แผนการรับมือภัยคุกคามทางไซเบอร์

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

สารบัญ

คำนิยาม

“กรมฯ” หมายถึง กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องของกรมฯ

“เหตุการณ์” หมายถึง

- เหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่ได้รับการรายงานเข้ามา แต่ยังไม่ได้รับการยืนยันว่าต้องรับมือและบริหารจัดการหรือไม่ หรือ
- เหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่ได้รับการรายงานเข้ามา และได้รับการยืนยันว่าต้องรับมือและบริหารจัดการ

แผนการรับมือภัยคุกคามทางไซเบอร์

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ต้องการให้เกิดความเชื่อมั่นและมั่นใจว่ามีกลไกการตอบสนองและรับมืออย่างเหมาะสมและมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้น หรือคาดว่าจะเกิดขึ้น โดยเหตุการณ์เหล่านั้นมีความเชื่อมโยงกับเจ้าหน้าที่ ระบบสารสนเทศ เครื่องคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลทั้งหมดที่อยู่ในความดูแลและรับผิดชอบของกรมฯ

วัตถุประสงค์

เพื่อให้กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม สามารถตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและประสิทธิผล และเป็นไปตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดไว้

ขอบเขต

แผนการรับมือภัยคุกคามทางไซเบอร์นี้ครอบคลุมถึงเจ้าหน้าที่ ข้อมูล ระบบสารสนเทศและระบบเครือข่ายทั้งหมดของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

สาระสำคัญของแผนการรับมือภัยคุกคามทางไซเบอร์

ประกอบด้วย

- กำหนดโครงสร้างการรับมือภัยคุกคามทางไซเบอร์
- แสดงภาพรวมและขั้นตอนในการรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้น
- ประชุมหารือและตัดสินใจดำเนินการต่างๆ ตามสถานการณ์ของเหตุที่เกิดขึ้น
- การเรียกใช้แผนรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น
- การสื่อสารต่างๆ ที่จำเป็นทั้งภายในและภายนอกไปยังผู้ที่เกี่ยวข้อง
- ข้อมูลสำหรับการติดต่อต่างๆ ที่จำเป็นสำหรับทีม หน่วยงานภายใน และหน่วยงานภายนอก
- กำหนดให้สิ้นสุดภารกิจ การสรุปภารกิจ และการทบทวนเหตุการณ์ที่เกิดขึ้นทั้งหมด

ทีมและสมาชิกที่เกี่ยวข้องที่กล่าวถึงในเอกสารฉบับนี้จะต้องมีสำเนาของแผนฉบับนี้ติดตัวตลอดเวลา เพราะภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นจะไม่สามารถระบุ หรือคาดคะเนวันเวลาที่จะเกิดขึ้นได้ ทุกคนจึงต้องเตรียมความพร้อมโดยมีแผนฉบับนี้ไว้กับตัวเองตลอดเวลา

ข้อมูลติดต่อสำหรับทีมและสมาชิกดังกล่าวจะมีการทบทวน และปรับปรุงปีละ 2 ครั้ง เพื่อให้ข้อมูลมีความถูกต้อง และสามารถใช้ในการติดต่อได้ในยามที่จำเป็น

ข้อมูลส่วนตัว เช่น เบอร์โทรศัพท์ส่วนตัว ที่ใช้ในแผนฉบับนี้มีจุดประสงค์เพื่อใช้ในการบริหารจัดการภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเท่านั้น ไม่อนุญาตให้นำไปใช้เพื่อจุดประสงค์อื่นๆ

โครงสร้างการรับมือภัยคุกคามทางไซเบอร์

คณะทำงานบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม มีหน้าที่และความรับผิดชอบดังนี้

1. จัดทำ ทบทวน และปรับปรุงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 3 ครั้ง

2. สื่อสารสร้างความตระหนักให้ข้าราชการและเจ้าหน้าที่ผู้ที่เกี่ยวข้องของกรมฯ ปฏิบัติตามนโยบายและแนวปฏิบัติที่ได้กำหนดไว้ อย่างเคร่งครัด

3. ทบทวนการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ ตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประเมินและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมฯ อย่างน้อย ปีละ 1 ครั้ง

4. จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ และปรับปรุงอย่างน้อยปีละ 1 ครั้ง รวมทั้งจัดให้มีการซ้อมแผนดังกล่าวเป็นระยะ เพื่อให้มีความพร้อมในการปฏิบัติเมื่อเกิดเหตุฉุกเฉิน

5. จัดทำ ทบทวนและปรับปรุงโครงสร้างแผนกู้คืนระบบของกรมฯ กำกับดูแลทีมรับมือภัยคุกคามทางไซเบอร์ เพื่อให้การรับมือเป็นไปอย่างมีประสิทธิภาพ

6. ติดตามภัยคุกคามใหม่ๆ ที่อาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมฯ รวมทั้งกำหนดมาตรการรองรับที่จำเป็น

7. รายงานภัยคุกคามทางไซเบอร์ ที่เกิดขึ้นและให้คำแนะนำที่จะเป็นประโยชน์ในการปรับปรุงการดำเนินการ

ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล (Incident Response Manager)

มีหน้าที่และความรับผิดชอบดังนี้

- กำหนดขอบเขตและผลกระทบของเหตุการณ์จากข้อมูลภัยคุกคามทางไซเบอร์ที่ได้รับรายงานเข้ามา
- ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้น
- ประเมินเหตุที่เกิดขึ้นว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่
- ขออนุมัติการใช้แผนเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น
- บริหารทีมรับมือภัยคุกคามทางไซเบอร์เพื่อจัดการกับเหตุที่เกิดขึ้น
- ติดตามข้อมูลการอัพเดทสถานการณ์ของภัยคุกคามทางไซเบอร์เป็นระยะๆ
- รายงานให้คณะทำงานบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ได้ทราบถึงการอัพเดทของสถานการณ์เป็นระยะๆ
- พิจารณาการยุติการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น
- จัดทำรายงานสรุปภายหลังภัยคุกคามทางไซเบอร์สิ้นสุดลง

ทีมรับมือภัยคุกคามทางไซเบอร์

มีหน้าที่และความรับผิดชอบดังนี้

- ใช้แผนการรับมือภัยคุกคามทางไซเบอร์เพื่อรับมือกับเหตุการณ์ที่เกิดขึ้น
- จำกัดผลกระทบของเหตุการณ์ที่เกิดขึ้น
- ประเมินและระบุสาเหตุโดยพื้นฐานของเหตุการณ์ที่เกิดขึ้น
- แก้ไขปัญหาจนกระทั่งเหตุการณ์ยุติลง
- กู้คืนระบบตามความจำเป็น
- จัดเก็บข้อมูลคอมพิวเตอร์เพื่อใช้เป็นหลักฐานสำหรับเหตุการณ์ที่เกิดขึ้น
- รายงานสถานการณ์ให้ ผู้ประสานงานทีม ได้รับทราบ

หน่วยรับแจ้งเหตุการณ์

มีหน้าที่และความรับผิดชอบดังนี้

- รับแจ้งและบันทึกเหตุการณ์ที่ได้รับรายงานเข้ามาจากผู้ประสบเหตุการณ์
- วิเคราะห์และประเมินเหตุการณ์ที่ได้รับแจ้งว่ามีผลกระทบและความรุนแรงในระดับใด
- ประสานงานแจ้งเหตุการณ์ที่ได้รับแจ้งให้ ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัลทราบ

ผู้ประสานงานทีม

มีหน้าที่และความรับผิดชอบดังนี้

- ประสานงานติดต่อทีมรับมือภัยคุกคามทางไซเบอร์ เพื่อขอให้เข้าร่วมประชุมหารือเกี่ยวกับเหตุการณ์ที่เกิดขึ้น
- ทำหน้าที่เป็นเลขานุการในที่ประชุมและบันทึกรายงานการประชุม
- ติดตามและรวบรวมข้อมูลจากทีมรับมือภัยคุกคามทางไซเบอร์เกี่ยวกับสถานการณ์ที่เกิดขึ้น ประเมินสรุปสถานภาพ และรายงานผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล ทราบเพื่อใช้เป็นข้อมูลในการตัดสินใจดำเนินการ

ข้อมูลสำหรับการติดต่อ กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

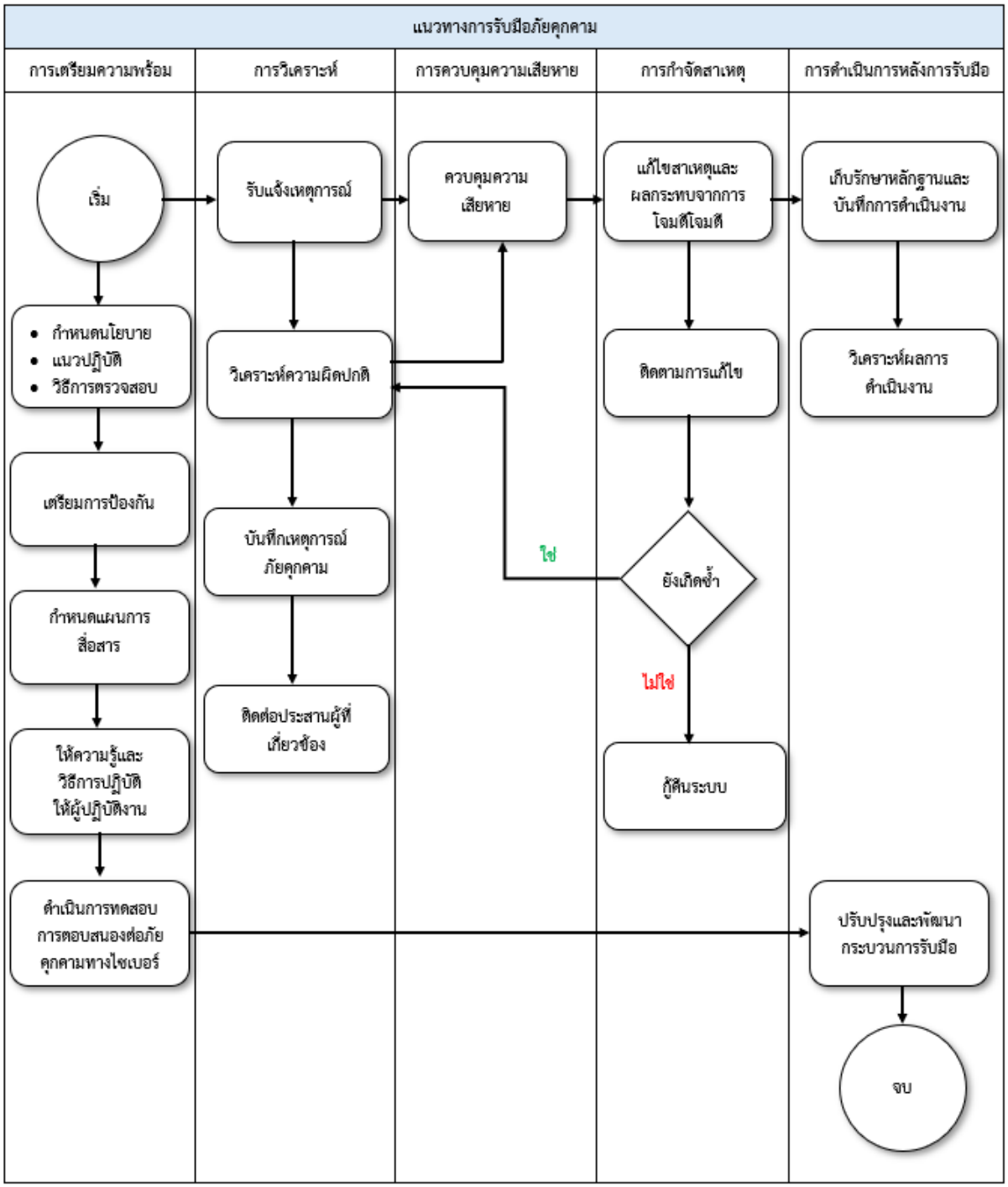
บทบาทหน้าที่ตามโครงสร้าง	ชื่อและตำแหน่งงานในองค์กร	ข้อมูลสำหรับการติดต่อ (อีเมล/เบอร์โทรศัพท์)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)	รองอธิบดี นายปวิช เกศววงศ์	pavichk@dcce.mail.go.th 02-2788423 095-3917425
คณะกรรมการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์	ผู้อำนวยการกองขับเคลื่อนการลดก๊าซเรือนกระจก (ประธานคณะทำงาน) นายศิวัช แก้วเจริญ	sivach@dcce.mail.go.th 081-9910690
Incident Response Manager	ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล นายสมชาย ภูนาสี	somchai.phu@dcce.mail.go.th 063-2034315
ทีมรับมือภัยคุกคามทางไซเบอร์		
– ทีมบริการให้ความช่วยเหลือ นายวิทยา ขำศิริ นายชรินทร์ เดชโชติ นางสาวศณารัตน์ มุสิกวัตร์ นายเกียรติศักดิ์ อ่อนศรี นายศศิน ทองหญิง	 นักวิชาการคอมพิวเตอร์ชำนาญการ นักวิชาการคอมพิวเตอร์ชำนาญการ นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์	 081-8374409 086-7658694 062-6696461 082-7771770 085-9076967
– ทีมผู้ดูแลเครือข่าย นายสมชาย ภูนาสี นายอรุณ ทรัพย์ประเสริฐ นางสาวอรอุมา กลางประพันธ์	 ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล นักวิชาการคอมพิวเตอร์ นักวิชาการคอมพิวเตอร์	 063-2034315 089-4861446 093-9969563

บทบาทหน้าที่ตามโครงสร้าง	ชื่อและตำแหน่งงานในองค์กร	ข้อมูลสำหรับการติดต่อ (อีเมล/เบอร์โทรศัพท์)
นางวรรณภา ตันติวิศาลเกษตร	นักวิชาการคอมพิวเตอร์	089-6395939
นายเกียรติศักดิ์ อ่อนศรี	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	082-7771770
– ทีมผู้ดูแลระบบ		
นายสมชาย ภูนาสี	ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล	063-2034315
นางสาวไพลิน พันธุ์แน่น	นักวิชาการคอมพิวเตอร์ชำนาญการ	063-9399878
นายชรินทร์ เดชโชติ	นักวิชาการคอมพิวเตอร์ชำนาญการ	086-7658694
นายโชคดี มั่นคง	นักวิชาการคอมพิวเตอร์	089-6823335
นายธไนสวรรค์ กุลบุตร	นักวิชาการคอมพิวเตอร์	080-9913380
นายศศิน ทองหญิง	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	085-9076967
– ทีมพัฒนาระบบ		
นายสมชาย ภูนาสี	ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล	063-2034315
นายวิทยา ขำศิริ	นักวิชาการคอมพิวเตอร์ชำนาญการ	081-8374409
นางสาวไพลิน พันธุ์แน่น	นักวิชาการคอมพิวเตอร์ชำนาญการ	063-9399878
นายโชคดี มั่นคง	นักวิชาการคอมพิวเตอร์	089-6823335
นายเจษฎา แสนสุภา	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	082-8414124
หน่วยรับแจ้งเหตุการณ์		
นายชรินทร์ เดชโชติ	นักวิชาการคอมพิวเตอร์ชำนาญการ	086-7658694
นางสาวศณารัตน์ มุสิกวัตร์	นักวิชาการคอมพิวเตอร์	062-6696461
นางวรรณภา ตันติวิศาลเกษตร	นักวิชาการคอมพิวเตอร์	089-6395939
นายอรุณ ทรัพย์ประเสริฐ	นักวิชาการคอมพิวเตอร์	089-4861446
นายธไนสวรรค์ กุลบุตร	นักวิชาการคอมพิวเตอร์	080-9913380
นายเจษฎา แสนสุภา	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	082-8414124
ผู้ประสานงานทีม		
นายอรุณ ทรัพย์ประเสริฐ	นักวิชาการคอมพิวเตอร์	089-4861446
นางสาวอรอุมา กลางประพันธ์	นักวิชาการคอมพิวเตอร์	093-9969563
นายเกียรติศักดิ์ อ่อนศรี	เจ้าหน้าที่ระบบคอมพิวเตอร์	082-7771770
นายเจษฎา แสนสุภา	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	082-8414124

ข้อมูลสำหรับการติดต่อ อาคารศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

บทบาทหน้าที่ตามโครงสร้าง	ชื่อและตำแหน่งงานในองค์กร	ข้อมูลสำหรับการติดต่อ (อีเมล/เบอร์โทรศัพท์)
ทีมกู้คืนระบบ		
นายรัฐ เรืองโชติวิทย์	นักวิชาการสิ่งแวดล้อมชำนาญการพิเศษ	081-3066407
นางชลธิชา มาลากุล	นักจัดการงานทั่วไปปฏิบัติการ	099-2383995
นายบรรดิษฐ์ สารีบุญ	นักวิชาการคอมพิวเตอร์	081-9653740
ทีมกู้คืนเครือข่าย		
นายรัฐ เรืองโชติวิทย์	นักวิชาการสิ่งแวดล้อมชำนาญการพิเศษ	081-3066407
นางชลธิชา มาลากุล	นักจัดการงานทั่วไปปฏิบัติการ	099-2383995
นายบรรดิษฐ์ สารีบุญ	นักวิชาการคอมพิวเตอร์	081-9653740
ทีมกู้คืนระบบปฏิบัติการ		
นายรัฐ เรืองโชติวิทย์	นักวิชาการสิ่งแวดล้อมชำนาญการพิเศษ	081-3066407
นางชลธิชา มาลากุล	นักจัดการงานทั่วไปปฏิบัติการ	099-2383995
นายบรรดิษฐ์ สารีบุญ	นักวิชาการคอมพิวเตอร์	081-9653740
ทีมแก้ไขกรณีถูกแทรกแซงระบบ		
นายรัฐ เรืองโชติวิทย์	นักวิชาการสิ่งแวดล้อมชำนาญการพิเศษ	081-3066407
นางชลธิชา มาลากุล	นักจัดการงานทั่วไปปฏิบัติการ	099-2383995
นายบรรดิษฐ์ สารีบุญ	นักวิชาการคอมพิวเตอร์	081-9653740
ทีมประเมินความเสียหาย		
นายรัฐ เรืองโชติวิทย์	นักวิชาการสิ่งแวดล้อมชำนาญการพิเศษ	081-3066407
นางชลธิชา มาลากุล	นักจัดการงานทั่วไปปฏิบัติการ	099-2383995
นายบรรดิษฐ์ สารีบุญ	นักวิชาการคอมพิวเตอร์	081-9653740

ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์



แต่ละขั้นตอนการรับมือเป็นดังนี้

1. การพบและการรายงานภัยคุกคามทางไซเบอร์

1.1 การพบภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอาจมีการพบเห็น หรือตรวจพบด้วยวิธีการต่างๆ เช่น มีผู้ประสบเหตุระบบมีการแจ้งเตือนไปยังทีมเฝ้าระวัง และด้วยวิธีการอื่นๆ เมื่อมีการพบภัยคุกคามทางไซเบอร์เกิดขึ้น ให้รีบดำเนินการรายงานไปยัง หน่วยรับแจ้งเหตุการณ์ โดยเร็วที่สุดตามข้อมูลในตารางที่ 1 ด้านล่าง

1.2 การรายงานหรือการแจ้งภัยคุกคามทางไซเบอร์

ผู้ประสบเหตุสามารถรายงานไปยังหน่วยรับแจ้งเหตุการณ์ได้ตามข้อมูลติดต่อที่ปรากฏในตารางด้านล่างโดยสามารถรายงานได้ตลอด 24 ชั่วโมง

หน่วยงาน	ชื่อผู้ติดต่อ	เบอร์โทรศัพท์
หน่วยรับแจ้งเหตุการณ์	นายชรินทร์ เดชโชติ นักวิชาการคอมพิวเตอร์ชำนาญการ	086-765-8694
	นายโชคดี มั่นคง นักวิชาการคอมพิวเตอร์	089-6823335

ตาราง 1 – ข้อมูลสำหรับติดต่อหน่วยรับแจ้งเหตุการณ์

1.3 การบันทึกรายละเอียดของภัยคุกคามทางไซเบอร์

เมื่อได้รับแจ้งเตือนถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้น หน่วยรับแจ้งเหตุการณ์ จะต้องบันทึกรายละเอียดดังต่อไปนี้ไว้เป็นข้อมูลพื้นฐานเพื่อใช้ในการจัดการต่อไป

- ชื่อและนามสกุลของผู้แจ้งเหตุ
- ข้อมูลติดต่อกลับของผู้แจ้งเหตุ
- วันเวลาที่ได้รับแจ้งเหตุ
- ผู้รับแจ้งเหตุ
- รายละเอียดของเหตุที่เกิดขึ้น ได้แก่
    - วันและเวลาของเหตุที่เกิดขึ้น
    - สภาพของเหตุที่พบ
    - ทรัพย์สินที่ได้รับความเสียหาย
    - สถานที่ที่พบเหตุ
    - การประมาณการของระดับผลกระทบ
    - ข้อมูลที่จะเป็นประโยชน์อื่น ๆ

หน่วยรับแจ้งเหตุการณ์ กำหนดและจำแนกประเภทของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ตามแนวทางที่ปรากฏในตารางด้านล่างนี้ (อ้างอิงจากเอกสารประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564)

ข้อ 1 การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์	
หมวดหมู่	**คำอธิบาย**
0	เหตุการณ์จำลอง และ การฝึกจู่โจมของหน่วยงานเอง (Training and Exercises)
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

2. การประเมินผลกระทบ

จากข้อมูลที่ได้มีการสอบถามจากผู้ที่แจ้งเหตุ หน่วยรับแจ้งเหตุการณ์ ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นโดย อ้างอิงเกณฑ์การประเมินผลกระทบหรือความรุนแรงของเหตุการณ์ที่เกิดขึ้นจากเอกสาร ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 ซึ่งแบ่งเป็น 3 ระดับ

- ระดับไม่ร้ายแรง
- ระดับร้ายแรง
- ระดับวิกฤต

3. การติดต่อ ผู้อำนวยการกองขับเคลื่อนการลดก๊าซเรือนกระจก

หน่วยรับแจ้งเหตุการณ์ จะต้องรีบดำเนินการติดต่อผู้อำนวยการกองขับเคลื่อนการลดก๊าซเรือนกระจก หรือบุคคลที่ได้รับมอบหมาย บุคคลที่ได้รับมอบหมายในลำดับถัดไปโดยเร็วที่สุด มีจุดประสงค์เพื่อ กรณีที่ผู้อำนวยการกองขับเคลื่อนการลดก๊าซเรือนกระจก ไม่อยู่หรือไม่ได้มาปฏิบัติหน้าที่ไม่ว่าจะด้วยสาเหตุใดก็ตาม ผู้ที่ได้รับมอบหมายในลำดับถัดไปจะสามารถทำหน้าที่ทดแทนได้โดยทันที โดยใช้ข้อมูลติดต่อด้านล่างนี้

ชื่อ	บทบาทตามแผน	เบอร์โทรศัพท์สำนักงาน	เบอร์โทรศัพท์ที่บ้าน	เบอร์โทรศัพท์มือถือ
นายศิวัช แก้วเจริญ	ผู้อำนวยการกองขับเคลื่อนการลดก๊าซเรือนกระจก	02-2985634	–	081-9910690

ชื่อ	บทบาทตามแผน	เบอร์โทรศัพท์สำนักงาน	เบอร์โทรศัพท์ที่บ้าน	เบอร์โทรศัพท์มือถือ
นายสมชาย ภูนาสี	ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล	02-2985637	–	063-2034315

ตาราง 2 – ข้อมูลติดต่อของ ผู้อำนวยการกองขับเคลื่อนการลดก๊าซเรือนกระจก และผู้ที่ได้รับมอบหมายในลำดับถัดไป

4. การตัดสินใจและขออนุมัติการรับมือกับภัยคุกคามทางไซเบอร์

ทันทีที่ได้รับแจ้งภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัลต้องตัดสินใจจากข้อมูลและระดับผลกระทบหรือความรุนแรงและขอบเขตของเหตุที่เกิดขึ้น แนวทางการตัดสินใจในการรับมือคือให้พิจารณาจากเงื่อนไขดังต่อไปนี้

- เกิดการหยุดชะงักต่อกระบวนงานสำคัญ
- ก่อให้เกิดความเสียหายต่อชื่อเสียงและภาพลักษณ์ของกรมฯ
- ก่อให้เกิดการละเมิดกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง หรือ
- ก่อให้เกิดการละเมิดข้อมูลส่วนบุคคล

จากนั้น ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล ขออนุมัติใช้แผนเพื่อรับมือกับภัยคุกคามทางไซเบอร์จากประธานคณะทำงานบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม เมื่อได้รับอนุมัติแล้ว จะทำการระดมทีมเพื่อรับมือกับเหตุที่เกิดขึ้น

5. การระดม ประชุมทีม และรับมือภัยคุกคามทางไซเบอร์

ผู้ประสานงานทีม ประสานงานติดต่อทีมรับมือภัยคุกคามทางไซเบอร์ทั้งหมด และขอให้ไปประชุมหารือร่วมกันที่ศูนย์การดำเนินการและประสานงาน ซึ่งตั้งอยู่ที่

[กลุ่มพัฒนาเทคโนโลยีดิจิทัล กองขับเคลื่อนการลดก๊าซเรือนกระจก หมายเลข 02-2985637 หมายเลขติดต่อ ภายใน 02-2788400 ต่อ 1630-1633 1642 1646]

แผนที่สำหรับการเดินทางไปยังศูนย์การดำเนินการและประสานงานอยู่ใน ภาคผนวก I ของเอกสารฉบับนี้

ในการติดต่อ ผู้ประสานงานทีม บันทึกผลการติดต่อว่าสำเร็จหรือไม่ลงในแบบฟอร์มบันทึกผลการติดต่อสมาชิกของทีมฯ ในภาคผนวก A

การประชุมทีม

เมื่อทีมรับมือภัยคุกคามทางไซเบอร์มาพร้อมกันที่ศูนย์การดำเนินการและประสานงานแล้ว ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล จะทำการเปิดประชุม กล่าวถึงสถานการณ์ที่เกิดขึ้น ขอให้ทีมร่วมกันให้ข้อคิดเห็นสำหรับการดำเนินการต่างๆ ตัดสินใจดำเนินการ มอบหมายหน้าที่ความรับผิดชอบไปยังผู้ที่เกี่ยวข้อง และมอบให้ผู้ประสานงานทีมสื่อสารภายในและภายนอกตามความจำเป็น

การตัดสินใจรับมือกับเหตุที่เกิดขึ้นนั้นจะมีความเกี่ยวข้องกับการเรียกใช้แผนรับมือแยกตามประเภทของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นตามที่ปรากฏในตารางด้านล่าง

เลขที่อ้างอิงแผน	ชื่อแผน	รายละเอียดของแผน
แผน001	แผนการจัดการกับโปรแกรมไม่ประสงค์ดี	
แผน002	แผนการจัดการกับเหตุการณ์ระบบถูกโจมตีอย่างต่อเนื่องจนกระทั่งไม่สามารถให้บริการได้	
แผน003	แผนการจัดการกับเหตุการณ์ระบบถูกสแกน	
แผน004	แผนกการจัดการกับเหตุการณ์ระบบถูกบุกรุกและถูกเข้าถึงภายในระบบ	
แผน005	แผนการจัดการกับเหตุการณ์หน้าเว็บไซต์หลักขององค์กรถูกเปลี่ยน	

ตาราง 3 – แผนรับมือแยกตามประเภทของภัยคุกคามทางไซเบอร์

เมื่อมีการเรียกใช้แผนรับมือแผนใด ให้ทำการบันทึกการเรียกใช้แผนโดยใช้แบบฟอร์มที่ปรากฏในภาคผนวก C เพื่อทำการบันทึก

การประชุมจะมีวาระการประชุมตามเอกสารที่ปรากฏใน ภาคผนวก H ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล จะเป็นผู้กำหนดความถี่ในการประชุมว่าจะดำเนินการประชุมอีกครั้งหนึ่งเมื่อใด ผู้ประสานงานทีม ทำหน้าที่เป็นเลขาในที่ประชุมและบันทึกรายงานการประชุม

การอัพเดทสถานการณ์ที่เปลี่ยนแปลงไปตามเวลาจะมีการบันทึกไว้ในแบบฟอร์มการอัพเดทรายงานสถานการณ์ใน ภาคผนวก B

การบันทึกกิจกรรมหรือการตัดสินใจที่สำคัญๆ ควรมีการบันทึกไว้ในแบบฟอร์มสำหรับการบันทึกกิจกรรมที่สำคัญๆ ที่ได้มีการตัดสินใจหรือดำเนินการใน ภาคผนวก D

ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล รายงานอัพเดทของสถานการณ์ให้คณะทำงานบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ได้รับทราบเป็นระยะๆ เพื่อให้คำแนะนำต่างๆ

6. การลงมือดำเนินการ การเฝ้าระวังสถานการณ์ และการสื่อสารไปยังผู้ที่เกี่ยวข้อง

6.1 การจำกัดหรือลดผลกระทบที่เกิดขึ้น

ทีมรับมือภัยคุกคามทางไซเบอร์ พยายามจำกัดหรือลดผลกระทบของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยขึ้นอยู่กับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ทีมฯ อาจเลือกใช้การจำกัดหรือลดผลกระทบดังต่อไปนี้

- ปิดการทำงานของเซิร์ฟเวอร์ชั่วคราว
- ตัดการเชื่อมต่อทางเครือข่าย
- ยกเลิกบัญชีผู้ใช้งานชั่วคราว
- แก้ไขคอนฟิกของไฟร์วอลล์เพื่อตัดการเชื่อมต่อทางเครือข่าย

6.2 การขจัดปัญหาที่สาเหตุและดำเนินการเปลี่ยนแปลงระบบเพื่อแก้ไขปัญหา

ทีมรับมือภัยคุกคามทางไซเบอร์ วิเคราะห์หาสาเหตุที่แท้จริงว่าเกิดจากสาเหตุใด เพื่อกำหนดแนวทางในการแก้ไขปัญหา และดำเนินการเปลี่ยนแปลงระบบเพื่อแก้ไขปัญหาตามแนวทางการแก้ปัญหาที่กำหนดไว้นั้น

6.3 การกู้คืนระบบ

ทีมรับมือภัยคุกคามทางไซเบอร์ นำระบบที่ได้รับความเสียหายหรือที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์กลับคืนสู่สภาพปกติ

กรณีที่ระบบหลักไม่สามารถให้บริการได้อันเกิดจากภัยคุกคามทางไซเบอร์ และมีความจำเป็นต้องเปิดใช้งานระบบสำรอง ทีมรับมือภัยคุกคามทางไซเบอร์ ประสานงานกับ ทีมกู้คืนระบบเพื่อดำเนินการกู้ระบบตามความจำเป็น

6.4 การจัดเก็บข้อมูลหลักฐานด้านคอมพิวเตอร์

หากมีความจำเป็นต้องเก็บข้อมูลหลักฐานด้านคอมพิวเตอร์เพื่อไว้ใช้ในการดำเนินคดีในชั้นศาล ผู้รับผิดชอบเก็บหลักฐานจะต้องได้รับการฝึกอบรมในการจัดเก็บหลักฐานอย่างถูกต้องเพื่อให้หลักฐานสามารถยอมรับได้ในชั้นศาล ดังนั้นข้อมูลที่จะมีการจัดเก็บจะต้องไม่มีการเปลี่ยนแปลงโดยเด็ดขาด ไม่ว่าจะจงใจหรือโดยไม่จงใจก็ตาม (ซึ่งจะส่งผลให้หลักฐานไม่สามารถใช้ในชั้นศาลได้) ข้อมูลต้นฉบับที่จัดเก็บไว้จะต้องนำไปเก็บไว้ในสถานที่ที่ปลอดภัยจากการถูกเข้าถึง

หลักการโดยทั่วไปดังต่อไปนี้จะต้องปฏิบัติตามอย่างเคร่งครัด

- **หลักการที่ 1** : ห้ามเปลี่ยนแปลงข้อมูลต้นฉบับที่จัดเก็บโดยเด็ดขาด
- **หลักการที่ 2** : เข้าถึงข้อมูลต้นฉบับที่จัดเก็บไว้เฉพาะกรณีจำเป็นเท่านั้น ปกติแล้วการดำเนินการวิเคราะห์ข้อมูลที่จัดเก็บไว้จะกระทำกับข้อมูลที่เป็นสำเนาเท่านั้น จะไม่มีการเข้าถึงข้อมูลต้นฉบับเว้นแต่กรณีที่มีความจำเป็นจริงๆ เท่านั้น
- **หลักการที่ 3** : บันทึกกิจกรรมการดำเนินการกับข้อมูลหลักฐาน ผู้ดำเนินการ วันเวลาที่ดำเนินการ และรายละเอียดอื่นๆ ที่จำเป็น
- **หลักการที่ 4** : เมื่อมีการส่งมอบหรือส่งต่อข้อมูลต้นฉบับ (ที่อาจเรียกว่าวัตถุพยาน) ไปยังผู้ที่เกี่ยวข้องต่างๆ (ซึ่งถือเป็นการเปลี่ยนมือของผู้ครอบครองวัตถุพยาน) ผู้ครอบครองตามลำดับที่มีการเปลี่ยนมือมา จะต้องแสดงให้เห็นถึงลูกโซ่ของการครอบครองวัตถุยาน (ดูความหมายและรายละเอียดใน<u>ภาคผนวก J</u>) ทั้งนี้เพื่อให้เกิดความเชื่อมั่นว่าหลักฐานนั้นเป็นหลักฐานที่เชื่อถือได้ว่ามิได้มีการถูกเปลี่ยนแปลงแก้ไขแต่อย่างใด

6.5 การเฝ้าระวังสถานการณ์

ผู้ประสานงานทีม เฝ้าระวังและติดตามสถานการณ์จากทีมรับมือภัยคุกคามทางไซเบอร์หมั่นติดตามการอัพเดทสถานการณ์ล่าสุดจากทีมดังกล่าวเพื่อรายงานให้ ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล ได้รับทราบ

6.6 การสื่อสารไปยังผู้ที่เกี่ยวข้อง

การสื่อสารไปยังผู้ที่เกี่ยวข้องในทุกระดับมีความสำคัญอย่างยิ่งยวดต่อความสำเร็จ และความได้ผลของการจัดการกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

6.6.1 วิธีการสื่อสาร

วิธีการสื่อสารที่เป็นพื้นฐานในช่วงที่เหตุการณ์หยุดชะงักกำลังดำเนินไป คือ

- เสียงตามสาย
- โทรศัพท์ (ทั้งโทรศัพท์สำนักงานและโทรศัพท์มือถือ)
- อีเมล
- SMS Line

โดยจะเริ่มต้นใช้วิธีการสื่อสารเรียงตามลำดับในข้างต้นจากบนลงมาล่าง กรณีที่ใช้วิธีการในลำดับแรกๆ ไม่ได้จะเลื่อนลำดับลงมายังวิธีการในลำดับถัดไป

6.6.2 การสื่อสารภายในองค์กร

<u>การติดต่อศูนย์การดำเนินการและประสานงาน</u>

เบอร์โทรหลักสำหรับการติดต่อมายังศูนย์การดำเนินการและประสานงานคือ 02-2985637

<u>การติดต่อบุคลากรหรือหน่วยงานภายในต่างๆ</u>

กรณีมีความจำเป็นต้องติดต่อบุคลากรหรือหน่วยงานภายในต่างๆ ให้ดูข้อมูลสำหรับการติดต่อได้ใน <u>*ภาคผนวก F*</u>

6.6.3 การสื่อสารภายนอกองค์กร

หน่วยงานภายนอกที่กรมฯ จำเป็นต้องติดต่อสื่อสารด้วย ได้แก่

- ผู้ให้บริการอินเทอร์เน็ต
- ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย
- ผู้รับจ้าง หรือผู้ให้บริการภายนอก
- อื่น ๆ

ให้ดูข้อมูลสำหรับการติดต่อหน่วยงานเหล่านั้นใน <u>*ภาคผนวก G*</u>

7. การยุติการรับมือภัยคุกคามทางไซเบอร์และการสิ้นสุดภารกิจ

ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล จะเป็นผู้พิจารณาการยุติการรับมือกับภัยคุกคามทางไซเบอร์และขออนุมัติจากประธานคณะทำงานบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม เพื่อประกาศการสิ้นสุดภารกิจการรับมืออย่างเป็นทางการ

เงื่อนไขในการยุติการรับมือกับภัยคุกคามทางไซเบอร์ และสิ้นสุดภารกิจประกอบด้วย

- สถานการณ์ได้รับการแก้ไขหรือเยียวยาโดยสมบูรณ์
- สถานการณ์อยู่ในขั้นที่มีเสถียรภาพที่ดี
- การรับมือกับภัยคุกคามทางไซเบอร์อยู่ในระหว่างการดำเนินการ และแผนที่เรียกใช้มีความคืบหน้าตามกำหนดการและเป็นไปได้ด้วยดี
- หน่วยงานภายในที่ได้รับผลกระทบกลับคืนสู่สภาวะที่สามารถปฏิบัติงานต่อไปได้ แม้ว่าจะอยู่ในระดับที่น้อยกว่าสภาวะตามปกติก็ตาม
- ระดับความเสี่ยงที่มีต่อกรมฯ ลดลงในระดับที่ยอมรับได้

การยุติการรับมือกับภัยคุกคามทางไซเบอร์ ควรมีการบันทึกไว้ในแบบฟอร์มใน ภาคผนวก D แบบฟอร์มสำหรับการบันทึกกิจกรรมที่สำคัญๆ ที่ได้มีการตัดสินใจ หรือดำเนินการ

8. การสรุปภารกิจและการทบทวนเหตุการณ์ที่เกิดขึ้นทั้งหมด

หลังจากภารกิจเสร็จสิ้นลงแล้ว ผู้อำนวยกลุ่มพัฒนาเทคโนโลยีดิจิทัล จะต้องทำการสรุปภาพรวมทั้งหมดของภารกิจภายใน 48 ชั่วโมง ข้อมูลที่บันทึกไว้ในภาคผนวกทั้งหมดจะต้องนำมาประกอบการพิจารณาทบทวนนี้ด้วย

ผู้อำนวยกลุ่มพัฒนาเทคโนโลยีดิจิทัล จะต้องทำการทบทวนเหตุการณ์ที่เกิดขึ้นทั้งหมดนับตั้งแต่การเตรียมการล่วงหน้าต่างๆ ที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ การดำเนินการรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น การดำเนินการรับมือในระหว่างทาง ตลอดจนการสิ้นสุดภารกิจการรับมือว่ามีสิ่งใดที่จำเป็นต้องปรับปรุง หรือแก้ไขหรือไม่ ผลการทบทวนทั้งหมดจะต้องมีการบันทึกไว้ในรายงาน After Action Report ซึ่งควรมีเนื้อหาครอบคลุมในประเด็นดังนี้

- การระบุสาเหตุของเหตุการณ์ที่เกิดขึ้น
- มูลค่าความเสียหายที่เกิดขึ้น
- ผลกระทบของเหตุที่เกิดขึ้น ซึ่งรวมถึงผลกระทบต่อชื่อเสียงและภาพลักษณ์ของกรมฯ
- การระบุการดำเนินการเชิงแก้ไขหรือเชิงป้องกันเพื่อป้องกันการเกิดขึ้นซ้ำอีกของเหตุการณ์นี้ในอนาคต
- ความเหมาะสมในการตัดสินใจดำเนินการเพื่อรับมือและจัดการกับเหตุที่เกิดขึ้น
- ในกรณีที่เหตุการณ์ที่เกิดขึ้นทำให้เกิดการหยุดชะงักต่อกระบวนงานสำคัญ ให้ประเมินความเหมาะสมด้านระยะเวลาที่ใช้ไปในแก้ไขเพื่อให้กระบวนงานนั้นกลับคืนมาให้บริการได้
- ความเหมาะสมด้านสิ่งต่างๆ ที่ได้เตรียมการไว้ก่อนล่วงหน้า
- การทบทวนจากข้อมูลที่บันทึกไว้ระหว่างเกิดเหตุว่ามีสิ่งใดที่มองข้ามไป คาดการณ์ผิด หรือเป็นข้อบกพร่องที่ต้องแก้ไข
- การพิจารณาว่าแผนการรับมือภัยคุกคามทางไซเบอร์ควรปรับปรุงแก้ไขในจุดใดเพื่อให้มีความครบถ้วน ถูกต้อง และใช้งานได้อย่างมีประสิทธิภาพมากขึ้น
- การพิจารณาว่าจำเป็นต้องมีการอบรม ฝึกฝน หรือสร้างความตระหนักเพิ่มเติมหรือไม่
- การระบุสิ่งที่ต้องดำเนินการปรับปรุงหรือแก้ไขเพิ่มเติม เช่น นโยบายและแนวปฏิบัติต่างๆ

ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล จัดส่งรายงานสรุปให้คณะทำงานบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมเพื่อพิจารณาและให้ข้อคิดเห็นต่างๆ ตามความจำเป็น พร้อมทั้งรายงานผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมเพื่อทราบต่อไป

ภาคผนวก A แบบฟอร์มบันทึกผลการติดต่อสมาชิกของทีมรับมือภัยคุกคามทางไซเบอร์

ตารางด้านล่างใช้ในการบันทึกข้อมูลผลการติดต่อสมาชิกของทีมรับมือภัยคุกคามทางไซเบอร์ว่าติดต่อได้สำเร็จหรือไม่

ชื่อ ผู้รับการติดต่อ	บทบาทตามแผน	เบอร์โทรศัพท์ สำนักงาน	เบอร์โทรศัพท์ ที่บ้าน	เบอร์โทรศัพท์ มือถือ	วันเวลาที่ ติดต่อ	ผลลัพธ์การติดต่อ (ติดต่อสำเร็จหรือไม่สำเร็จ ข้อความที่ทิ้งไว้)	ข้อคิดเห็น ความเห็น หรืออื่นๆ
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			
		Xxx xxx xxx	Xxx xxx xxx	Xxx xxx xxx			

ภาคผนวก B การอัพเดทรายงานสถานการณ์ที่เปลี่ยนแปลงไปตามเวลา

ภัยคุกคามทางไซเบอร์:		**สถานที่ที่เกิด:**	

วันที่	**เวลา**	**การอัพเดทข้อมูลสถานการณ์เป็นระยะๆ**	**โดย**	**ผู้ลงนาม**

ภาคผนวก C แบบฟอร์มสำหรับการเรียกใช้แผนรับมือภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์:		**สถานที่ที่เกิด:**	

วันที่	เวลา	กิจกรรมที่ได้รับผลกระทบ	ระดับของผลกระทบ	แผนรับมือภัยคุกคามทางไซเบอร์ที่มีการเรียกใช้	วันที่ที่เรียกใช้แผน	เวลาที่เรียกใช้แผน

ภาคผนวก D แบบฟอร์มสำหรับการบันทึกกิจกรรมที่สำคัญๆ ที่ได้มีการตัดสินใจหรือดำเนินการ

ภัยคุกคามทางไซเบอร์:		**สถานที่ที่เกิด:**	

วันที่	เวลา	การดำเนินการ	โดย	ความคิดเห็น คำแนะนำ หรืออื่นๆ	ผู้ลงนาม

ภาคผนวก E แบบฟอร์มสำหรับบันทึกข้อมูลหรือข้อความที่ได้มีการติดต่อสื่อสารกันโดยผ่านทางช่องทางการสื่อสารที่กำหนดไว้

ข้อมูลที่ได้มีการสื่อสารกันควรจะมีการบันทึกไว้อย่างถูกต้องและชัดเจนโดยใช้แบบฟอร์มด้านล่างนี้

ภัยคุกคามทางไซเบอร์:		**สถานที่ที่เกิด:**	

วันที่ที่ติดต่อ	เวลาที่ติดต่อ	ผู้ติดต่อ	เบอร์โทรของผู้ติดต่อ	ผู้รับการติดต่อ	เบอร์โทรศัพท์ของผู้รับการติดต่อ	ข้อความที่มีการสื่อสาร

ภาคผนวก F ข้อมูลสำหรับการติดต่อหน่วยงานหรือบุคลากรภายในองค์กร

ข้อมูลในตารางด้านล่างนี้เป็นข้อมูลสำหรับการติดต่อหน่วยงานหรือบุคลากรภายในองค์กร

ชื่อผู้ที่ต้องการติดต่อ	ตำแหน่ง	แผนก/ฝ่าย	เบอร์โทรศัพท์	อีเมล์

ภาคผนวก G ข้อมูลสำหรับการติดต่อหน่วยงานภายนอก

ข้อมูลในตารางด้านล่างนี้เป็นข้อมูลสำหรับการติดต่อหน่วยงานภายนอก

ชื่อผู้ที่ต้องการติดต่อ	ตำแหน่ง	หน่วยงาน	ที่อยู่	เบอร์โทรศัพท์	อีเมล์
ISP					
DGA					
News					
Vendor					

ภาคผนวก H วาระการประชุมทีมรับมือภัยคุกคามทางไซเบอร์

วาระการประชุมทีมรับมือภัยคุกคามทางไซเบอร์และความถี่ในการประชุมทีมจะขึ้นอยู่กับการตัดสินใจของผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีดิจิทัล เป็นผู้กำหนดให้ดำเนินการ

วาระการประชุม

ผู้เข้าร่วมประชุม: [ระบุผู้เข้าร่วมประชุม]

สถานที่ประชุม: ศูนย์การดำเนินการและประสานงาน

ความถี่ในการประชุม: [ระบุความถี่ในการประชุม เช่น ทุกๆ 1 วัน จนกว่าจะสิ้นสุดภารกิจ]

ประธานในที่ประชุม: ผู้อำนวยการกองขับเคลื่อนการลดก๊าซเรือนกระจก

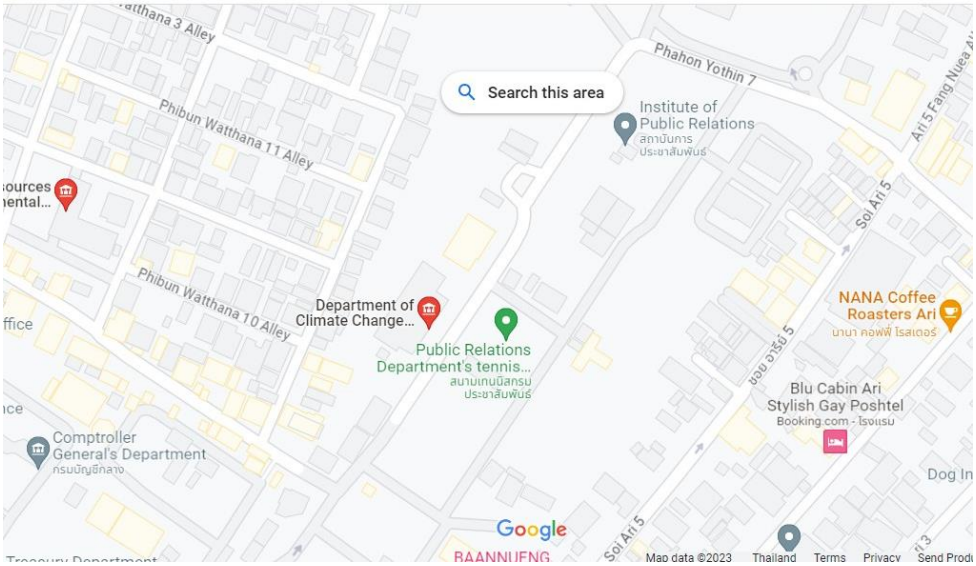
วาระการประชุมตามลำดับ:

1. การรายงานผลการดำเนินการจากการประชุมครั้งที่แล้ว
2. การอัพเดทสถานการณ์ที่เกิดขึ้น
3. การตัดสินใจดำเนินการ
4. การมอบหมายงานไปยังผู้ที่เกี่ยวข้อง
5. การสื่อสารภายใน
6. การสื่อสารภายนอก
7. การสิ้นสุดภารกิจ
8. เรื่องอื่นๆ ถ้ามี

ภาคผนวก I ศูนย์การดำเนินการและประสานงาน

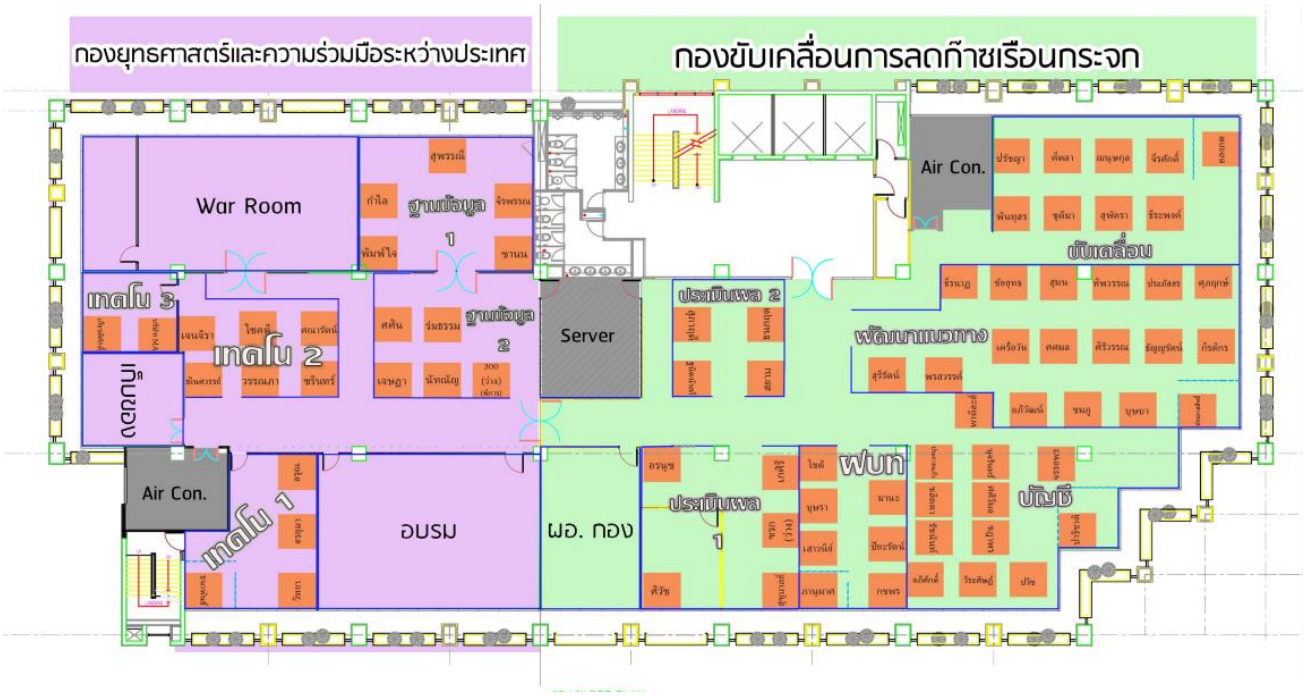
แผนที่สำหรับการเดินทางไปยังศูนย์การดำเนินการและประสานงาน

แผนที่สำหรับการเดินทางไปยังศูนย์การดำเนินการและประสานงานดังปรากฏอยู่ในรูปด้านล่าง



ผังแสดงพื้นที่ในส่วนต่างๆ ของศูนย์การดำเนินการและประสานงาน

แผนผังแสดงพื้นที่ในส่วนต่าง ๆ ของศูนย์การดำเนินการและประสานงานดังปรากฏอยู่ในรูปด้านล่าง



ภาคผนวก J ลูกโซ่ของการครอบครองวัตถุยาน

ตามรูปที่ปรากฏด้านล่าง

แต่ละขั้นตอนสามารถอธิบายได้ดังนี้

- **การจัดการ:** ผู้รับผิดชอบจะต้องดำเนินการจัดการกับข้อมูลต้นฉบับ (ซึ่งอาจเรียกว่า วัตถุพยาน) เช่น โดยการสำเนาเก็บไว้
- **การจัดเก็บ:** ถัดมา ผู้รับผิดชอบอาจจะนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัย
- **การขนส่ง:** เมื่อจำเป็นต้องนำวัตถุพยานนั้นไปใช้ในการดำเนินการในชั้นศาล อาจจะต้องผ่านกลไกการขนส่ง กล่าวคือ การจัดส่งวัตถุพยานนั้นไปยังศาลยุติธรรม
- **การส่งมอบ**: เมื่อไปถึงปลายทาง ก็จะมีการส่งมอบวัตถุพยานนั้นไปยังผู้รับ
- **การนำไปใช้ในชั้นศาล**: และสุดท้าย วัตถุพยานถูกนำไปใช้ในชั้นศาล

ในแต่ละขั้นตอนตามที่อธิบายในข้างต้นนั้น วัตถุพยานจะมีการครอบครองและเปลี่ยนมือไปยังผู้ที่เกี่ยวข้องตามลำดับ ผู้ครอบครองจะต้องมีการบันทึกไว้เป็นเอกสาร ระบุการครอบครองวัตถุพยาน รายละเอียดที่เกี่ยวข้องของกิจกรรมการดำเนินการกับวัตถุพยาน พร้อมลงลายมือชื่อของผู้ครอบครอง

โดยรวมสามารถเรียกขั้นตอนทั้งหมดตามที่ปรากฏในรูปว่าลูกโซ่ของการครอบครองวัตถุพยาน ภาษาอังกฤษใช้คำว่า Chain of Custody

การดำเนินการเช่นนี้เพื่อให้เกิดความน่าเชื่อถือของวัตถุพยานว่าสามารถใช้เป็นหลักฐานในการพิสูจน์ความจริงในชั้นศาลได้ เนื่องจากในทุกจังหวะของการครอบครองวัตถุพยาน จะมีเอกสารอย่างเป็นลายลักษณ์อักษรเพื่อแสดงเสมอว่าใครเป็นผู้ครอบครองและมีการดำเนินการอะไรบ้างกับวัตถุพยานดังกล่าว