการเตรียมการทรัพยากรที่สำคัญจะพิจารณาจากผลกระทบใน 5 ด้าน ดังนี้

1. ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงาน กรณีอาคาร/สถานที่ปฏิบัติงานหลัก ได้รับความเสียหาย จนไม่สามารถเข้าไปปฏิบัติได้ชั่วคราวหรือระยะยาว

2. ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ กรณีเหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญ หรือไม่สามารถจัดหา /จัดส่งวัสดุอุปกรณ์ที่สำคัญได้

3. ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบงานเทคโนโลยี หรือระบบสารสนเทศ หรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ

4. ผลกระทบด้านบุคลากรหลัก เป็นเหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

5. ผลกระทบด้านคู่ค้า / ผู้ให้บริการที่สำคัญ / ผู้มีส่วนได้ส่วนเสีย หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

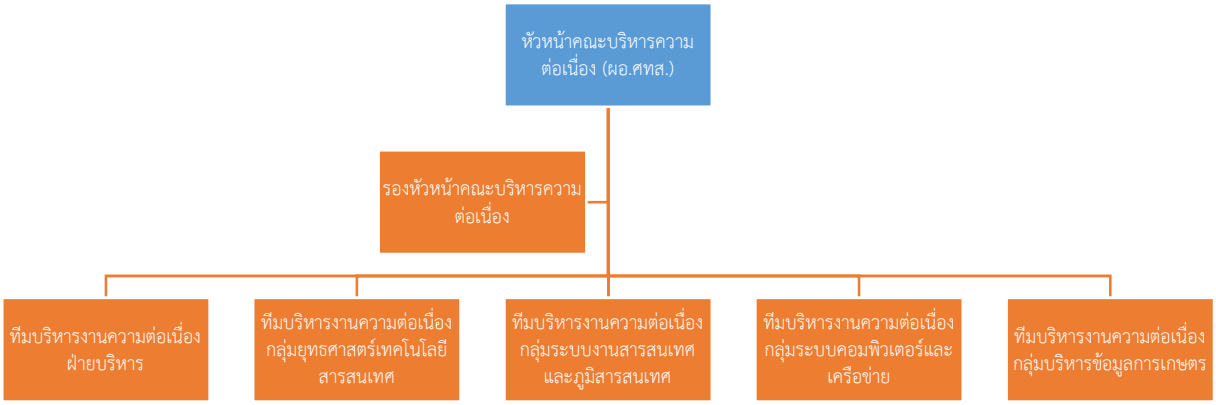
5. สรุปเหตุการณ์ของภัยคุกคาม และผลกระทบจากเหตุการณ์

ตารางที่ 1 ผลกระทบของเหตุการณ์วิกฤตที่มีต่อทรัพยากรทั้ง 5 ด้าน

เหตุการณ์วิกฤต / ภัยคุกคาม	ผลกระทบ				
	ด้านอาคาร / สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญ / การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากร	ด้านคู่ค้า / ผู้ให้บริการที่สำคัญ / ผู้มีส่วนได้ส่วนเสีย
เหตุการณ์หรือภัยที่เกิดจากการจารกรรมข้อมูล/ภัยคุกคามทางไซเบอร์		✓	✓		✓

แผนบริหารความต่อเนื่อง (BCP) ฉบับนี้ ไม่รองรับการปฏิบัติงานในกรณีที่เหตุขัดข้องเกิดขึ้นจากการดำเนินงานในภาวะปกติ และเหตุขัดข้องดังกล่าวไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ เนื่องจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ ยังสามารถจัดการหรือปรับปรุงแก้ไขได้สถานการณ์ได้ภายในระยะเวลาที่เหมาะสม

6. โครงสร้างทีมงานแผนบริหารความต่อเนื่อง



บุคลากรหลัก		บทบาท	บุคลากรสำรองและทีมงาน	
ชื่อ - นามสกุล	เบอร์มือถือ		ชื่อ - นามสกุล	เบอร์มือถือ
1. นายสัญชัย รัศมีจีรวิไล	095-541-5522	หัวหน้าคณะบริหารความต่อเนื่อง (ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)	นางสาววรัญญา แสงจันทรา	098-824-2202
2. นางสาววรัญญา แสงจันทรา	098-824-2202	รองหัวหน้าคณะบริหารความต่อเนื่อง (ผู้ประสานงาน)	1. นางสาวยุพาพร พัชราพินิจจัย 2. นางชาลิกา ธัญธนาวุฒิ	062-669-6241 098-824-2201
3. นางสาววรัญญา แสงจันทรา	098-824-2202	หัวหน้าทีมบริหารความต่อเนื่องกลุ่มยุทธศาสตร์เทคโนโลยีสารสนเทศ	1. นางสาวแสงเดือน นาคศรีสุข 2. นางสาวปาณรีย์ กำลัง 3. นางสาวเขมิสรา ถ้วยทอง	088-992-8282 098-397-4194 089-115-4787
4. นางสาวยุพาพร พัชราพินิจจัย	062-669-6241	หัวหน้าทีมบริหารความต่อเนื่องกลุ่มระบบงานสารสนเทศและภูมิสารสนเทศ	1. นายณัฐภัทร ปรัชญาธิวัฒน์ 2. นายกิตติชัย คำขันธ์ 3. นางสาวสมฤดี กิริมิตร 4. นางสาวปรัยวริน มาตราช 5. นางสาวอรอุษา ทองม้วน 6. นางสาวพูลสุข อ่อนละมูล	062-716-4442 086-358-3275 097-987-1651 097-106-6261 088-768-8648 092-765-8342
5. นายเทเวศวร์ ปัญญาแก้ว	098-824-2207	หัวหน้าทีมบริหารความต่อเนื่องกลุ่มระบบคอมพิวเตอร์และเครือข่าย	1. นายศิริชัย เธียรเจริญชัย 2. นายธีศิษฏ์ สหภัทรากุล 3. นายไววุฒิ แก้วพาดี 4. นางสาวณัฐวรรณ ประเสริฐอินทร์ 5. นายภูมิพัฒน์ เดชะ	081-627-1356 091-101-3352 086-426-6145 093-662-9893 091-326-0210
6. นางลลิตา สีพนมวัน	097-953-6519	หัวหน้าทีมบริหารความต่อเนื่องกลุ่มบริหารข้อมูลการเกษตร	1. นางบุรินทร์พรรณ โพธิ์ทอง 2. นายชัยทัต สุบรรณภาส 3. นายอภิรักษ์ ร่วมสนิท 4. นางสาวอรอุมา บัวเล็ก	086-594-6036 085-119-2888 085-118-9845 098-089-2252
7. นายธราวุธ กล่อมผ่อง	084-702-0592	หัวหน้าทีมบริหารความต่อเนื่องฝ่ายบริหารงานทั่วไป	1. นางชาลิกา ธัญธนาวุฒิ 2. นายเสริมศักดิ์ วรรณวรพร 3. นางสาวบุศกร ยิ้มเรือน 4. นางสาวภัทรวดี อุตมะพันธุ์	098-824-2201 081-737-9550 091-850-1992

บุคลากรหลัก		บทบาท	บุคลากรสำรองและทีมงาน	
ชื่อ - นามสกุล	เบอร์มือถือ		ชื่อ - นามสกุล	เบอร์มือถือ
			5. ว่าที่ร้อยตรีจิรวัฒน์ เลิศสุวรรณโรจน์	085-649-0696
			6. นางสาวภัทรภา โตคมขำ	090-989-2054
			7. นางสาวประภาพร พึงรุ่งเรืองวัฒนา	099-726-9244

7. กลยุทธ์และแนวทางในการบริหารความต่อเนื่อง (Business Continuity strategy)

กลยุทธ์ความต่อเนื่อง เป็นแนวทางในการจัดการและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤตจากภัยคุกคามทางไซเบอร์ ซึ่งพิจารณาใน 5 ด้าน ดังนี้

ทรัพยากร	กลยุทธ์ความต่อเนื่องเมื่อมีเกตุการณ์จากภัยคุกคามทางไซเบอร์
อาคาร/สถานที่ปฏิบัติงานสำรอง	ไม่ได้รับผลกระทบ
วัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ	1. กำหนดให้สำรองข้อมูลที่สำคัญจากเครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำ เพื่อให้สามารถดึงไฟล์หรือข้อมูลมาใช้ได้อย่างเร่งด่วน ในกรณีที่เกิดเหตุการณ์สภาวะวิกฤต 2. จัดเตรียมบัญชีรายชื่อและข้อมูลของหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อประสานงาน กับหน่วยงานด้านการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศ ได้แก่ - ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โทร 02 114 3531 - กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)
บุคลากรหลัก	ประสานงานบุคลากรของหน่วยงานภายนอกด้านการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อขอรับการสนับสนุนการแก้ไขเหตุภัยคุกคามทางไซเบอร์
ระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ	1. ศทส. จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) 2. ศทส. จัดเตรียมระบบสารสนเทศภายในให้สามารถเรียกใช้จากภายนอกได้ อาทิ ระบบสารบรรณอิเล็กทรอนิกส์ ระบบจดหมายอิเล็กทรอนิกส์ 3. ในกรณีที่เครือข่ายหรือระบบคอมพิวเตอร์ถูกคุกคามจนไม่สามารถใช้งานได้ ให้หน่วยงานประกาศใช้ช่องทางการให้บริการแบบ Manual 4. ศทส. จัดเตรียมระบบเครือข่ายอินเทอร์เน็ต Leased line จำนวน 2 วงจร และจัดทำBorder Gateway Protocol (BGP) โดยการทำให้ระบบอินเทอร์เน็ตที่มีอยู่ 2 วงจร สามารถสลับการทำงานอัตโนมัติหากวงจรใดวงจรหนึ่งขัดข้อง 5. ศทส. จัดเตรียมอุปกรณ์และระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ได้แก่ IPS, Firewall, e-Mail Security, Web Application Firewall และ Anti-Virus เป็นต้น
คู่ค้า/ผู้รับบริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย	1. ประสานงานผู้พัฒนาระบบให้ดำเนินการเตรียมความพร้อมสำหรับการใช้แผน BCP 2. ประชาสัมพันธ์หน่วยงานที่เกี่ยวข้อง/ผู้มีส่วนได้ส่วนเสีย ใช้ช่องทางการให้บริการแบบManual (กรณีที่ระบบเครือข่ายหรือระบบคอมพิวเตอร์ได้รับผลกระทบจากเหตุการณ์สภาวะวิกฤตจนไม่สามารถใช้งานได้) 3. ประสานงานคู่ค้า/ผู้ให้บริการของอุปกรณ์และระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ ศทส. ดูแล ให้เตรียมความพร้อมและร่วมสนับสนุนการแก้ไขเหตุภัยคุกคามไซเบอร์

8. กระบวนการแก้ไขปัญหาจากสถานการณ์ภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ ซึ่งอาจเกิดจากการเจาะข้อมูล/ทำลายระบบและข้อมูลโดยเจตนา การโจมตี หรือก่อกวนระบบเครือข่ายทำให้ไม่สามารถใช้งานได้ตามปกติ มีข้อปฏิบัติดังนี้

1. **ควบคุมสถานการณ์**
   1) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา
   2) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย
   3) เตรียมการสาหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก
2. **วิเคราะห์การถูกโจมตี**
   1) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System File) และไฟล์อื่นๆ
   2) วิเคราะห์ล็อกไฟล์ (Log File) ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้
   3) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System
   4) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ
3. **กู้คืนระบบคอมพิวเตอร์ (Backup & Recovery)**
   1) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่
   2) งดใช้เซอร์วิสที่ไม่จำเป็น
   3) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)
   4) อุดช่องโหว่ในระบบเครือข่าย
   5) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว
4. **เมื่อกลับเข้าสู่สภาวะปกติ จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่ายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้ที่เกี่ยวข้องทั้งหมดเพื่อรับทราบ**

ผู้รับผิดชอบหลัก	
นายเทเวศวร์ ปัญญาแก้ว	08-1993-0730
ผู้รับผิดชอบสำรอง	
นายธีศิษฏ์ สหภัทรากุล	09-1101-3352
นางสาวณัฐวรรณ ประเสริฐอินทร์	09-3662-9893