ด่วน

บันทึกข้อความ

ส่วนราชการ ศูนย์สารสนเทศ กรมประมง โทร./โทรสาร. ๐ ๒๙๔๐ ๖๒๒๕ ภายใน ๑๓๕๐๗

ที่ กษ ๐๕๐๘/ ๖๒๒๕ **วันที่** ๒๖ สิงหาคม ๒๕๕๔

เรื่อง ลงนามประกาศ

เรียน ท่านรองฯ นันทิยา อุ่นประเสริฐ

ศูนย์สารสนเทศขอเสนอประกาศนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมประมง และ ประกาศแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ กรมประมง ซึ่งได้ปรับแก้ไขแล้วมาเพื่อโปรดพิจารณา ดังรายละเอียดแนบพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบด้วยดำริ โปรดกรุณามอบฝ่ายนิติการ สจป. ตรวจสอบเสนอภายในวันที่ ๓๐ สิงหาคม ๒๕๕๔ (เนื่องจากข้อกำหนดการปฏิบัติราชการ PMQA หมวด ๔ กำหนดให้ส่วนราชการจัดทำและประกาศนโยบายและแผนดังกล่าว ให้แล้วเสร็จภายใน ๓๑ สิงหาคม ๒๕๕๔) เพื่อลงนามประกาศใช้ และแจ้งเวียนให้หน่วยงานทราบต่อไป

(นายจุฬ สินชัยพานิช)
ผู้อำนวยการศูนย์สารสนเทศ

มอบฝ่ายนิติการ สจป
ตรวจสอบ ภายใน 30 สิงหาคม

(นางนันทิยา อุ่นประเสริฐ)
รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมประมง
๒๙ ส.ค. ๒๕๕๔

เรียน ผ.กนก.
เพื่อโปรดพิจารณา

(นางกานต์พิชชา พึ่งพร)
นิติกรชำนาญการพิเศษ
รักษาราชการแทนผู้อำนวยการสำนักบริหารจัดการด้านการประมง
๓๐ ส.ค. ๒๕๕๔

เรียน ผ. กลุ่มนิติการ
- ทราบ/ตรวจสอบ

(นายประเทศ ขอรักษ์)
หัวหน้ากลุ่มนิติการ

คุณกานต์พิชชา
ตรวจสอบ

๓๐ ส.ค. ๕๔
(นางกานต์พิชชา พึ่งพร)
หัวหน้าฝ่ายนิติกรรมและสัญญา

บันทึกข้อความ

ส่วนราชการ สำนักบริหารจัดการด้านการประมง กลุ่มนิติการ โทร ๐ ๒๕๖๑ ๒๙๒๘ ,๒๒๐๓

ที่ กษ ๐๕๑๐.๔/ ส๐๙ **วันที่** ๓๐ สิงหาคม ๒๕๕๔

เรื่อง ตรวจสอบประกาศ

เรียน ผู้อำนวยการสำนักบริหารจัดการด้านการประมง (ผ่านหัวหน้ากลุ่มนิติการ)

ตามที่ศูนย์สารสนเทศได้มีหนังสือ ที่ กษ ๐๕๐๘/๑๘๘๔ ลงวันที่ ๒๖ สิงหาคม ๒๕๕๔ ขอให้กลุ่มนิติการ สำนักบริหารจัดการด้านการประมง พิจารณาตรวจสอบประกาศนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมประมง และประกาศแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ กรมประมง นั้น

กลุ่มนิติการได้พิจารณาตรวจสอบประกาศดังกล่าวแล้วเห็นว่า ข้อความตามประกาศมีเนื้อหาสาระครอบคลุมสอดคล้องกับวัตถุประสงค์แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้วยสารสนเทศของหน่วยงานของรัฐแล้ว

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบโปรดเสนอท่านรองฯ นันทิยา อุ่นประเสริฐ ด้วย จะขอบคุณมาก

(นายศรชัย อำนวย)
นิติกรปฏิบัติการ

๓๐ ส.ค. ๕๔
(นางกานต์พิชชา พึ่งพร)
หัวหน้าฝ่ายนิติกรรมและสัญญา

เรียน ท่านรองนันทิยา ฯ
เพื่อโปรดพิจารณา

(นางกานต์พิชชา พึ่งพร)
นิติกรชำนาญการพิเศษ
รักษาราชการแทนผู้อำนวยการสำนักบริหารจัดการด้านการประมง
๓๑ ส.ค. ๒๕๕๔

(นางรสสนา สามมาน)
หัวหน้าฝ่ายสารบรรณ
แทนเลขานุการกรม
๓๑ ส.ค. ๒๕๕๔

(นางนันทิยา อุ่นประเสริฐ)
รองอธิบดี รักษาราชการแทน
อธิบดีกรมประมง
๓๑ ส.ค. ๒๕๕๔

ประกาศกรมประมง

เรื่อง แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ กรมประมง

(IT Contingency Plan)

ด้วยข้อมูลสารสนเทศถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ กรมประมงได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบ ทำให้ระบบฐานข้อมูลและสารสนเทศรวมทั้งระบบอุปกรณ์เสียหายได้

ดังนั้น เพื่อเป็นการป้องกันปัญหาดังกล่าว จึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อกำหนดขั้นตอนและรายละเอียดการปฏิบัติสำหรับการแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
๒. การกำหนดแนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
๕. การกำหนดมาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ
๖. การกู้คืนระบบกลับสู่สภาพปกติเดิม
๗. การติดตามและรายงานผล

โดยมีรายละเอียดดังต่อไปนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๑.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่ ๑) ภัยพิบัติจากภายนอก เช่น ภัยธรรมชาติ ระบบกระแสไฟฟ้าขัดข้อง การโจรกรรมอุปกรณ์คอมพิวเตอร์และแม่ข่าย ๒) ภัยพิบัติจากภายใน เช่น ระบบฐานข้อมูลหลักเสียหาย ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์

๑.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ (Security Log Management System) โดยเจ้าหน้าที่ศูนย์สารสนเทศ เพื่อนำมาสรุปเป็นข้อมูลต่อไป

/๒. การกำหนด...

๒. การกำหนดแนวทางการป้องกันและการเตรียมการเบื้องต้น

๒.๑ การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารแสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ

๒.๒ กระบวนการดำเนินงาน (Procedure)

องค์กรมีการจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น

๒.๓ การติดต่อสื่อสาร (Communication)

องค์กรมีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้ในการติดต่อประสานด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น นอกจากนี้องค์กรมีการเตรียมการประสานงานกับสถานีดับเพลิง เรื่องแผนที่อาคารและเส้นทางการเดินทางด้วย

๒.๔ การจัดเตรียมอุปกรณ์ที่จำเป็น

องค์กรมีการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศขององค์กร โดยศูนย์สารสนเทศเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ ซึ่งอุปกรณ์ที่จำเป็นต้องเตรียมพร้อมมีดังนี้

๒.๔.๑ แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
๒.๔.๒ เทปสำรองข้อมูลและระบบงานที่สำคัญ
๒.๔.๓ แผ่นโปรแกรม antivirus/spyware
๒.๔.๔ แผ่น driver อุปกรณ์ต่างๆ
๒.๔.๕ ระบบสำรองไฟฉุกเฉิน
๒.๔.๖ อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๒.๕ การสำรองข้อมูล (Backup)

องค์กรมีการสำรองข้อมูลเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้

๒.๖ การป้องกันไวรัสคอมพิวเตอร์

องค์กรมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบ และอัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย

๒.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

องค์กรมีการป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ ดังนี้

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

/๒.๗.๒ เปิดเครื่อง...

๒.๗.๒ เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๒.๗.๓ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๒.๗.๔ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๒.๘ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

องค์กรมีการป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย โดยมีแนวทาง ดังนี้

๒.๘.๑ มาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์สารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้า-ออก มีการติดตั้งระบบ Access Control โดยใช้ Key Card และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๒.๘.๒ มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

๒.๘.๓ มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๒.๘.๔ มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๒.๘.๕ การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๒.๘.๖ มีการป้อนชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิ์ก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๒.๙ การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

องค์กรมีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ ดังนี้

๒.๙.๑ เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ

๒.๙.๒ ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

๒.๙.๓ ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า

๒.๙.๔ ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๒.๙.๕ ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๒.๙.๖ ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจนและเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

/๓. การเตรียมความพร้อม...

๓. การเตรียมความพร้อม

๓.๑ การเตรียมความพร้อมรับสถานการณ์ฉุกเฉิน เมื่อเกิดเหตุไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

องค์กรมีการเตรียมความพร้อมรับสถานการณ์ฉุกเฉิน เมื่อเกิดเหตุไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๓.๑.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อไฟระเบิด

๓.๑.๒ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าโดยประมาณ ๓๐-๖๐ นาที

๓.๑.๓ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓.๑.๔ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๓.๑.๕ ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

๓.๒ การเตรียมความพร้อมรับสถานการณ์ฉุกเฉิน เมื่อเกิดเหตุไฟไหม้

องค์กรมีการเตรียมความพร้อมรับสถานการณ์ฉุกเฉินเมื่อเกิดเหตุไฟไหม้ เพื่อเป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๓.๒.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

๓.๒.๒ ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่ายเพื่อการควบคุมเพลิงในเบื้องต้น

๓.๒.๓ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๓.๓ การเตรียมความพร้อมรับสถานการณ์ฉุกเฉิน เมื่อเกิดเหตุน้ำท่วม/น้ำรั่ว

องค์กรมีการเตรียมความพร้อมรับสถานการณ์ฉุกเฉินเมื่อเกิดเหตุน้ำท่วม/น้ำรั่ว เพื่อเป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม/น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ โดยกำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศดังนี้

๓.๓.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม/น้ำรั่ว

๓.๓.๒ มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

๓.๓.๓ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

/๓.๔. การเตรียม...

๓.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

องค์กรมีการเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว เพื่อเป็นการเตรียมความพร้อมเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัยได้ดังนี้

๓.๔.๑ ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัย จากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

๑) กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย (www.tmd.go.th)

๒) ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า (www.ndwc.thaigov.go.th)

๓) กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม/แผ่นดินไหว (www.dmr.go.th)

๔) หน่วยงานสำรวจเชิงภูมิศาสตร์ ประเทศสหรัฐอเมริกา : ข้อมูลสถานการณ์แผ่นดินไหวทั่วโลก (www.earthquake.usgs.gov)

๕) กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการและแนวทางปฏิบัติ (www.disaster.go.th)

๓.๔.๒ การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

๑) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู

๒) แมลงสาบจำนวนมากวิ่งเพ่นพ่าน

๓) หนู งู วิ่งออกมาจากที่อาศัยถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน

๔) ปลากระโดดขึ้นมาจากผิวน้ำ

๓.๔.๓ การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

๑) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน

๒) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่างๆ ตามความจำเป็นและเหมาะสม

๓) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรขององค์กร

๔) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

/๕) จัดเตรียม...

๕) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่างๆ

๓.๔.๔ การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

๑) สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

๒) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

๓.๔.๕ การปฏิบัติขั้นเตรียมการ

๑) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม

๒) การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญภัย

๓) อบรม ให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่บุคลากรในองค์กร

๔) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๓.๕ การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

องค์กรมีการเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล เพื่อเป็นการเตรียมความพร้อมเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัยได้ดังนี้

๓.๕.๑ ดำเนินการหาข่าวจากแหล่งต่างๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

๓.๕.๒ จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๓.๕.๓ ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ให้อยู่ในสภาพที่พร้อมใช้งาน

๓.๕.๔ ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรมีการจัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๔.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

อธิบดีกรมประมง (CEO)

รองอธิบดีกรมประมง (CIO)

ผู้อำนวยการศูนย์สารสนเทศ

/๔.๒ ระดับ...

๔.๒ ระดับปฏิบัติ

๔.๒.๑ ทีมบริหารจัดการการกู้คืนระบบ มีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ

๔.๒.๒ ทีมกู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ

๔.๒.๓ ทีมกู้คืนแอพพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน

๔.๒.๔ ทีมประเมินความเสียหาย เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน

๔.๒.๕ ทีมอาคารสถานที่ เป็นทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร แอร์ ให้พร้อมใช้งาน

๔.๒.๖ ทีมการจัดการทั่วไป เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทำงาน

๔.๒.๗ ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ศูนย์สารสนเทศได้จัดหาไว้

๔.๒.๘ ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ/หม้อไฟระเบิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่

๔.๒.๙ ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม

๔.๒.๑๐ ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย

๔.๒.๑๑ ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์

๕. การกำหนดมาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

องค์กรมีการกำหนดมาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ โดยกำหนดแนวทางให้บุคลากรปฏิบัติ ดังนี้

๕.๑ กรณีเครื่องลูกข่าย

๕.๑.๑ ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุขัดข้องให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศของหน่วยงานทราบ หรือในกรณีเกิดจากศูนย์สารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์สารสนเทศต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

๕.๑.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๕.๑.๓ ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้ ให้แจ้งเหตุขัดข้องให้ศูนย์สารเทศเพื่อแก้ไขปัญหาต่อไป

/๕.๒ กรณี...

๕.๒ กรณีเครื่องแม่ข่ายบริการ (Server)

๕.๒.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๕.๒.๒ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๕.๒.๓ ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๕.๒.๔ ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๕.๒.๕ กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว

๕.๒.๖ รีบดำเนินการขนย้ายเครื่องไว้ในที่ปลอดภัย

๕.๒.๗ ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๕.๒.๘ ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์ มาเปลี่ยนโดยเร็วที่สุด

๕.๒.๙ ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์สารสนเทศทราบโดยเร็ว

๖. การกู้คืนระบบกลับสู่สภาพปกติเดิม

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่าย และอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้เร็วที่สุด จึงได้จัดทำแผนการกู้คืนระบบกลับสู่สภาพปกติเดิม เป็นขั้นตอนปฏิบัติเพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลสามารถกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการ ดังนี้

๖.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๖.๒ เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๖.๓ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๖.๔ ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๖.๕ นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๖.๖ ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

ทั้งนี้องค์กรมีแผนจัดทำการสำรองแหล่งข้อมูลที่ศูนย์สำรอง (ไซต์สำรอง) เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ โดยแบ่งไซต์ได้ ๓ ไซต์ คือ

๑) Hot Site เป็นไซต์ที่มีอุปกรณ์และซอฟต์แวร์เหมือนไซต์หลัก มีความพร้อมใช้งานทำให้เวลาในการกู้คืนระบบน้อยแต่จะมีต้นทุนการจัดทำที่สูง

๒) Warm Site เป็นไซต์ที่คล้ายกับ Hot site แต่อาจจะมีอุปกรณ์ไม่ครบทำให้ความพร้อมใช้งานต่ำกว่า Hot site ใช้ระยะเวลาในการกู้คืนมากกว่า แต่ต้นทุนราคาการจัดทำน้อยกว่า Hot site

๓) Cold Site เป็นไซต์ที่มีแต่สถานที่ ไม่มีอุปกรณ์ทั้ง Hardware และ Software ในการกู้คืนมีต้นทุนการจัดทำต่ำ แต่ระยะเวลาในการกู้คืนนาน

/๗. การติดตาม...

๗. การติดตามและรายงานผล

องค์กรมีการกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้อำนวยการศูนย์สารสนเทศทราบ เพื่อนำเสนอรายงานสรุปให้ CEO หรือ CIO และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงทีในกรณีที่เกิดภัยพิบัติต่อไป

องค์ประกอบของแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัตินี้เป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๓๑ สิงหาคม พ.ศ. ๒๕๕๔

(นางนันทิยา อุ่นประเสริฐ)
รองอธิบดีกรมประมง
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง