ประกาศกรมสรรพสามิต
เรื่อง นโยบายและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ และควบคุมความเสี่ยง
ด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Policy) พ.ศ. ๒๕๖๗

เพื่อให้กรมสรรพสามิตมีแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปตามที่กำหนดไว้ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ลงวันที่ ๒ สิงหาคม ๒๕๖๔ ซึ่งออกตามความในมาตรา ๑๓ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ อธิบดีกรมสรรพสามิตจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้มีนโยบายในความมั่นคงปลอดภัยไซเบอร์ และควบคุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์เกี่ยวกับเรื่องดังต่อไปนี้

(๑) มีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการธำรงไว้ซึ่งการรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้

(๒) จัดให้มีการประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือตามมาตรฐานสากล อย่างน้อยปีละ ๑ ครั้ง เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้น

(๓) กำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ หรือขั้นตอนปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ เพื่อตอบสนองต่อเหตุการณ์ และแก้ไขปัญหาที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

(๔) ปรับปรุงนโยบายและและแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และควบคุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญให้สอดคล้องกับกฎหมาย กฎระเบียบ และภัยคุกคามในปัจจุบัน หรือที่อาจเกิดขึ้นในอนาคต

(๕) มีการจัดสรรทรัพยากร ด้านทรัพยากรบุคคล และด้านการบริหารจัดการเทคโนโลยีเพื่อกำกับและติดตามการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ภายในกรมสรรพสามิต และเพื่อเป็นแนวทางการควบคุมอุปกรณ์สารสนเทศ และการปฏิบัติงานจากภายนอกที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ ให้เป็นไปตามแนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ และควบคุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์ท้ายประกาศนี้

ข้อ ๒ ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๑ กรกฎาคม พ.ศ. ๒๕๖๗

(นายเอกนิติ นิติทัณฑ์ประภาศ)
อธิบดีกรมสรรพสามิต

แนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ และควบคุมความเสี่ยง ด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Policy) ของกรมสรรพสามิต

สารบัญ

๑. แนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ และควบคุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Policy)

ข้อ ๑ ให้มีคณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีตัวแทนจากทางหน่วยงานที่มีความเชี่ยวชาญและหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์เป็นผู้รับผิดชอบความมั่นคงปลอดภัยทางไซเบอร์ และให้กำหนดหน้าที่ความรับผิดชอบพร้อมทั้งวิธีการบริหารจัดการ

ข้อ ๒ ให้มีการจัดอบรมให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) เพื่อสร้างความตระหนักรู้ ความรับผิดชอบ และความเข้าใจการรับมือกับภัยคุกคามทางไซเบอร์ให้กับข้าราชการลูกจ้างประจำ พนักงานราชการ และลูกจ้างชั่วคราว สังกัดกรมสรรพสามิต อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓ ให้บุคลากรในกรมสรรพสามิตมีการติดตามข่าวสารช่องทางต่าง ๆ จากกลุ่มผู้เชี่ยวชาญ คู่ค้า พันธมิตร หรือผู้ให้บริการภายนอก ให้ครอบคลุมด้านความมั่นคงปลอดภัยทางด้านไซเบอร์ด้วย

ข้อ ๔ พัฒนาและรักษากรอบการดำเนินงานหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้สอดคล้องกับมาตรฐานสากล และติดตามกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง และพิจารณาการปฏิบัติตามให้สอดคล้อง

ข้อ ๕ ปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมถึงความมั่นคงปลอดภัยทางไซเบอร์ และปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ ๖ ให้นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีการกำหนดวิธีการและเครื่องมือที่เหมาะสมกับการเฝ้าระวังความเสี่ยงด้านไซเบอร์ขององค์กร มีการกำหนดให้มีการปรับปรุงแผนการกู้คืนระบบให้เป็นปัจจุบันอยู่เสมอ รวมถึงจัดให้มีการทำ Lesson learn ภายหลังการกู้คืนระบบ

ข้อ ๗ ให้มีการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ โดยการประเมินจากภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) ความเป็นไปได้ (Likelihoods) และผลกระทบ (Impact) ต่อบริการ รวมทั้งให้มีการจัดการความเสี่ยงที่มีความสอดคล้องกับการบริหารความเสี่ยงในระดับองค์กร โดยขอบเขตของการบริหารความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงสินทรัพย์และบุคลากรทั้งหมดของกรมสรรพสามิต อีกทั้งหน่วยงานภายนอกที่เกี่ยวข้อง

ข้อ ๘ ให้มีการติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุกด้านไซเบอร์ ให้ครอบคลุมระบบสารสนเทศของกรมสรรพสามิต พร้อมทั้งจัดให้มีการเฝ้าระวัง และให้หน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ ต้องรายงานข้อมูลภัยคุกคามด้านไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างน้อยปีละครั้ง

ข้อ ๙ ให้ระบุระบบที่องค์กรใช้งานซึ่งติดตั้งอยู่ภายนอกพื้นที่ของกรมสรรพสามิตให้ครบถ้วนในรายการทรัพย์สิน เพื่อจะได้กำหนดมาตรการควบคุมให้เหมาะสมกับความเสี่ยงที่อาจจะเกิดขึ้น

ข้อ ๑๐ ให้จัดทำแผนการตอบสนองเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการจัดการเหตุการณ์ผิดปกติได้อย่างรวดเร็วและมีประสิทธิภาพ พร้อมทั้งลดผลกระทบต่อการดำเนินการที่สำคัญ

ข้อ ๑๑ ให้จัดทำแผนฟื้นฟูหลังจากเกิดเหตุการณ์ผิดปกติ เพื่อลดผลกระทบต่อการดำเนินการที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนฟื้นฟูฯ เพื่อประเมินความถูกต้องและมีประสิทธิผลของแผนอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ให้จัดทำ Data Flow Diagram เพื่อเป็นข้อมูลเกี่ยวกับการทำงานของระบบและใช้ในการวิเคราะห์เมื่อระบบทำงานผิดปกติ

ข้อ ๑๓ ให้มีการใช้งานระบบในรูปแบบผสมผสาน ทั้งแบบ on-premise และแบบ on-cloud รวมไปถึงการเลือกใช้งานระบบจากหลากหลายผู้ผลิต เพื่อที่หากมีช่องโหว่ของผู้ผลิตใด ๆ ทางกรมสรรพสามิตจะยังมีระบบของอีกผู้ผลิตที่ไม่มีช่องโหว่ ทำการป้องกันภัยคุกคามนั้น ๆ ได้อยู่

ข้อ ๑๔ ตั้งค่าระบบ Patch Management ให้มีรอบในการอัปเดตให้ทันต่อเหตุการณ์

ข้อ ๑๕ ห้ามดำเนินการบันทึกรหัสผ่านไว้ในเอกสารคู่มือใด ๆ และให้ดำเนินการตั้ง Bad password list เพื่อป้องกันการใช้รหัสผ่านที่เป็นที่รู้โดยทั่วกันในระบบงานสำคัญ

ข้อ ๑๖ ให้มีการเพิ่มแนวทางการจัดการด้านประชาสัมพันธ์ในระหว่างเกิดเหตุ และหลังจากการฟื้นคืน

ข้อ ๑๗ ให้มีการจัดทำ Incident response plan และปรับปรุงแผนการตอบสนองให้เหมาะสมกับความเสี่ยงด้าน cybersecurity ตามเหตุการณ์ปัจจุบัน รวมถึงการแบ่งปันข้อมูลให้กับหน่วยงานภายนอกเพื่อรับการแจ้งเตือนเกี่ยวกับ Incident

ข้อ ๑๘ ให้มีการตรวจประเมินช่องโหว่ (Vulnerability Assessment) หรือ การทดสอบเจาะระบบ (Penetration Test) โดยครอบคลุมระบบโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) และโปรแกรมประยุกต์ (Application) สำหรับระบบสารสนเทศที่มีความเสี่ยงจากภัยคุกคามด้านไซเบอร์อย่างน้อยปีละ ๑ ครั้ง ดังนี้

(๑) การเข้าถึงและควบคุมการใช้งานสารสนเทศ
(๒) การจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน
(๓) การตรวจสอบและประเมินความเสี่ยง
(๔) การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิต
(๕) การรับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศของกรมสรรพสามิต
(๖) การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๗) การปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(๘) การรับมือภัยคุกคามทางไซเบอร์

ข้อ ๑๙ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิต ดังนี้
(๑) การควบคุมการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ (Access Control)
(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
(๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)
(๗) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)
(๘) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
(๙) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)
(๑๐) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา (Mobile Device)
(๑๑) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ (Information Classification)
(๑๒) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)
(๑๓) การใช้งานระบบอินเทอร์เน็ต (Internet)
(๑๔) การใช้งานอุปกรณ์ป้องกันการบุกรุก (Firewall)
(๑๕) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
(๑๖) การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Files)
(๑๗) นโยบายการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Cryptographic Control)
(๑๘) นโยบายการดำเนินงานร่วมกับหน่วยงานภายนอก (Supplier relationship management)
(๑๙) การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

ข้อ ๒๐ วิธีปฏิบัติเพื่อรักษาความปลอดภัยด้านสารสนเทศของผู้ดูแลระบบ ดังนี้
(๑) การปฏิบัติหน้าที่โดยทั่วไปของผู้ดูแลระบบ
(๒) การกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล
(๓) การควบคุมการเข้าถึงระบบสารสนเทศ
(๔) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(๕) การควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
(๖) การควบคุมการเข้าถึงระบบปฏิบัติการ
(๗) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๘) การปฏิบัติเมื่อเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย กรณีการเข้าถึงระบบ โดยไม่ได้รับอนุญาต
(๙) การปฏิบัติภายหลังการเกิดเหตุละเมิดการรักษาความมั่นคงปลอดภัย
(๑๐) การสำรองข้อมูล
(๑๑) การสำรองและกู้คืนข้อมูล
(๑๒) การสร้างความตระหนัก
(๑๓) การตรวจสอบและการประเมินผล
(๑๔) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๒๑ วิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบุคคลภายนอก ดังนี้
(๑) การปฏิบัติการเข้าออกพื้นที่ภายในสำนักงาน
(๒) การกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกสำนักงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานได้

๒. การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

ข้อกำหนดหลักในการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ มีรายละเอียด ดังนี้

ข้อ ๑. การระบุความเสี่ยงด้านไซเบอร์ (Identify) ต้องระบุความเสี่ยงด้านไซเบอร์ กระบวนการดำเนินงานและทรัพย์สินสารสนเทศที่มีความเสี่ยงต่อการโดนโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบต่าง ๆ ทรัพย์สินและข้อมูลของกรมสรรพสามิต

ข้อ ๒. การป้องกันความเสี่ยงด้านไซเบอร์ (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสม เพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านการป้องกันภัยคุกคามทางไซเบอร์

ข้อ ๓. การตรวจจับความเสี่ยงด้านไซเบอร์ (Detect) ต้องมีกระบวนการตรวจสอบ ติดตามและเฝ้าระวังเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอกอย่างต่อเนื่อง เพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกันความเสี่ยงและผลกระทบที่จะเกิดขึ้นกับกรมสรรพสามิตในอนาคต

ข้อ ๔. การตอบสนองความเสี่ยงด้านไซเบอร์ (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อการเผชิญเหตุ เมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ โดยครอบคลุมถึงการวางแผนรับมืออย่างต่อเนื่อง การสื่อสาร การวิเคราะห์ การแก้ไข เหตุการณ์ความเสี่ยงด้านไซเบอร์

ข้อ ๕. การฟื้นคืนสภาพ (Recovery) ซึ่งเป็นการจัดทำและดำเนินกิจกรรมตามแผนงานเพื่อรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ให้สามารถกลับมาดำเนินการได้ตามปกติภายในระยะเวลาที่กำหนด เพื่อช่วยให้สามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงการดำเนินการทบทวนปรับปรุงแผนการกู้คืนให้เป็นปัจจุบันทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด โดยมีเอกสารที่มีความสัมพันธ์กับเอกสาร ISO ๒๗๐๐๑ คือ เอกสารแผนสำรองฉุกเฉิน Disaster Recovery Plan (DRP)

โดยมีขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ ดังนี้

ขั้นตอน	รายละเอียด
ตรวจพบภัยคุกคามทางไซเบอร์	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่าง ๆ ตามที่กำหนด ซึ่งจะช่วยให้กรมสรรพสามิตสามารถตรวจพบคุกคามทางไซเบอร์อย่างรวดเร็ว
ตรวจสอบภัยคุกคามทางไซเบอร์	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๐
การควบคุมภัยคุกคามทางไซเบอร์	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุดและป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วน กรมสรรพสามิตจะทำการปิดระบบ หรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
แก้ได้ / แก้ไม่ได้ — แก้ไขปัญหา	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นทันที
ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้ จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ
แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามทางไซเบอร์ในลักษณะเดิม	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว กรมสรรพสามิตจะดำเนินการตรวจสอบหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่ายหรือเครื่องมืออื่นๆ และหาวิธีเพื่อป้องกันภัยคุกคามไซเบอร์ต่อไป
สมบูรณ์ / ไม่สมบูรณ์ — ทดสอบระบบ	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญของระบบเทคโนโลยีสารสนเทศของกรมสรรพสามิตว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืน
กู้คืนระบบ	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ กรมสรรพสามิตจะพิจารณาดำเนินการใช้งานแผนสำรองฉุกเฉิน (Disaster Recovery Plan)
ระบบสามารถใช้งานได้ตามปกติ	เมื่อโครงสร้างพื้นฐานสำคัญของระบบเทคโนโลยีสารสนเทศของกรมสรรพสามิตสามารถทำงานได้ตามปกติแล้ว ผู้รับผิดชอบของกรมสรรพสามิตจะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามทางไซเบอร์
สรุปผลในการดำเนินการรับมือภัยคุกคามฯและจัดทำรายงาน	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และผู้ที่เกี่ยวข้องต่อไป