BOI	วิธีปฏิบัติงาน (Work Instruction) ชื่องาน : การจัดทำแผนการบริหารความต่อเนื่องให้กับธุรกิจ งานย่อย : แผนสร้างความต่อเนื่องให้กับธุรกิจ (Business Continuity Plan)	
	รหัสเอกสาร W IT BC 02-00 ชุดที่ 06	หน้าที่ 1 ของ 26
ผู้ทบทวน นายชนินทร์ ขาวจันทร์ (ตำแหน่ง ผศท.)	ผู้อนุมัติ นายฤตม์ เทอดสถีรศักดิ์ (ตำแหน่ง รท-น.)	เริ่มใช้ 20/09/61

สารบัญ

สารบัญ

บทที่ 1. บทนำ

1.1 บทนำ

สำนักงานคณะกรรมการส่งเสริมการลงทุนเป็นหน่วยงานหลักของรัฐบาล ที่กระตุ้นให้เกิดการลงทุนในประเทศไทย โดยให้สิทธิประโยชน์ต่าง ๆ ทั้งในด้านการยกเว้นหรือลดหย่อนภาษีอากรและอื่น ๆ แก่โครงการลงทุนต่าง ๆ ที่มีคุณสมบัติตามเป้าหมายในการพัฒนาเศรษฐกิจของประเทศ และยังจัดกิจกรรมส่งเสริมการลงทุน ทั้งในประเทศและต่างประเทศ เพื่อให้เกิดการลงทุนเพิ่มมากขึ้น รวมถึงการให้บริการอย่างครบครันเกี่ยวกับการดำเนินธุรกิจแก่นักลงทุนและผู้สนใจ นับตั้งแต่ให้คำแนะนำแก่นักลงทุนในขั้นตอนขอรับการส่งเสริมและขอใบอนุญาตต่าง ๆ การหาผู้ร่วมลงทุน ตลอดจนช่วยเหลือนักลงทุนไทยที่สนใจลงทุนในต่างประเทศ

ปัจจุบันสำนักงานคณะกรรมการส่งเสริมการลงทุนได้นำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาช่วยสนับสนุนการให้บริการอย่างมาก และสำนักงานคณะกรรมการส่งเสริมการลงทุนได้เล็งเห็นถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ จึงได้ดำเนินการจัดทำและพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 โดย ได้จัดทำแผนการบริหารความต่อเนื่องในการดำเนินงาน (Business Continuity Plan) เพื่อให้มั่นใจได้ว่าระบบสารสนเทศหลักที่มีความสำคัญต่อภารกิจและการบริการของสำนักงานคณะกรรมการส่งเสริมการลงทุนจะสามารถดำเนินงานได้อย่างต่อเนื่อง

แผนการบริหารความต่อเนื่องให้กับธุรกิจ (Business Continuity Plan) ประกอบด้วยการกำหนดขั้นตอนในการปฏิบัติงาน การบริหาร กำหนดและมอบหมายหน้าที่ ให้กับบุคคลต่าง ๆ ในขณะที่เกิดเหตุการณ์ที่มีผลทำให้การดำเนินธุรกิจหยุดชะงัก อาทิ ภัยพิบัติ วินาศกรรม และการประท้วง แผนนี้ช่วยทำให้การใช้เวลา และการกู้ระบบเป็นไปอย่างมีประสิทธิภาพ

แผนการบริหารความต่อเนื่องในการดำเนินงานฉบับนี้มีเนื้อหาประกอบด้วย ขอบเขตการบริหารความต่อเนื่องให้กับธุรกิจ การประเมินผลกระทบและความเสี่ยงที่มีผลต่อการดำเนินธุรกิจ โครงสร้างการตอบสนองต่อวิกฤติการณ์ การเตรียมการก่อนการเกิดวิกฤติ การตอบสนองต่อวิกฤติการณ์ กรณีสมมุติ และขั้นตอนในการกู้คืนสภาพการดำเนินธุรกิจ

1.2 ขอบเขตการใช้แผนการบริหารความต่อเนื่องให้กับธุรกิจ

ในขั้นตอนการจัดทำแผนการบริหารความต่อเนื่องให้กับธุรกิจนั้น สำนักงานคณะกรรมการส่งเสริมการลงทุนได้ดำเนินการวิเคราะห์และประเมินระบบสารสนเทศหลักที่มีความสำคัญต่อภารกิจและการบริการของสำนักงานคณะกรรมการส่งเสริมการลงทุน พบว่าระบบสารสนเทศซึ่งมีความสำคัญและมีความจำเป็นต้องจัดทำแผนเพื่อรองรับการบริหารความต่อเนื่องให้กับธุรกิจ ได้แก่

- ระบบ Active Directory
- ระบบ Website BOI (www.boi.go.th)
- ระบบ e-Mail

จึงได้กำหนดขอบเขตการใช้แผนการบริหารความต่อเนื่องในการดำเนินงานของทั้ง 3 ระบบ ดังนี้

1.2.1 แผนการบริหารความต่อเนื่องให้กับธุรกิจ (Business Continuity Plan: BCP) จะถูกนำมาใช้งานในกรณีที่เกิดวิกฤติการณ์หรือสถานการณ์ฉุกเฉิน โดยส่งผลให้มีการหยุดชะงักของกิจกรรมการให้บริการหลักของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail อย่างรุนแรง <u>ซึ่งทำให้ไม่สามารถให้บริการเป็นระยะเวลาเกินกว่า 24 ชั่วโมง</u>

1.2.2 แผนการบริหารความต่อเนื่องให้กับธุรกิจนี้ มีขอบเขตครอบคลุมการวางแผนรองรับวิกฤติการณ์หรือสถานการณ์ฉุกเฉินหรือเหตุการณ์ฉุกเฉิน การวางแผนการกู้คืนระบบ และการวางแผนการเริ่มดำเนินงานใหม่ สำหรับบริการหลักของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail

1.2.3 แผนการบริหารความต่อเนื่องให้กับธุรกิจต้องได้รับการทบทวนเมื่อมีเงื่อนไขดังต่อไปนี้เกิดขึ้น:

- มีการเปลี่ยนแปลงในฟังก์ชั่นทางธุรกิจและระบบสนับสนุนต่าง ๆ
- มีการเปลี่ยนแปลงด้านสภาพแวดล้อม
- มีการเปลี่ยนแปลงด้านการควบคุมทางด้านเทคนิคและสภาพแวดล้อม
- มีการเปลี่ยนแปลงด้านบุคลากรและตำแหน่งความรับผิดชอบ
- การเปลี่ยนแปลงอื่น ๆ ซึ่งอาจทำให้เกิดผลกระทบต่อการทำงานปกติของแผนการบริหารความต่อเนื่องให้กับธุรกิจ

1.3 สมมุติฐานของแผนการบริหารความต่อเนื่อง

สถานที่และระบบเทคโนโลยีสารสนเทศสำรองที่ได้จัดเตรียมไว้ ต้องไม่ได้รับผลกระทบจากเหตุการณ์ฉุกเฉิน จนไม่สามารถใช้งานได้เช่นเดียวกันกับสถานที่และระบบเทคโนโลยีสารสนเทศหลัก

บทที่ 2. การประเมินผลกระทบและความเสี่ยงที่มีผลต่อการดำเนินธุรกิจ และโครงสร้างการตอบสนองต่อวิกฤติการณ์

ในบทนี้จะกล่าวถึงสรุปผลการประเมินผลกระทบและความเสี่ยงที่มีผลต่อการดำเนินธุรกิจ ซึ่งเป็นการพิจารณาจากความเสี่ยงของเหตุการณ์ที่มีผลทำให้การดำเนินธุรกิจหรือการให้บริการหลักของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail หยุดชะงัก รวมถึงโครงสร้างการตอบสนองต่อวิกฤติการณ์เพื่อรับมือกับวิกฤติการณ์หรือสถานการณ์ฉุกเฉิน โดยจะประกอบด้วยทีมงาน และบทบาท หน้าที่ ความรับผิดชอบในการบริหารความต่อเนื่องให้กับธุรกิจ ซึ่งมีรายละเอียดเนื้อหาของส่วนต่าง ๆ ดังนี้

2.1 คำอธิบายระบบ Active Directory ระบบ Website BOI และระบบ e-Mail

2.1.1 วัตถุประสงค์

ระบบ Active Directory ทำหน้าที่จัดเก็บข้อมูล การบริหาร และการจัดการกับทรัพยากร อาทิ บัญชีผู้ใช้งาน (User Account), กลุ่มผู้ใช้งาน (Group), บัญชีคอมพิวเตอร์ (Computer Account) รวมถึงเครื่องพิมพ์ (Printer) และแชร์โฟลเดอร์ (Public Share Folder) แอพพลิเคชั่นต่าง ๆ โดยผู้ใช้งานที่จะเข้าใช้งานบริการ Directory จำเป็นต้องผ่านกระบวนการพิสูจน์ตัวตนหรือ Authentication จากเครื่องคอมพิวเตอร์แม่ข่ายระบบ Active Directory จึงจะสามารถเข้าใช้บริการได้ เพื่อเป็นการควบคุมความปลอดภัยของข้อมูล

ระบบ Website BOI (www.boi.go.th) เป็นเว็บไซต์ที่ให้บริการข้อมูลข่าวสารแก่นักลงทุนและผู้สนใจทั่วไป โดยมีทั้งภาษาไทย ภาษาอังกฤษ ภาษาจีน ภาษาฝรั่งเศส ภาษาเยอรมัน ภาษาเกาหลี ภาษาญี่ปุ่น และภาษาเยอรมัน มีข้อมูลเกี่ยวกับการส่งเสริมการลงทุน ข่าวสารเกี่ยวกับการลงทุน และการบริการออนไลน์ อาทิ การขอรับการส่งเสริมออนไลน์ ดาวน์โหลดแบบฟอร์มต่างๆ รวมถึงบริการวารสารต่างๆ

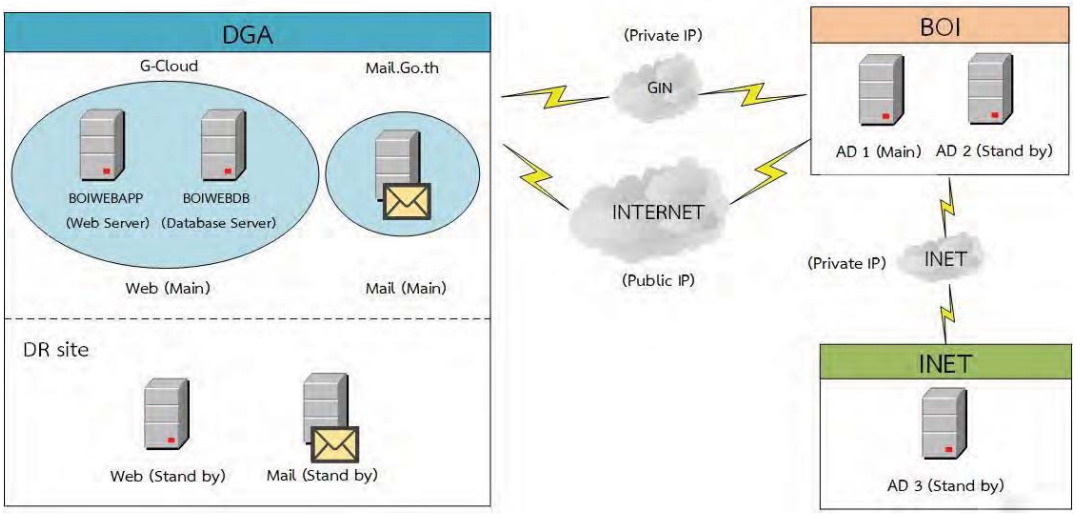
ระบบ e-Mail เป็นระบบรับ-ส่งจดหมายอิเล็กทรอนิกส์ ที่ให้บริการติดต่อสื่อสารทั้งเจ้าหน้าที่ภายในสำนักงานฯ เอง และกับบุคคลภายนอกสำนักงานฯ

2.1.2 เทคโนโลยีที่ใช้

สำนักงานคณะกรรมการส่งเสริมการลงทุน ได้ดำเนินการวิเคราะห์และประเมินเทคโนโลยีที่ใช้ของระบบที่มีความสำคัญต่อภารกิจและการบริการของสำนักงานฯ ได้แก่

- ระบบ Active Directory
- ระบบ Website BOI (www.boi.go.th)
- ระบบ e-Mail

ซึ่งกระบวนการทำงานของระบบต่าง ๆ ข้างต้น แสดงดังภาพและรายละเอียดข้างล่างนี้



ภาพ 2.1-1 แสดงการทำงานของระบบ Active Directory, ระบบ Website BOI และ ระบบ e-Mail

2.1.2.1 ระบบ Active Directory ติดตั้งใช้งานบนระบบปฏิบัติการ Microsoft Window Server 2012 R2 ซึ่งใช้เทคโนโลยีการทำ Clustering ในรูปแบบ Active/Standby ระหว่างเครื่องคอมพิวเตอร์แม่ข่ายหลัก และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง (1) ซึ่งติดตั้งอยู่ในห้องคอมพิวเตอร์แม่ข่ายที่ BOI และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง (2) ซึ่งติดตั้งอยู่ที่บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) (INET) โดยในแต่ละวัน ระบบจะทำการสำเนาข้อมูล (Data Replication) จากเครื่องคอมพิวเตอร์แม่ข่ายหลัก ไปจัดเก็บไว้บนเครื่องคอมพิวเตอร์แม่ข่ายสำรอง (1 และ 2) เพื่อ Stand by เป็นระบบสำรองในการให้บริการได้อย่างต่อเนื่อง สำหรับกรณีเกิดเหตุฉุกเฉิน ซึ่งส่งผลให้ระบบ Active Directory หลัก ไม่สามารถให้บริการได้

2.1.2.2 ระบบ Website BOI (www.boi.go.th) ถูกพัฒนาขึ้น ด้วยภาษา PHP Version 5.0 โดยมีระบบฐานข้อมูล คือ Microsoft SQL Server 2012 และระบบปฏิบัติการ คือ Microsoft Windows 2012 R2 STD และใช้เทคโนโลยีการทำ Virtual Machine สำหรับระบบ Website หลักและสำรอง ติดตั้งบนระบบ Cloud ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร. หรือ DGA) เพื่อให้สามารถบริการได้อย่างต่อเนื่อง สำหรับกรณีเกิดเหตุฉุกเฉิน ซึ่งส่งผลให้ระบบ Website หลัก ไม่สามารถให้บริการได้

2.1.2.3 ระบบ e-Mail เป็นระบบจดหมายอิเล็กทรอนิกส์ โดยใช้ซอฟต์แวร์ MailGoThai ของ สพร. เป็นหลักในการให้บริการ โดยระบบ e-Mail หลักและสำรอง ติดตั้งที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร. หรือ DGA) โดยเชื่อมโยงกับระบบ Government ID (GovID) เพื่อให้เจ้าหน้าที่ของหน่วยงานภาครัฐสามารถเข้าใช้บริการได้ด้วยบัญชีเดียว มีการจัดเก็บล็อก (Log) ผู้รับ-ผู้ส่ง เวลา และ IP Address ซึ่งมีอายุในการเก็บอย่างน้อย 90 วัน รองรับการรับและส่งอีเมล์ด้วยการเข้ารหัสข้อมูลแบบ SSL Protocol มีการสำรองข้อมูลแบบ Onsite และ Offsite ให้สามารถใช้งานได้อย่างต่อเนื่อง รวมถึงมีการใช้งานผ่าน Web-browser ได้

2.1.2.4 ผู้ให้บริการระบบเครือข่ายสื่อสารการใช้งาน ได้แก่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) (INET)

2.1.2.5 ผู้ให้บริการระบบ และการบำรุงรักษา

- ระบบและเครื่องคอมพิวเตอร์แม่ข่าย Active Directory ได้แก่ บริษัท ดีเอ็กซ์พี (ไทยแลนด์) จำกัด
- ระบบและเครื่องคอมพิวเตอร์แม่ข่าย e-Mail ได้แก่ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
- ระบบ Website BOI ได้แก่ บริษัท เน็ตเซอร์วิส จำกัด
- เครื่องคอมพิวเตอร์แม่ข่าย Website BOI ได้แก่ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
- บริการคลาวด์ภาครัฐ (G-Cloud) ได้แก่ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)

2.2 การประเมินผลกระทบและความเสี่ยงที่มีผลต่อการดำเนินธุรกิจ

2.2.1 การประเมินผลกระทบและความเสี่ยงที่มีผลต่อการดำเนินธุรกิจ สำนักงานคณะกรรมการส่งเสริมการลงทุนจะพิจารณาในเงื่อนไข ดังนี้

- ผลกระทบของวิกฤตการณ์หรือเหตุการณ์นั้น ๆ จะต้องทำให้การให้บริการหลักของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail หยุดชะงัก ไม่น้อยกว่า 24 ชั่วโมง
- ความเสี่ยงที่ระบุไว้จะยึดตามกรณีที่เลวร้ายที่สุด (Worst Case Scenario)

จากการประเมินความเสี่ยง สามารถสรุปผลโอกาสที่จะเกิดความเสี่ยง ผลกระทบ และแนวทางการจัดการในแต่ละกรณี โดยพิจารณาอ้างอิงตามคุณลักษณะที่ต้องควบคุมป้องกันของ TRIS (หมายเหตุ: TRIS เป็นสถาบันประเมิน KPI หน่วยงานภาครัฐ) ดังนี้

ตาราง 2.2-1 สรุปผลโอกาสที่จะเกิดความเสี่ยง ผลกระทบ และแนวทางการจัดการในแต่ละกรณี

ลำดับที่	ภัยคุกคาม (Threats)	โอกาสที่เกิด (Likelihood)	กลยุทธ์ในการลดความเสี่ยงและผลกระทบ	ผลกระทบต่อองค์กร	การเตรียมแผนกู้คืนระบบ
1	ฝุ่น (Dust)	ต่ำ	- ควบคุมสภาวะแวดล้อมของห้องคอมพิวเตอร์แม่ข่าย ให้เป็นพื้นที่ปิด	ต่ำ	ไม่มี
2	ควัน (Smoke)	ต่ำ	- ควบคุมสภาวะแวดล้อมของห้อง Data Center ให้เป็นพื้นที่ปิด - มีการจัดการระบบระบายอากาศของห้อง Data Center ให้เหมาะสม	ต่ำ	ไม่มี
3	เพลิงไหม้ (Fire)	ต่ำ	- ห้องคอมพิวเตอร์แม่ข่าย ได้ทำการติดตั้งระบบ Fire Suppression System ได้แก่ 1) อุปกรณ์ตรวจจับควัน 2) ระบบสัญญาณเตือนอัคคีภัยอัตโนมัติ 3) ระบบดับเพลิงอัตโนมัติ ถังดับเพลิง - มีแผนการจัดทำศูนย์สำรองข้อมูล DR - Site - มีการตรวจสอบอุปกรณ์เกี่ยวกับระบบไฟฟ้าต่าง ๆ เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ปลอดภัยอย่างสม่ำเสมอ - มีการตรวจสอบการทำงาน Fire Suppression System เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ใช้งานได้เสมอ	สูง	**มี**
4.	น้ำดับเพลิง/ น้ำท่วมขัง/ รอยรั่วที่เกิดจากการสร้างไม่ได้มาตรฐาน (Water or Supply Failure)	ต่ำ	- ตัดระบบกระจายน้ำดับเพลิงอัตโนมัติที่ติดตั้งอยู่ภายในห้อง Data Center	ปานกลาง	ไม่มี

ตาราง 2.2-1 สรุปผลโอกาสที่จะเกิดความเสี่ยง ผลกระทบ และแนวทางการจัดการในแต่ละกรณี (ต่อ)

ลำดับที่	ภัยคุกคาม (Threats)	โอกาสที่เกิด (Likelihood)	กลยุทธ์ในการลดความเสี่ยงและผลกระทบ	ผลกระทบต่อองค์กร	การเตรียมแผนกู้คืนระบบ
5	แรงสั่นสะเทือน (Vibration)	ต่ำ	- ห้อง Data Center ตั้งอยู่ในพื้นที่ห่างจากแรงสั่นสะเทือนจากรถไฟ และแผ่นดินไหว	ต่ำ	ไม่มี
6	ถูกโจรกรรม/วินาศกรรม (Theft)	ต่ำ	- มีศูนย์สำรองข้อมูล DR Site - มีระบบการควบคุมการเข้าออกพื้นที่ (Access Control System)	สูง	**มี**
7	การประท้วง/ปิดล้อมสถานที่	ต่ำ	- มีศูนย์สำรองข้อมูล DR Site - มีระบบการควบคุมการเข้าออกพื้นที่ (Access Control System)	สูง	**มี**
8	ระบบไฟฟ้า - ขัดข้อง ระบบไฟฟ้าลัดวงจร (Electrical Supply Interference)	สูง	- ติดตั้งอุปกรณ์ UPS และเครื่องกำเนิดไฟฟ้า เพื่อรองรับความไม่เสถียรของระบบไฟฟ้า ที่จ่ายไฟให้กับระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญทั้งหมด - มีการตรวจสอบอุปกรณ์ UPS เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้อยู่ในสถานะที่ใช้งานได้เสมอ	สูง	**มี**
9	อุทกภัย	ปานกลาง	- มีศูนย์สำรองข้อมูล DR Site	ปานกลาง	**มี**

2.2.2 การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

จากการประเมินผลกระทบต่อการดำเนินงานและความเสี่ยงของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail สามารถสรุปถึงโอกาสที่จะเกิดความเสี่ยง ผลกระทบ และแนวทางการจัดการในแต่ละกรณี ได้ดังนี้

ตาราง 2.2-2 สรุปผลการวิเคราะห์และประเมินผลกระทบต่อการดำเนินงานของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail

บริการหลัก	กิจกรรม				ลำดับความสำคัญ (Critical) (ใช่/ไม่ใช่)	เป้าหมายการบริหารความต่อเนื่อง (Business Continuity Objective)		
	ระบบไฟฟ้า	ระบบเครือข่ายภายใน	ระบบเครือข่ายภายนอก	เครื่องคอมพิวเตอร์แม่ข่าย		MTPD (ชม.)	RPO (ชม.)	RTO (ชม.)
ระบบบริหารจัดการทรัพยากร (Active Directory)	✓	✓	✓	✓	Yes	24	24	4
บริการข้อมูลข่าวสาร (www.boi.go.th)	✓	✓	✓	✓	Yes	24	24	4
บริการจดหมายอิเล็กทรอนิกส์ (E-Mail)	✓	✓	✓	✓	Yes	24	24	4

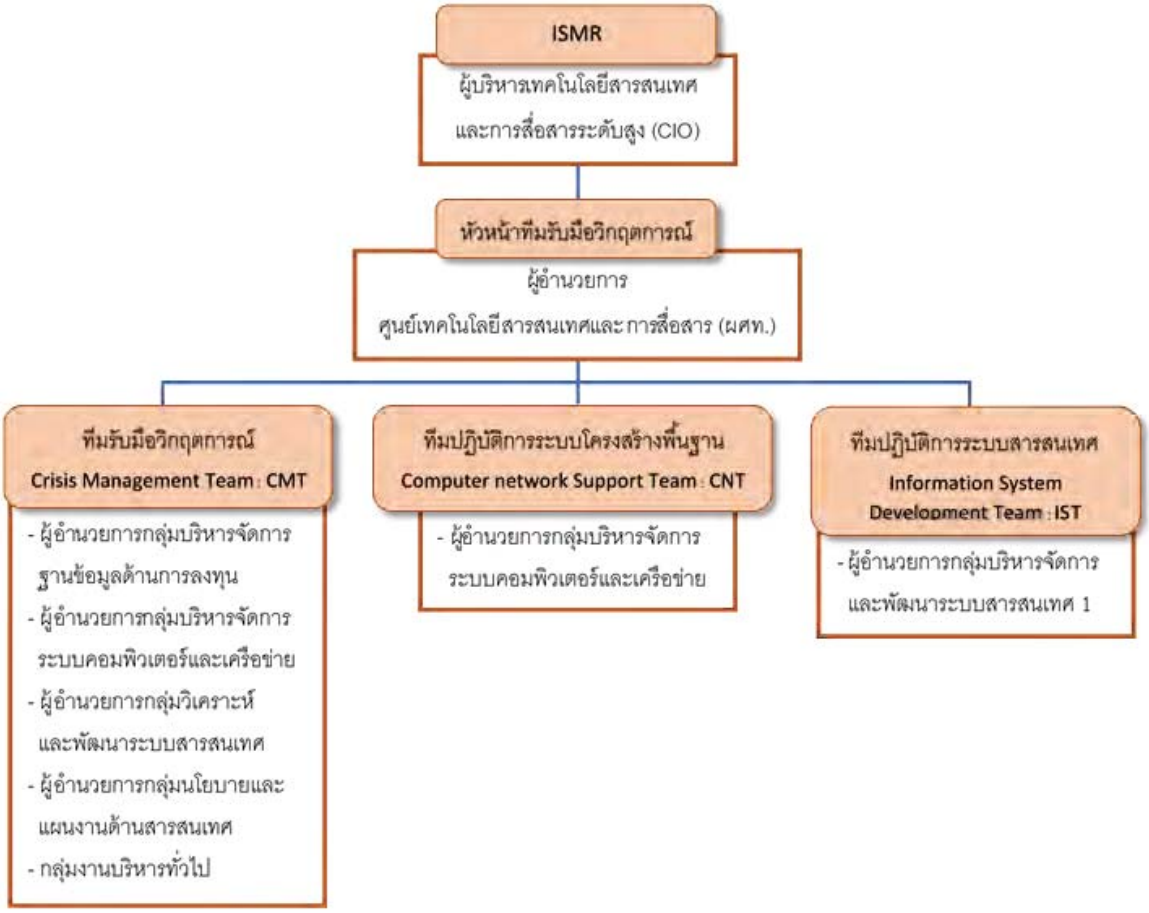
หมายเหตุ:

(1) MTPD (Maximum Tolerable Period of Disruption) หมายถึง ช่วงระยะเวลาการหยุดชะงักที่องค์กรยอมรับได้สูงสุด

(2) RPO (Recovery Point Objective) หมายถึง ระยะเวลาที่ข้อมูลหรือ Service สามารถนำย้อนกลับมาได้

(3) RTO (Recovery Time Objective) หมายถึง ระยะเวลาที่ต้องใช้ในการกู้คืนข้อมูลหรือ Service สู่สภาพการดำเนินงานปกติ หลังจากเกิด Incident

2.3 โครงสร้างการตอบสนองต่อวิกฤติการณ์ (Incident Response Structure)



ภาพ 2.3-1 โครงสร้างการตอบสนองต่อวิกฤติการณ์ (Incident Response Structure)

2.4 บทบาทและความรับผิดชอบในการบริหารความต่อเนื่องให้กับธุรกิจ

ระบบ Active Directory ระบบ Website BOI และระบบ e-Mail มีผู้บริหาร คือ ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูง (CIO) มีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ผศท.) เป็นหัวหน้าทีมรับมือวิกฤตการณ์ และทีมงาน 3 ชุดหลัก ได้แก่

1. ทีมรับมือวิกฤตการณ์ (Crisis Management Team: CMT) ประกอบด้วย ผู้อำนวยการกลุ่มบริหารจัดการระบบคอมพิวเตอร์และเครือข่าย, ผู้อำนวยการกลุ่มวิเคราะห์และพัฒนาระบบสารสนเทศ, ผู้อำนวยการกลุ่มบริหารจัดการฐานข้อมูลด้านการลงทุน, ผู้อำนวยการกลุ่มนโยบายและแผนงานด้านสารสนเทศ, และกลุ่มงานบริหารทั่วไป

2. ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน (Computer Network Support Team: CNT) ประกอบด้วย กลุ่มบริหารจัดการระบบคอมพิวเตอร์และเครือข่าย

3. ทีมปฏิบัติการระบบสารสนเทศ (Information System Development Team: IST) ประกอบด้วย กลุ่มวิเคราะห์และพัฒนาระบบสารสนเทศ

โดยมีบทบาทและความรับผิดชอบในการบริหารความต่อเนื่องให้กับธุรกิจของแต่ละทีม ดังนี้

2.4.1 <u>ทีมรับมือวิกฤติการณ์ (Crisis Management Team: CMT)</u>

2.4.1.1 มีหน้าที่รับผิดชอบในการกำหนดทิศทาง ในการดำเนินการฟื้นฟูการปฏิบัติงานเพื่อการบริการระบบ Active Directory ระบบ Website BOI และระบบ e-Mail โดยต้องดำเนินการสรุประดับของความเสียหาย ประสานงานติดตามการกู้คืนของทีมปฏิบัติการระบบโครงสร้างพื้นฐาน และทีมปฏิบัติการระบบสารสนเทศ รวมถึงบริษัทผู้รับจ้าง และจัดสรรทรัพยากรเพื่อใช้ในการกู้คืนและฟื้นฟูระบบที่ได้รับความเสียหาย นอกจากนั้นทีมรับมือวิกฤติการณ์ยังเป็นจุดติดต่อหลัก เพื่อทำการปรับปรุงสถานะให้กับผู้ที่เกี่ยวข้องในหน่วยงานต่าง ๆ และมีหน้าที่ในการสนับสนุนข้อมูลให้กับสำนักงานคณะกรรมการส่งเสริมการลงทุน สื่อสารและประชาสัมพันธ์กับสื่อต่าง ๆ ตามความเหมาะสม

2.4.1.2 มีหน้าที่รับผิดชอบในการสนับสนุนข้อมูลและร่วมพิจารณากับบริษัทผู้รับจ้าง เพื่อตัดสินใจว่าสถานการณ์นั้น ๆ จำเป็นต้องนำกระบวนการกู้คืนจากภัยพิบัติมาใช้หรือไม่ หากตัดสินใจว่าจะต้องใช้กระบวนการกู้คืนจากภัยพิบัติ ทีมรับมือวิกฤติการณ์จะร่วมกันปฏิบัติงานและประสานงานกับทีมที่เกี่ยวข้องตลอดช่วงระยะเวลาที่ใช้ในการกู้คืนจากภัยพิบัติ

2.4.1.3 มีหน้าที่ในการติดตามข้อมูลข่าวสารและสถานการณ์ของวิกฤตการณ์หรือสถานการณ์ฉุกเฉิน โดยกำหนดให้เจ้าหน้าที่ของบริษัทผู้รับจ้างแจ้งสถานการณ์ของวิกฤตการณ์เป็นระยะ เพื่อรายงานสถานการณ์ปัจจุบัน

2.4.2 <u>ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน (Computer Network Support Team: CNT)</u>

2.4.2.1 มีหน้าที่รับผิดชอบในการประสานงานกับบริษัทผู้รับจ้างเพื่อกู้คืนการทำงานของระบบคอมพิวเตอร์และเครือข่าย และดำเนินกิจกรรมของห้องคอมพิวเตอร์เพื่อให้บริการอย่างต่อเนื่อง ตามกำหนดการในการกู้สำหรับระบบสำคัญ

2.4.2.2 มีหน้าที่รับผิดชอบในการสร้างสภาพแวดล้อมที่เหมาะสม (ทั้งสถานที่และขั้นตอนการปฏิบัติงาน) ของสถานที่ที่ต้องการจะฟื้นฟู และจัดตั้งการดำเนินการให้บริการห้องระบบคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายขึ้นใหม่ ซึ่งรวมทั้งการจัดหาและการติดตั้งคอมพิวเตอร์และอุปกรณ์สื่อสารต่าง ๆ และรับผิดชอบต่อสภาพแวดล้อมโดยทั่วไป ซึ่งรวมถึงอาคารสถานที่ บริการ และอุปกรณ์อื่น ๆ ที่จำเป็นร่วมกับทีมปฏิบัติการระบบสารสนเทศ

2.4.3 <u>ทีมปฏิบัติการระบบสารสนเทศ (Information System Development Team: IST)</u>

2.4.3.1 มีหน้าที่รับผิดชอบในการประสานงานกับบริษัทผู้รับจ้าง เพื่อการกู้คืนข้อมูลสารสนเทศของระบบสารสนเทศที่สำคัญ ตามที่ระบุไว้ในแผนการบริหารความต่อเนื่องให้กับธุรกิจเพื่อสามารถให้บริการได้อย่างต่อเนื่อง

2.4.3.2 มีหน้าที่รับผิดชอบในการกู้คืนระบบสารสนเทศ และตรวจสอบการทำงานของระบบให้สามารถใช้งานได้ตามที่ระบุไว้ในแผนการบริหารความต่อเนื่องให้กับธุรกิจ เพื่อสามารถให้บริการได้อย่างต่อเนื่อง

บทที่ 3. การจัดเตรียมความพร้อมสำหรับรับมือกับวิกฤติการณ์หรือสถานการณ์ฉุกเฉิน

ในบทนี้จะกล่าวถึงการจัดเตรียมความพร้อมสำหรับรับมือกับวิกฤตการณ์หรือสถานการณ์ฉุกเฉินของการให้บริการระบบ Active Directory ระบบ Website BOI และระบบ E-Mail ซึ่งประกอบด้วยรายละเอียดของสิ่งที่ต้องเตรียมการ ดังนี้

3.1 ศูนย์ปฏิบัติการสำรอง (Alternate Site)

เมื่อเกิดวิกฤตการณ์หรือสถานการณ์ฉุกเฉินเกิดขึ้น และไม่สามารถเข้าพื้นที่สำนักงานคณะกรรมการส่งเสริมการลงทุนได้ เจ้าหน้าที่สามารถปฏิบัติงานได้ ณ สถานที่ดังนี้

1) ศูนย์ประสานการบริการด้านการลงทุน (ศปบ.)
ชั้น 18 อาคารจัตุรัสจามจุรี ถนนพญาไท เขตปทุมวัน กรุงเทพฯ 10330
สายด่วน : 02-209-1100

ภาพ 3.2-1 แผนที่แสดงที่ตั้งศูนย์ปฏิบัติการสำรอง (Alternate Site)

การเดินทางมาศูนย์ประสานการบริการด้านการลงทุน

วิธีที่ 1 โดยรถโดยสารประจำทาง

ซึ่งวิ่งผ่านอาคารจัตุรัสจามจุรี ได้แก่ รถประจำทาง : สาย 4, 16, 21, 25, 29, 34, 36, 40, 45, 47, 50, 67, 93, 113, 141, 163, 172, 501

วิธีที่ 2 โดยรถไฟฟ้าใต้ดิน MRT

ลงที่สถานีสามย่าน ทางออกประตู 2 อาคารจัตุรัสจามจุรี อยู่ติดสถานีรถไฟฟ้าใต้ดิน

วิธีที่ 3 โดยรถไฟฟ้าลอยฟ้า บีทีเอส

เดินทางโดยรถไฟฟ้า บีทีเอส ลงที่สถานี ศาลาแดง เดินเท้าไปยังถนนพระราม 4 ไปทางแยกสามย่าน ก่อนถึงแยกที่สอง อาคารจัตุรัสจามจุรี จะอยู่ด้านขวามือติดกับรถไฟฟ้าใต้ดิน MRT สถานีสามย่าน

วิธีที่ 4 โดยพาหนะส่วนตัว หรือรถรับจ้างเหมาคัน (TAXI)

ตามเส้นทาง ถนนพญาไท จากห้างมาบุญครอง และผ่านจุฬาลงกรณ์มหาวิทยาลัย ไปแยกสามย่าน อาคารจัตุรัสจามจุรี อยู่ด้านซ้ายมือของทางแยก

3.2 การจัดเตรียมเครื่องมือสนับสนุนการทำงานของศูนย์ปฏิบัติการสำรอง (Alternate Site)

เพื่อให้ศูนย์ปฏิบัติการสำรอง มีความพร้อมสำหรับใช้งานและการเข้าปฏิบัติงานของเจ้าหน้าที่ ศทส. ที่เกี่ยวข้อง ซึ่งต้องมีการดำเนินการจัดเตรียมความพร้อมในด้านต่างๆ ดังนี้

3.2.1 จัดเตรียมสิ่งอำนวยความสะดวก ซึ่งจำเป็นต้องใช้ในการปฏิบัติงาน ตามตาราง 3.2-1

ตาราง 3.2-1 รายการสิ่งอำนวยความสะดวกของศูนย์ปฏิบัติการสำรอง (Alternate Site)

รายการ	จำนวน	จัดหาและเตรียมความพร้อมโดย
1. คู่สายโทรศัพท์และเครื่องโทรศัพท์ (พร้อมใช้งาน)	2 คู่สาย	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
2. คู่สายโทรศัพท์และเครื่องแฟกซ์ (พร้อมใช้งาน)	1 คู่สาย	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
3. คอมพิวเตอร์แบบพกพา (พร้อมใช้งาน)	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
4. เครื่องพิมพ์	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
5. โต๊ะ-เก้าอี้	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
6. กระดานไวท์บอร์ด/ปากกาเขียนไวท์บอร์ด	1 ชุด/2 ด้าม	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
7. เครื่องเขียน - ปากกา ดินสอ	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
8. ตู้จัดเก็บเอกสาร	1 ตู้	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
9. Internet สำหรับใช้งาน	-	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน

3.2.2 ทำการสำรองสื่อและบันทึกที่สำคัญ ๆ ตามตาราง 3.2-2

ตาราง 3.2-2 รายการสื่อและบันทึกที่สำคัญ

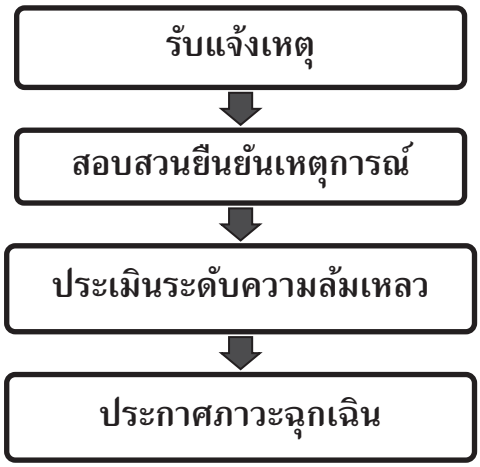
รายการ	จำนวน	จัดหาและเตรียมความพร้อมโดย
1. แผนการบริหารความต่อเนื่องในการดำเนินงาน	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
2. คู่มือการเรียกคืนข้อมูลของระบบ Active Directory ระบบ Web BOI และระบบ e-mail	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน ทีมปฏิบัติการระบบสารสนเทศ
3. รายชื่อพนักงาน/เจ้าหน้าที่ของ ศทส.	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน
4. รายชื่อบริษัทฯ ที่เกี่ยวข้องกับระบบ	1 ชุด	ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน ทีมปฏิบัติการระบบสารสนเทศ

บทที่ 4. การตอบสนองต่อวิกฤติการณ์

ในบทนี้จะกล่าวถึงรายละเอียดขั้นตอนการตอบสนองต่อวิกฤติการณ์ การส่งต่อ และเริ่มใช้แผนการบริหารความต่อเนื่องให้กับธุรกิจ รวมถึงรายละเอียดข้อมูลสำหรับติดต่อประสานงานกับเจ้าหน้าที่ ศทส. และผู้มีส่วนเกี่ยวข้อง ซึ่งมีรายละเอียด ดังนี้

4.1 การส่งต่อและการเริ่มใช้แผนการบริหารความต่อเนื่องในการดำเนินงาน

ในกรณีที่เกิดวิกฤติการณ์หรือสถานการณ์ฉุกเฉิน ศทส. มีขั้นตอนการปฏิบัติเพื่อตอบสนองต่อวิกฤติการณ์นั้น ๆ ดังนี้



ภาพ 4.1-1 ขั้นตอนการปฏิบัติเพื่อตอบสนองต่อวิกฤติการณ์

1) เมื่อทีมรับมือวิกฤติการณ์ ได้รับแจ้งเหตุ (T0 : เวลาที่ได้รับแจ้งเหตุการณ์วิกฤติ)
   - ต้องทำการสอบสวนเพื่อตรวจสอบยืนยันความเชื่อถือได้ของการแจ้งเหตุ
   - ต้องพิจารณาตามระดับความรุนแรงของสถานการณ์เบื้องต้น หากมีความรุนแรงและเป็นอันตรายต่อเจ้าหน้าที่ต้องอพยพเจ้าหน้าที่ ออกจากที่เกิดเหตุโดยด่วนที่สุด
   - แจ้งเตือนหน่วยงานพยาบาล หน่วยงานรักษาความปลอดภัย และหน่วยงานฉุกเฉินตามความเหมาะสม
   - ต้องรายงานข้อมูลวิกฤตการณ์หรือสถานการณ์ฉุกเฉินให้ผู้บังคับบัญชาได้รับทราบตามลำดับชั้นการบังคับบัญชา
2) ทีมรับมือวิกฤติการณ์ เริ่มการประเมินความเสียหาย (T1 : เวลาเริ่มประเมินความเสียหายของเหตุการณ์วิกฤติ) และต้องเสร็จสิ้นการประเมินความเสียหายภายใน 1 ชั่วโมงถัดไป (T1 + 1.00)
3) หัวหน้าทีมรับมือวิกฤตการณ์ต้องอธิบายลักษณะและระดับของสถานการณ์ที่เกิดขึ้นให้กับผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูง (CIO) รับทราบ

4) ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูง (CIO) ประกาศภาวะภัยพิบัติ (T2 : เวลาที่ประกาศภาวะภัยพิบัติ)

จากลำดับขั้นตอนของการส่งต่อและการเริ่มใช้แผนการบริหารความต่อเนื่องให้กับธุรกิจสามารถแสดงภาพความสัมพันธ์ของช่วงระยะเวลาในการตอบสนองต่อวิกฤตการณ์ได้ดังภาพ 4.1-2

ภาพ 4.1-2 ระยะเวลาในการตอบสนองต่อวิกฤตการณ์

4.2 การติดต่อผู้ที่เกี่ยวข้อง (Call Tree)

เมื่อมีการประกาศภาวะภัยพิบัติ ทีมรับมือวิกฤติการณ์ จะเริ่มโทรแจ้งทีมปฏิบัติการระบบโครงสร้างพื้นฐาน และทีมปฏิบัติการระบบสารสนเทศตามรายชื่อผู้ที่เกี่ยวข้อง (Call Tree) โดยทีมปฏิบัติการระบบโครงสร้างพื้นฐาน และทีมปฏิบัติการระบบสารสนเทศจะโทรแจ้งผู้ที่เกี่ยวข้องตามรายชื่อบุคคลสำคัญหรือหน่วยงานภายนอกองค์กรตามความรับผิดชอบเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องเริ่มเข้าปฏิบัติงานตามแผนการบริหารความต่อเนื่องให้กับธุรกิจ ซึ่งมีขั้นตอนการติดต่อ ดังนี้

4.2.1 ขั้นตอนการปฏิบัติเพื่อติดต่อกับผู้ที่เกี่ยวข้อง

1) แจ้งเจ้าหน้าที่ให้ทราบถึงการเริ่มใช้แผนการบริหารความต่อเนื่องให้กับธุรกิจรวมทั้งการดำเนินการที่ต้องปฏิบัติ

2) หากสามารถติดต่อผู้ที่อยู่ในรายชื่อผู้ที่เกี่ยวข้องได้ ให้ถ่ายทอดข้อมูลดังต่อไปนี้:

- สถานะของภัยพิบัติ
- การดำเนินการที่ต้องปฏิบัติ
- เตรียมพร้อมจนกว่าจะได้รับการติดต่อเพื่อแจ้งให้ทราบถึงคำสั่งที่ต้องดำเนินการต่อไป หรือไปรายงานตัวตามเวลา หรือสถานที่ที่กำหนด โดยนำบัตรประจำตัวและบัตรผ่านประตูต่าง ๆ ไปด้วย
- จะต้องไม่กระจาย ข่าวสถานการณ์นั้นออกสู่สาธารณะ (ต้องให้ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูง (CIO) เป็นผู้แจ้งสถานการณ์ออกสู่สาธารณะเท่านั้น)

3) หากไม่สามารถติดต่อบุคคลในรายการได้ ให้ฝากข้อความให้บุคคลนั้นโทรกลับมา

4) หากไม่สามารถติดต่อบุคคลนั้นได้นานกว่า 5 นาที ให้โทรหาบุคคลถัดไป

5) หลังจากนั้น ให้รายงานรายชื่อบุคคลซึ่งไม่สามารถติดต่อได้ให้แก่หัวหน้าทีมรับมือวิกฤติการณ์ทราบ

4.2.2 รายชื่อผู้ที่เกี่ยวข้อง (Call Tree)

ตาราง 4.2-1 รายชื่อบุคลากรหลักที่ต้องติดต่อเมื่อเกิดวิกฤตการณ์หรือสถานการณ์ฉุกเฉิน

ชื่อ	ตำแหน่ง	โทรศัพท์พื้นฐาน	โทรศัพท์มือถือ
ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูง (ISMR)			
นายนฤตม์ เทอดสถีรศักดิ์	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)	-	081-174-4125
หัวหน้าทีมรับมือวิกฤตการณ์			
นายชนินทร์ ขาวจันทร์	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	02-5538330	081-174-4121
ทีมรับมือวิกฤตการณ์ (CMT)			
นายธันว์ ตังสุรัตน์	- ผู้อำนวยการกลุ่มบริหารจัดการฐานข้อมูลด้านการลงทุน - ผู้อำนวยการกลุ่มบริหารจัดการและพัฒนาระบบสารสนเทศ 2	02-5538170	080-571-0011
นายอำนาจ จุลชาต	- ผู้อำนวยการกลุ่มนโยบายและแผนงานด้านสารสนเทศ	02-5538375	092-360-8282
นายวีระ ชัยวีระวัฒนะ	- ผู้อำนวยการกลุ่มบริหารจัดการระบบคอมพิวเตอร์และเครือข่าย - ผู้อำนวยการกลุ่มบริหารจัดการและพัฒนาระบบสารสนเทศ 1	02-5538292	081-648-8633
นายพิเชฐ เครือเนตร	- รก.ผู้อำนวยการกลุ่มวิเคราะห์และพัฒนาระบบสารสนเทศ	02-5538239	065-221-3054
นางพิมลดา อู่อ้น	เจ้าพนักงานธุรการชำนาญงาน	02-5538243	086-572-9719
นางปนัดดา ชวจุมพล	เจ้าพนักงานธุรการชำนาญงาน	02-5538190	081-734-1616
ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน (CNT)			
นายวีระ ชัยวีระวัฒนะ	ผู้อำนวยการกลุ่มบริหารจัดการระบบคอมพิวเตอร์และเครือข่าย	02-5538292	081-648-8633
นายณัฐพงษ์ จัตุรเขษม	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	02-5538415	083-925-5049
นายปองพล รอดสวัสดิ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	02-5538395	096-324-5631
นายวัชรพงษ์ ไชยมงคล	พนักงานส่งเสริมการลงทุน	02-5336174	086-103-3613
ทีมปฏิบัติการระบบสารสนเทศ (IST)			
นายวีระ ชัยวีระวัฒนะ	ผู้อำนวยการกลุ่มบริหารจัดการและพัฒนาระบบสารสนเทศ 1	02-5538292	081-648-8633
นายพงค์พัฒน์ ศรีทิพงศ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	02-5538228	089-853-2233
นายปองพล รอดสวัสดิ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	02-5538395	096-324-5631

ตาราง 4.2-2 รายชื่อบุคคลสำคัญหรือหน่วยงานภายนอกองค์กรที่ต้องติดต่อเมื่อเกิดวิกฤตการณ์หรือเกิดสถานการณ์ฉุกเฉิน

หน้าที่	ชื่อ	โทรศัพท์พื้นฐาน	โทรศัพท์มือถือ
1. ผู้ดูแลระบบ AD - บริษัท ดีเอ็กซ์พี (ไทยแลนด์) จำกัด	คุณสุนทร พยัคสี คุณสมบูรณ์	-	089-899-9307 081-615-3302
2. ผู้ดูแลระบบ e-Mail - สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.)	คุณฐายิกา ภู่ธงแก้ว	02-612-6000 ต่อ 3107	098-991-6445
3. ผู้ดูแลระบบ Web BOI - บริษัท เน็ตเซอร์วิส จำกัด - สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.)	 คุณนันท์นภัส สุขเจริญ คุณฐายิกา ภู่ธงแก้ว	 02-632-9396 ถึง 99 02-612-6000 ต่อ 3107	 080-639-7507 098-991-6445
4. ผู้ดูแลระบบเครือข่ายและการสื่อสาร - บริษัท อินเทอร์เน็ตประเทศไทย จำกัด	INET Data Center หรือ (NOC)	02-257-7111	-
5. ผู้ดูแลเครื่องกำเนิดไฟฟ้า - ฝ่ายอาคารสถานที่ (สกท.)	คุณอัญชรี ทั่งศรี	02-553-8374	081-567-7136 -
6. การไฟฟ้านครหลวง	MEA Care Customer	1130	-
7. เจ้าหน้าที่สารสนเทศ สมาคมสโมสรนักลงทุน	คุณสมโภช เผือกจันทึก	02-936-1429	081-923-2177
8. ผู้ให้บริการคลาวด์ภาครัฐ (G-Cloud) - สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.)	คุณฐายิกา ภู่ธงแก้ว	02-612-6000 ต่อ 3107	098-991-6445

4.3 จัดตั้งสถานที่

เมื่อมีการประกาศภาวะภัยพิบัติ และจำเป็นต้องจัดตั้งศูนย์บัญชาการ มีขั้นตอนการปฏิบัติเพื่อให้การดำเนินงานจัดตั้งศูนย์บัญชาการเป็นไปอย่างมีประสิทธิภาพ และพร้อมรองรับการปฏิบัติงานเมื่อมีการประกาศภาวะภัยพิบัติ ดังนี้

1) ทีมรับมือวิกฤติการณ์แจ้งให้ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน ดำเนินการจัดตั้งศูนย์บัญชาการและศูนย์ปฏิบัติงานสำรอง หรือ เข้าตรวจสอบสภาพสิ่งอำนวยความสะดวกของศูนย์บัญชาการและศูนย์ปฏิบัติงานสำรองให้อยู่ในสภาพพร้อมใช้งาน

2) ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน เข้าตรวจสอบสภาพหรือจัดเตรียมสิ่งอำนวยความสะดวกของศูนย์บัญชาการและศูนย์ปฏิบัติงานสำรองให้อยู่ในสภาพพร้อมใช้งาน และรายงานผลให้กับทีมรับมือวิกฤตการณ์รับทราบ

3) ทีมปฏิบัติการระบบโครงสร้างพื้นฐานจัดทำป้ายและแผนที่เส้นทางเพื่อให้ข้อมูลกับเจ้าหน้าที่ผู้ปฏิบัติงานของทีมอื่น ๆ ได้รับทราบ

4) เมื่อเจ้าหน้าที่ของทีมปฏิบัติการระบบโครงสร้างพื้นฐานและทีมปฏิบัติการระบบสารสนเทศพร้อมดำเนินการปฏิบัติงาน ณ ศูนย์ปฏิบัติงานสำรองให้ทีมรับมือวิกฤติการณ์แจ้งดำเนินการติดต่อแจ้งให้ผู้ใช้งานทราบถึงการเริ่มใช้แผนการบริหาร ความต่อเนื่องในการดำเนินงาน โดยจะต้องแจ้งให้ทราบถึงข้อมูลดังต่อไปนี้

- ข้อมูลเกี่ยวกับภัยพิบัติที่เกิดขึ้น
- ข้อมูลเกี่ยวกับการตัดสินใจของฝ่ายบริหาร
- ข้อมูลเกี่ยวกับตำแหน่งที่ตั้งของศูนย์ปฏิบัติงานสำรอง
- ข้อมูลเพื่อช่วยให้ผู้ใช้งานสามารถเตรียมพร้อมกับการกู้คืนจากภัยพิบัติ

4.4 การรายงานสถานการณ์/วิกฤติการณ์

ผู้บริหารเทคโนโลยีสารสนเทศและการสื่อสารระดับสูงของสำนักงานคณะกรรมการส่งเสริมการลงทุน หรือ CIO จะเป็นผู้ประสานงานหลักในการสื่อสารกับบุคคลภายนอกในระหว่างภัยพิบัติ และพนักงานที่ไม่ได้รับการมอบหมายให้เป็นโฆษกผู้รายงานหรือผู้รับผิดชอบในการประสานงานจะต้องไม่สื่อสารกับบุคคลภายนอก รวมทั้งสื่อหรือนักข่าว เกี่ยวกับเหตุการณ์ที่เกิดขึ้นไม่ว่าในเรื่องใด ๆ ทั้งสิ้น

บทที่ 5. กรณีสมมุติและขั้นตอนในการกู้คืนสภาพการดำเนินธุรกิจ

ในบทนี้จะกล่าวถึงรายละเอียดของการประเมินระดับความล้มเหลวการให้บริการหลักของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail รวมถึงกรณีสมมุติและขั้นตอนในการกู้คืนสภาพการดำเนินงานของระบบ ซึ่งมีรายละเอียดดังนี้

5.1 เกณฑ์การประเมินระดับความล้มเหลว

- กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้ และ **คาดว่าใช้ระยะเวลาการแก้ไขมากกว่า 24 ชั่วโมง**

- กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ห้อง Data Center ที่ BOI (ถ.วิภาวดี) ไม่สามารถให้บริการได้ และ **คาดว่าใช้ระยะเวลาการแก้ไขมากกว่า 24 ชั่วโมง**

5.2 การจัดกลุ่มกรณีสมมุติ

จากเกณฑ์ประเมินระดับความล้มเหลวที่จะส่งผลกระทบต่อการให้บริการระบบ Active Directory ระบบ Website BOI และระบบ e-Mail เกิดหยุดชะงักหรือหยุดการบริการ เพื่อพิจารณานำไปสู่การเริ่มต้นของการนำแผนการบริหารความต่อเนื่องให้กับธุรกิจมาใช้งาน ทั้งนี้เพื่ออำนวยความสะดวกในการกำหนดลำดับขั้นตอน เพื่อสร้างความต่อเนื่องในการดำเนินงาน สำนักงานคณะกรรมการส่งเสริมการลงทุนได้พิจารณากรณีสมมุติเหตุการณ์ด้านความเสี่ยงต่าง ๆ ไว้ ดังนี้

ลำดับ	เหตุการณ์ด้านความเสี่ยง	ระบบที่เกี่ยวข้อง กรณีเกิดเหตุการณ์ฉุกเฉิน	กรณี ประเภท
1	เกิดเพลิงไหม้อย่างรุนแรงที่ สพร. ทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้	- ระบบ Website BOI - ระบบ e-Mail	A
2	เกิดเพลิงไหม้อย่างรุนแรงที่อาคารสำนักงานฯ BOI (ถ.วิภาวดี) ทำให้ห้อง Data Center ไม่สามารถให้บริการได้	- ระบบ Active directory - ชุดที่ 1 (AD ระบบหลัก-BOI) - ชุดที่ 2 (AD ระบบสำรอง-BOI)	B
3	เกิดการโจรกรรมและวินาศกรรมที่ สพร. ทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้	- ระบบ Website BOI - ระบบ e-Mail	A
4	เกิดการโจรกรรมและวินาศกรรมที่อาคารสำนักงานฯ BOI (ถ.วิภาวดี) ทำให้ห้อง Data Center ไม่สามารถให้บริการได้	- ระบบ Active directory - ชุดที่ 1 (AD ระบบหลัก-BOI) - ชุดที่ 2 (AD ระบบสำรอง-BOI)	B
5	มีเหตุการณ์ชุมนุมปิดล้อมที่ สพร.ทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้	- ระบบ Website BOI - ระบบ e-Mail	A
6	มีเหตุการณ์ชุมนุมปิดล้อมที่อาคารสำนักงานฯ BOI (ถ.วิภาวดี) ทำให้ห้อง Data Center ไม่สามารถให้บริการได้	- ระบบ Active directory - ชุดที่ 1 (AD ระบบหลัก-BOI) - ชุดที่ 2 (AD ระบบสำรอง-BOI)	B
7	ระบบไฟฟ้าขัดข้องเป็นวงกว้าง จนมีผลทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้	- ระบบ Website BOI - ระบบ e-Mail	A
8	ระบบไฟฟ้าขัดข้องเป็นวงกว้าง จนมีผลทำให้ห้อง Data Center ที่อาคารสำนักงาน BOI (ถ.วิภาวดี) ไม่สามารถให้บริการได้	- ระบบ Active directory - ชุดที่ 1 (AD ระบบหลัก-BOI) - ชุดที่ 2 (AD ระบบสำรอง-BOI)	B
9	เกิดอุทกภัย จนมีผลทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้	- ระบบ Website BOI - ระบบ e-Mail	A
10	เกิดอุทกภัย จนมีผลทำให้ห้อง Data Center ที่อาคารสำนักงานฯ BOI (ถ.วิภาวดี) ไม่สามารถให้บริการได้	- ระบบ Active directory - ชุดที่ 1 (AD ระบบหลัก-BOI) - ชุดที่ 2 (AD ระบบสำรอง-BOI)	B

หมายเหตุ:

กรณีประเภท A หมายถึง กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้

กรณีประเภท B หมายถึง กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ห้อง Data Center ที่อาคารสำนักงานฯ BOI (ถ.วิภาวดี) ไม่สามารถให้บริการได้

5.3 ข้อกำหนดทางด้านเวลาในการตอบสนองและกำลังคนขั้นต่ำ

เพื่อให้การดำเนินการกู้คืนระบบเป็นไปอย่างมีประสิทธิภาพ ศทส. มีการกำหนดทีมงาน และเวลาในการตอบสนองสูงสุด รวมทั้งความต้องการทรัพยากรขั้นต่ำทางด้านกำลังคน ในช่วงเวลาปกติ และช่วงเวลาวิกฤติไว้ดังนี้

ตาราง 5.3-1 ความต้องการทรัพยากรขั้นต่ำของบุคลากรเพื่อการดำเนินการกู้คืนระบบ

ทีมกู้คืนระบบ	เวลาในการตอบสนอง	ความต้องการด้านกำลังคนปกติ	ความต้องการด้านกำลังคนในภาวะวิกฤติ
ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน	1 ชั่วโมง	3	1
ทีมปฏิบัติการระบบสารสนเทศ	1 ชั่วโมง	3	2

หมายเหตุ : เวลาในการตอบสนอง หมายถึง ระยะเวลาความพร้อม

5.4 ระยะเวลาในการเริ่มดำเนินการใหม่และการกู้คืนระบบ

การดำเนินการกู้คืนระบบให้มีความต่อเนื่องได้นั้น ศทส. ได้กำหนดระยะเวลา และกลยุทธ์ตามบริการที่สำคัญไว้ ดังนี้

ตาราง 5.4-1 ระยะเวลาในการเริ่มดำเนินการใหม่และการกู้คืนระบบ

ลำดับที่	บริการ	เป้าหมายด้านระยะเวลาที่ใช้ในการกู้ระบบ - T2	การกำหนดกลยุทธ์
1	การให้บริการระบบ Active Directory	T2 + 4 hours	Hot Site
2	การให้บริการระบบ Website BOI	T2 + 4 hours	Warm Site
3	การให้บริการ e-Mail	T2 + 4 hours	Hot Site

หมายเหตุ:

- T2 หมายถึง เวลาที่ประกาศภาวะภัยพิบัติ

- Hot Site หมายถึง ระบบสำรองที่สามารถทำงานได้ทันที ที่ระบบหลักมีปัญหา มีลักษณะเป็น Mirror Site (ระบบสำรองที่ทำงานเหมือนระบบจริง ติดตั้งอยู่อีกสถานที่หนึ่ง ซึ่งมีการเชื่อมเครือข่ายถึงกัน และปรับปรุงข้อมูลแบบเรียลไทม์)

- Warm Site หมายถึง ระบบสำรองที่สามารถทำงานได้ก็ต่อเมื่อ มีการดำเนินการติดตั้งระบบ อัพเดทข้อมูล ฐานข้อมูล หรือระบบงานบ้างถึงจะใช้งานได้

5.5 ขั้นตอนการปฏิบัติเพื่อสร้างความต่อเนื่อง ตามกรณีสมมุติ/เหตุการณ์

เพื่อให้การดำเนินงานกู้คืนสภาพการดำเนินงานของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail เป็นไปอย่างมีประสิทธิภาพ ศทส. ได้กำหนดขั้นตอนการปฏิบัติของการดำเนินงานตามกรณีสมมุติทั้ง 2 กรณีในข้อ 5.2 ดังนี้

กรณีเหตุการณ์ประเภท A

ชื่อกรณีสมมุติ/เหตุการณ์ - กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้			
รายละเอียดของกรณีสมมุติ - กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้			
สมมุติฐาน - ระบบบริการคลาวด์ภาครัฐ (G-Cloud) ของ สพร. ไม่สามารถให้บริการได้ - ระบบไฟฟ้า/ระบบเครือข่าย ไม่สามารถใช้งานได้ - มีผลให้ระบบ Web boi ไม่สามารถให้บริการได้ - มีผลให้ระบบ E-Mail ไม่สามารถให้บริการได้ - DR-Site : ติดตั้งอยู่ที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)			
ระยะเวลาเป้าหมายในการกู้คืนการให้บริการ - 4 ชั่วโมง			
กระบวนการกู้คืนการให้บริการ			
เวลา (ชั่วโมง)	**ขั้นตอนในการรับมือกับวิกฤติการณ์**	**หมายเหตุ / เอกสารอ้างอิง**	**ดำเนินการโดย**
T0	- รับแจ้งเหตุ		- ทีมรับมือวิกฤตการณ์ (CMT)
T0 + 0.05	- ตรวจสอบข้อเท็จจริง ประเมินสถานการณ์เบื้องต้น และแจ้งผู้เกี่ยวข้อง	- รายชื่อผู้ที่เกี่ยวข้อง (Call Tree)	- ทีมรับมือวิกฤตการณ์ (CMT)
T1 + 1.00	- ประเมินความเสียหายให้แล้วเสร็จภายใน 1 ชั่วโมง		- ทีมรับมือวิกฤตการณ์ (CMT)
T2	- ประกาศภาวะภัยพิบัติ		- ISMR
T2 + 0.01	- แจ้งทีมปฏิบัติการระบบโครงสร้างพื้นฐาน (CNT) และทีมปฏิบัติการระบบสารสนเทศ (IST) เพื่อให้เริ่มปฏิบัติงานตามแผนการบริหารความต่อเนื่องให้กับธุรกิจ	- รายชื่อทีม (CNT) - รายชื่อทีม (IST)	- ทีมรับมือวิกฤตการณ์ (CMT)

เวลา (ชั่วโมง)	ขั้นตอนในการรับมือกับวิกฤติการณ์	หมายเหตุ / เอกสารอ้างอิง	ดำเนินการโดย
T2 + 0.15	- ประสานงานกับผู้ดูแลระบบ E-Mail และ Web Site BOI เพื่อตรวจสอบ และนำข้อมูลที่ทำการสำรองไว้ ไปปรับปรุงข้อมูลให้เป็นปัจจุบัน และปรับแต่ง Service ของระบบ E-Mail และ Website BOI บน Cloud ของ สพร. ให้สามารถให้บริการแทนระบบหลักได้	- รายชื่อบุคคลสำคัญหรือหน่วยงานภายนอกองค์กร	- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 0.30	- แจ้งผู้ใช้งานทราบถึงสาเหตุและระยะเวลาที่ใช้ในการแก้ไขโดยประมาณผ่านทาง SMS		- ทีมรับมือวิกฤตการณ์ (CMT)
T2 + 1.15	- สอบถามความคืบหน้ากับผู้ดูแลระบบ E-Mail และ Website BOI ถึงการดำเนินการปรับแต่งระบบสำรองให้สามารถใช้งานแทนระบบหลัก (ในกรณีที่ผู้ดูแลระบบดำเนินการนานเกินกว่า 1 ชั่วโมงและไม่มีการแจ้งผลกลับมาที่ IST) - กำหนดเวลาดำเนินการแล้วเสร็จภายใน 2 ชม. นับจาก (T2 + 1.15)	- รายชื่อบุคคลสำคัญหรือหน่วยงานภายนอกองค์กร	- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.15	- สอบถามผลสำเร็จในการแก้ไขระบบ E-Mail และ Website BOI กับผู้ดูแลระบบ	-	- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.30	- ดำเนินการทดสอบการใช้งานระบบ E-Mail และ Website BOI	-	- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.45	- แจ้งทีมรับมือวิกฤตการณ์ (CMT) ถึงผลการทดสอบการใช้งานระบบ E-Mail และ Website BOI	-	- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.50	- แจ้งให้ผู้ใช้งานทราบว่าระบบ E-Mail และ Website BOI พร้อมใช้งานแล้วผ่านทาง SMS และ E-Mail	-	- ทีมรับมือวิกฤตการณ์ (CMT)

กรณีเหตุการณ์ประเภท B

ชื่อกรณีสมมุติ/เหตุการณ์ - กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ศูนย์ข้อมูลที่ BOI (ถ.วิภาวดี) ไม่สามารถให้บริการได้			
รายละเอียดของกรณีสมมุติ - กรณีเกิดเหตุภัยพิบัติ/เหตุการณ์ จนมีผลทำให้ศูนย์ข้อมูลที่ BOI (ถ.วิภาวดี) ไม่สามารถให้บริการได้			
สมมุติฐาน - ศูนย์ข้อมูลที่ BOI (ถ.วิภาวดี) ไม่สามารถให้บริการได้ - ระบบไฟฟ้า/ระบบเครือข่าย ไม่สามารถใช้งานได้ - มีผลให้ระบบ Active Directory ไม่สามารถให้บริการได้ - DR-Site: ติดตั้งอยู่ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) (INET)			
ระยะเวลาเป้าหมายในการกู้คืนการให้บริการ - 4 ชั่วโมง			
กระบวนการกู้คืนการให้บริการ			
เวลา (ชั่วโมง)	**ขั้นตอนในการรับมือกับวิกฤติการณ์**	**หมายเหตุ / เอกสารอ้างอิง**	**ดำเนินการโดย**
T0	- รับแจ้งเหตุ	-	- ทีมรับมือวิกฤตการณ์ (CMT)
T0 + 0.05	- ตรวจสอบข้อเท็จจริง ประเมินสถานการณ์เบื้องต้น และแจ้งผู้เกี่ยวข้อง	- รายชื่อผู้ที่เกี่ยวข้อง (Call Tree)	- ทีมรับมือวิกฤตการณ์ (CMT)
T1 + 1.00	- ประเมินความเสียหายให้แล้วเสร็จภายใน 1 ชั่วโมง	-	- ทีมรับมือวิกฤตการณ์ (CMT)
T2	- ประกาศภาวะภัยพิบัติ		- ISMR
T2 + 0.01	- แจ้งทีมปฏิบัติการระบบโครงสร้างพื้นฐาน (CNT) และทีมปฏิบัติการระบบสารสนเทศ (IST) เพื่อให้เริ่มปฏิบัติงานตามแผนการบริหารความต่อเนื่องให้กับธุรกิจ	- รายชื่อทีม (CNT) - รายชื่อทีม (IST)	- ทีมรับมือวิกฤตการณ์ (CMT)
T2 + 0.15	- แจ้งผู้ดูแลระบบเครือข่ายและการสื่อสารของ INET เพื่อปรับแต่ง DNS ให้เรียกไปที่ระบบ Active Directory ที่ติดตั้งไว้ที่ ศูนย์ IDC ของ INET รวมถึงปรับแต่ง DNS ให้เรียกไปที่ระบบ E-Mail และ Website BOI บน Cloud ของ สพร. โดยผ่าน INTERNET (Public IP)	- รายชื่อบุคคลสำคัญหรือหน่วยงานภายนอกองค์กร - เอกสารคู่มือการกู้คืนระบบ	- ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน (CNT)

เวลา (ชั่วโมง)	ขั้นตอนในการรับมือกับวิกฤติการณ์	หมายเหตุ / เอกสารอ้างอิง	ดำเนินการโดย
T2 + 0.15	- ประสานงานกับผู้ดูแลระบบ Active Directory เพื่อดำเนินการสลับมาใช้งานระบบ Active Directory ที่ติดตั้งไว้ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)	- รายชื่อบุคคลสำคัญหรือหน่วยงานภายนอกองค์กร	- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 0.30	- แจ้งให้ผู้ใช้งานทราบถึงสาเหตุและระยะเวลาที่ใช้ในการแก้ไขโดยประมาณผ่านทาง SMS	-	- ทีมรับมือวิกฤตการณ์ (CMT)
T2 + 1.15	- สอบถามความคืบหน้ากับผู้ดูแลระบบ Active Directory ถึงการดำเนินการสลับมาใช้งานระบบ Active Directory ที่ติดตั้งไว้ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) (INET) (ในกรณีที่ผู้ดูแลระบบดำเนินการนานเกินกว่า 1 ชั่วโมงและไม่มีการแจ้งผลกลับมาที่ IST) - กำหนดเวลาดำเนินการแล้วเสร็จภายใน 2 ชม. นับจาก (T2 + 1.15)	-	- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.15	- สอบถามผลสำเร็จในการแก้ไขระบบระบบ Active Directory กับผู้ดูแลระบบ		- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.30	- ดำเนินการทดสอบการใช้งานระบบ Active Directory		- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.45	- แจ้งทีมรับมือวิกฤตการณ์ (CMT) ถึงผลการทดสอบการใช้งานระบบ Active Directory		- ทีมปฏิบัติการระบบสารสนเทศ (IST)
T2 + 3.50	- แจ้งให้ผู้ใช้งานทราบว่าระบบ Active Directory พร้อมใช้งานแล้วผ่านทาง SMS และ E-Mail		- ทีมรับมือวิกฤตการณ์ (CMT)

5.6 การทดสอบแผนการบริหารความต่อเนื่องให้กับธุรกิจ การประเมินผลการทดสอบ และการพิจารณาปรับปรุง

ทีมรับมือวิกฤติการณ์ ทีมปฏิบัติการระบบโครงสร้างพื้นฐาน และทีมปฏิบัติการระบบสารสนเทศควร **ซักซ้อมทดสอบแผนฯ อย่างน้อยปีละ 1 ครั้ง** เพื่อให้แน่ใจว่าสิ่งที่ระบุภายในแผนฯ หรือสิ่งที่เปลี่ยนแปลงเพิ่มเติมใหม่ สามารถใช้งานได้จริง และแผนฉบับนี้ได้ปรับปรุงตามผลการทดสอบของครั้งที่ผ่านมา