แผนการสื่อสารในภาวะวิกฤต
(Crisis Communication Management)
เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
ของกรมกิจการสตรีและสถาบันครอบครัว

คำนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศกลายเป็นหัวใจสำคัญของการดำเนินงานของหน่วยงาน ความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นประเด็นที่มีความสำคัญอย่างยิ่งและเป็นความท้าทายที่หน่วยงานทุกแห่งต้องเผชิญ การจัดการกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ไม่เพียงแต่เป็นการป้องกันการสูญเสียข้อมูลและการหยุดชะงักของดำเนินงาน แต่ยังมีผลกระทบต่อความเชื่อมั่นของประชาชนผู้รับบริการและผู้มีส่วนได้เสีย ซึ่งต้องการการตอบสนองที่รวดเร็วและมีประสิทธิภาพ

แผนการสื่อสารในภาวะวิกฤตนี้ถูกออกแบบมาเพื่อจัดการกับสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นระบบและมีประสิทธิภาพ โดยการจัดตั้งทีมสื่อสารวิกฤต ซึ่งประกอบด้วย ทีม IT ทีมประชาสัมพันธ์ ทีมกฎหมาย และทีมบริหารความเสี่ยง เพื่อให้การสื่อสารมีความแม่นยำและตรงตามสถานการณ์ที่เกิดขึ้น ทีมงานเหล่านี้จะทำงานร่วมกันเพื่อให้แน่ใจว่าข้อมูลที่เผยแพร่จะเป็นไปอย่างถูกต้องและทันเวลา

การจัดทำแผนการสื่อสารนี้ไม่เพียงแต่จะช่วยให้การรับมือกับวิกฤตเป็นไปอย่างเป็นระบบ แต่ยังเป็นการสร้างความเชื่อมั่นให้กับประชาชนผู้รับบริการและผู้มีส่วนได้เสียว่าหน่วยงานมีความสามารถในการจัดการกับเหตุการณ์ที่ไม่คาดคิดอย่างมืออาชีพและมีประสิทธิภาพ โดยมุ่งหวังว่าแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Management) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์นี้จะเป็นเครื่องมือที่สำคัญในการลดผลกระทบของเหตุการณ์และทำให้กระบวนการฟื้นฟูและการตอบสนองเป็นไปอย่างมีประสิทธิภาพสูงสุด

กองยุทธศาสตร์และแผนงาน
กรมกิจการสตรีและสถาบันครอบครัว

สารบัญ

1. หลักการและเหตุผล 1
2. วัตถุประสงค์ 1
3. ขอบเขต 2
4. คำนิยาม 3
5. แผนการดำเนินงาน 4
   (1) กำหนดและจัดประเภทเหตุการณ์ที่อาจเป็นวิกฤตทางไซเบอร์ 5
   (2) จัดตั้งทีมสื่อสารในภาวะวิกฤต (Crisis Communication Team: CCT) 5
   (3) การวางแผนและการเตรียมความพร้อม 8
   (4) การสื่อสารภายในหน่วยงาน 9
   (5) การสื่อสารกับประชาชนและผู้มีส่วนได้เสีย 10
   (6) การติดตามและประเมินผล 10
   (7) การฟื้นฟูและการดำเนินการหลังเหตุการณ์ 11
   (8) การฝึกอบรมและการทบทวนแผนการสื่อสารในภาวะวิกฤต 12
6. แนวปฏิบัติเมื่อเกิดเหตุการณ์วิกฤต 13
7. การทบทวนปรับปรุงแผน 18

แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Management) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ของกรมกิจการสตรีและสถาบันครอบครัว

1. หลักการและเหตุผล

ในยุคที่การพึ่งพาเทคโนโลยีสารสนเทศสูงขึ้น การรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงกลายเป็นภารกิจที่สำคัญสำหรับหน่วยงานทุกระดับ การเกิดเหตุการณ์วิกฤตทางไซเบอร์ เช่น การโจมตีทางไซเบอร์ การรั่วไหลของข้อมูล หรือการบุกรุกระบบ สามารถสร้างผลกระทบร้ายแรงต่อการดำเนินงานของหน่วยงาน รวมถึงความเชื่อมั่นของประชาชนผู้รับบริการและผู้มีส่วนได้เสีย การมีแผนการสื่อสารในภาวะวิกฤตที่มีความชัดเจนและมีประสิทธิภาพจึงเป็นสิ่งจำเป็นในการจัดการกับสถานการณ์เหล่านี้อย่างรวดเร็วและมีประสิทธิภาพ

การออกแบบแผนการสื่อสารในภาวะวิกฤตนี้มีพื้นฐานมาจากหลักการสำคัญหลายประการ เช่น การรักษาความโปร่งใสในการสื่อสาร การจัดการข้อมูลอย่างมีระบบ และการตอบสนองอย่างรวดเร็วและแม่นยำ ดังนั้น กรมกิจการสตรีและสถาบันครอบครัว จึงได้จัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Management) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ โดยมุ่งเน้นการประสานงานอย่างใกล้ชิดระหว่างทีม IT ทีมประชาสัมพันธ์ ทีมกฎหมาย และทีมบริหารความเสี่ยง เพื่อให้การสื่อสารในสถานการณ์วิกฤตมีความถูกต้องและทันเวลา ช่วยลดความเสียหายและผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์วิกฤต

2. วัตถุประสงค์

(1) เพื่อให้หน่วยงานสามารถตอบสนองต่อเหตุการณ์วิกฤตทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ ลดผลกระทบต่อการดำเนินงานและความเชื่อมั่นของประชาชนและผู้มีส่วนได้เสีย

(2) เพื่อให้การสื่อสารในภาวะวิกฤตมีความโปร่งใสและแม่นยำ โดยการให้ข้อมูลที่ถูกต้อง และทันเวลาต่อประชาชนและผู้มีส่วนได้เสีย ลดการเผยแพร่ข่าวสารที่ผิดพลาดและป้องกันความสับสน

(3) เพื่อให้การสื่อสารในภาวะวิกฤตเป็นไปอย่างมีระบบ โดยการจัดการข้อมูลที่เผยแพร่ให้มีระเบียบและสอดคล้องกัน เพื่อความเข้าใจที่ชัดเจน

(4) เพื่อให้หน่วยงานมารถฟื้นฟูการดำเนินงานและการบริการกลับสู่สภาวะปกติได้อย่างรวดเร็วและมีประสิทธิภาพ โดยการลดผลกระทบจากเหตุการณ์วิกฤตและเสริมสร้างความเชื่อมั่นของหน่วยงานในการจัดการกับสถานการณ์ที่ไม่คาดคิด

3. ขอบเขต

แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Management) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของกรมกิจการสตรีและสถาบันครอบครัว มีขอบเขตครอบคลุม ดังนี้

(1) การระบุเหตุการณ์วิกฤต

- กำหนดและจัดประเภทเหตุการณ์ที่อาจเป็นวิกฤตทางไซเบอร์ เช่น การโจมตีทางไซเบอร์ การรั่วไหลของข้อมูลสำคัญ การแทรกแซงระบบ หรือปัญหาด้านความมั่นคงที่ร้ายแรง
- การประเมินความรุนแรงและผลกระทบของเหตุการณ์ที่เกิดขึ้น เพื่อกำหนดลำดับความสำคัญในการตอบสนอง

(2) การจัดตั้งทีมสื่อสารวิกฤต

- การจัดตั้งและระบุสมาชิกทีมสื่อสารวิกฤต ซึ่งรวมถึงทีม IT ทีมประชาสัมพันธ์ ทีมกฎหมาย และทีมบริหารความเสี่ยง
- การกำหนดบทบาทและความรับผิดชอบของแต่ละทีมในการตอบสนองและจัดการกับเหตุการณ์วิกฤต

(3) การวางแผนและการเตรียมความพร้อม

- การพัฒนาแผนการสื่อสารที่ครอบคลุมกลยุทธ์และแนวทางในการจัดการกับสถานการณ์วิกฤตทางไซเบอร์
- การเตรียมข้อความหลักและข้อมูลที่ต้องการเผยแพร่ในกรณีที่เกิดวิกฤต รวมถึงการเตรียมตัวสำหรับการประชาสัมพันธ์และการตอบสนองต่อสื่อมวลชน

(4) การสื่อสารภายในหน่วยงาน

- การสื่อสารข้อมูลที่เกี่ยวข้องกับเหตุการณ์วิกฤตให้กับเจ้าหน้าที่ภายในหน่วยงานอย่างรวดเร็วและมีประสิทธิภาพ
- การจัดให้มีการประชุมหรือการอัปเดตสถานการณ์อย่างสม่ำเสมอเพื่อให้ข้อมูลล่าสุดแก่บุคลากร

(5) การสื่อสารกับประชาชนและผู้มีส่วนได้เสีย

- การเผยแพร่ข้อมูลที่ถูกต้องและทันเวลาให้กับประชาชนและผู้มีส่วนได้เสีย ผ่านช่องทางการสื่อสารที่หลากหลาย เช่น เว็บไซต์ สื่อสังคมออนไลน์ และการแถลงข่าว
- การจัดการกับคำถามและข้อกังวลที่เกิดขึ้นจากประชาชนและผู้มีส่วนได้เสีย

(6) การติดตามและประเมินผล

- การติดตามสถานการณ์และผลกระทบของเหตุการณ์วิกฤตอย่างต่อเนื่อง
- การประเมินความมีประสิทธิภาพของการสื่อสารและการตอบสนองที่ดำเนินการ เพื่อทำการปรับปรุงแผนการสื่อสารและการตอบสนองในอนาคต

(7) การฟื้นฟูและการดำเนินการหลังเหตุการณ์

- การประเมินผลกระทบจากเหตุการณ์วิกฤตและดำเนินการฟื้นฟูการดำเนินงานของหน่วยงานให้กลับสู่สภาวะปกติ

- การสรุปบทเรียนที่ได้รับจากเหตุการณ์วิกฤตและการปรับปรุงแผนการสื่อสารให้มีประสิทธิภาพมากยิ่งขึ้นสำหรับสถานการณ์ในอนาคต

(8) การฝึกอบรมและการทบทวนแผนการสื่อสารในภาวะวิกฤต

- การฝึกอบรมบุคลากรที่เกี่ยวข้องให้มีความรู้และทักษะในการจัดการกับเหตุการณ์วิกฤต
- การทบทวนและปรับปรุงแผนการสื่อสารในภาวะวิกฤตอย่างสม่ำเสมอเพื่อให้ทันสมัยและเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลง

4. คำนิยาม

(1) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Management Plan) หมายถึง เอกสารหรือกลยุทธ์ที่จัดทำขึ้นเพื่อกำหนดวิธีการและขั้นตอนในการสื่อสารภายในและภายนอกหน่วยงานในช่วงที่เกิดเหตุการณ์วิกฤตที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ โดยมีวัตถุประสงค์เพื่อให้การสื่อสารมีความชัดเจน ถูกต้อง และมีประสิทธิภาพในการจัดการกับสถานการณ์ที่ไม่คาดคิด

(2) เหตุการณ์วิกฤต (Crisis Event) หมายถึง สถานการณ์ที่เกิดขึ้นอย่างไม่คาดคิดและมีผลกระทบอย่างรุนแรงต่อการดำเนินงานของหน่วยงาน ซึ่งอาจรวมถึงการโจมตีทางไซเบอร์ การรั่วไหลของข้อมูลสำคัญ การแทรกแซงระบบ หรือปัญหาด้านความมั่นคงที่อาจสร้างความเสียหายต่อหน่วยงานและผู้มีส่วนได้เสีย

(3) ทีมจัดการวิกฤต (Crisis Management Team: CMT) หมายถึง กลุ่มบุคคลที่มีหน้าที่จัดการและประสานงานในการตอบสนองต่อเหตุการณ์วิกฤตที่มีผลกระทบอย่างร้ายแรงต่อการดำเนินงานของหน่วยงาน ซึ่งประกอบด้วยสมาชิกที่มีความเชี่ยวชาญในด้านต่าง ๆ และมีบทบาทสำคัญในการวางแผน ตัดสินใจ และดำเนินการเพื่อบรรเทาผลกระทบและฟื้นฟูสถานการณ์ให้กลับสู่สภาวะปกติ

(4) ทีมสื่อสารวิกฤต (Crisis Communication Team: CCT) หมายถึง กลุ่มบุคคลที่มีความเชี่ยวชาญเฉพาะในด้านการสื่อสารในช่วงเหตุการณ์วิกฤต โดยมีหน้าที่หลักในการสร้างและเผยแพร่ข้อมูลที่ถูกต้องและเป็นปัจจุบันให้กับประชาชน สื่อมวลชน และผู้มีส่วนได้เสีย เพื่อรักษาความโปร่งใสและลดความวิตกกังวล

(5) ผู้จัดการวิกฤต (Crisis Manager) หมายถึง บุคคลที่รับผิดชอบในการนำทีมจัดการวิกฤต (CMT) และมีหน้าที่หลักในการวางแผนและตัดสินใจในสถานการณ์วิกฤต โดยทำหน้าที่เป็นผู้นำในการกำหนดกลยุทธ์ การตัดสินใจที่สำคัญ และการประสานงานเพื่อให้การตอบสนองเป็นไปอย่างมีประสิทธิภาพและรวดเร็ว

(6) ข้อความหลัก (Key Messages) หมายถึง ข้อมูลหรือเนื้อหาสำคัญที่ต้องการสื่อสารออกไปในช่วงวิกฤต ซึ่งถูกออกแบบให้ชัดเจนและตรงประเด็น เพื่อให้ทุกฝ่ายที่เกี่ยวข้องได้รับข้อมูลที่ถูกต้องและเป็นปัจจุบัน

(7) การตอบสนอง (Response) หมายถึง การดำเนินการและการตอบสนองของหน่วยงานต่อเหตุการณ์วิกฤต ซึ่งรวมถึงการจัดการข้อมูล การสื่อสารกับสื่อมวลชน การประชาสัมพันธ์ไปยังประชาชน และการดำเนินการภายในเพื่อบรรเทาผลกระทบ

(8) ความโปร่งใส (Transparency) หมายถึง การเปิดเผยข้อมูลที่เป็นความจริงและถูกต้องเกี่ยวกับเหตุการณ์วิกฤต โดยไม่ปกปิดข้อมูลที่สำคัญ ซึ่งช่วยลดความสับสนและสร้างความเชื่อมั่นให้กับประชาชนและผู้มีส่วนได้เสีย

(9) การฟื้นฟู (Recovery) หมายถึง กระบวนการในการฟื้นฟูการดำเนินงานและการบริการของหน่วยงานกลับสู่สภาวะปกติหลังจากเหตุการณ์วิกฤต โดยการจัดการผลกระทบและปรับปรุงแผนการสื่อสารให้มีประสิทธิภาพมากยิ่งขึ้น

(10) การประเมินผล (Evaluation) หมายถึง การวิเคราะห์และประเมินผลกระทบจากเหตุการณ์วิกฤต รวมถึงการประเมินความมีประสิทธิภาพของการตอบสนองและการสื่อสาร เพื่อหาบทเรียนที่ได้และทำการปรับปรุงแผนการสื่อสารให้ดีขึ้นในอนาคต

(11) ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง การป้องกันและการปกป้องข้อมูล ระบบคอมพิวเตอร์ และเครือข่ายจากการเข้าถึง การใช้ การเปิดเผย การรบกวน การเปลี่ยนแปลง หรือการทำลายที่ไม่ได้รับอนุญาต ความมั่นคงปลอดภัยทางไซเบอร์ครอบคลุมถึงการป้องกันภัยคุกคามทั้งจากภายในและภายนอกที่อาจทำให้ข้อมูลสูญหาย ถูกขโมย ถูกทำลาย หรือถูกเปลี่ยนแปลง ซึ่งอาจส่งผลต่อความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูลและระบบ

5. แผนการดำเนินงาน

แผนการดำเนินงานการสื่อสารในภาวะวิกฤต (Crisis Communication Management) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของกรมกิจการสตรีและสถาบันครอบครัว มีดังนี้

(1) กำหนดและจัดประเภทเหตุการณ์ที่อาจเป็นวิกฤตทางไซเบอร์

(1.1) การกำหนดและจัดประเภทเหตุการณ์ที่อาจเป็นวิกฤตทางไซเบอร์

- การโจมตีทางไซเบอร์ (Cyber Attack) การโจมตีที่มุ่งหวังที่จะทำให้ระบบคอมพิวเตอร์หรือเครือข่ายทำงานผิดพลาดหรือถูกทำลาย เช่น Malware (ไวรัส/ซอฟต์แวร์ที่เป็นอันตราย) Phishing (การหลอกลวงเพื่อขโมยข้อมูลสำคัญ) Ransomware (การเข้ารหัสข้อมูลและเรียกค่าไถ่เพื่อปลดล็อกข้อมูล)
- การรั่วไหลของข้อมูลสำคัญ (Data Breach) การเข้าถึงหรือควบคุมระบบโดยไม่ได้รับอนุญาตที่ส่งผลให้ระบบทำงานผิดพลาดหรือหยุดทำงาน เช่น การแทรกแซงระบบควบคุม (การเข้าถึงระบบที่ควบคุมโครงสร้างพื้นฐานสำคัญ) การควบคุมระบบ (การเปลี่ยนแปลงข้อมูลหรือการตั้งค่าที่มีผลกระทบต่อการดำเนินงาน)
- ปัญหาด้านความมั่นคงที่ร้ายแรง (Serious Security Issues) เหตุการณ์ที่ไม่ได้เกิดจากการโจมตี แต่เป็นปัญหาด้านความมั่นคงที่สามารถส่งผลกระทบร้าย เช่น ช่องโหว่ของระบบ (การตั้งค่าที่ผิดพลาดหรือช่องโหว่ที่อาจถูกใช้ในการโจมตี) การละเลยข้อกำหนดด้านความปลอดภัย (การไม่ปฏิบัติตามมาตรฐานความปลอดภัยที่กำหนด)

(1.2) การประเมินความรุนแรงและผลกระทบของเหตุการณ์

- การประเมินความรุนแรง โดยการวิเคราะห์ผลกระทบ (ประเมินว่าผลกระทบของเหตุการณ์นั้นเป็นอันตรายเพียงใด เช่น ความเสียหายที่เกิดขึ้นต่อข้อมูล ระบบ หรือชื่อเสียง) การตรวจสอบการแพร่กระจาย (วัดว่าการโจมตีหรือการรั่วไหลได้แพร่กระจายไปยังส่วนต่าง ๆ ของหน่วยงานหรือไม่) การพิจารณาผลกระทบระยะยาว (วิเคราะห์ผลกระทบในระยะยาว เช่น การฟื้นฟูและการกู้คืนระบบ)

- การประเมินผลกระทบ โดยประเมินผลกระทบต่อการดำเนินงาน (วิเคราะห์ว่าผลกระทบต่อการดำเนินงานอย่างไร เช่น ความสามารถในการให้บริการ ผลกระทบทางการเงิน หรือผลกระทบต่อผู้รับบริการและคู่ค้า) ผลกระทบต่อผู้มีส่วนได้ส่วนเสีย (พิจารณาผลกระทบต่อผู้มีส่วนได้ส่วนเสียที่สำคัญ เช่น ผู้รับบริการ เจ้าหน้าที่ และผู้มีส่วนได้ส่วนเสีย) การควบคุมความเสียหาย (การประเมินความสามารถในการควบคุมและลดความเสียหายจากเหตุการณ์ที่เกิดขึ้น)

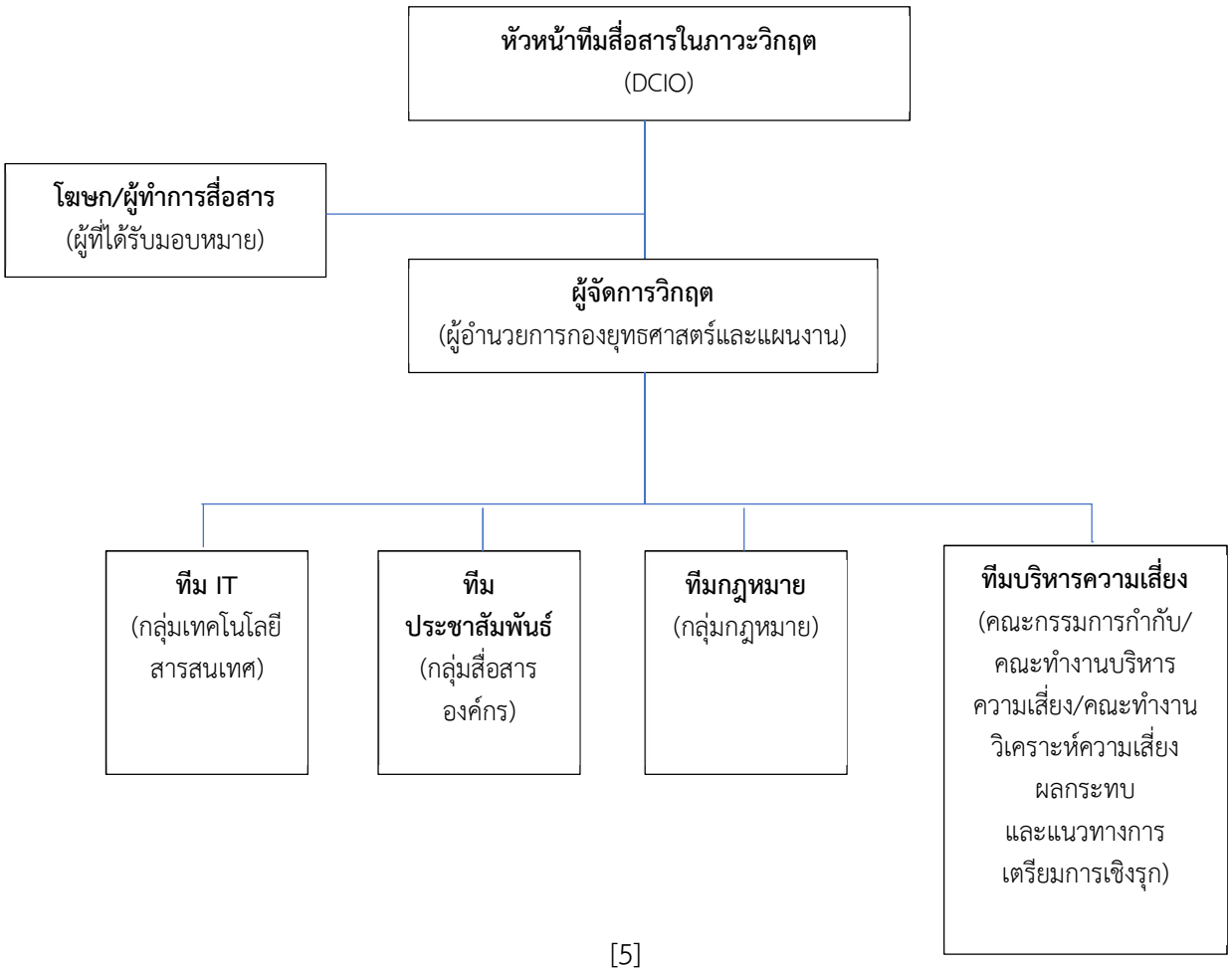
(1.3) การกำหนดลำดับความสำคัญ

- การจัดลำดับความสำคัญ โดยการกำหนดลำดับความสำคัญในการตอบสนองตามความรุนแรงและผลกระทบของเหตุการณ์ เช่น เหตุการณ์ที่มีความรุนแรงสูงและผลกระทบร้ายแรงควรได้รับการตอบสนองเป็นอันดับแรก
- การจัดสรรทรัพยากร โดยการวางแผนในการจัดสรรทรัพยากร เช่น ทีมงาน งบประมาณ และเครื่องมือในการจัดการวิกฤต

(2) จัดตั้งทีมสื่อสารในภาวะวิกฤต (Crisis Communication Team: CCT)

เพื่อให้การปฏิบัติงานด้านการสื่อสารประชาสัมพันธ์ในภาวะวิกฤตเป็นไปด้วยความรวดเร็วและมีประสิทธิภาพ จึงได้จัดโครงสร้างทีมสื่อสารในภาวะวิกฤตให้สอดคล้องกับหน่วยงาน ซึ่งประกอบด้วย

(2.1) โครงสร้างทีมสื่อสารในภาวะวิกฤต



(2.2) บทบาทและหน้าที่

ตำแหน่ง	ตำแหน่งใน Crisis Management Plan	หน้าที่ความรับผิดชอบ
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)	หัวหน้าทีมสื่อสารในภาวะวิกฤต	กำกับดูแลการสื่อสารในภาวะวิกฤตที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานทั้งหมด รับผิดชอบการตัดสินใจหลัก และสื่อสารกับผู้บริหารระดับสูง (หัวหน้าส่วนราชการ)
ผู้ที่ได้รับมอบหมาย	โฆษก/ผู้ทำการสื่อสาร	เป็นตัวแทนของหน่วยงานที่มีหน้าที่ในการให้ข่าวกับสื่อมวลชน ชี้แจง ข้อเท็จจริง ตอบข้อซักถามสื่อมวลชน อำนวยความสะดวกในการให้ข้อมูลข่าวสารกับผู้มีส่วนได้ส่วนเสีย
ผู้อำนวยการกองยุทธศาสตร์และแผนงาน	ผู้จัดการวิกฤต	รับแจ้งเหตุวิกฤต ประสานงาน และควบคุมทีม รวมทั้งติดตามสถานการณ์ ตลอดจนรายงานความคืบหน้าในการดำเนินงานเพื่อให้การจัดการวิกฤตเป็นไปอย่างมีประสิทธิภาพ
ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ และเจ้าหน้าที่	ทีม IT	จัดการปัญหาด้านเทคนิคที่เกิดจากเหตุการณ์วิกฤตทางไซเบอร์ และให้ข้อมูลที่เกี่ยวข้องแก่ทีมประชาสัมพันธ์เพื่อการสื่อสารที่ถูกต้องและทันเวลา
ผู้อำนวยการกลุ่มสื่อสารองค์กรและเจ้าหน้าที่	ทีมประชาสัมพันธ์	จัดการการสื่อสารกับสื่อมวลชนและประชาชน โดยการสร้างและเผยแพร่ข้อมูลเกี่ยวกับเหตุการณ์วิกฤต
ผู้อำนวยการกลุ่มกฎหมาย และเจ้าหน้าที่	ทีมกฎหมาย	ให้คำแนะนำด้านกฎหมายและตรวจสอบความถูกต้องของข้อมูลที่เกี่ยวข้องกับเหตุการณ์วิกฤต
คณะกำกับบริหารความเสี่ยง/ คณะทำงานบริหารความเสี่ยง/ คณะทำงานวิเคราะห์ความเสี่ยง ผลกระทบ และแนวทางการเตรียมการเชิงรุก	ทีมบริหารความเสี่ยง	ประเมินและบริหารความเสี่ยงที่เกิดจากเหตุการณ์วิกฤต เพื่อจัดการผลกระทบที่อาจเกิดขึ้น

(2.3) ขั้นตอนการดำเนินการของทีมสื่อสารในภาวะวิกฤต (CCT)

ขั้นตอน	การดำเนินการ
ประเมินสถานการณ์	- ตรวจสอบข้อมูลกับหน่วยงานที่เกิดเหตุวิกฤต - ศึกษาการรับรู้ของกลุ่มเป้าหมายว่า กลุ่มเป้าหมายมีความกังวลเรื่องอะไร และจะดำเนินการคลี่คลายหรือบรรเทาความกังวลนั้นได้อย่างไร
กำหนดทิศทางการสื่อสาร	- กำหนดข้อความหลักในการสื่อสาร (key message) - วางกลยุทธ์ในการสื่อสารให้ตรงกลุ่มเป้าหมาย
การประสานงานกับทีมอื่น ๆ	- ประสานงานภายในโดยทำงานร่วมกับทีม IT ทีมกฎหมาย และทีมบริหารความเสี่ยง - ให้การสนับสนุนด้านการสื่อสารแก่ทีมจัดการวิกฤต
กำหนด/ร่างข้อมูลที่ใช้ในการสื่อสาร แบบต่าง ๆ	- จัดทำเนื้อหา (Content) ต่าง ๆ เช่น หนังสือถึง ผู้ได้รับผลกระทบ คำแถลงการณ์ ข่าวประชาสัมพันธ์ รูปภาพ คลิปวิดีโอ - ตรวจสอบความถูกต้อง แม่นยำ และความสมบูรณ์ของข้อมูลก่อนนำเสนอต่อผู้ให้ข่าว ผู้บริหาร และ สื่อมวลชน
เลือกผู้แทนในการให้ข่าว	- คัดเลือกผู้ให้ข่าว (Spokesperson) ที่เหมาะสม - เตรียมพร้อมและซักซ้อมกับผู้ให้ข่าวก่อน - ตอบคำถามจากสื่อมวลชนและประชาชนอย่างชัดเจนและตรงประเด็น - จัดการกับข้อกังวลและข้อร้องเรียนจากประชาชนและผู้มีส่วนได้เสีย
บริหารจัดการช่องทางการสื่อสาร	- ตรวจสอบรายนามสื่อมวลชน (Media list) - สื่อที่มีอยู่แล้ว - สื่อที่เผยแพร่โดยไม่เสียเงิน - ใช้ช่องทางการสื่อสารที่เหมาะสม เช่น Website Social Media การประชุมออนไลน์ ฯลฯ
ติดตามและประเมินผล	- ติดตามผลกระทบของการสื่อสารที่เผยแพร่ - ประเมินความสำเร็จของการสื่อสารและปรับกลยุทธ์ตามสถานการณ์
บันทึกและจัดทำรายงาน	- บันทึกการสื่อสารทั้งหมดที่ดำเนินการในช่วงวิกฤต - จัดทำรายงานสรุปเกี่ยวกับการสื่อสารวิกฤตเพื่อการวิเคราะห์และปรับปรุง
ฝึกอบรมและการจำลองสถานการณ์	- การฝึกอบรมให้กับทีมงานและโฆษก - ดำเนินการจำลองสถานการณ์วิกฤตเพื่อทดสอบความพร้อมและการตอบสนอง

(2.4) อุปกรณ์สำหรับปฏิบัติการด้านการสื่อสาร

- โต๊ะประชุม หรือ War Room
- กระดาษ ปากกา/ดินสอ
- กระดานและอุปกรณ์สำนักงานอื่น ๆ
- คอมพิวเตอร์ อินเทอร์เน็ตและ Printer
- โทรสาร
- วิทยุ โทรทัศน์ ที่สามารถรับชมช่องข่าวต่าง ๆ ได้
- เครื่องถ่ายเอกสาร

(2.5) การจัดเตรียมเอกสารตามความจำเป็นและความเหมาะสมของแต่ละสถานการณ์

- ข้อความและแนวทางปฏิบัติสำหรับแจ้งให้บุคลากรภายในหน่วยงานถือปฏิบัติ
- คำแถลงการณ์ (Media Statement)
- จดหมายแจ้งหน่วยงานภายนอกที่เกี่ยวข้อง และสื่อมวลชน
- ข่าวเผยแพร่ (News release)
- เอกสารข้อเท็จจริง (Fact sheet)
- แนวทางคำถาม-คำตอบ (Q&A)
- ไฟล์ภาพถ่ายผู้บริหาร
- VDO Footage (ถ้ามี)
- ข้อมูลการติดต่อ แผนที่ หากต้องดำเนินงาน ณ สถานที่สำรอง

(3) การวางแผนและการเตรียมความพร้อม

การวางแผนและการเตรียมความพร้อมสำหรับการจัดการวิกฤตทางไซเบอร์เป็นกระบวนการที่สำคัญและควรดำเนินการอย่างรอบคอบ เพื่อให้สามารถตอบสนองต่อเหตุการณ์วิกฤตได้อย่างมีประสิทธิภาพและลดผลกระทบที่อาจเกิดขึ้น โดยมีขั้นตอนหลักในการวางแผนและการเตรียมความพร้อม ดังนี้

(3.1) การวางแผนล่วงหน้า

- การสร้างแผนการสื่อสารในภาวะวิกฤต โดยระบุภัยคุกคามทางไซเบอร์ที่เป็นไปได้และจัดทำแผนการตอบสนองสำหรับแต่ละประเภทของภัยคุกคาม พร้อมทั้งสร้างแผนการสื่อสารที่ชัดเจน ซึ่งรวมถึงการระบุผู้มีส่วนได้ส่วนเสียที่ต้องการการสื่อสาร การกำหนดช่องทางการสื่อสารที่ใช้ การเตรียมข้อความที่พร้อมใช้งาน (การยืนยันสถานการณ์ ข้อมูลการตอบสนอง และข้อกำหนดในการติดต่อ) ตลอดจนผู้รับผิดชอบการสื่อสารและการจัดการวิกฤต
- การพัฒนาแผนการตอบสนอง โดยสร้างกลไกการประสานงานระหว่างทีมที่เกี่ยวข้อง กำหนดขั้นตอนการตอบสนองที่ชัดเจน (การตรวจสอบและยืนยันเหตุการณ์ การระงับเหตุการณ์ และการฟื้นฟูระบบ) และการพัฒนาแผนการกู้คืนที่ครอบคลุมทั้งการฟื้นฟูระบบ IT และการฟื้นฟูความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย
- การวางแผนการฝึกอบรมและการทดสอบ โดยการจัดการฝึกอบรมให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับมาตรการความปลอดภัยทางไซเบอร์และการตอบสนองต่อวิกฤต และดำเนินการทดสอบแผนการตอบสนองในสถานการณ์จำลองเพื่อทดสอบความพร้อมและปรับปรุงแผนการตามข้อบกพร่องที่พบ

(3.2) การเตรียมความพร้อม

- การสร้างทีมตอบสนอง โดยระบุตัวบุคคลที่มีทักษะและความรู้ในการจัดการวิกฤตทางไซเบอร์ เช่น ผู้เชี่ยวชาญด้านความปลอดภัย นักวิเคราะห์ภัยคุกคาม และผู้จัดการด้านการสื่อสาร รวมทั้งกำหนดบทบาทและความรับผิดชอบของแต่ละสมาชิกในทีมในการจัดการวิกฤต
- การจัดเตรียมเครื่องมือและทรัพยากร โดยจัดเตรียมเครื่องมือและเทคโนโลยีที่จำเป็นสำหรับการตรวจสอบและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งจัดเตรียมทรัพยากรสำรอง เช่น ระบบสำรองข้อมูลและการจัดเก็บข้อมูล เพื่อใช้ในการกู้คืนหากจำเป็น
- การสร้างช่องทางการสื่อสาร โดยตรวจสอบระบบการสื่อสารที่เชื่อถือได้และมีความปลอดภัย เช่น การตั้งค่าช่องทางการติดต่อฉุกเฉินและการติดตั้งระบบแจ้งเตือน รวมทั้งการเตรียมคำแถลงการณ์และข้อมูลที่สามารถใช้ได้ในกรณีฉุกเฉิน

(3.3) การฝึกอบรมและการทบทวน

- การฝึกอบรมในด้านความปลอดภัยไซเบอร์และการตอบสนองต่อวิกฤต โดยเน้นที่ขั้นตอนที่ต้องปฏิบัติในสถานการณ์ฉุกเฉิน รวมถึงดำเนินการฝึกซ้อมในสถานการณ์จำลองเพื่อให้ทีมงานสามารถปฏิบัติได้ตามแผนการ
- การทบทวนและปรับปรุงแผน โดยประเมินผลการฝึกซ้อมและรวบรวมข้อเสนอแนะเพื่อปรับปรุงแผนการ พร้อมทั้งปรับปรุงแผนการสื่อสารและการตอบสนองตามข้อมูลที่ได้รับจากการฝึกซ้อมและการวิเคราะห์เหตุการณ์จริง

(4) การสื่อสารภายในหน่วยงาน

(4.1) สื่อสารข้อมูลที่เกี่ยวข้องกับเหตุการณ์วิกฤต

- แจ้งเหตุ ประเมินสถานการณ์ และแนวโน้มของสถานการณ์ผ่านสื่อที่รวดเร็ว เช่น โทรศัพท์ LINE กลุ่ม Email หรือเสียงตามสาย
- เนื้อความที่จะสื่อสาร ควรระบุวัน/เดือน/ปี และเวลาในส่วนต้นของข้อความไว้ด้วย เพื่อการอ้างอิงในอนาคต
- ส่วนท้ายของเนื้อความ ให้ลงชื่อ หรืออ้างอิงหน่วยงานภายในพร้อมหมายเลขโทรศัพท์ติดต่อไว้ด้วย เพื่อการตรวจสอบข้อมูลของผู้รับสาร
- ให้คำแนะนำในการปฏิบัติตนขั้นต้น เช่น อย่าเพิ่งให้ข่าว หรือความเห็นใด ๆ กับสื่อมวลชน อย่าเผยแพร่ภาพความเสียหายผ่านสื่อสังคมออนไลน์
- ชี้แจงแนวทางดำเนินการ
- ให้เจ้าหน้าที่มีส่วนร่วมเผยแพร่ข้อความประชาสัมพันธ์ตามที่ CCT กำหนด

(4.2) จัดให้มีการประชุมหรือการอัปเดตสถานการณ์อย่างสม่ำเสมอ

- การประชุมทีมวิกฤต โดยจัดการประชุมกับทีมที่เกี่ยวข้องอย่างสม่ำเสมอเพื่อหารือเกี่ยวกับสถานการณ์ปัจจุบัน การดำเนินการที่ต้องทำ และปัญหาที่พบ รวมทั้งเผยแพร่ข้อมูลที่เป็นปัจจุบัน วางแผนการดำเนินการ และจัดการกับข้อกังวลที่มี

- การอัปเดตสถานการณ์เป็นประจำ โดยจัดให้มีการประชุมหรือการอัปเดตสถานการณ์ในช่วงเวลาที่กำหนด เช่น ทุก 1-2 ชั่วโมง หรือเมื่อมีข้อมูลใหม่ที่สำคัญ พร้อมทั้งรายงานสถานการณ์เป็นระยะ ๆ ที่สรุปข้อมูลล่าสุดและความก้าวหน้าของการจัดการวิกฤต

(5) การสื่อสารกับประชาชนและผู้มีส่วนได้เสีย

(5.1) การเผยแพร่ข้อมูลที่ถูกต้องและทันเวลา

- การเผยแพร่ข้อมูลที่ถูกต้องและทันเวลาให้กับประชาชนและผู้มีส่วนได้เสีย ผ่านช่องทางการสื่อสารที่หลากหลาย เช่น เว็บไซต์ของหน่วยงานเพื่อเผยแพร่ข้อมูลที่เป็นทางการ (การประกาศสถานการณ์ การอัปเดตสถานการณ์ และข้อกำหนดด้านความปลอดภัย) สื่อสังคมออนไลน์เพื่อเผยแพร่ข้อมูลสำคัญและตอบสนองต่อคำถามจากประชาชน และประชุมแถลงข่าวหรือการประชุมออนไลน์เพื่อให้ข้อมูลที่เป็นทางการและคำชี้แจงเกี่ยวกับสถานการณ์

- การเตรียมข้อความหลัก เพื่ออธิบายสถานการณ์ปัจจุบันอย่างชัดเจน เช่น ลักษณะของวิกฤต ขอบเขตของปัญหา และขั้นตอนที่กำลังดำเนินการ ตลอดจนเตรียมคำแถลงการณ์ที่สามารถใช้ได้ทันที เช่น การยืนยันสถานการณ์ การขอโทษหากจำเป็น และการให้ข้อมูลการติดต่อ

- การควบคุมข้อมูล โดยตรวจสอบข้อเท็จจริงของข้อมูลก่อนเผยแพร่เพื่อป้องกันการเผยแพร่ข้อมูลผิดพลาด และจัดการแก้ไขข่าวลือหรือข้อมูลเท็จที่อาจแพร่กระจาย

(5.2) การจัดการกับคำถามและข้อกังวล

- การจัดตั้งศูนย์ติดต่อ/บริการข้อมูล หรือหมายเลขโทรศัพท์เฉพาะสำหรับการสอบถามข้อมูลจากประชาชนและผู้มีส่วนได้เสีย รวมทั้งจัดเตรียมบุคลากรที่สามารถตอบคำถามและข้อกังวลได้อย่างรวดเร็วและมีประสิทธิภาพ

- การจัดการคำถามจากสื่อมวลชน โดยจัดให้มีการสัมภาษณ์กับเจ้าหน้าที่ที่มีความเชี่ยวชาญในการตอบคำถามจากสื่อมวลชน และเตรียมข้อมูลที่ตอบคำถามที่คาดว่าจะเกิดขึ้นและให้ข้อมูลที่เป็นทางการ

- การตอบสนองต่อข้อกังวลของประชาชน โดยรับฟังและจัดการกับข้อกังวลที่ประชาชนหรือผู้มีส่วนได้ส่วนเสียที่เกิดขึ้น เช่น ความปลอดภัยของข้อมูล ผลกระทบต่อบริการ และการดำเนินการที่ได้ดำเนินงาน โดยให้ข้อมูลที่ชัดเจนและโปร่งใสเกี่ยวกับการดำเนินการที่หน่วยงานกำลังทำเพื่อจัดการกับวิกฤต

(6) การติดตามและประเมินผล

(6.1) การติดตามสถานการณ์และผลกระทบของเหตุการณ์วิกฤตอย่างต่อเนื่อง

- การติดตามข้อมูล โดยตรวจสอบข้อมูลเกี่ยวกับสถานการณ์วิกฤตอย่างต่อเนื่องจากแหล่งข้อมูลที่เชื่อถือได้ เช่น ระบบตรวจจับภัยคุกคาม รายงานจากทีมตอบสนอง และข้อมูลจากหน่วยงานภายนอก รวมทั้งวิเคราะห์สถานการณ์ เพื่อประเมินความรุนแรงและพัฒนาการของเหตุการณ์ เช่น ความเสี่ยงที่เพิ่มขึ้นหรือการเปลี่ยนแปลงในรูปแบบของการโจมตี

- การติดตามผลกระทบ โดยประเมินผลกระทบที่เกิดขึ้นจากเหตุการณ์วิกฤต เช่น การเสียหายของระบบ การรั่วไหลของข้อมูล และผลกระทบต่อการดำเนินงาน โดยการรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น การสอบถามจากผู้ใช้บริการ การวิเคราะห์การเปลี่ยนแปลงในระบบ และรายงานจากทีมงาน

- การรายงานสถานการณ์และผลกระทบให้กับทีมงานและผู้บริหารเพื่อให้มีข้อมูลที่ครบถ้วนในการตัดสินใจ ทั้งนี้ หากจำเป็นให้รายงานสถานการณ์และผลกระทบให้กับผู้มีส่วนได้ส่วนเสียและประชาชนตามความเหมาะสม

(6.2) การประเมินความมีประสิทธิภาพของการสื่อสารและการตอบสนอง

- การประเมินการสื่อสาร โดยตรวจสอบข้อความที่สื่อสารออกไปว่าชัดเจนและตรงตามความต้องการของผู้รับสารหรือไม่ เช่น ความถูกต้องของข้อมูล ความตรงประเด็น และการจัดทำเอกสารที่เข้าใจง่าย รวมทั้งการติดตามผลการสื่อสาร โดยวัดผลของการสื่อสาร เช่น การตอบรับจากประชาชน การมีส่วนร่วมของสื่อมวลชน และการประเมินผลของการประชาสัมพันธ์

- การประเมินการตอบสนอง โดยตรวจสอบว่าขั้นตอนการตอบสนองที่ดำเนินการมีประสิทธิภาพและเป็นไปตามแผนที่วางไว้หรือไม่ เช่น ความเร็วในการตอบสนอง การประสานงานระหว่างทีมและการใช้ทรัพยากร พร้อมทั้งวิเคราะห์ผลลัพธ์ของการตอบสนอง เช่น การลดผลกระทบจากวิกฤต การฟื้นฟูระบบ และการจัดการกับข้อกังวลของผู้มีส่วนได้ส่วนเสีย

- การรวบรวมข้อเสนอแนะ โดยขอความคิดเห็นจากทีมงาน ผู้มีส่วนได้ส่วนเสียและประชาชนเกี่ยวกับการจัดการวิกฤตและการสื่อสาร รวมถึงการจัดทำแบบสอบถาม เพื่อรวบรวมข้อเสนอแนะและความคิดเห็นเกี่ยวกับกระบวนการตอบสนองและการสื่อสาร ตลอดจนปรับปรุงแผนการสื่อสารและการตอบสนองโดยใช้ข้อมูลที่รวบรวมได้เพื่อวิเคราะห์ข้อบกพร่องและจุดแข็งของการตอบสนองและการสื่อสาร ปรับปรุงแผนการสื่อสารและการตอบสนองตามข้อเสนอแนะและบทเรียนที่ได้เรียนรู้จากเหตุการณ์ และดำเนินการฝึกซ้อมหรือการทดสอบแผนที่ปรับปรุงเพื่อให้มีความพร้อมในการรับมือกับวิกฤตในอนาคต

(7) การฟื้นฟูและการดำเนินการหลังเหตุการณ์

(7.1) การประเมินผลกระทบจากเหตุการณ์วิกฤตและดำเนินการฟื้นฟูการดำเนินงานของหน่วยงานให้กลับสู่สภาวะปกติ

- รวบรวมข้อมูลเกี่ยวกับผลกระทบที่เกิดจากเหตุการณ์วิกฤต เช่น ความเสียหายที่เกิดขึ้นกับระบบ การรั่วไหลของข้อมูล การหยุดชะงักของบริการ และผลกระทบต่อการดำเนินงาน นำมาวิเคราะห์ผลกระทบที่เกิดขึ้นเพื่อประเมินระดับความรุนแรงและความต่อเนื่องของปัญหา เช่น การประเมินระยะเวลาที่ใช้ในการฟื้นฟู ต้นทุนที่เกิดขึ้น และความเสี่ยงที่ยังคงมีอยู่

- การฟื้นฟูการดำเนินงาน โดยจัดลำดับความสำคัญในการฟื้นฟูระบบและบริการตามความสำคัญต่อการดำเนินงาน เช่น การคืนค่าการเข้าถึงข้อมูลสำคัญ การฟื้นฟูการทำงานของระบบหลักและการกลับมาของการบริการประชาชน เป็นต้น โดยดำเนินการตามแผนฟื้นฟูที่กำหนด เช่น การซ่อมแซมหรือการเปลี่ยนแปลงระบบที่ได้รับผลกระทบ การคืนค่าการเข้าถึงข้อมูล และการทดสอบระบบ รวมทั้งตรวจสอบและทดสอบระบบที่ฟื้นฟูแล้ว เพื่อให้แน่ใจว่าทำงานได้อย่างปกติและไม่มีปัญหาใหม่เกิดขึ้น

- สื่อสารกับผู้มีส่วนได้ส่วนเสีย โดยแจ้งให้ผู้มีส่วนได้ส่วนเสียทราบถึงสถานการณ์ฟื้นฟูและความก้าวหน้าในการกลับสู่สภาวะปกติ รวมทั้งจัดการกับความคาดหวังและความกังวลของผู้มีส่วนได้ส่วนเสียเกี่ยวกับการฟื้นฟูและการดำเนินงานที่กลับสู่สภาวะปกติ

(7.2) การสรุปบทเรียนและการปรับปรุงแผนการสื่อสาร

- การสรุปบทเรียนที่ได้รับ โดยการจัดประชุมหลังเหตุการณ์กับทีมที่เกี่ยวข้องเพื่อหารือและรวบรวมบทเรียนที่ได้เรียนรู้จากเหตุการณ์วิกฤต เช่น ข้อบกพร่องที่พบ การจัดการที่ได้ผลดี และปัญหาที่ต้องแก้ไข รวมถึงรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น ข้อมูลการตอบสนอง ข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสีย และความคิดเห็นของทีมงาน

- การวิเคราะห์บทเรียน โดยวิเคราะห์ข้อบกพร่องที่เกิดขึ้นในกระบวนการตอบสนองและการสื่อสาร เช่น การสื่อสารที่ไม่ชัดเจน การตอบสนองที่ล่าช้า หรือปัญหาการประสานงาน รวมถึงการระบุสิ่งที่ทำได้ดีและประสบความสำเร็จในกระบวนการตอบสนอง เช่น การจัดการสถานการณ์ที่มีประสิทธิภาพ การสื่อสารที่มีความชัดเจน หรือการจัดการกับข่าวลือ

- การปรับปรุงแผนการสื่อสาร โดยปรับปรุงแผนการสื่อสารตามบทเรียนที่ได้เรียนรู้ เช่น การเพิ่มช่องทางการสื่อสารใหม่ การปรับปรุงข้อความที่สื่อสาร หรือการปรับปรุงขั้นตอนการสื่อสาร รวมทั้งจัดการฝึกอบรมและการจำลองสถานการณ์ใหม่เพื่อเตรียมความพร้อมสำหรับการจัดการวิกฤตในอนาคต

- การประเมินและการปรับปรุงแผนการฟื้นฟู โดยทบทวนและปรับปรุงแผนการฟื้นฟูให้สามารถตอบสนองต่อเหตุการณ์วิกฤตได้ดีขึ้น เช่น การเพิ่มกระบวนการตรวจสอบใหม่ การปรับปรุงขั้นตอนการฟื้นฟู หรือการจัดเตรียมทรัพยากรเพิ่มเติม

(8) การฝึกอบรมและการทบทวนแผนการสื่อสารในภาวะวิกฤต

(8.1) การฝึกอบรมบุคลากรที่เกี่ยวข้องให้มีความรู้และทักษะในการจัดการกับเหตุการณ์วิกฤต

- กำหนดวัตถุประสงค์การฝึกอบรม โดยระบุวัตถุประสงค์ที่ชัดเจน เช่น การเข้าใจบทบาทและหน้าที่ในสถานการณ์วิกฤต การเรียนรู้ขั้นตอนการตอบสนอง และการพัฒนาทักษะการสื่อสารในภาวะวิกฤต พร้อมทั้งระบุบุคลากรที่ต้องเข้ารับการฝึกอบรม เช่น ทีมวิกฤต เจ้าหน้าที่สื่อสาร และผู้จัดการด้านความเสี่ยง

- ออกแบบและจัดทำหลักสูตรการฝึกอบรมที่ครอบคลุมหัวข้อสำคัญ เช่น การระบุและจัดการกับเหตุการณ์วิกฤต การสื่อสารกับผู้มีส่วนได้ส่วนเสีย และการใช้เครื่องมือการสื่อสารในสถานการณ์ฉุกเฉิน โดยการฝึกอบรมใช้วิธีการที่หลากหลาย เช่น การอบรมเชิงปฏิบัติ การจำลองสถานการณ์ และการศึกษากรณีตัวอย่าง

- ดำเนินการฝึกอบรมตามแผนที่กำหนดและใช้วิธีการที่มีประสิทธิภาพ เช่น การสอนในห้องเรียน การอบรมออนไลน์ หรือการจัดกิจกรรมการฝึกปฏิบัติ พร้อมทั้งประเมินความเข้าใจและทักษะของผู้เข้าฝึกอบรม เช่น การทดสอบความรู้ การสอบถามความคิดเห็น และการประเมินผลจากการจำลองสถานการณ์

- การสนับสนุนและการติดตาม โดยให้การสนับสนุนและคำปรึกษาแก่บุคลากรหลังการฝึกอบรมเพื่อช่วยในการนำความรู้ไปใช้ และติดตามการประยุกต์ใช้ทักษะที่ได้เรียนรู้และให้ข้อเสนอแนะในการปรับปรุง

(8.2) การทบทวนและปรับปรุงแผนการสื่อสารในภาวะวิกฤต

- การทบทวนแผนการสื่อสาร โดยวิเคราะห์ผลลัพธ์จากการจัดการวิกฤตที่ผ่านมา เช่น ความสำเร็จในการสื่อสาร การจัดการกับคำถามและข้อกังวล และความเร็วในการตอบสนอง รวมถึงการรวบรวมข้อมูลจากประสบการณ์การจัดการวิกฤตและความคิดเห็นจากผู้ที่มีส่วนเกี่ยวข้อง เช่น ข้อเสนอแนะจากทีมงานและผู้มีส่วนได้ส่วนเสีย

- ปรับปรุงแผนการสื่อสาร โดยปรับปรุงเนื้อหาและขั้นตอนของแผนการสื่อสารให้ทันสมัยและเหมาะสมกับสถานการณ์ เช่น การอัปเดตข้อมูลช่องทางการสื่อสาร การปรับปรุงข้อความที่สื่อสาร และการเสริมสร้างกระบวนการจัดการคำถาม รวมทั้งเพิ่มประสิทธิภาพของแผนการสื่อสาร เช่น การเพิ่มช่องทางการสื่อสารใหม่ การใช้เทคโนโลยีใหม่ๆ และการปรับปรุงกระบวนการตัดสินใจ

- ทดสอบแผนการสื่อสารที่ปรับปรุงแล้วผ่านการฝึกซ้อมหรือการจำลองสถานการณ์เพื่อให้แผนทำงานได้ดีในสถานการณ์จริง พร้อมทั้งจัดการฝึกซ้อมประจำปีหรือระยะถี่เพื่อให้ทุกคนคุ้นเคยกับแผนและสามารถตอบสนองได้อย่างรวดเร็วและมีประสิทธิภาพ

- ติดตามความก้าวหน้าในการดำเนินการตามแผนและทบทวนอย่างสม่ำเสมอเพื่อทำการปรับปรุงเพิ่มเติม รวมทั้งปรับปรุงแผนตามข้อเสนอแนะที่ได้รับจากการฝึกซ้อมและการประเมิน

6. แนวปฏิบัติเมื่อเกิดเหตุการณ์วิกฤต

การปฏิบัติเมื่อเกิดเหตุฉุกเฉิน หรือรับรู้วิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ มีดังนี้

(1) แจ้ง Crisis Manager โดยเร็วที่สุด

(2) กรอกแบบฟอร์มรายงานวิกฤตการณ์ ประกอบด้วย

- วันที่รับรายงาน และเวลาที่รับรายงาน
- เหตุการณ์/วิกฤตการณ์ วัน/เวลา และสถานที่เกิดเหตุ
- การรับรู้ (รับรู้เป็นการภายใน รับรู้ถึงชุมชนรอบข้างแต่ยังไม่ขยายวงกว้าง มีการโพสต์ลง Social Media มีการโพสต์ลง Social Media และเกิดการส่งต่อ รับรู้ถึงสื่อมวลชน รับรู้ถึงผู้รับบริการ คู่ค้า พันธมิตร)
- รายละเอียดความเสียหาย
- ผลกระทบต่อการปฏิบัติงาน
- ผลกระทบที่คาดว่าจะเกิดขึ้นกับภายนอก

ตัวอย่างแบบฟอร์มรายงานวิกฤตการณ์

แบบรายงานวิกฤตการณ์

วันที่รับรายงาน.....
วันที่รับรายงาน.....

เหตุการณ์/วิกฤตการณ์. .....
วันที่/เวลา .....
สถานที่เกิดเหตุ .....

การรับรู้ (โปรดทำเครื่องหมาย / หน้าตัวเลือก)

..... รับรู้เป็นการภายใน
..... มีการโพสต์ลง Social Media
..... รับรู้ถึงสื่อมวลชน
..... รับรู้ถึงขุมชนรอบข้างแต่ยังไม่ขยายวงกว้าง
..... มีการโพสต์ลง Social Media และเกิดการส่งต่อ
..... รับรู้ถึงผู้รับบริการ คู่ค้า พันธมิตร

รายละเอียดความเสียหาย
ความเสียหายต่อทรัพย์สิน .....
ความเสียหายต่อข้อมูล .....
ความเสียหายต่อบุคคล .....
ความเสียหาย .....

ผลกระทบต่อการปฏิบัติงาน
.....ไม่ส่งผลกระทบต่อการทำงาน ยังคงปฏิบัติงานได้ตามปกติ
.....ส่งผลกระทบต่อการทำงาน .....ไม่ต้องหยุดงาน .....ต้องหยุดงาน (เข้าแผน BCP)
.....ส่งผลกระทบต่อชุมชนรอบข้าง ระบุ .....
ผลกระทบอื่น ๆ ระบุ .....
ผลกระทบที่คาดว่าจะเกิดกับภายนอก .....
.....

(3) ตรวจสอบข้อมูล และประเมินสถานการณ์เบื้องต้น โดยมีคำถามช่วยประเมินสถานการณ์เบื้องต้นดังนี้

คำถามช่วยประเมินสถานการณ์เบื้องต้น

ทำเครื่องหมาย (X)	การประเมินสถานการณ์เบื้องต้น
	(1) เหตุการณ์ลักษณะนี้ เคยเกิดขึ้นหรือไม่
	(2) เกิดขึ้นเป็นประจำหรือไม่
	(3) เคยแก้ปัญหาเหตุการณ์ลักษณะนี้ได้หรือไม่
	(4) จะเกิดการขยายผล หรือยกระดับความรุนแรงหรือไม่
	(5) ส่งผลกระทบต่อความรู้สึก และความเชื่อมั่นของผู้รับบริการหรือไม่
	(6) เป็นที่สนใจของสาธารณชนในวงกว้างหรือไม่
	(7) ส่งผลกระทบต่อภาพลักษณ์องค์กรหรือไม่
	(8) ส่งผลกระทบต่อภาพลักษณ์ของผู้บริหารหรือไม่

หมายเหตุ: ถ้ามีข้อใดข้อหนึ่งอยู่ในข้อ (4) – (8) ถือว่าเป็นวิกฤตการณ์

(3.1) ในกรณีประเด็นปัญหาที่มักเกิดขึ้นเป็นประจำ โดยมากสามารถแก้ไขและควบคุมได้ ให้แจ้งหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการต่อไป

(3.2) ในกรณีเป็นวิกฤตการณ์ ซึ่งเป็นเหตุการณ์ที่มีความรุนแรง จนอาจส่งผลกระทบต่อการดำเนินงาน หรือกระทบความเชื่อมั่นต่อหน่วยงานและผู้บริหารได้ หรือส่งผลกระทบต่อประชาชน ให้ดำเนินการแจ้งผู้บริหารตามสายงาน และแจ้งหน่วยงานภายนอกที่เกี่ยวข้อง พร้อมทั้งระดมทีม CCT

(4) ในกรณีเป็นวิกฤตการณ์ ให้ทีม CCT ประเมินสถานการณ์ และประเมินความรุนแรง

(4.1) ประเมินสถานการณ์ในมุมมองของประชาชน อย่างน้อยดังนี้

- ความกังวลของผู้ได้รับผลกระทบอยู่ตรงไหน
- ผู้ได้รับผลกระทบอยากได้ยินอะไร
- การรับรู้ (รับรู้เป็นการภายในหรือภายนอก ขยายวงกว้างมากน้อยแค่ไหน)
- ความเสียหาย (เกิดความเสียหายต่อบุคคล สินทรัพย์ หรือข้อมูลอย่างไร)
- ผลกระทบ (ผลกระทบต่อการทำงาน ผลกระทบต่อชุมชนรอบข้าง ผลกระทบต่อภาพลักษณ์ ชื่อเสียง และความน่าเชื่อถือของหน่วยงาน)

(4.2) ประเมินความรุนแรงของวิกฤตการณ์ โดยแบ่งระดับความรุนแรง ดังนี้

ระดับ	สถานการณ์
น้อย	- วิกฤตการณ์เป็นการภายใน - สื่อมวลชนยังไม่เกิดการรับรู้ หรือ เกิดข่าวลือแบบปากต่อปากหรือทางสื่อสังคมออนไลน์ แต่ยังไม่มีข่าวในสื่อกระแสหลัก - ไม่เกิดผลกระทบต่อประชาชน - สามารถดำเนินงานได้ตามปกติ - เอกสาร ข้อมูล ระบบ IT ไม่เสียหาย
ปานกลาง	- มีการเผยแพร่ข่าวผ่านสื่อสังคมออนไลน์ และสื่อมวลชน - ประชาชนเกิดความสงสัย และคาดเดาไปต่าง ๆ นานา - มีผู้เสียหาย หรือได้รับผลกระทบเล็กน้อย - สถานที่ทำงาน หรืออาคารได้รับความเสียหายไม่สามารถปฏิบัติงานได้ชั่วคราว (เข้าสู่แผน BCP) - เอกสาร ข้อมูล หรือระบบ IT เสียหายบางส่วน/เล็กน้อย
มาก	- มีกระแสเรื่องเหตุฉุกเฉินที่เกิดขึ้นในสื่อสังคมออนไลน์ และสื่อมวลชนสายหลักในวงกว้าง - เกิดผลกระทบต่อชื่อเสียงและภาพลักษณ์ของหน่วยงานและผู้บริหาร - เกิดผลกระทบต่อประชาชน หรือมีโอกาสเกิดผลกระทบรุนแรงต่อชีวิตและทรัพย์สิน เกิดความกลัว ตื่นตระหนก - เกิดผลกระทบต่อทรัพย์สิน หรือไม่สามารถปฏิบัติงานได้ตามปกติต้องย้ายที่ทำการชั่วคราว (เข้าสู่แผน BCP) - ข้อมูล หรือระบบ IT เสียหาย

(5) พิจารณาแนวทางการสื่อสารประชาสัมพันธ์ ดังนี้

ประเด็น	คำถามเพื่อพิจารณา	คำตอบ/แนวทางการสื่อสาร
เนื้อหา	- ใครคือผู้รับสารเป้าหมายของการสื่อสาร - ความกังวลของผู้ได้รับผลกระทบ คืออะไร - อะไรควรพูด/อะไรไม่ควรพูด - สิ่งได้ทำอะไรไปแล้ว - สิ่งที่จะทำต่อไป - ระยะเวลาที่ใช้ในการแก้ไขวิกฤตการณ์ได้แล้วเสร็จ	
ช่องทางการสื่อสาร	- สื่อหรือช่องทางใดสามารถเข้าถึงผู้รับสารเป้าหมายได้ดีที่สุด	
รูปแบบวิธีการ	- ต้องมีการแถลงข่าวหรือไม่ ใครจะเป็นผู้แถลง - ควรใช้ผู้มีอิทธิพลทางความคิด (Influencer) คนกลาง หรือบุคคลที่สาม ในการพูดแทนหรือไม่/ตนนั้นคือใคร	

ทั้งนี้ ในการจัดการการสื่อสารประชาสัมพันธ์ที่เกี่ยวข้องกับเหตุการณ์วิกฤต หน่วยงานอาจมีแนวทางการสื่อสารที่หลากหลายขึ้นอยู่กับสถานการณ์ โดยในบางกรณี อาจไม่มีความจำเป็นต้องสื่อสารใด ๆ และปล่อยให้เรื่องเงียบไปเพื่อหลีกเลี่ยงการกระตุ้นความสนใจ หรือการเผยแพร่ข้อมูลที่อาจก่อให้เกิดความตื่นตระหนกโดยไม่จำเป็น แต่ในสถานการณ์ที่ต้องการการจัดการอย่างระมัดระวัง อาจจำเป็นต้องสื่อสารกับภายในหน่วยงานเพื่อให้มีความเข้าใจร่วมกันและช่วยกันบรรเทาปัญหา เช่น การประชุมภายในเพื่อให้ข้อมูลและการสนับสนุนที่จำเป็น ต่อมาอาจต้องสื่อสารโดยตรงกับผู้ที่ได้รับผลกระทบโดยตรงเพื่อให้การจัดการปัญหาเป็นไปอย่างมีประสิทธิภาพและป้องกันไม่ให้ปัญหาลุกลามใหญ่โตขึ้น สุดท้ายอาจต้องสื่อสารออกไปภายนอกองค์กรในวงกว้างเพื่อสร้างความเข้าใจที่ถูกต้องและป้องกันการตื่นตระหนกของประชาชน โดยการให้ข้อมูลที่ชัดเจนและโปร่งใสเกี่ยวกับสถานการณ์ และการดำเนินการที่กำลังดำเนินอยู่

(6) ระบุกิจกรรมและผู้รับผิดชอบในการดำเนินการสื่อสารแต่ละกิจกรรม เช่น เข้าพบผู้ได้รับผลกระทบชี้แจงข้อเท็จจริง สื่อสารภายในองค์กร ไลน์กลุ่มที่เกี่ยวข้อง โพสต์หน้าเฟสบุ๊ค โพสต์ทางทวิตเตอร์ ทำหนังสือชี้แจง ส่งคำแถลงการณ์ให้สื่อมวลชน เปิดแถลงข่าว/เชิญสื่อมวลชนมาร่วมทำข่าว/สัมภาษณ์ ส่งผลการดำเนินงานสื่อสารในภาวะวิกฤตให้ฝ่ายประชาสัมพันธ์รับทราบ เป็นต้น ทั้งนี้ หากไม่สามารถดำเนินการสื่อสารประชาสัมพันธ์ได้เอง อาจต้องจัดหาที่ปรึกษาประชาสัมพันธ์หรือขอความร่วมมือจากหน่วยงานภายนอก เพื่อดำเนินการจัดทำแผนร่วมกัน

(7) สรุปความเป็นมา และแนวทางทางการดำเนินการ พร้อมทั้งรายงานผู้บริหาร และดำเนินการตามกระบวนการ/ขั้นตอน CCT

(8) ดำเนินการสื่อสารประชาสัมพันธ์ตามแผนงานที่กำหนด โดยเริ่มต้นจากการดำเนินการตามกลยุทธ์ที่วางไว้ ซึ่งรวมถึงการสร้างเนื้อหาที่สอดคล้องกับข้อความหลักและเป้าหมายที่ตั้งไว้ในแผนการสื่อสาร จากนั้นใช้ช่องทางที่ระบุในแผน เช่น ข่าวประชาสัมพันธ์ สื่อสังคมออนไลน์ และการประชุมเพื่อส่งมอบข้อมูลให้กับกลุ่มเป้าหมายอย่างมีประสิทธิภาพ การติดตามและตอบสนองต่อข้อซักถามหรือข้อกังวลจากผู้มีส่วนได้ส่วนเสียเป็นสิ่งสำคัญในการรักษาความสัมพันธ์ที่ดีและป้องกันการแพร่กระจายของข้อมูลที่ผิดพลาด หรือการสร้างความตื่นตระหนก ขณะเดียวกันควรมีการประเมินผลการสื่อสารอย่างสม่ำเสมอเพื่อช่วยให้สามารถปรับปรุงแผนการสื่อสารให้มีประสิทธิภาพยิ่งขึ้นและตอบสนองต่อสถานการณ์ที่เปลี่ยนแปลงได้อย่างทันท่วงที

(9) รายงานสรุปผลการดำเนินงานประชาสัมพันธ์ในภาวะวิกฤต โดยรวบรวมข้อมูลที่ครอบคลุมเกี่ยวกับการดำเนินการตามแผนการสื่อสาร เช่น การเผยแพร่ข้อความหลักและข้อมูลสำคัญผ่านช่องทางที่กำหนด การตอบสนองต่อข้อซักถามและข้อกังวลจากผู้มีส่วนได้ส่วนเสีย รวมถึงการจัดการกับความคิดเห็นหรือข่าวลือที่อาจเกิดขึ้น นอกจากนี้ ควรรวมการประเมินผลลัพธ์ เช่น การวัดผลกระทบของการสื่อสาร ความเข้าใจของประชาชน และการปรับปรุงที่จำเป็นในกระบวนการสื่อสาร รวมถึงบทเรียนที่ได้เรียนรู้และข้อเสนอแนะสำหรับการปรับปรุงแผนการสื่อสารในอนาคต เพื่อให้สามารถพัฒนาและเตรียมพร้อมสำหรับสถานการณ์วิกฤตในอนาคตได้ดียิ่งขึ้น

7. การทบทวนปรับปรุงแผน

กรมกิจการสตรีและสถาบันครอบครัว ควรกำหนดให้มีการฝึกปฏิบัติตามแผนเป็นประจำ และให้คณะกรรมการกำกับการบริหารความเสี่ยงดำเนินการทบทวนรายชื่อทีมสื่อสารวิกฤต (CTC) ให้เป็นปัจจุบันทุกปี เพื่อให้มีความเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป

****