ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
เรื่อง แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีเจตนารมณ์กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

ดังนั้น เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัยเป็นไปด้วยความเรียบร้อย บรรลุวัตถุประสงค์อย่างมีประสิทธิภาพ จึงอาศัยอำนาจตามความในมาตรา ๒๔ และมาตรา ๒๗ แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. ๒๕๔๘ จึงออกประกาศไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๔ ให้อธิการบดีเป็นผู้รักษาการตามประกาศนี้ กรณีที่มีปัญหาจากการปฏิบัติตามประกาศนี้หรือที่ประกาศนี้มิได้กำหนดไว้ ให้อธิการบดีเป็นผู้วินิจฉัยและคำวินิจฉัยนั้นให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๑๗ กันยายน พ.ศ. ๒๕๖๙

(ศาสตราจารย์สุวัจน์ ธัญรส)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

๑. หลักการและเหตุผล

แผนฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย และเพื่อให้การดำเนินงานของมหาวิทยาลัยสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกาศ หลักเกณฑ์ แนวทาง และมาตรฐานที่ออกตามพระราชบัญญัติดังกล่าว ตลอดจนกฎหมายและข้อกำหนดอื่นที่เกี่ยวข้องที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติโดยเร็ว โดยบทบัญญัติดังกล่าวกำหนดให้ประมวลแนวทางปฏิบัติของหน่วยงานต้องประกอบด้วยแผนงานสำคัญอย่างน้อย ๒ ส่วนหลัก ดังต่อไปนี้

(๑) แผนการรับมือภัยคุกคามทางไซเบอร์ คือ แผนงานและขั้นตอนการปฏิบัติเตรียมพร้อมไว้สำหรับเผชิญเหตุ ตอบสนอง และรับมือเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ขึ้นกับหน่วยงานได้อย่างทันท่วงที เพื่อลดความเสียหายและกู้คืนระบบให้กลับมาทำงานได้อย่างทันท่วงที

(๒) แผนการตรวจสอบและประเมินความเสี่ยง คือ แผนงานที่กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอกอย่างน้อยปีละหนึ่งครั้ง

การจัดทำแผนฉบับนี้เป็นการดำเนินการที่สอดคล้องกับประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ถือเป็นแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลศรวีชัย พ.ศ. ๒๕๖๖ และนโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเทคโนโลยีราชมงคลศรวีชัย พ.ศ. ๒๕๖๖ เพื่อยกระดับความมั่นคงปลอดภัยในการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ของระบบสารสนเทศและข้อมูลดิจิทัลทั้งหมดของมหาวิทยาลัย

๒. วัตถุประสงค์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ฉบับนี้ มีวัตถุประสงค์สำคัญดังนี้

๒.๑ เพื่อกำหนดขั้นตอนและแนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์ ของมหาวิทยาลัยฯ อย่างเป็นระบบและเป็นมาตรฐาน ตั้งแต่กระบวนการตรวจจับ วิเคราะห์ ระงับภัย ไปจนถึงการฟื้นฟูระบบให้กลับมาทำงานปกติ

๒.๒ เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบ ของทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (CIRT) และหน่วยงานสนับสนุนต่าง ๆ ภายในมหาวิทยาลัยฯ ในการประสานความร่วมมือเพื่อระงับเหตุอย่างมีประสิทธิภาพ

๒.๓ เพื่อกำหนดเกณฑ์ในการจำแนกประเภทและระดับความรุนแรงของภัยคุกคาม ช่วยให้ผู้ปฏิบัติงานสามารถประเมินสถานการณ์และตัดสินใจดำเนินมาตรการระงับเหตุได้อย่างถูกต้องเหมาะสมตามสภาพการณ์

๒.๔ เพื่อสร้างกลไกการรายงานเหตุภัยคุกคามทางไซเบอร์ ที่ถูกต้อง รวดเร็ว และสอดคล้องกับข้อบังคับทางกฎหมายภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒.๕ เพื่อกำหนดแนวทางการสื่อสารและการประสานงาน ไปยังผู้มีส่วนได้ส่วนเสีย ทั้งหน่วยงานภายในและภายนอกอย่างเหมาะสมในภาวะวิกฤต เพื่อป้องกันความตื่นตระหนกและรักษาภาพลักษณ์ของมหาวิทยาลัยฯ

๒.๖ เพื่อลดผลกระทบ ความสูญเสีย หรือความเสียหาย ที่อาจเกิดขึ้นต่อการดำเนินงาน พันธกิจ และระบบสารสนเทศของมหาวิทยาลัยฯ ให้เหลือน้อยที่สุด

๓. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ มีขอบเขตการบังคับใช้และครอบคลุมการดำเนินงาน ดังต่อไปนี้

๓.๑ ด้านหน่วยงานและพื้นที่ทางกายภาพ ครอบคลุมหน่วยงานทุกระดับและพื้นที่ตั้งทั้งหมดของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ได้แก่

- สำนักงานอธิการบดี กอง และหน่วยงานส่วนกลาง พื้นที่สงขลาทั้งหมด
- สำนักงานวิทยาเขตตรัง สำนักงานวิทยาเขตนครศรีธรรมราช (พื้นที่ทุ่งใหญ่ และพื้นที่ไสใหญ่) และสถานีวิจัยและฝึกอบรมราชมงคลศรีวิชัย ชุมพร
- คณะ และวิทยาลัยทุกพื้นที่
- โครงสร้างพื้นฐานทางกายภาพด้านไอที ห้อง Data Center อาคาร ๕๙

๓.๒ ด้านเทคโนโลยีและทรัพย์สินสารสนเทศ ครอบคลุมระบบและทรัพย์สินสารสนเทศของมหาวิทยาลัยฯ ทั้งหมด ทั้งที่ดูแลโดยส่วนกลางและหน่วยงานย่อย ได้แก่

- เครือข่ายไร้สาย (Wi-Fi) ระบบเครือข่ายภายใน (LAN/WAN) อุปกรณ์สวิตช์ (Switch) อุปกรณ์เราเตอร์ (Router) และระบบป้องกันเครือข่าย (IPS/Firewall)
- ระบบอีเมล เว็บไซต์มหาวิทยาลัย ระบบฐานข้อมูล ระบบสารสนเทศเพื่อการบริการการศึกษาและการจัดการองค์กรสมัยใหม่ของมหาวิทยาลัยฯ
- อุปกรณ์คอมพิวเตอร์สำนักงาน เครื่องคอมพิวเตอร์พกพา และอุปกรณ์พกพาอื่น ๆ ที่เชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยฯ
- ระบบจัดเก็บข้อมูลกลาง และระบบ Back Up Storage

๓.๓ ด้านข้อมูล ครอบคลุมข้อมูลดิจิทัลทั้งหมดที่ถูกจัดเก็บ ประมวลผล หรือส่งผ่านระบบสารสนเทศของมหาวิทยาลัยฯ ได้แก่

- ข้อมูลสำคัญที่ใช้ในการดำเนินงานของมหาวิทยาลัยฯ
- ข้อมูลส่วนบุคคลของบุคลากร นักศึกษา และบุคคลภายนอก ที่อยู่ภายใต้การคุ้มครองตามนโยบายและหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยฯ

๓.๔ ด้านบุคคลและผู้ใช้ระบบ ครอบคลุมบุคคลทุกคนที่มีสิทธิ์เข้าใช้งาน หรือเชื่อมต่ออุปกรณ์ใด ๆ เข้ากับระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยฯ ได้แก่

- ผู้บริหาร คณาจารย์ และบุคลากรของมหาวิทยาลัยฯ
- นักศึกษา และผู้รับบริการภายนอก
- ผู้ให้บริการภายนอก ผู้รับจ้างเหมาบริการระบบ (Outsource) และคู่สัญญาทางธุรกิจที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศของมหาวิทยาลัยฯ

๔. หน้าที่การทบทวนแผน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ในฐานะหน่วยงานรับผิดชอบหลัก โดยมีผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ทำหน้าที่เป็นเจ้าของแผน มีหน้าที่ในการควบคุมดูแล ประสานงาน การจัดทำและปรับปรุงทบทวนแผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ให้มีความทันสมัยและสอดคล้องกับสถานการณ์ปัจจุบัน โดยการทบทวนแผนและเสนอขออนุมัติต่ออธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย (หรือผู้บริหารสูงสุดที่ได้รับมอบอำนาจ) จะต้องดำเนินการภายใต้หลักเกณฑ์และเงื่อนไขดังต่อไปนี้

๔.๑ รอบเวลาการทบทวนตามปกติ มีการดำเนินการทบทวนและปรับปรุงเอกสารแผนรับมือฯ นี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดรับกับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ประจำปี โดยจะต้องกำหนดวันที่การตรวจสอบเอกสารครั้งถัดไป ในตารางควบคุมเอกสารให้ชัดเจนทุกครั้ง

๔.๒ การทบทวนกรณีพิเศษเมื่อเกิดเหตุการณ์กระตุ้น นอกเหนือจากวงรอบประจำปีแล้ว จะต้องดำเนินการทบทวนและปรับปรุงแผนรับมือฯ โดยทันทีเมื่อเกิดกรณีใดกรณีหนึ่ง ดังนี้

- หลังการฝึกซ้อมแผนประจำปี เมื่อมีการฝึกซ้อมแผนรับมือภัยคุกคามทางไซเบอร์ (ทั้งรูปแบบ Tabletop หรือ Simulation) และได้จัดทำรายงานสรุปผลการฝึกซ้อม เพื่ออุดช่องว่างที่ค้นพบ
- หลังการเผชิญเหตุการณ์ภัยคุกคามจริง เมื่อมหาวิทยาลัยฯ เผชิญกับภัยคุกคามทางไซเบอร์จริง (โดยเฉพาะระดับสูงหรือวิกฤต) และมีการประชุมหาแนวทาง เพื่อนำข้อบกพร่อง ช่องโหว่ และสถิติต่าง ๆ มาปรับปรุงแนวทางการตอบสนอง
- เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานไอทีหรือเทคโนโลยีสำคัญ เช่น การติดตั้งระบบตรวจจับใหม่ (ระบบ SIEM / EDR) หรือเมื่อบริการสำคัญของมหาวิทยาลัยมีการปรับเปลี่ยนเชิงโครงสร้าง
- เมื่อมีการเปลี่ยนแปลงโครงสร้างทีมรับมือฯ (CIRT) เช่น การปรับเปลี่ยนรายชื่อ ข้อมูลการติดต่อ หรือผู้รับผิดชอบหลักและตัวสำรองในทีม
- เมื่อมีการปรับปรุงกฎหมายหรือข้อกำหนดภายนอก เช่น สกมช. หรือ อว. ออกประกาศ เกณฑ์ หรือคู่มือแนวทางการรายงานภัยคุกคามทางไซเบอร์ฉบับปรับปรุงใหม่

๔.๓ ขั้นตอนการยื่นขออนุมัติทบทวนแผน ในการปรับปรุงแผนทุกครั้ง เจ้าของแผน (Plan Owner) จะต้องประสานงานร่วมกับผู้แทนจากสำนักงานนิติการ (นิติกร) เพื่อตรวจสอบความถูกต้องด้านกฎหมายและความสอดคล้องกับ พ.ร.บ. ไซเบอร์ฯ ก่อนจะนำเสนอเอกสารฉบับปรับปรุงต่ออธิการบดีเพื่อพิจารณาลงนามอนุมัติและปรับปรุงเวอร์ชันของเอกสารในตารางให้เป็นปัจจุบัน

๕. หน้าที่ในการดำเนินการตามแผน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการ ตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุน ประกอบด้วย หน่วยงานระดับคณะฯ/วิทยาลัย รวมถึง สำนักส่งเสริมวิชาการและงานทะเบียน สำนักงานอธิการบดี สำนักการจัดการนวัตกรรมและถ่ายทอดเทคโนโลยี สำนักงานวิทยาเขตตรัง สำนักงานวิทยาเขตนครศรีธรรมราช พื้นที่ทุ่งใหญ่ สำนักงานวิทยาเขตนครศรีธรรมราช พื้นที่ไสใหญ่ สถานีวิจัยและฝึกอบรมราชมงคลศรีวิชัย ชุมพร กองบริหารงานบุคคล กองพัฒนานักศึกษา กองนโยบายและแผน กองคลัง และสถาบันวิจัยและพัฒนา เพื่อให้การบังคับใช้แผนรับมือเหตุภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพและสามารถระงับภัยได้อย่างทันท่วงที มหาวิทยาลัยฯ จึงกำหนดหน้าที่และความรับผิดชอบของหน่วยงานต่าง ๆ ในการดำเนินการตามแผนไว้ดังต่อไปนี้

๕.๑ หน่วยงานรับผิดชอบหลัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ (สวส.) ทำหน้าที่เป็นศูนย์กลางในการดำเนินมาตรการเฝ้าระวัง ตรวจจับ วิเคราะห์ และระงับเหตุภัยคุกคามทางไซเบอร์ของมหาวิทยาลัยฯ ตลอด ๒๔ ชั่วโมง รวมถึงจัดตั้งทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (CIRT) เพื่อปฏิบัติการด้านเทคนิค ประสานงานกับหน่วยงานภายนอก (สกมช. / Thai-CERT / อว.) และเป็นแกนหลักในการฟื้นฟูระบบสำคัญให้กลับคืนสู่สภาวะปกติ

๕.๒ หน่วยงานสนับสนุนระดับพื้นที่และวิชาการ

- หน่วยงานระดับคณะ/วิทยาลัย สำนักงานวิทยาเขตทุกพื้นที่ และสถานีวิจัยและฝึกอบรมราชมงคลศรีวิชัยชุมพร ทำหน้าที่ตรวจสอบ สอดส่องดูแลความปลอดภัย และรายงานเหตุผิดปกติของระบบสารสนเทศภายในหน่วยงานของตนแก่ทีม CIRT ตลอดจนร่วมมือกับฝ่ายเทคนิคในการจำกัดวงความเสียหาย เช่น การตัดการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ในความดูแลเมื่อเกิดเหตุการณ์วิกฤต
- สำนักส่งเสริมวิชาการและงานทะเบียน และ กองพัฒนานักศึกษา ทำหน้าที่สนับสนุนข้อมูลและพิกัดของระบบบริการการศึกษา ระบบฐานข้อมูลนักศึกษา และเป็นหน่วยงานร่วมตรวจสอบประสานงานหลักในกรณีที่เกิดเหตุภัยคุกคามหรือการรั่วไหลของข้อมูลส่วนบุคคล ที่เกี่ยวข้องกับนักศึกษา

๕.๓ หน่วยงานสนับสนุนระดับการบริหารจัดการและกฎหมาย

- สำนักงานอธิการบดี (งานประกันคุณภาพการศึกษา/งานบริหารความเสี่ยง) ทำหน้าที่ร่วมประเมินและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของมหาวิทยาลัยฯ เพื่อนำข้อมูลข้อบกพร่องไปใช้วิเคราะห์และรายงานตามโครงสร้างบริหารความเสี่ยงองค์กร
- สำนักงานนิติการ ทำหน้าที่ตรวจสอบสอดคล้องทางกฎหมาย รวบรวมข้อมูลพยานหลักฐานทางดิจิทัล ดำเนินการรายงานเหตุภัยคุกคามร้ายแรง/วิกฤต ไปยังหน่วยงานกำกับดูแลตามกรอบเวลาที่กฎหมายกำหนด ตลอดจนดำเนินการร้องทุกข์ กล่าวโทษ หรือดำเนินคดีความทางกฎหมายกับผู้กระทำความผิด
- กองบริหารงานบุคคล ทำหน้าที่ประสานงานและดำเนินการทางวินัยหรือกฎระเบียบที่เกี่ยวข้อง กรณีที่ผลการสืบสวนระบุว่าเหตุภัยคุกคามหรือความเสียหายเกิดขึ้นจากการจงใจ กระทำโดยมิชอบ หรือความประมาทเลินเล่ออย่างร้ายแรงของบุคลากรภายในมหาวิทยาลัยฯ
- กองคลัง และ กองนโยบายและแผน ทำหน้าที่สนับสนุนและอำนวยความสะดวกในกระบวนการจัดซื้อจัดจ้างหรือจัดสรรงบประมาณฉุกเฉินอย่างเร่งด่วน เพื่อจัดหาทรัพยากร ซอฟต์แวร์ อุปกรณ์ หรือผู้เชี่ยวชาญจากภายนอกเข้ามาช่วยระงับเหตุและฟื้นฟูระบบให้กลับมาทำงานได้ตามปกติ
- สถาบันวิจัยและพัฒนา และ สำนักการจัดการนวัตกรรมและถ่ายทอดเทคโนโลยี ทำหน้าที่ประสานงานและดูแลความปลอดภัยของระบบฐานข้อมูลวิจัย ทรัพย์สินทางปัญญา และสิทธิบัตรดิจิทัลของมหาวิทยาลัย ในกรณีที่พบว่าข้อมูลที่มีความอ่อนไหวสูงเหล่านี้ถูกเข้าถึงหรือรั่วไหลจากการโจมตีทางไซเบอร์

๖. รายละเอียดการบังคับใช้เอกสาร

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดรายละเอียดที่เกี่ยวข้องกับการควบคุม ตรวจสอบ และอนุมัติใช้เอกสารแผนรับมือเหตุภัยคุกคามทางไซเบอร์ เพื่อให้เกิดความรับผิดชอบและการกำกับดูแลเอกสารอย่างเป็นระบบ แสดงดังตารางที่ ๑ และมีรายละเอียดของการเปลี่ยนแปลงเอกสารดังตารางที่ ๒

ตารางที่ ๑ รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร	ข้อมูลผู้รับผิดชอบ / กำหนดเวลา	หมายเหตุ / ตำแหน่งปฏิบัติการ
ผู้จัดทำเอกสาร (Author)	นายกนกพล เมืองรักษ์	เจ้าหน้าที่รับมือฯ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
ผู้ดำเนินการตามเอกสาร (Owner)	ผศ.สิทธิโชค อุ่นแก้ว	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
วันที่จัดทำเอกสาร (Date created)	๑๖ กุมภาพันธ์ ๒๕๖๙	เริ่มร่างกรอบแผนรับมือฯ
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	ผศ.ดร.ศักดิ์ชัย ตันติวิวัทน์ และผู้แทน นิติกร สำนักงานนิติการ	เจ้าหน้าที่รับมือฯ / นิติกร (ผู้ตรวจกฎหมายและความสอดคล้อง)
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	๑๕ กันยายน ๒๕๖๙	ตรวจสอบเนื้อหาและข้อกฎหมายเสร็จสิ้น
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	ศาสตราจารย์ ดร.สุวัจน์ ธัญรส (อนุมัติ ณ วันที่ กันยายน ๒๕๖๙)	อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	กันยายน ๒๕๗๐	วันที่กำหนดชัดเจน เพื่อให้สอดคล้องกับมาตรา ๔๔ พ.ร.บ. ไซเบอร์ฯ ที่ระบุให้ทบทวนอย่างน้อยปีละหนึ่งครั้ง

ตารางที่ ๒ การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๐.๑	๑๖ กุมภาพันธ์ ๒๕๖๙	ผศ.สิทธิโชค อุ่นแก้ว	ร่างเอกสารฉบับแรก และส่งต่อให้ผู้เชี่ยวชาญและนิติกรตรวจสอบความถูกต้อง
จริง (๑.๐)	กันยายน ๒๕๖๙	ศาสตราจารย์ ดร.สุวัจน์ ธัญรส	อนุมัติและประกาศใช้งานจริงเป็นแผนรับมือเหตุภัยคุกคามทางไซเบอร์อย่างเป็นทางการของมหาวิทยาลัย

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

การกำหนดขั้นตอนและการปฏิบัติงานตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ ได้รับการออกแบบและพัฒนาขึ้นให้สอดคล้องกับข้อกำหนด นโยบาย และกรอบมาตรฐานความปลอดภัยสารสนเทศทั้งภายในและภายนอกหน่วยงาน ดังนี้

๗.๑ ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๙

๗.๒ ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๖

๗.๓ ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๖

๗.๔ ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง หลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๖

๗.๕ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (โดยเฉพาะบทบัญญัติในมาตรา ๔๔ และมาตรา ๖๐)

๗.๖ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

๗.๗ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๗.๘ ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๘

๗.๙ คู่มือประกอบแนวทางการแจ้งรายงานเหตุภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๙ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน่วยงานของรัฐ

๘. นิยาม

๘.๑ เหตุการณ์ (Event) หมายความว่า เหตุการณ์หรือสิ่งที่เกิดขึ้นและสามารถตรวจพบหรือสังเกตได้จากระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย อุปกรณ์ กระบวนการ หรือการปฏิบัติงานของบุคลากร ซึ่งอาจเป็นเหตุการณ์ปกติหรือผิดปกติ และอาจมีหรือไม่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศก็ได้

๘.๒ เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่เกิดขึ้นหรือมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งส่งผลหรืออาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) หรือความพร้อมใช้งาน (Availability) ของระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือข้อมูลของมหาวิทยาลัย และจำเป็นต้องมีการตรวจสอบ ประเมิน หรือดำเนินการตอบสนองตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของมหาวิทยาลัย

๘.๓ ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ ที่มุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ทั้งนี้ให้เป็นไปตามความหมายที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมาย ประกาศ หลักเกณฑ์ หรือแนวทางที่เกี่ยวข้อง

๘.๔ เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นต่อระบบสารสนเทศของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะและเกณฑ์ไว้ในระดับไม่ร้ายแรง ระดับร้ายแรง หรือระดับวิกฤต ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และระดับร้ายแรงหรือระดับวิกฤเข้าเงื่อนไขที่จะต้องดำเนินการแจ้งหรือรายงานต่อสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานควบคุมหรือกำกับดูแล ตามประมวลแนวทางปฏิบัติและมาตรฐานขั้นต่ำที่กำหนดไว้ตามมาตรา ๔๙ แห่งพระราชบัญญัติดังกล่าว

๘.๕ เหตุภัยคุกคามทางไซเบอร์ที่มีความรุนแรง (Severe Cybersecurity Incident) หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่มีระดับความรุนแรงหรือมีผลกระทบในระดับที่มหาวิทยาลัยกำหนดให้ต้องยกระดับการตอบสนอง การควบคุมเหตุการณ์ การประสานงาน หรือการรายงานต่อผู้บริหารและหน่วยงานที่เกี่ยวข้องตามกฎหมายหรือหลักเกณฑ์ที่ใช้บังคับ

๘.๖ เหตุภัยคุกคามทางไซเบอร์วิกฤต (Critical Cybersecurity Incident) หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่มีผลกระทบร้ายแรงต่อระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย ข้อมูล การให้บริการ ภารกิจสำคัญของมหาวิทยาลัย หรือผู้มีส่วนได้ส่วนเสีย และจำเป็นต้องยกระดับการตอบสนองและการบริหารจัดการเหตุการณ์ในระดับวิกฤต รวมทั้งดำเนินการแจ้งหรือรายงานต่อหน่วยงานหรือผู้มีอำนาจหน้าที่ตามกฎหมายแล้วแต่กรณี

๘.๗ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)” หมายความว่า หน่วยงานหรือระบบที่เข้าข่ายและได้รับการกำหนดให้เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมาย ประกาศ หรือหลักเกณฑ์ที่เกี่ยวข้อง

๘.๘ การแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ หมายความว่า การแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานหรือผู้มีอำนาจหน้าที่ตามกฎหมาย โดยดำเนินการตามแบบ วิธีการ ช่องทาง และกรอบระยะเวลาที่กฎหมาย ประกาศ หลักเกณฑ์ หรือแนวทางที่ใช้บังคับกำหนด

๘.๙ ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย (RUTS Computer Security Incident Response Team: RUTS-CSIRT) หมายความว่า หน่วยงานหรือคณะทำงานที่มหาวิทยาลัยมอบหมายให้มีหน้าที่เฝ้าระวัง ตรวจจับ วิเคราะห์ ประเมิน ตอบสนอง ควบคุม แก้ไข ฟื้นฟู และประสานงานเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ รวมถึงดำเนินการตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของมหาวิทยาลัย

๘.๑๐ ระบบสารสนเทศสำคัญ หมายความว่า ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือบริการดิจิทัลของมหาวิทยาลัยที่มีความสำคัญต่อการดำเนินภารกิจ การให้บริการ การบริหารจัดการ การเรียนการสอน การวิจัย การบริการวิชาการ การเงิน การบริหารบุคลากร หรือภารกิจอื่นที่มหาวิทยาลัยกำหนด

๘.๑๑ ข้อมูลหลักฐานดิจิทัล (Digital Evidence) หมายความว่า ข้อมูลหรือสารสนเทศในรูปแบบดิจิทัลที่สามารถใช้ประกอบการตรวจสอบ วิเคราะห์ สืบสวน หรือดำเนินการตามกฎหมายหรือระเบียบที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์ โดยต้องมีการรักษาความถูกต้องครบถ้วน ความน่าเชื่อถือ และความสามารถในการตรวจสอบย้อนกลับของหลักฐานตามหลักเกณฑ์ที่เกี่ยวข้อง

๘.๑๒ ตัวบ่งชี้การบุกรุกหรือการโจมตี (Indicator of Compromise: IoC) หมายความว่า ข้อมูลหรือรูปแบบทางเทคนิคที่สามารถใช้เป็นตัวบ่งชี้หรือหลักฐานประกอบการตรวจพบว่าระบบสารสนเทศ ระบบคอมพิวเตอร์ หรือระบบเครือข่ายอาจถูกบุกรุก ถูกโจมตี หรือมีพฤติกรรมที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เช่น ที่อยู่ไอพี ชื่อโดเมน ค่าแฮชของไฟล์ ชื่อไฟล์ รูปแบบการเชื่อมต่อ หรือข้อมูลอื่นที่เกี่ยวข้อง

๘.๑๓ การตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response) หมายความว่า กระบวนการดำเนินการตั้งแต่การเตรียมความพร้อม การตรวจจับ การวิเคราะห์ การควบคุมและจำกัดขอบเขตของเหตุการณ์ การกำจัดสาเหตุของภัยคุกคาม การกู้คืนระบบ การติดตามเฝ้าระวัง และการทบทวนบทเรียนภายหลังเกิดเหตุ เพื่อจำกัดผลกระทบและลดโอกาสการเกิดเหตุซ้ำ

๘.๑๔ การตีความคำศัพท์หรือข้อความที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งมิได้กำหนดไว้ในแผนฉบับนี้ ให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กฎหมายลำดับรอง ประกาศ หลักเกณฑ์ มาตรฐาน หรือแนวทางของหน่วยงานที่มีอำนาจหน้าที่ และกฎหมายอื่นที่เกี่ยวข้อง ซึ่งมีผลใช้บังคับในขณะนั้น

๘.๑๕ ในกรณีที่มหาวิทยาลัยหรือระบบสารสนเทศของมหาวิทยาลัยอยู่ในข่ายหรือได้รับการกำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ดำเนินการเพิ่มเติมตามบทบัญญัติ กฎ ประกาศ หลักเกณฑ์ มาตรฐาน และแนวทางที่ใช้บังคับกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศโดยเคร่งครัด

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัยกำหนดโครงสร้าง บทบาทหน้าที่ และกระบวนการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถป้องกัน ตรวจจับ รับแจ้ง ตรวจสอบ วิเคราะห์ ประเมิน ควบคุม จำกัดขอบเขต ตอบสนอง ฟื้นฟู และติดตามเหตุภัยคุกคามทางไซเบอร์ได้อย่างเป็นระบบและทันท่วงที รวมทั้งสามารถประสานงานกับผู้บริหาร หน่วยงานภายใน หน่วยงานภายนอก และหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมายได้อย่างเหมาะสม

การดำเนินการตามแผนฉบับนี้ให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กฎหมายลำดับรอง ประกาศ หลักเกณฑ์ และแนวทางที่เกี่ยวข้อง ตลอดจนกฎหมายอื่นที่เกี่ยวข้องกับเหตุการณ์นั้นแล้วแต่กรณี

๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัยกำหนดให้มี ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และช่องทางการแจ้งเหตุอย่างเป็นทางการ เพื่อเป็นจุดรับแจ้งเหตุเบื้องต้นของมหาวิทยาลัย โดยมีหน้าที่รับข้อมูลเหตุการณ์ ตรวจสอบข้อมูลเบื้องต้น ประเมินความเร่งด่วนและผลกระทบในเบื้องต้น และประสานส่งต่อเหตุการณ์ให้แก่ผู้รับผิดชอบด้านการตอบสนองเหตุภัยคุกคามทางไซเบอร์ของมหาวิทยาลัยตามระดับความรุนแรงและลักษณะของเหตุการณ์

ผู้รับแจ้งเหตุมีหน้าที่ ดังต่อไปนี้

(๑) รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์จากบุคลากร นักศึกษา ผู้ใช้บริการระบบสารสนเทศหน่วยงานภายใน หรือแหล่งข้อมูลอื่นที่เกี่ยวข้อง ผ่านช่องทางที่มหาวิทยาลัยกำหนด

(๒) บันทึกข้อมูลการรับแจ้งเหตุ ได้แก่ วันและเวลาที่รับแจ้ง ผู้แจ้ง ช่องทางการแจ้ง ระบบหรือบริการที่เกี่ยวข้อง ลักษณะเหตุการณ์ ข้อมูลเบื้องต้นเกี่ยวกับผลกระทบ และข้อมูลอื่นที่จำเป็นต่อการตรวจสอบและตอบสนองต่อเหตุการณ์

(๓) ตรวจสอบและประเมินเหตุการณ์ในเบื้องต้น เพื่อพิจารณาว่าเป็นเหตุการณ์ปกติ เหตุการณ์ผิดปกติ เหตุอันควรสงสัย หรือเหตุภัยคุกคามทางไซเบอร์ และพิจารณาระดับความเร่งด่วนเบื้องต้น

(๔) แจ้งและประสานผู้รับผิดชอบด้านการตอบสนองเหตุภัยคุกคามทางไซเบอร์ หรือทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัย เพื่อดำเนินการตรวจสอบ วิเคราะห์ และตอบสนองต่อเหตุการณ์ตามแผน

(๕) ในกรณีที่เหตุการณ์อาจส่งผลกระทบอย่างมีนัยสำคัญต่อระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย ข้อมูล หรือภารกิจสำคัญของมหาวิทยาลัย ให้เร่งประสานผู้รับผิดชอบและผู้บังคับบัญชาตามลำดับโดยไม่ชักช้า

(๖) สนับสนุนการรวบรวมข้อมูลและหลักฐานเบื้องต้นที่เกี่ยวข้องกับเหตุการณ์ โดยหลีกเลี่ยงการดำเนินการที่อาจทำให้ข้อมูลหรือหลักฐานดิจิทัลสูญหาย เปลี่ยนแปลง หรือไม่สามารถตรวจสอบย้อนกลับได้

(๗) ดำเนินการรักษาความลับของข้อมูลเกี่ยวกับเหตุการณ์ ผู้แจ้งเหตุ ระบบสารสนเทศ ข้อมูลส่วนบุคคล และข้อมูลอื่นที่เกี่ยวข้อง โดยเปิดเผยข้อมูลเท่าที่จำเป็นต่อการปฏิบัติหน้าที่และการประสานงานตามกฎหมายและระเบียบที่เกี่ยวข้อง

(๘) ในกรณีที่เหตุการณ์เข้าข่ายต้องแจ้งหรือรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือหน่วยงานอื่นตามกฎหมาย ให้ประสานผู้มีหน้าที่รับผิดชอบเพื่อดำเนินการตามกฎหมาย ประกาศ หลักเกณฑ์ แบบ วิธีการ ช่องทาง และกรอบระยะเวลาที่ใช้บังคับในขณะนั้น

(๙) ติดตามสถานะของเหตุการณ์จนกว่าจะมีการส่งมอบให้ผู้รับผิดชอบในการตอบสนองเหตุการณ์อย่างเป็นทางการ และบันทึกการส่งต่อเหตุการณ์เพื่อให้สามารถตรวจสอบย้อนกลับได้

มหาวิทยาลัยโดยสำนักวิทยบริการและเทคโนโลยีสารสนเทศ กำหนดให้มีบุคลากรปฏิบัติหน้าที่ เฝ้าระวังและเตรียมพร้อมรับแจ้งเหตุ (On-call) ตามความเหมาะสมของภารกิจ ความเสี่ยง และทรัพยากรของมหาวิทยาลัย เพื่อให้สามารถรับแจ้งและประสานการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นนอกเวลาราชการได้อย่างทันท่วงที

การจัดเวรเฝ้าระวังและเตรียมพร้อมรับแจ้งเหตุ (On-call) ดังกล่าวเป็นมาตรการภายในของมหาวิทยาลัย เพื่อสนับสนุนการบริหารจัดการเหตุการณ์และมิให้การรับแจ้งหรือการประสานงานล่าช้า ทั้งนี้ มิให้ตีความว่าเป็นการกำหนดระยะเวลาการรายงานตามกฎหมาย โดยการแจ้งหรือรายงานต่อหน่วยงานภายนอกให้ดำเนินการตามกฎหมาย ประกาศ หลักเกณฑ์ และแนวทางที่มีผลใช้บังคับในขณะเกิดเหตุ

รายชื่อบุคลากร ผู้รับผิดชอบ ช่องทางการติดต่อ และตารางการปฏิบัติหน้าที่เฝ้าระวังและเตรียมพร้อมรับแจ้งเหตุ (On-call) ตามความเหมาะสม เพื่อให้สามารถรับแจ้งและประสานการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นนอกเวลาราชการได้อย่างทันท่วงที (ดังภาคผนวกหรือเอกสารควบคุมภายในของแผน เพื่อให้สามารถปรับปรุงข้อมูลได้โดยไม่จำเป็นต้องแก้ไขแผนทั้งฉบับ และตารางที่ ๓ ไม่ควรใส่หมายเลขโทรศัพท์มือถือส่วนบุคคลไว้ในตัวแผนฉบับที่เผยแพร่ทั่วไป แนะนำให้ทำเป็น บัญชีรายชื่อและช่องทางติดต่อ RUTS-CIRT — เอกสารควบคุม”)

ตารางที่ ๓ บุคลากรปฏิบัติหน้าที่เฝ้าระวังและเตรียมพร้อมรับแจ้งเหตุ (On-call)

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายพีรศักดิ์ ชูส่งแสง	๒๔ ชั่วโมง / ๗ วัน	โทรศัพท์ : ๐๘๖-๙๖๔-๐๖๔๗ e-mail : peerasak.c@rmutsv.ac.th	รับแจ้งเหตุ	รับแจ้งและตรวจสอบเหตุเบื้องต้น ประสานงานกับผู้บังคับบัญชา
๒	นายภานุวัฒน์ หนูนคง	๒๔ ชั่วโมง / ๗ วัน	โทรศัพท์ : ๐๙๔-๘๙๕-๕๔๖๖ e-mail : panuwat.n@rmutsv.ac.th	รับแจ้งเหตุ	รับแจ้งและตรวจสอบเหตุเบื้องต้น ประสานงานกับผู้บังคับบัญชา
๓	นายกนกพล เมืองรักษ์	๒๔ ชั่วโมง / ๗ วัน	โทรศัพท์ : ๐๙๙-๓๕๖-๙๙๙๕ e-mail : kanokpon.m@rmutsv.ac.th	รับแจ้งเหตุ	รับแจ้งและตรวจสอบเหตุเบื้องต้น ประสานงานกับผู้บังคับบัญชา

๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัยกำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) ในลักษณะการบริหารจัดการแบบรวมศูนย์ (Centralized Incident Response) เพื่อให้การประสานงาน การสั่งการ การวิเคราะห์และประเมินสถานการณ์ การควบคุมและระงับเหตุการณ์ การกำจัดสาเหตุของเหตุการณ์ การกู้คืนระบบ และการติดตามผลการดำเนินงานเป็นไปอย่างเป็นระบบ มีเอกภาพ และสามารถประสานงานระหว่างหน่วยงานภายในมหาวิทยาลัยได้อย่างมีประสิทธิภาพ

โครงสร้างของ CIRT ให้ประกอบด้วยบุคลากรจากหน่วยงานหรือส่วนงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบสารสนเทศ ระบบความมั่นคงปลอดภัยไซเบอร์ การบริหารจัดการเหตุการณ์ กฎหมายและการคุ้มครองข้อมูล ตลอดจนหน่วยงานที่เกี่ยวข้องกับภารกิจของมหาวิทยาลัยตามความเหมาะสม โดยกำหนดบทบาท หน้าที่ ความรับผิดชอบ และสายการประสานงานของแต่ละส่วนอย่างชัดเจน

CIRT มีหน้าที่หลักในการประสานและสนับสนุนการดำเนินการเมื่อเกิดหรือมีเหตุอันควรสงสัยว่าเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ภายในมหาวิทยาลัย รวมทั้งยกระดับเหตุการณ์ตามระดับความรุนแรงและผลกระทบที่กำหนดไว้ในแผนฉบับนี้ และดำเนินการประสานหรือรายงานต่อหน่วยงานภายนอกตามกฎหมาย ระเบียบ ประกาศ หลักเกณฑ์ หรือแนวทางที่เกี่ยวข้อง เมื่อเข้าเงื่อนไขที่ต้องดำเนินการตามกฎหมายหรือหลักเกณฑ์ที่ใช้บังคับในขณะนั้น

ทั้งนี้ การกำหนด CIRT เป็นโครงสร้างการบริหารจัดการภายในของมหาวิทยาลัย ไม่กระทบต่ออำนาจหน้าที่ หรือความรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานที่มีอำนาจตามกฎหมาย และในกรณีที่เหตุการณ์หรือระบบของมหาวิทยาลัยอยู่ภายใต้หลักเกณฑ์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ดำเนินการตามกฎหมายและหลักเกณฑ์ที่ใช้บังคับกับหน่วยงานหรือระบบดังกล่าวเป็นการเฉพาะ

ให้กำหนดรายชื่อผู้ปฏิบัติหน้าที่ของ CIRT บทบาท หน่วยงาน ตำแหน่ง ช่องทางการติดต่อ และผู้ปฏิบัติหน้าที่สำรองไว้ในบัญชีรายชื่อหรือภาคผนวกที่มหาวิทยาลัยกำหนด และให้ปรับปรุงข้อมูลดังกล่าวเมื่อมีการเปลี่ยนแปลงบุคลากรหรือช่องทางการติดต่อ โดยไม่จำเป็นต้องแก้ไขเนื้อหาหลักของแผนรับมือเหตุภัยคุกคามทางไซเบอร์ทุกครั้งโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (CIRT) ปรากฏตามตารางที่ ๔

ตารางที่ ๔ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (CIRT)

ลำดับ	ชื่อ - นามสกุล	บทบาท/ตำแหน่ง CIRT	หน่วยงาน/ส่วนงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่ความรับผิดชอบหลัก
๑	ผศ.สิทธิโชค อุ่นแก้ว	หัวหน้าทีม CIRT (CIRT Team Lead)	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ/ผู้อำนวยการ	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๐๐ ต่อ ๑๑๖๐ – ๑๑๖๑ โทรศัพท์มือถือ : ๐๙๔-๕๙๘-๒๔๕๓ Email: sittichok.a@rmutsv.ac.th	ควบคุมและประสานการปฏิบัติงานของทีม CIRT และประสานการยกระดับเหตุการณ์ และสื่อสารรายงานต่อผู้บริหารของหน่วยงาน
๒	ดร.อรรถพล คงหวาน	รองหัวหน้าทีมรับมือฯ	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ/รองผู้อำนวยการ	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๐๐ ต่อ ๑๑๖๐ – ๑๑๖๑ โทรศัพท์มือถือ : ๐๘๖-๕๙๗-๓๘๑๙ Email: authapon.k@rmutsv.ac.th	ปฏิบัติหน้าที่แทนหัวหน้าทีมกรณีฉุกเฉิน
๓	ผศ.ดร.ศักดิ์ชัย ตันติวิวัทน์	เจ้าหน้าที่รับมือ (Incident lead)	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ/รองผู้อำนวยการ	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๐๐ ต่อ ๑๑๖๐ – ๑๑๖๑ โทรศัพท์มือถือ : ๐๘๘-๗๘๒-๖๔๔๒ Email: sugchai.t@rmutsv.ac.th	ควบคุมผลกระทบและสืบสวนภัยคุกคามทางเทคนิค

ลำดับ	ชื่อ - นามสกุล	บทบาท/ตำแหน่ง CIRT	หน่วยงาน/ส่วนงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่ความรับผิดชอบหลัก
๔	นายพีรศักดิ์ ชูส่งแสง	เจ้าหน้าที่เฝ้าระวังและตรวจจับ (Monitoring and Detection)	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ/หัวหน้างานวิศวกรรมเครือข่าย	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๔๖ โทรศัพท์มือถือ : ๐๘๖-๙๖๔-๐๖๔๗ Email: peerasak.c@rmutsv.ac.th	- เฝ้าระวัง ตรวจจับ วิเคราะห์สัญญาณหรือเหตุการณ์ผิดปกติ ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ และตัดสินใจในระดับปฏิบัติการ และแจ้งเหตุ - ประสานงาน ปฏิบัติการควบคุมผลกระทบทางเทคนิค
๕	นายภานุวัฒน์ หนูนคง	งานระบบและโครงสร้างพื้นฐาน (Infrastructure and Network)	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ/งานวิศวกรรมเครือข่าย	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๔๖ โทรศัพท์มือถือ : ๐๙๔-๘๙๕-๕๔๖๖ Email: panuwat.n@rmutsv.ac.th	วิเคราะห์เหตุการณ์ ประเมินผลกระทบ ควบคุมและจำกัดขอบเขต กำจัดสาเหตุ และสนับสนุนการกู้คืน
๖	นายกนกพล เมืองรักษ์	เจ้าหน้าที่เทคนิคฯ (Technical lead)	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ/งานวิศวกรรมเครือข่าย	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๔๖ โทรศัพท์มือถือ : ๐๙๙-๓๕๖-๙๙๙๕ Email: kanokpon.m@rmutsv.ac.th	ให้ความเห็นด้านเทคนิคเพื่อควบคุมภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังตารางที่ ๕

ตารางที่ ๕ ทีมสนับสนุนในการรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ลำดับ	บทบาท	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่ความรับผิดชอบ
๑	ผู้ควบคุมและจัดสรรทรัพยากร (Resource and Policy Director)	ผศ.สิทธิโชค อุ่นแก้ว (ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ)	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๐๐ ต่อ ๑๑๖๐ – ๑๑๖๑ โทรศัพท์มือถือ : ๐๙๔-๕๙๘-๒๔๕๓ Email: sittichok.a@rmutsv.ac.th arit@rmutsv.ac.th	กำกับ ประสานการรับมือเหตุการณ์โดยรวม ควบคุมและจัดการผลกระทบเชิงนโยบายจากเหตุภัยคุกคามทางไซเบอร์ อำนวยการ จัดสรรทรัพยากร อุปกรณ์ กำลังพล และอนุมัติงบประมาณฉุกเฉินเพื่อสนับสนุนการปฏิบัติงานของทีม CIRT
๒	ผู้แทนด้านกฎหมายและการปฏิบัติตามข้อกำหนด	ผู้แทน นิติกร สำนักงานนิติการมหาวิทยาลัยฯ	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๐๐	ทำหน้าที่เป็นเจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย รวบรวมข้อมูล หลักฐานดิจิทัล และเอกสารเพื่อรองรับการดำเนินคดี จัดทำรายงานแจ้งเหตุภัยคุกคามทางไซเบอร์ส่ง สกมช. และดำเนินคดีความตามกฎหมาย
๓	ผู้ทดสอบเจาะระบบและตรวจช่องโหว่	ผู้แทนหน่วยงานภายนอก	โทรศัพท์ภายใน : - โทรศัพท์มือถือ : -	ทำหน้าที่วิเคราะห์ช่องโหว่ของระบบและตรวจประเมินความปลอดภัยเชิงเทคนิคหลังเกิดเหตุคุกคาม ทดสอบระบบเครือข่ายและจัดทำรายงานสรุปผลการเจาะระบบ (Penetration Test Report) เพื่อแจ้งให้มหาวิทยาลัยทราบแนวทางปิดช่องทางเข้าถึง

ลำดับ	บทบาท	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่ความรับผิดชอบ
๔	ผู้รับผิดชอบบริหารจัดการความเสี่ยงองค์กร	รองอธิการบดี ดร. ภาณุมาศ สุยบางดำ (งานประกันคุณภาพการศึกษา)	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๐๐ Email: panumas.s@rmutsv.ac.th	ทำหน้าที่รวบรวมข้อมูลสถิติภัยคุกคามและสรุปผลกระทบที่เกิดขึ้นของมหาวิทยาลัย ดำเนินการวิเคราะห์ ทบทวน และนำข้อมูลไปประกอบการปรับปรุงแผนบริหารความเสี่ยงองค์กรในภาพรวม
๕	ผู้รับผิดชอบการสื่อสารในภาวะวิกฤต	รองอธิการบดี ผศ. ปิยะ ประสงค์จันทร์ (งานประชาสัมพันธ์)	โทรศัพท์ภายใน : ๐-๗๔๓๑๗๑๐๐ โทรศัพท์มือถือ :- Email: piya.p@rmutsv.ac.th	ทำหน้าที่เป็นโฆษกและผู้รับผิดชอบสื่อสารข้อมูลความมั่นคงปลอดภัยไซเบอร์ไปยังผู้มีส่วนได้ส่วนเสีย กลั่นกรองข้อมูลเทคนิคจากทีม CIRT เพื่อจัดทำแถลงการณ์และประชาสัมพันธ์แก่บุคลากร นักศึกษา และสาธารณชนอย่างเหมาะสมเพื่อลดผลกระทบด้านภาพลักษณ์

๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ได้จัดเตรียมและรวบรวมข้อมูลช่องทางการติดต่อสื่อสารของหน่วยงานภายนอกที่มีบทบาทเกี่ยวข้องในการควบคุม กำกับดูแล และให้ความช่วยเหลือเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ รวมถึงผู้ให้บริการภายนอกเพื่อรองรับการตรวจพิสูจน์พยานหลักฐานทางนิติวิทยาศาสตร์ดิจิทัลและการฟื้นฟูระบบ ดังรายละเอียดตารางที่ ๖

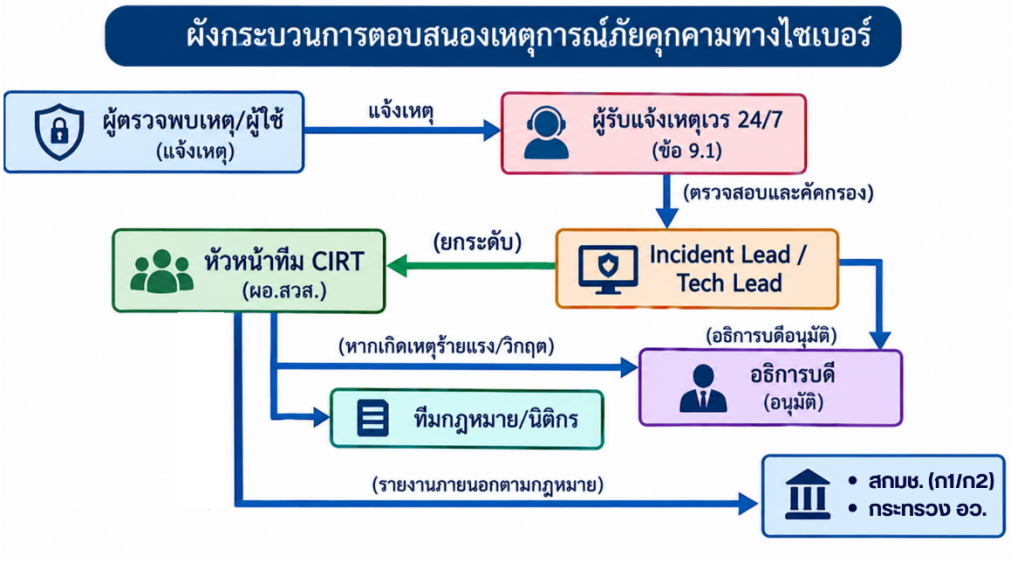
ตารางที่ ๖ หน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	ผู้แทน สำนักงาน คณะกรรมการการ รักษาความมั่นคง ปลอดภัยไซเบอร์ แห่งชาติ (สกมช.)	เบอร์โทรศัพท์มือถือ : Email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคาร บี) ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐	สำนักงาน คณะกรรมการการ รักษาความมั่นคง ปลอดภัยไซเบอร์ แห่งชาติ (สกมช.)	เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
๒	ผู้แทน กระทรวงการ อุดมศึกษา วิทยาศาสตร์ วิจัยและ นวัตกรรม (อว.)	โทรศัพท์ : ๐๒ ๓๓๓ ๓๗๐๐ ที่อยู่สำนักงาน : ๗๕/๔๗ อาคารพระจอมเกล้า ถ.พระราม ๖ แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐	กระทรวงการ อุดมศึกษา วิทยาศาสตร์ วิจัยและ นวัตกรรม	หน่วยงานกำกับดูแล
๓	ผู้แทน ศูนย์ประสานการรักษา ความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ แห่งชาติ THAI – CERT	โทรศัพท์ : ๐๒ ๑๔๒ ๖๘๘๘ Email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารบี)	ศูนย์ประสานการ รักษาความมั่นคง ปลอดภัยระบบ คอมพิวเตอร์แห่งชาติ THAI – CERT	ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานภายใต้การดูแล เพื่อเฝ้าระวัง ติดตาม และ

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
		ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ๑ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐		เตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๙.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดสายการบังคับบัญชาและขั้นตอนการไหลของข้อมูลการรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Workflow) ของบุคลากรภายในและทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (CIRT) ดังภาพที่ ๑ เพื่อให้สามารถสกัดกั้นภัยคุกคามได้อย่างทันท่วงที และสอดคล้องกับภาระหน้าที่การแจ้งรายงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยแบ่งกระบวนการรายงานออกเป็น ๔ ขั้นตอนหลัก



ภาพที่ ๑ กระบวนการในการรายงานเหตุภัยคุกคามทางไซเบอร์

ขั้นตอนที่ ๑ การตรวจพบและแจ้งเหตุการณ์เบื้องต้น (Detection and Local Reporting)

เมื่อผู้ใช้งาน บุคลากร หรือเจ้าหน้าที่ระบบ ตรวจพบความผิดปกติหรือเหตุภัยคุกคามทางไซเบอร์ ให้แจ้งข้อมูลไปยังผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน (เวร On-call ๒๔/๗) ผ่านหมายเลขโทรศัพท์เคลื่อนที่หรืออีเมลที่กำหนดไว้ในข้อ ๙.๑ ทันที

ขั้นตอนที่ ๒ การตรวจสอบ คัดกรอง และประเมินเบื้องต้น (Triage and Verification)

ผู้รับแจ้งเหตุ (นายพีรศักดิ์ หรือ นายภานุวัฒน์) ดำเนินการลงทะเบียนรับเรื่อง บันทึกข้อมูลเบื้องต้นลงในระบบ และประสานงานร่วมกับ Technical Lead และ Incident Lead เพื่อวิเคราะห์ข้อมูลจราจร (Log) สภาพการณ์ความผิดปกติ และระบุประเภทระดับความรุนแรงของภัยคุกคามตามมิติผลกระทบต่อการบริการและข้อมูล

ขั้นตอนที่ ๓ การรายงานและยกระดับเหตุการณ์ภายในหน่วยงาน (Internal Escalation)

กรณีภัยคุกคามระดับทั่วไป (ต่ำ - กลาง) Incident Lead ควบคุมดูแลการระงับเหตุร่วมกับฝ่ายเทคนิค และทำรายงานสรุปเสนอต่อหัวหน้าทีม CIRT ตามวงรอบปกติ

กรณีภัยคุกคามระดับร้ายแรง หรือ ระดับวิกฤต Incident Lead ต้องรายงานตรงไปยัง หัวหน้าทีม CIRT (ผู้อำนวยการสำนักวิทยบริการฯ) โดยทันที เพื่อเรียกประชุมทีมปฏิบัติการฉุกเฉิน และแจ้งประสานงานไปยังผู้แทน นิติกร สำนักงานนิติการ เพื่อเตรียมข้อมูลทางกฎหมายและรวบรวมสำเนาพยานหลักฐานดิจิทัล

ขั้นตอนที่ ๔ การรายงานต่อหน่วยงานกำกับดูแลภายนอกตามกฎหมาย (External Legal Reporting)

การรายงานเหตุไปยังหน่วยงานภายนอก จะดำเนินการควบคู่กับการระงับภัยทางเทคนิค โดยมอบหมายให้ทีมกฎหมาย/นิติกร ร่วมกับเจ้าหน้าที่รับมือฯ ดำเนินการตามกรอบกฎหมายของ สกมช. ดังนี้

- การรายงานเหตุภัยคุกคามทั่วไป (ก๑) จัดทำแบบรายงาน ก๑ เพื่อแจ้งประสานงานการตรวจสอบและผลวิเคราะห์ภัยคุกคามเบื้องต้นให้ สกมช. และกระทรวง อว. ทราบตามช่องทางปกติ
- การรายงานเหตุภัยคุกคามที่มีนัยสำคัญ (ก๒) หากพบว่าการโจมตีส่งผลกระทบต่อบริการสำคัญหรือระบบเครือข่ายหลักของมหาวิทยาลัยอย่างมีนัยสำคัญ ให้จัดทำแบบรายงาน ก๒ เสนออธิการบดีพิจารณาอนุมัติ และจัดส่งรายงานไปยัง สกมช. ภายในระยะเวลา ๒๔ ชั่วโมง นับแต่ทราบเหตุภัยคุกคาม
- การรายงานสรุปสถิติประจำปี (ก๓) สำนักวิทยบริการฯ และสำนักงานนิติการ จะร่วมกันรวบรวมสถิติเหตุการณ์ภัยคุกคามทั้งหมดที่เกิดขึ้นในรอบปี จัดทำรายงานแบบ ก๓ ส่งไปยัง สกมช. ภายในวันที่ ๓๑ มกราคมของปีถัดไป เป็นประจำทุกปี

๑๐. ขั้นตอนการรับมือ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ กำหนดขั้นตอนการรับมือตามหลักการสากล NIST SP 800-61r2 และประสานสอดคล้องกับข้อกำหนดทางกฎหมายของประเทศ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคาม มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามแต่ละระดับ พ.ศ. ๒๕๖๔ และประกาศ สกมช. พ.ศ. ๒๕๖๖ และ พ.ศ. ๒๕๖๘ ที่เกี่ยวข้อง โดยมีลำดับขั้นตอนการปฏิบัติงาน ๔ ระยะหลัก ดังภาพที่ ๒

ภาพที่ ๒ ผังวงจรการตอบสนองต่อเหตุการณ์

ข้อมูลอ้างอิงจากเว็บไซต์ https://dx.doi.org/10.6028/NIST.SP.800-61r2

๑๐.๑ ขั้นการเตรียมการ (preparation)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ดำเนินมาตรการเชิงรุกเพื่อเตรียมความพร้อมของบุคลากร เครื่องมือ และระบบก่อนเกิดภัยคุกคาม เพื่อให้สามารถตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที โดยมีมาตรการเตรียมการดังต่อไปนี้

ด้านบุคลากรและสายการรายงาน

- จัดตั้งโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (CIRT) ที่ระบุบทบาทและข้อมูลติดต่ออย่างชัดเจน (ตามข้อ ๙.๒)
- กำหนดสายการรายงานเหตุการณ์ (Escalation Path) และโครงสร้างการตัดสินใจ (ตามข้อ ๙.๔)
- กำหนดเกณฑ์และขั้นตอนการเปิดใช้งานแผน (Activate Plan) เมื่อเกิดเหตุภัยคุกคามตามระดับความรุนแรง

ด้านสถานที่และโครงสร้างพื้นฐานฉุกเฉิน

- กำหนดให้ ห้องประชุม ๕๙๒๐๓ เป็นศูนย์ปฏิบัติการและประสานงานสื่อสารส่วนกลางของทีม CIRT
- กำหนดให้ ห้อง Data Center อาคาร ๕๙ เป็นสถานที่จัดเก็บหลักฐานที่มั่นคงปลอดภัย (Secure Storage Facility) สำหรับเก็บข้อมูลดิจิทัลและพยานวัตถุสำคัญ

ด้านเครื่องมือและเทคโนโลยี

- จัดเตรียมและเปิดใช้งานระบบวิเคราะห์และบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (SIEM) ซึ่งได้รับการติดตั้งเสร็จสิ้นและปรับแต่งกฎตรวจจับ (Rule set) เรียบร้อยแล้ว เพื่อใช้ประสานการวิเคราะห์ Log จากอุปกรณ์เครือข่ายและเครื่องแม่ข่ายทั้งหมดของมหาวิทยาลัยฯ
- จัดให้มีช่องทางการรับแจ้งเหตุและติดตามสถานการณ์ตลอด ๒๔ ชั่วโมง ผ่านเจ้าหน้าที่เวรปฏิบัติการ (ตามข้อ ๙.๑)

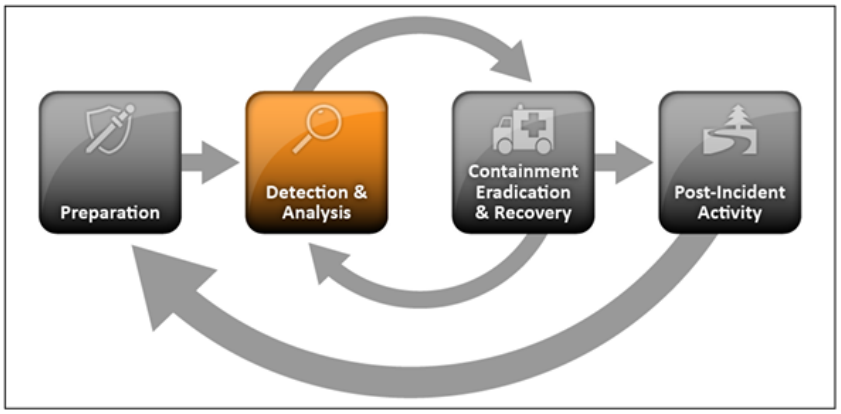
ด้านการประเมินและการฝึกซ้อมประจำปี

- จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment) ของระบบสารสนเทศสำคัญอย่างน้อยปีละหนึ่งครั้ง
- จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน (ตามภาคผนวก ๑) และดำเนินการฝึกซ้อมแผนรับมือภัยคุกคามไซเบอร์ร่วมกับหน่วยงานสนับสนุนเป็นประจำทุกปี

นอกจากนี้ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย มีการพิจารณาดำเนินงานตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

การดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) แสดงดังภาพที่ ๓ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น



ภาพที่ ๓ แผนผังวงจรตอบสนองต่อเหตุการณ์ : การตรวจจับและวิเคราะห์

มหาวิทยาลัยฯ กำหนดกระบวนการตรวจจับสิ่งผิดปกติ คัดกรอง และวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อจำกัดผลกระทบและแจ้งเตือนภัยได้อย่างทันท่วงที โดยดำเนินการดังนี้

๑๐.๒.๑ การตรวจจับและการใช้เครื่องมือเฝ้าระวัง

ทีม CIRT และผู้ดูแลระบบจะคัดกรองข้อมูลแจ้งเตือนที่แบ่งออกเป็น ๒ ประเภท คือ Precursor (ข้อมูลบ่งบอกว่าเหตุการณ์อาจเกิดขึ้นในอนาคต) และ Indicator (ข้อมูลบ่งบอกว่าการโจมตีเกิดขึ้นแล้วหรือกำลังเกิดขึ้น) โดยอ้างอิงแหล่งข้อมูลตรวจจับ ดังนี้

- ระบบป้องกันและตรวจจับ (Alerts) ระบบป้องกันการบุกรุกเครือข่าย (IPS) ระบบจัดการเหตุการณ์ความปลอดภัย (SIEM) และระบบป้องกันมัลแวร์ (Anti-Malware) ที่ทำหน้าที่ตรวจสอบทั้งระดับเครือข่ายและอุปกรณ์ปลายทาง
- บันทึกข้อมูลจราจรคอมพิวเตอร์ (Logs) บันทึกเหตุการณ์ของระบบปฏิบัติการและแอปพลิเคชัน (OS and Application Logs) และบันทึกของอุปกรณ์เครือข่าย (Network Device Logs)
- แหล่งข้อมูลภายนอกและบุคคล ข้อมูลช่องโหว่ใหม่จากแหล่งสาธารณะ (Threat Intelligence) และการรายงานแจ้งเหตุจากบุคลากรผู้ใช้งานภายในองค์กร

๑๐.๒.๒ การวิเคราะห์ความผิดปกติและการพิสูจน์ทราบ

เมื่อได้รับแจ้งเหตุหรือพบการแจ้งเตือนจากระบบ เจ้าหน้าที่เทคนิคจะดำเนินการวิเคราะห์ตามแนวทางดังต่อไปนี้

- ตรวจสอบ Log ย้อนหลัง โดยการดึงข้อมูล Log จากอุปกรณ์ที่เกี่ยวข้องตามนโยบายจัดเก็บ Log (Log Retention Policy) เพื่อสืบหาต้นตอของการบุกรุก

- ประสานเวลาอุปกรณ์ (Clock Synchronization) โดยตรวจสอบให้อุปกรณ์ไอทีทุกชิ้นบนเครือข่ายได้รับการซิงโครไนซ์เวลาให้ตรงกัน (NTP) เพื่อเปรียบเทียบหาความสัมพันธ์ของเหตุการณ์ตามลำดับเวลาได้อย่างถูกต้อง
- ดักจับข้อมูลเครือข่าย โดยการดำเนินการวิเคราะห์และดักจับข้อมูลจราจรทางเครือข่าย (Sniff and Analyze Network Data) เพื่อวิเคราะห์พฤติกรรมแปลกปลอม
- ขอความช่วยเหลือภายนอก (Seek Assistance) ในกรณีทีม CIRT ไม่สามารถวิเคราะห์หาสาเหตุหรือกำจัดผู้บุกรุกออกไปได้ ให้เร่งขอคำปรึกษาและช่วยเหลือทางเทคนิคจาก Thai-CERT หรือ สกมช. ทันที

๑๐.๒.๓ การบันทึกและประเมินระดับความรุนแรงของเหตุการณ์

การลงบันทึกรายละเอียดเหตุการณ์ลงในแบบฟอร์มบันทึกสถานการณ์ภัยคุกคาม (ตามภาคผนวก ๒) และประเมินระดับผลกระทบและความรุนแรงของภัยคุกคามใน ๓ ด้านเพื่อจัดลำดับความสำคัญในการระงับเหตุ ได้แก่

- ผลกระทบต่อการให้บริการ (Functional Impact) แบ่งระดับความเสียหายเป็น ระดับ ๐ (ต่ำ - ทำงานช้าลง) ระดับ ๑ (กลาง - กระทบบางกลุ่ม) ระดับ ๒ (สูง - หยุดชะงักแต่กู้คืนได้) และระดับ ๓ (สุดขีด - หายนะล่มถาวร)
- ผลกระทบต่อข้อมูล (Information Impact) พิจารณาความเสียหายต่อความลับ ความครบถ้วน และความพร้อมใช้ของข้อมูล โดยจำแนกเป็น ไม่มีผลกระทบ (None) ข้อมูลส่วนบุคคลรั่วไหล (Privacy Breach) ข้อมูลความลับองค์กรรั่วไหล (Proprietary Breach) และข้อมูลถูกเปลี่ยนแปลง/ทำลาย (Integrity Loss)
- ความยากง่ายในการฟื้นฟูระบบ (Recoverability) ประเมินระยะเวลาและทรัพยากรที่ต้องใช้ในการกู้คืนระบบ โดยแบ่งเป็น ระดับปกติ (Regular) ต้องใช้ทรัพยากรเพิ่มเติม (Supplemented) ต้องใช้ทรัพยากรและผู้เชี่ยวชาญภายนอก (Extended) และกู้คืนไม่ได้/ข้อมูลรั่วไหลสู่สาธารณะแล้ว (Not Recoverable)

๑๐.๒.๔ มาตรการแจ้งรายงานเหตุภัยคุกคามตามกฎหมายของ สกมช.

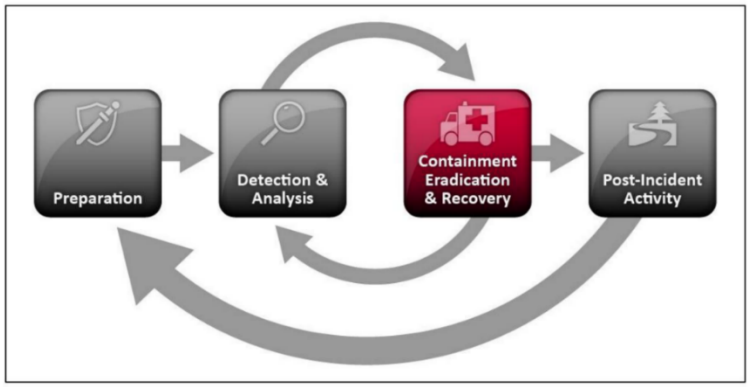
มหาวิทยาลัยฯ กำหนดบทบาทให้ทีมกฎหมายประสานงานร่วมกับทีม CIRT เพื่อส่งแบบรายงานแจ้งเหตุภัยคุกคามไปยัง สกมช. และกระทรวง อว. ตามที่กฎหมายกำหนด ดังนี้

- การรายงานเหตุภัยคุกคามทั่วไป (แบบรายงาน ก๑) ใช้รายงานข้อมูลการประสานงานและผลวิเคราะห์ตรวจสอบภัยคุกคามเบื้องต้นแก่ สกมช. และ อว. เพื่อขอคำแนะนำ (ตามภาคผนวก ๔)

- การรายงานเหตุภัยคุกคามระดับร้ายแรง/มีนัยสำคัญ (แบบรายงาน ก๒) ต้องดำเนินการส่งแบบรายงาน ก๒ เสนออธิการบดีพิจารณาลงนาม และจัดส่งไปยัง สกมช. ภายใน ๒๔ ชั่วโมง นับแต่มหาวิทยาลัยฯ ตรวจพบหรือทราบเหตุ (ตามภาคผนวก ๔)
- การรายงานสรุปสถิติประจำปี (แบบรายงาน ก๓) รวบรวมสถิติภัยคุกคามจำแนกตามหมวดหมู่ ทรัพย์สิน และระดับความรุนแรงในรอบปี แล้วจัดส่งรายงาน ก๓ ให้แก่ สกมช. ภายในวันที่ ๓๑ มกราคมของปีถัดไป เป็นประจำทุกปี (ตามภาคผนวก ๔)

๑๐.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบแสดงดังภาพที่ ๔



ภาพที่ ๔ แผนผังวงจรตอบสนองต่อเหตุการณ์ : การกักกัน การกำจัดและการฟื้นฟู

การกำหนดขั้นตอนการปฏิบัติให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่ อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมา ดำเนินงานหรือให้บริการ

ได้ตามปกติ เมื่อตรวจพบภัยคุกคามหรือได้รับแจ้งเหตุ ทีม CIRT และฝ่ายเทคนิคจะดำเนินการระงับเหตุและฟื้นฟูระบบสารสนเทศตามระดับความรุนแรงและลักษณะของเหตุการณ์ควบคู่กันไป ดังนี้

๑๐.๓.๑ วิธีการควบคุมจำกัดวงความเสียหาย (Containment)

การดำเนินการระงับภัยและจำกัดวงความเสียหายของระบบโดยเลือกใช้วิธีปฏิบัติงานที่เหมาะสมกับสถานการณ์ เช่น

- ตัดการเชื่อมต่อเครือข่าย (Network Disconnection) โดยการตัดการเชื่อมต่อระบบเครือข่ายภายนอกและภายในทันทีเพื่อระงับการแพร่กระจายมัลแวร์ โดยอาจยกเว้นการเชื่อมต่อเฉพาะพอร์ตหรือช่องทางทำงานของระบบตรวจจับ Endpoint Detection and Response (EDR) Agent เท่านั้น
- หยุดการทำงานเฉพาะฟังก์ชัน (Disabling Certain Functions) โดยการปิดการทำงานของฟังก์ชันหรือแอปพลิเคชันที่ได้รับผลกระทบเพื่อความต่อเนื่องทางธุรกิจบางส่วน
- ล่อลวงผู้บุกรุก (Redirection) เบี่ยงเบนพฤติกรรมและความสนใจของผู้บุกรุกไปที่ระบบจำลองความปลอดภัย เช่น Sandbox หรือ Honeypot เพื่อวิเคราะห์การโจมตี

๑๐.๓.๒ การรวบรวมและจัดเก็บหลักฐานทางดิจิทัลอย่างถูกต้องตามกฎหมาย

การรวบรวมหลักฐานดิจิทัลก่อนเริ่มการกู้คืน เพื่อรักษาสภาพหลักฐานเดิมให้สมบูรณ์และสามารถนำไปยอมรับในชั้นศาลได้ตามข้อบังคับทางกฎหมาย โดยถือปฏิบัติดังนี้

- การจัดเก็บพยานหลักฐานตามระดับความผันผวน (Order of Volatility) โดยให้จัดความสำคัญรวบรวมข้อมูลที่มีโอกาสสูญหายได้ง่ายที่สุดเมื่อไม่มีกระแสไฟฟ้าหรือผ่านการใช้งานระบบ เช่น ข้อมูลในหน่วยความจำชั่วคราว (RAM/Cache) เป็นอันดับแรกสุด ก่อนทำการปิดเครื่องเพื่อสำรองข้อมูลจาก Hard Disk
- การทำสำเนาหลักฐานที่ถูกต้อง (Acquisition) โดยใช้เครื่องมือทำสำเนาพยานหลักฐานดิจิทัลแบบครบถ้วนทุกบิต (Bit-for-bit Duplication) ผ่านอุปกรณ์ป้องกันการบันทึกทับข้อมูลพยานหลักฐาน (Hardware Write Blocker) เสมอ เพื่อป้องกันไม่ให้หลักฐานต้นฉบับเกิดการเปลี่ยนแปลง
- การรับรองความถูกต้องพยานหลักฐาน (Authentication) โดยการคำนวณรหัสค่าธรรมเนียมตรวจสอบข้อมูลพยานหลักฐานทางคณิตศาสตร์ด้วยเทคนิค Cryptographic Hash (เช่น SHA-256) เพื่อพิสูจน์เปรียบเทียบว่าพยานหลักฐานที่ทำสำเนาขึ้นมีความถูกต้องและตรงกับพยานหลักฐานต้นฉบับ ๑๐๐%

- การจัดทำห่วงโซ่การคุ้มครองหลักฐาน (Chain of Custody) โดยการบันทึกประวัติการถือครองและควบคุมหลักฐานอย่างรัดกุมในแบบฟอร์มห่วงโซ่หลักฐาน ทุกครั้งที่มีการเคลื่อนย้ายหรือส่งมอบหลักฐานเพื่อพิสูจน์ความน่าเชื่อถือของพยานหลักฐานในชั้นศาล (ตามรายละเอียดข้อ ๙.๒ และภาคผนวก)

๑๐.๓.๓ ขั้นตอนการปราบปรามและกำจัดสาเหตุภัยคุกคาม (Eradication)

ภายหลังการจำกัดวงความเสียหายและการสำรองหลักฐานดิจิทัลเสร็จสิ้น ให้ดำเนินการตรวจสอบหาสาเหตุหลัก (Root Cause) และกำจัดร่องรอยภัยคุกคามดังนี้

- ตรวจสอบและปิดกั้นช่องโหว่ทางเทคนิคที่ผู้โจมตีใช้บุกรุกระบบ
- ตรวจสอบและสแกนค้นหามัลแวร์ เครื่องมือ Backdoor หรือรหัสควบคุมระยะไกลที่ผู้บุกรุกฝังไว้ในระบบด้วยฐานข้อมูลดัชนีชี้วัดการบุกรุก (Indicators of Compromise: IoC) เพื่อลบออกจากระบบทั้งหมด
- ออกมาตรการบังคับให้ผู้ใช้งานระบบที่ได้รับผลกระทบทั้งหมด ทำการเปลี่ยนแปลงรหัสผ่าน (Password Reset) ในทันที

๑๐.๓.๔ กระบวนการกู้คืนและเปิดให้บริการระบบงาน (Recovery)

การนำระบบงานและบริการสำคัญกลับมาให้บริการตามปกติเพื่อความต่อเนื่องทางธุรกิจ ให้ดำเนินการดังนี้

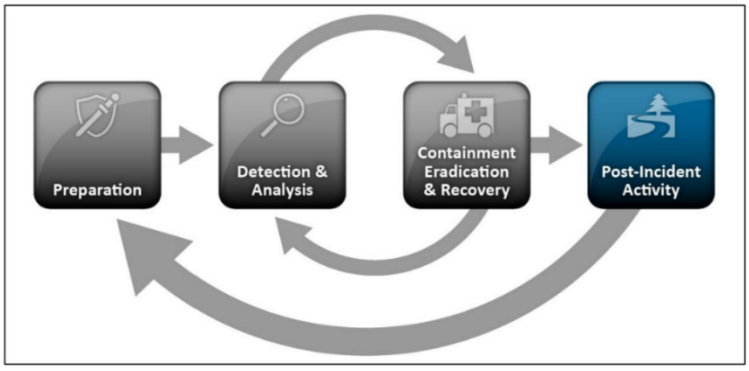
- ดำเนินการ Restore ระบบปฏิบัติการและซอฟต์แวร์ประยุกต์ต่าง ๆ จากแผ่น Master Image ที่ผ่านการตรวจสอบแล้วว่าสะอาด ปลอดภัย และไม่มีช่องโหว่
- นำข้อมูลชุดสถิติและข้อมูลสารสนเทศกลับคืนระบบไอทีจากระบบสำรองข้อมูล (Backup Storage) ที่จัดตั้งขึ้น
- ทำการทดสอบประสิทธิภาพ ความสมบูรณ์ และสแกนหาความมั่นคงปลอดภัยของระบบงานที่ทำการติดตั้งใหม่ ก่อนจะอนุมัติเปิดให้บุคคลภายนอกใช้งานจริง

๑๐.๓.๕ เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

๑๐.๓.๖ ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

๑๐.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

มหาวิทยาลัยฯ กำหนดมาตรการเรียนรู้จากบทเรียนภัยคุกคามซึ่งมีการดำเนินการแก้ปัญหาภัยคุกคามทางไซเบอร์ ดังภาพที่ ๕ และประเมินผลการดำเนินงานเพื่อความมั่นคงปลอดภัยระยะยาว ดังต่อไปนี้



ภาพที่ ๕ แผนผังวงจรตอบสนองต่อเหตุการณ์ : กิจกรรมหลังเหตุการณ์

การประชุมทบทวนหลังเกิดเหตุ (After-Action Review: AAR) หลังจากการสกัดกั้นและระงับภัยคุกคามได้เสร็จสิ้น และบริการต่าง ๆ กลับมาทำงานในสภาวะปกติอย่างมีเสถียรภาพแล้ว ทีม CIRT จะต้องจัดประชุมแลกเปลี่ยนความเห็นร่วมกับผู้ดูแลระบบและฝ่ายสนับสนุน เพื่อร่วมกันถอดบทเรียน (Lessons Learned) หาจุดบกพร่องในแผนรับมือ ช่องโหว่ของระบบเครือข่าย และกระบวนการดำเนินงาน เพื่อนำข้อมูลมาปรับปรุงแนวทางการตอบสนองเหตุการณ์ในอนาคต

การทำมาตรการป้องกันการเกิดเหตุซ้ำ โดยการสืบหาแนวทางแก้ไขปัญหาเชิงป้องกัน ปรับแต่งกฎตรวจจับและวิเคราะห์ในระบบ SIEM หรือสแกนตรวจหาช่องโหว่ทางเทคโนโลยีของมหาวิทยาลัยเพิ่มเติม เพื่ออุดโอกาสที่จะเกิดภัยคุกคามในลักษณะเดิมซ้ำอีกครั้งในอนาคต

การส่งมอบและรายงานข้อมูลสถิติ โดยมีการนำบันทึกรายงานเหตุการณ์ที่รวบรวมได้ มาจัดทำสถิติภัยคุกคามประจำสัปดาห์หรือประจำเดือน เสนอต่อคณะกรรมการรักษาความปลอดภัยไซเบอร์ของมหาวิทยาลัยฯ เพื่อประกอบการปรับปรุงนโยบายบริหารความเสี่ยงองค์กร

การรักษาสภาพและส่งมอบพยานหลักฐานเพื่อดำเนินคดี โดยการรักษาสภาพความปลอดภัยของพยานหลักฐานดิจิทัลและแบบฟอร์มห่วงโซ่หลักฐาน (Chain of Custody) ตลอดช่วงเวลาที่กฎหมายหรือกระบวนการพิจารณาคดีกำหนดไว้ เพื่อเป็นพยานวัตถุรองรับการดำเนินการสืบสวนคดีคอมพิวเตอร์และการดำเนินคดีความตามกฎหมายของสำนักงานนิติการ

๑๐.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ได้จัดเตรียมรายการตรวจสอบลำดับขั้นปฏิบัติการรับมือภัยคุกคาม (Incident Handling Checklist) เพื่ออำนวยความสะดวกให้แก่เจ้าหน้าที่ผู้สวมบทบาทรับแจ้งเหตุและวิเคราะห์ประเมิน ได้เปิดตรวจสอบขั้นตอนสำคัญและลงบันทึกสถานการณ์ดำเนินงานได้อย่างมีประสิทธิภาพและไม่ตกหล่น โดยรายละเอียดของรายการตรวจสอบทั้งหมดปรากฏตาม ภาคผนวก ๕ ของเอกสารฉบับนี้

๑๑. การกำกับการใช้งานแผนและเกณฑ์การประกาศเหตุ (Plan Governance and Activation)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดกลไกการกำกับดูแล การเปิดใช้งานแผนรับมือเหตุภัยคุกคามทางไซเบอร์ และเกณฑ์ในการตัดสินใจควบคุมสถานการณ์ เพื่อให้สายการบังคับบัญชาและการตัดสินใจเป็นไปอย่างมีประสิทธิภาพและทันท่วงทีในภาวะวิกฤต ดังนี้

๑๑.๑ การเป็นเจ้าของแผนและการบริหารจัดการเหตุการณ์ (Plan Ownership and Incident Management)

มหาวิทยาลัยฯ กำหนดให้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ (สวส.) ทำหน้าที่เป็นเจ้าของแผน (Plan Owner) โดยมีผู้อำนวยการสำนักวิทยบริการฯ เป็นผู้รับผิดชอบหลัก

เจ้าของแผนมีหน้าที่ในการประสานงานเพื่อเตรียมความพร้อม ดำเนินมาตรการเฝ้าระวัง เรียกประชุมและระดมพลทีม CIRT เมื่อเกิดเหตุการณ์ ติดตามสถานการณ์ และพิจารณาเสนอปิดเหตุการณ์ภัยคุกคาม

การตัดสินใจประกาศใช้แผนและยกระดับการรับมือภัยคุกคาม จะต้องได้รับการอนุมัติจากผู้มีอำนาจตัดสินใจตามระดับความรุนแรงของภัยคุกคามที่มหาวิทยาลัยฯ กำหนดไว้ (ตามข้อ ๑๒.๒)

๑๑.๒ เกณฑ์การเปิดใช้งานแผนรับมือภัยคุกคาม (Plan Activation Triggers)

หัวหน้าทีม CIRT หรือผู้รับแจ้งเหตุจะพิจารณาประกาศเปิดใช้งานแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Activate Plan) และเรียกประชุมทีมปฏิบัติการทันที เมื่อตรวจพบสถานการณ์ภัยคุกคามทางเทคนิคที่เข้าเกณฑ์อย่างใดอย่างหนึ่ง ดังต่อไปนี้

- ภัยคุกคามต่อระบบบริการสำคัญ (Service Outage Trigger) ระบบสารสนเทศหลักของมหาวิทยาลัยฯ (เช่น ระบบทะเบียนและบริการการศึกษา ระบบอีเมลกลาง หรือเว็บไซต์หลักของมหาวิทยาลัย) ได้รับผลกระทบจนไม่สามารถให้บริการแก่บุคลากรหรือนักศึกษาได้
- ภัยคุกคามด้านข้อมูลและสิทธิส่วนบุคคล (Data Breach Trigger) ตรวจพบหรือต้องสงสัยว่าเกิดการรั่วไหล การเข้าถึงโดยมิชอบ หรือการโจรกรรมข้อมูลสำคัญ ข้อมูลความลับองค์กร หรือข้อมูลส่วนบุคคล (PII) ของนักศึกษาและบุคลากรในปริมาณมาก

- ภัยคุกคามจากโปรแกรมประสงค์ร้าย (Malware Outbreak Trigger) ตรวจพบการแพร่ระบาดของมัลแวร์ หรือการทำงานของมัลแวร์เรียกค่าไถ่ (Ransomware) ที่พยายามเข้าถึงและเข้ารหัสลับข้อมูลในเครื่องแม่ข่ายสำคัญหรือระบบ Active Directory
- ภัยคุกคามต่อความพร้อมใช้งานของระบบเครือข่าย (DDoS and Defacement Trigger) เกิดการโจมตีเพื่อปฏิเสธการให้บริการ (DDoS Attack) ที่ทำให้ช่องสัญญาณอินเทอร์เน็ตของมหาวิทยาลัยเป็นอัมพาต หรือเกิดการลักลอบแก้ไขหน้าเว็บไซต์หลักของมหาวิทยาลัยฯ (Web Defacement)
- การยึดครองสิทธิ์ผู้ดูแลระบบ (Privilege Compromise Trigger) บัญชีผู้ใช้งานที่สิทธิ์ระดับสูง (Domain Admin / Super Admin) ของระบบเครือข่ายหรือระบบคลาวด์ ถูกบุกรุก บุกเจาะ หรือยึดครองสิทธิ์โดยไม่ได้รับอนุญาต
- การลุกลามข้ามเครือข่าย (Escalation Trigger) เหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นมีพฤติกรรมหรือแนวโน้มที่จะแพร่กระจายลุกลามข้ามไปยังหน่วยงานภายนอก หรือเครือข่ายพันธมิตรของมหาวิทยาลัย

๑๑.๓ การเก็บบันทึกประวัติและเลขที่เหตุการณ์ (Incident Registration and Logging)

เพื่อให้สามารถตรวจสอบย้อนหลังทางกฎหมายและประเมินผลการรับมือได้อย่างมีระบบ มหาวิทยาลัยฯ กำหนดให้ทุกเหตุภัยคุกคามที่ได้รับการแจ้งเหตุและเปิดใช้งานแผน ต้องมีการลงทะเบียนข้อมูลในระบบ Ticket หรือบันทึกเหตุการณ์ โดยต้องระบุข้อมูลสำคัญดังนี้

- หมายเลขอ้างอิงเหตุการณ์ (Incident ID) กำหนดรหัสเฉพาะสำหรับแต่ละเหตุการณ์ (เช่น INC-YYYY-XXXX)
- เจ้าของเหตุการณ์ (Incident Owner) เจ้าหน้าที่ในทีม CIRT ที่ได้รับมอบหมายให้เป็นผู้ดูแลรับผิดชอบ หลักในการควบคุมสถานการณ์
- วันและเวลาเริ่มต้นเหตุการณ์ (Start Time) วันและเวลาที่ระบุว่าเกิดภัยคุกคามขึ้นจริงตามระบบ Log
- วันและเวลาที่ประกาศใช้แผน (Activation Time) วันและเวลาที่ทีมงานอนุมัติให้ยกระดับและเปิดใช้งานแผนรับมือฯ
- ผู้อนุมัติประกาศใช้แผน (Approved by) รายชื่อและตำแหน่งของผู้มีอำนาจสั่งการในการอนุมัติใช้แผน
- ระดับความรุนแรงของภัยคุกคาม (Severity Level) ระดับความรุนแรงที่ประเมินได้จากตารางความรุนแรงเพื่อจัดระดับการทำงาน

๑๑.๔ อำนาจการตัดสินใจเฉพาะเรื่องในภาวะฉุกเฉิน (Emergency Decision-Making Authority)

เพื่อป้องกันความล่าช้าในการระงับเหตุ มหาวิทยาลัยฯ กำหนดตัวบุคคลผู้มีสิทธิ์และอำนาจในการสั่งการและตัดสินใจในเรื่องสำคัญ ๆ พร้อมสายบังคับบัญชาตัวสำรองกรณีปฏิบัติหน้าที่แทนเมื่อผู้รับผิดชอบหลักไม่สามารถปฏิบัติหน้าที่ได้ ดังตารางที่ ๗

ตารางที่ ๗ อำนาจการตัดสินใจเฉพาะเรื่องในภาวะฉุกเฉิน

ประเด็นการตัดสินใจ	ผู้มีอำนาจตัดสินใจหลัก	ผู้มีอำนาจตัดสินใจ (สำรอง)	ขอบเขตอำนาจและ เกณฑ์การตัดสินใจ
๑. การระงับเหตุและตัดระบบออกจากเครือข่าย	นายพีรศักดิ์ ชูส่งแสง	นายภานุวัฒน์ หนูนคง	มีอำนาจสั่งการทางปฏิบัติการเพื่อจำกัดวงความเสียหายโดยทันที เช่น การบล็อก IP การตัดการเชื่อมต่อเครือข่ายเฉพาะจุด หรือการปิดพอร์ตเชื่อมต่อที่พบความผิดปกติ
๒. การหยุดให้บริการระบบสำคัญชั่วคราว	ผศ.สิทธิโชค อุ่นแก้ว	นายภานุวัฒน์ หนูนคง	ตัดสินใจอนุมัติให้หยุดการให้บริการระบบสารสนเทศหลักในภาพรวมของมหาวิทยาลัยฯ (เช่น ระบบทะเบียน ระบบอีเมล หรือระบบเครือข่ายวิทยาเขต) ชั่วคราว เมื่อพบการแพร่ระบาดร้ายแรง
๓. การกู้คืนระบบและเปิดให้บริการใหม่	ผศ.สิทธิโชค อุ่นแก้ว	นายภานุวัฒน์ หนูนคง	ตรวจสอบผลการดำเนินงานและสแกนความมั่นคงปลอดภัยของระบบ ก่อนร่วมตัดสินใจกับหน่วยงานสนับสนุนเพื่ออนุมัติให้นำระบบหรือบริการสำคัญกลับมาเปิดใช้งานตามปกติ
๔. การสื่อสารสู่สาธารณะและแถลงข่าว	ศาสตราจารย์ ดร.สุวัจน์ ธัญรส (อธิการบดี)	ผศ.สิทธิโชค อุ่นแก้ว (ผู้อำนวยการสำนักวิทยบริการฯ)	อนุมัติข้อมูลและข้อความแถลงการณ์ในภาวะวิกฤต โดยมอบหมายให้ ผศ.ดร.ศักดิ์ชัย ตันติวิวัทน์ ในฐานะผู้รับผิดชอบด้านสื่อสารองค์กร หรือทีมงานที่เกี่ยวข้องเป็นผู้ชี้แจงอย่างเป็นทางการ

ประเด็นการตัดสินใจ	ผู้มีอำนาจตัดสินใจหลัก	ผู้มีอำนาจตัดสินใจ (สำรอง)	ขอบเขตอำนาจและ เกณฑ์การตัดสินใจ
๕. การประสานงานและรายงานหน่วยงานภายนอก	ผู้แทน นิติกร (สำนักงานนิติการ มหาวิทยาลัยฯ)	นายกนกพล เมืองรักษ์	ตรวจสอบความสอดคล้องทางกฎหมาย รวบรวมข้อมูลพยานหลักฐาน และดำเนินการลงนามส่งแบบรายงานแจ้งเหตุภัยคุกคาม (ก๑ / ก๒) ส่งไปยัง สกมช. และกระทรวง อว. ตามกรอบเวลา

๑๒. การจำแนกและยกระดับเหตุ (Classification, Severity and Escalation)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดให้เจ้าหน้าที่ในทีม CIRT และผู้ดูแลระบบดำเนินมาตรการประเมินเพื่อจำแนกประเภทและยกระดับเหตุภัยคุกคามทางไซเบอร์ เพื่อให้การจัดสรรกำลังพล ทรัพยากร และสายการรายงานสอดคล้องกับความเป็นจริงและทันท่วงที โดยปฏิบัติงานตามหลักเกณฑ์ดังต่อไปนี้

๑๒.๑ มิติในการจำแนกเหตุภัยคุกคาม

การคัดกรองเหตุการณ์ทุกครั้ง ให้เจ้าหน้าที่ผู้รับแจ้งเหตุร่วมกับเจ้าหน้าที่รับมือฯ ดำเนินการจำแนกเหตุโดยวิเคราะห์ข้อมูลอย่างน้อย ๔ มิติคู่ขนานกัน ดังนี้

- ผลกระทบต่อการให้บริการ (Functional Impact) ความเสียหายหรือผลกระทบที่เกิดขึ้นต่อระบบเครือข่ายและระบบบริการสารสนเทศหลักในการดำเนินงานของมหาวิทยาลัยฯ
- ผลกระทบต่อข้อมูลสำคัญ (Information Impact) ความเสียหายที่เกิดขึ้นต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล ตลอดจนมิติด้านข้อมูลส่วนบุคคลรั่วไหล (PDPA)
- ขอบเขตและปริมาณที่ได้รับผลกระทบ (Scope of Impact) ปริมาณจำนวนเครื่องคอมพิวเตอร์ เครื่องแม่ข่าย วิทยาเขต หรือจำนวนผู้ใช้งานที่ได้รับผลกระทบจากภัยคุกคามดังกล่าว
- ความยากง่ายและระยะเวลาในการกู้คืนระบบ (Recoverability Effort) ระยะเวลาและปริมาณทรัพยากร รวมถึงกำลังพลทางเทคนิคที่จำเป็นต้องใช้เพื่อให้ระบบกู้คืนกลับมาให้บริการได้ตามปกติ

๑๒.๒ การจำแนกระดับความรุนแรงของเหตุภัยคุกคาม (Severity Matrix)

มหาวิทยาลัยฯ กำหนดการรวมผลมิติทั้ง ๔ ด้านข้างต้น เพื่อสรุปเป็นระดับความรุนแรงของภัยคุกคามภายใน (Internal Severity Level) ออกเป็น ๔ ระดับ แสดงดังตารางที่ ๘ เพื่อใช้กำหนดระดับความเร่งด่วนในการตอบสนอง (SLA) และสายการบังคับบัญชาภายใน ดังนี้

ตารางที่ ๘ การจำแนกระดับความรุนแรงของเหตุภัยคุกคาม

ระดับความรุนแรงที่ประเมิน	ระยะเวลาบังคับรายงานตัวจริง	บุคคลและทีมสนับสนุนที่ต้องได้รับการแจ้งเหตุทันที	ช่องทางและวิธีการประสานงาน
ระดับ ๑ (ต่ำ)	ภายใน ๒๔ ชั่วโมง	เจ้าหน้าที่ในทีม CIRT ฝ่ายเทคนิค และเจ้าหน้าที่ผู้ดูแลระบบงานที่เกิดเหตุ	ส่งอีเมลแจ้งรายละเอียดปัญหา พร้อมบันทึกผลการเข้าจัดการ
ระดับ ๒ (ปานกลาง)	ภายใน ๔ ชั่วโมง	เจ้าของระบบสารสนเทศระดับคณะหรือวิทยาเขต	โทรศัพท์ประสานงานโดยตรง ร่วมกับการเปิด Incident Ticket
ระดับ ๓ (สูง)	ภายใน ๓๐ นาที	- อธิการบดี (ศาสตราจารย์ ดร.สุวัจน์) - ผู้อำนวยการสำนักวิทยบริการฯ (ผศ.สิทธิโชค) - ผู้แทน นิติกร สำนักงานนิติการ - เจ้าหน้าที่ DPO / คณะ ทำงาน PDPA - ฝ่ายสื่อสารองค์กร / กองประชาสัมพันธ์	โทรศัพท์มือถือสายตรงแบบ On-call ทันที และเรียกประชุมทีมปฏิบัติการด่วน ภายใน ๑ ชั่วโมง
ระดับ ๔ (วิกฤต)	โดยทันที	- อธิการบดีและคณะผู้บริหารมหาวิทยาลัยทั้งหมด - คณะทำงานด้านความปลอดภัยและนิติกรทุกท่าน - เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) - ผู้บริหารและเจ้าหน้าที่หน่วยงาน สกมช. และกระทรวง อว.	โทรศัพท์ด่วนเพื่อเรียกเปิดใช้แผนวิกฤตเต็มรูปแบบและเปิดระบบประชุมออนไลน์ ตลอด ๒๔ ชั่วโมง

๑๓. เป้าหมายระยะเวลาการตอบสนองภายใน (Internal Incident Response SLA)

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดเป้าหมายระยะเวลาในการดำเนินงาน (Service Level Agreement: SLA) สำหรับขั้นตอนหลักของการรับมือภัยคุกคามทางไซเบอร์ ดังตารางที่ ๙ เพื่อใช้เป็นเกณฑ์ควบคุมความเร็วในการปฏิบัติงานของทีม CIRT และเป็นดัชนีชี้วัดผลงานหลัก (KPI) ในกระบวนการทำงาน โดยเกณฑ์เวลานี้ได้รับการกำหนดให้สอดคล้องกับระดับความรุนแรงของภัยคุกคามตามข้อ ๑๒.๒ ดังต่อไปนี้

ตารางที่ ๙ เป้าหมายระยะเวลาการปฏิบัติงานภายใน (Internal SLA Matrix)

ระดับความรุนแรงของเหตุภัยคุกคาม	การรับแจ้งเหตุและออกเลขตั๋ว	การแจ้งเตือนหัวหน้าทีม/ผู้สนับสนุน	การเริ่มมาตรการจำกัดความเสียหาย	การอัปเดตและรายงานความคืบหน้า	เป้าหมายการระงับเหตุและกู้คืน
ระดับ ๑ (ต่ำ)	ภายใน ๒ ชั่วโมง	ภายใน ๒๔ ชั่วโมง	ภายใน ๔ ชั่วโมง	ทุก ๒๔ ชั่วโมง (หรือเมื่อปิดเหตุ)	ภายใน ๔๘ ชั่วโมง
ระดับ ๒ (ปานกลาง)	ภายใน ๑ ชั่วโมง	ภายใน ๔ ชั่วโมง	ภายใน ๒ ชั่วโมง	ทุก ๑๒ ชั่วโมง	ภายใน ๒๔ ชั่วโมง
ระดับ ๓ (สูง)	ภายใน ๑๕ นาที	ภายใน ๓๐ นาที	ภายใน ๑ ชั่วโมง	ทุก ๒ - ๔ ชั่วโมง	ภายใน ๑๒ ชั่วโมง(หรือตามความเหมาะสม)
ระดับ ๔ (วิกฤต)	ภายใน ๕ นาที	โดยทันที	ภายใน ๓๐ นาที	ทุก ๑ - ๒ ชั่วโมง (หรือแบบเรียลไทม์)	ขึ้นอยู่กับสถานการณ์ (ให้เน้นความปลอดภัยของข้อมูล)

๑๓.๑ การพิทักษ์เกณฑ์เวลาในการแจ้งเหตุรายงานตามกฎหมาย (Legal Compliance Priority)

มหาวิทยาลัยฯ กำหนดว่า เป้าหมายระยะเวลาตอบสนองภายใน (Internal SLA) ทั้งหมด เป็นเพียงเครื่องมือเชิงบริหารงานจัดการภายในของมหาวิทยาลัยเท่านั้น

การปฏิบัติงานตาม SLA จะต้องไม่สร้างความล่าช้า หรือส่งผลเสียต่อกรอบเวลาการรายงานเหตุภัยคุกคามทางไซเบอร์ตามกฎหมายของ สกมช. เป็นอันขาด

หากมีข้อกำหนดทางกฎหมาย ประกาศจาก สกมช. หรือกระทรวง อว. ที่กำหนดระยะเวลาการแจ้งเตือนหรือส่งแบบรายงาน (เช่น แบบ ก๒ บังคับส่งภายใน ๒๔ ชั่วโมงนับแต่ทราบเหตุที่มีนัยสำคัญ) ที่สั้นกว่าเป้าหมายที่กำหนดไว้ในตารางนี้ ให้ถือปฏิบัติตามระยะเวลาและเกณฑ์ทางกฎหมายฉบับล่าสุดเป็นหลักโดยไม่มีข้อยกเว้น

๑๓.๒ บันทึกเส้นเวลาของเหตุการณ์ที่มีการประทับเวลา (Time-stamped Incident Timeline)

ทีม CIRT และเจ้าหน้าที่ผู้ดูแลระบบงานที่เกิดเหตุ จะต้องจัดทำและบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยอย่างละเอียด (Incident Timeline) ลงในระบบหรือแบบบันทึก (ตามภาคผนวก ๓)

ทุกบันทึกกิจกรรมจะต้องมีการระบุตัวผู้ปฏิบัติงานอย่างชัดเจน และประทับเวลาที่บันทึกข้อมูล (Time-stamped) ตั้งแต่ขั้นตอนการรับแจ้งเหตุ การออกเลข Incident ID ขั้นตอนการยกระดับแจ้งผู้บังคับบัญชา วินาทีที่สั่งระงับตัดระบบ (Containment) ขั้นตอนสกัดกั้นปราบปรามมัลแวร์ วันเวลาที่ส่งแบบรายงาน ก๑/ก๒ ตลอดจนวันที่และเวลาปิดเหตุการณ์ความปลอดภัยอย่างเป็นทางการ

บันทึกประทับเวลา (Time-stamped Timeline) นี้ จะถูกรวบรวมจัดเก็บเป็นเอกสารดัชนีชี้วัดผลเพื่อใช้รองรับกระบวนการตรวจสอบและประเมินผลการรับมือภัยคุกคามไซเบอร์ของมหาวิทยาลัยฯ ในรอบปี

๑๔. การสื่อสารในภาวะวิกฤตและการประสานผู้มีส่วนได้ส่วนเสีย

มหาวิทยาลัยฯ กำหนดนโยบายและแนวทางปฏิบัติการสื่อสารในภาวะวิกฤตเพื่อลดผลกระทบด้านภาพลักษณ์ ป้องกันการตื่นตระหนก และให้ความคุ้มครองข้อมูลความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย โดยมีมาตรการดำเนินงานดังนี้

๑๔.๑ โครงสร้างและการเชื่อมโยงคณะทำงานสื่อสารในภาวะวิกฤต (Crisis Communication Integration)

กำหนดให้การดำเนินการตามแผนฉบับนี้ ต้องสอดประสานและเชื่อมโยงกับ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ในภาพรวมของมหาวิทยาลัยฯ โดยกำหนดบทบาทความรับผิดชอบไว้ดังนี้

- ผู้อนุมัติข้อความแถลงการณ์ (Approver) อธิการบดี หรือผู้บังคับบัญชาสูงสุดที่ได้รับมอบอำนาจ
- โฆษกหลักผู้ชี้แจงสถานการณ์ (Spokesperson) ผศ.ดร.ศักดิ์ชัย ตันติวิวัทน์ หรือผู้แทนจากกองประชาสัมพันธ์ที่ได้รับมอบหมายอย่างเป็นทางการ
- ผู้ประสานงานข้อมูลทางเทคนิค (Technical Advisor) หัวหน้าทีม CIRT (ผศ.สิทธิโชค อุ่นแก้ว) ทำหน้าที่ป้อนข้อมูลเทคนิคที่ได้รับการยืนยันแล้วแก่โฆษก
- ช่องทางสื่อสารฉุกเฉินสำรอง (Backup Channels) ในกรณีที่ระบบอีเมลกลางหรือเว็บไซต์ล่ม ให้ใช้ช่องทาง Social Media ทางการของมหาวิทยาลัยฯ หรือระบบโทรศัพท์สถาบันในการสื่อสาร

๑๔.๒ แนวทางและข้อกำหนดในการร่างข้อความประชาสัมพันธ์ (Message Guidelines and Restrictions)

การจัดเตรียมเนื้อหาเพื่อเผยแพร่ต่อผู้มีส่วนได้ส่วนเสียภายนอกและภายใน มหาวิทยาลัยฯ กำหนดหลักเกณฑ์ควบคุมการสื่อสารอย่างเคร่งครัด ดังนี้

- ยึดข้อเท็จจริงที่ได้รับการยืนยัน (Verified Facts) ข้อมูลที่จะเผยแพร่ต้องผ่านการลงนามยืนยันความถูกต้องจากหัวหน้าทีม CIRT และได้รับการอนุมัติจากอธิการบดีแล้วเท่านั้น
- องค์ประกอบของข้อความประชาสัมพันธ์ ข้อความต้องระบุอย่างชัดเจนใน ๕ ประเด็นสำคัญ ได้แก่ (๑) สิ่งที่ทราบแน่ชัดเกี่ยวกับเหตุการณ์ (๒) สิ่งที่ยังอยู่ระหว่างการสืบสวนตรวจสอบ (๓) ผลกระทบต่อผู้ใช้งาน (๔) มาตรการที่มหาวิทยาลัยฯ กำลังดำเนินการแก้ไข และ (๕) คำแนะนำเชิงปฏิบัติสำหรับผู้ใช้เพื่อป้องกันตัวเอง (เช่น การแนะนำเปลี่ยนรหัสผ่านทันที)
- ข้อจำกัดทางกฎหมายและความมั่นคงปลอดภัย (Security Safeguards) ห้ามเปิดเผยข้อมูลที่อาจส่งผลกระทบต่อกระบวนการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ ห้ามระบุรายละเอียดช่องโหว่ทางเทคนิคเชิงลึกที่แฮกเกอร์ใช้โจมตี และห้ามเปิดเผยข้อมูลส่วนบุคคลที่มากเกินจำเป็นเพื่อป้องกันการซ้ำเติมความเสียหาย

๑๔.๓ การประสานผู้มีส่วนได้ส่วนเสีย (Stakeholder Contact Matrix)

มหาวิทยาลัยฯ จัดทำตารางประสานข้อมูลผู้มีส่วนได้ส่วนเสียเพื่อแสดงผู้รับผิดชอบหลักและเป้าหมายระยะเวลาการประสานงานเมื่อเกิดวิกฤต แสดงดังตารางที่ ๑๐

ตารางที่ ๑๐ ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการจัดการภัยคุกคามไซเบอร์

กลุ่มผู้มีส่วนได้ส่วนเสีย	หน่วยงานรับผิดชอบการแจ้งประสาน	เป้าหมายระยะเวลาการแจ้ง (SLA)	ช่องทางสื่อสารที่กำหนด	ข้อมูลสาระสำคัญที่ต้องจัดส่ง
คณะผู้บริหารมหาวิทยาลัยฯ	หัวหน้าทีม CIRT (ผอ.สวส.)	ทันที (สำหรับเหตุระดับ ๓ และ ๔)	โทรศัพท์เคลื่อนที่สายตรง / ประชุม Conference	รายงานสถานการณ์ด่วน ระดับผลกระทบ และข้อเสนอแนะในการตัดสินใจปิดระบบ
หน่วยงานเจ้าของระบบงานที่เกิดเหตุ	เจ้าหน้าที่รับมือฯ (Incident Lead)	ภายใน ๓๐ นาที นับแต่พบเหตุ	โทรศัพท์ประสานงานตรง / อีเมล / Ticket	ข้อมูลความผิดปกติเชิงเทคนิค และคำสั่งปิดกั้นระบบชั่วคราวเพื่อกักกันภัย
บุคลากร และนักศึกษา (ผู้ใช้งาน)	ผู้รับผิดชอบด้านสื่อสารองค์กร (PR)	ภายใน ๒ ชั่วโมง (หลังได้รับการอนุมัติ)	Page Facebook และ เว็บไซต์หลักของ สำนักวิทยะฯ/มหาวิทยาลัยฯ	คำชี้แจงผลกระทบการงดให้บริการชั่วคราว และคำแนะนำขั้นตอนการปฏิบัติตนที่ปลอดภัย
ผู้ให้บริการภายนอก / คู่สัญญาไอที	เจ้าหน้าที่เทคนิคในทีม CIRT	ภายใน ๑ ชั่วโมง	โทรศัพท์ประสานสายด่วน / อีเมลเทคนิคกลาง	ข้อมูล Log บันทึกความผิดปกติเพื่อขอรับการช่วยเหลือและตรวจสอบอุปกรณ์
สกมช. / Thai-CERT	ผู้แทน นิติกร สำนักงานนิติการ	ภายใน ๒๔ ชั่วโมง (กรณีภัยมีนัยสำคัญ)	แบบรายงาน ก๑ / ก๒ ผ่านระบบออนไลน์หรืออีเมล	เอกสารรายงานเหตุภัยคุกคามทางไซเบอร์ตาม พ.ร.บ. ไซเบอร์ฯ (ตามภาคผนวก ๔)

กลุ่มผู้มีส่วนได้ส่วนเสีย	หน่วยงานรับผิดชอบการแจ้งประสาน	เป้าหมายระยะเวลาการแจ้ง (SLA)	ช่องทางสื่อสารที่กำหนด	ข้อมูลสาระสำคัญที่ต้องจัดส่ง
หน่วยงานบังคับใช้กฎหมาย	ผู้แทน นิติกร สำนักงานนิติการ	ภายใน ๔๘ ชั่วโมง (หากต้องดำเนินคดี)	เอกสารหนังสือราชการนำส่งผู้กำกับสถานีตำรวจ	ข้อมูลพยานหลักฐานดิจิทัล รายงานสถิติ และ เอกสารห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody)

๑๔.๔ การประสานงานร่วมกับฝ่ายคุ้มครองข้อมูลส่วนบุคคล (PDPA/DPO Coordination)

กรณีที่เหตุภัยคุกคามทางไซเบอร์เกี่ยวข้องหรืออาจส่งผลกระทบต่อ ข้อมูลที่ระบุตัวบุคคลได้ (Personal Identifiable Information: PII) ทีม CIRT จะต้องทำการส่งต่อเรื่องและประสานงานร่วมกับ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หรือคณะทำงานด้าน PDPA ของมหาวิทยาลัยฯ โดยทันที

- แจ้งรายงานตาม พ.ร.บ. ไซเบอร์ฯ โดยการจัดทำแบบรายงาน ก๒ ส่งให้ สกมช. ภายใน ๒๔ ชั่วโมง (ความรับผิดชอบของทีม CIRT และทีมกฎหมาย)
- รายงานเหตุละเมิดข้อมูลส่วนบุคคลตามกฎหมาย PDPA โดยการประเมินความเสี่ยงที่มีต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หากพบว่ามีความเสี่ยงสูง จะต้องดำเนินการจัดทำรายงานแจ้งเหตุละเมิดข้อมูลส่วนบุคคลส่งต่อ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ และแจ้งเยียวยาเจ้าของข้อมูลที่ได้รับผลกระทบด้วย

๑๕. การเชื่อมโยงกับ BCP/DR และการกู้คืนบริการ (Business Continuity and Disaster Recovery Integration)

มหาวิทยาลัยฯ กำหนดให้กระบวนการกู้คืนระบบสารสนเทศหลังเกิดเหตุภัยคุกคามทางไซเบอร์ ต้องประสานเป็นหนึ่งเดียวกับแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) และแผนกู้คืนระบบคอมพิวเตอร์จากภัยพิบัติ (Disaster Recovery Plan: DRP) ของมหาวิทยาลัยฯ เพื่อให้การฟื้นฟูระบบเป็นไปอย่างปลอดภัยและลดความสูญเสียให้ได้มากที่สุด โดยปฏิบัติตามแนวทางดังต่อไปนี้

๑๕.๑ การอ้างอิงเกณฑ์การวิเคราะห์ผลกระทบทางธุรกิจ (BIA, BCP and DR Plan Alignment)

กระบวนการกู้คืนและนำระบบสารสนเทศกลับมาเปิดให้บริการ จะต้องอ้างอิงตามผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) แผน BCP และแผน DR ของบริการไอทีนั้น ๆ โดยตรง

การบริหารเวลาและข้อมูลสูญหายสูงสุด ทีม CIRT และผู้ดูแลระบบงานที่ได้รับผลกระทบ ต้องพิจารณาเป้าหมายตัวชี้วัดที่ได้รับอนุมัติจากคณะผู้บริหารมหาวิทยาลัยฯ ได้แก่

- ระยะเวลาหยุดชะงักสูงสุดที่ยอมรับได้ (Maximum Tolerable Period of Disruption: MTPD): เพื่อไม่ให้ระบบหยุดทำงานนานเกินกว่าขีดความสามารถที่มหาวิทยาลัยฯ จะแบกรับได้
- เป้าหมายระยะเวลากู้คืนระบบ (Recovery Time Objective: RTO): กำหนดกรอบเวลาที่ต้องกู้ระบบให้กลับมาใช้งานได้ตามปกติ
- เป้าหมายจุดกู้คืนข้อมูล (Recovery Point Objective: RPO): กำหนดปริมาณข้อมูลสูญหายสูงสุดที่ยอมรับได้ เพื่อเลือกชุดข้อมูลสำรอง (Backup Data) ในการนำกลับมา Restore ได้อย่างถูกต้อง

กลไกการยกระดับเข้าสู่แผน BCP/DR ในกรณีที่เหตุภัยคุกคามทางไซเบอร์มีความรุนแรงสูงจนระบบล่มเป็นวงกว้าง และทีม CIRT คาดการณ์ว่าไม่สามารถระงับเหตุหรือกู้ระบบคืนมาได้ภายในกรอบเวลา RTO/MTPD ปกติ หัวหน้าทีม CIRT จะต้องประสานงานแจ้งอธิการบดีทันที เพื่อสั่งการเปิดใช้งานแผน BCP และแผนกู้คืนภัยพิบัติ (DR Plan) ของมหาวิทยาลัยฯ ในภาพรวม เพื่อสลับไปใช้ระบบสำรองหรือไซต์สำรอง (DR Site) หรือเปลี่ยนไปใช้วิธีการปฏิบัติงานแบบแมนนวล (Manual Process) ทดแทนชั่วคราว

๑๕.๒ เกณฑ์ความปลอดภัยขั้นสูงสุดก่อนนำระบบกลับมาเปิดให้บริการ (Sanitized Recovery Criteria)

การป้องกันไม่ให้ระบบที่กู้คืนกลับมาถูกแฮกซ้ำจากช่องทางเดิม มหาวิทยาลัยฯ กำหนดว่าก่อนที่จะนำระบบคอมพิวเตอร์หรือซอฟต์แวร์ประยุกต์ใด ๆ กลับมาเปิดใช้งานตามปกติ (Go-Live) จะต้องผ่านกระบวนการตรวจสอบและได้รับการอนุมัติอย่างเป็นทางการ โดยมีขั้นตอนการทดสอบ (Checklist) ดังนี้

- การตรวจสอบความสะอาดปลอดภัย (System Cleansing Verification) ทดสอบสแกนหาช่องโหว่ (Vulnerability Scanning) และสแกนหามัลแวร์ รหัส Backdoor หรือสิ่งบ่งชี้การบุกรุก (Indicators of Compromise: IoC) ในสภาพแวดล้อมจำลอง (Sandbox) ก่อนที่จะนำข้อมูลสำรอง (Backup) มาทำการกู้คืน (Restore)
- การปิดช่องโหว่ทางเทคนิค (Vulnerability Patching) ดำเนินการอัปเดตระบบปฏิบัติการ ซอฟต์แวร์ และแอปพลิเคชันให้เป็นเวอร์ชันล่าสุด พร้อมติดตั้ง Patch ความปลอดภัยเพื่ออุดช่องโหว่ที่เป็นต้นเหตุของเหตุการณ์
- การเปลี่ยนข้อมูลรับรองความปลอดภัย (Credential Reset) บังคับเปลี่ยนรหัสผ่าน (Password Reset) ของทุกบัญชีผู้ใช้งาน โดยเฉพาะอย่างยิ่งบัญชีผู้ดูแลระบบ (Domain Admin / Application

Admin) รวมถึงการยกเลิกสิทธิ์กุญแจเข้ารหัส API Key และสิทธิ์ในการเข้าถึง (Access Rights) ที่ลักลอบสร้างขึ้นใหม่โดยไม่ได้รับอนุญาต

- การทดสอบการทำงานและความมั่นคงปลอดภัย (Security Testing) ทดสอบฟังก์ชันการทำงานขั้นพื้นฐาน ตรวจสอบบันทึก Log และทดสอบเจาะระบบเฉพาะจุด (Penetration Testing) เพื่อยืนยันว่าไม่มีสิทธิ์แอบแฝงหลงเหลืออยู่
- การอนุมัติอย่างเป็นทางการ (Formal Sign-off) เจ้าหน้าที่รับมือฯ และผู้ดูแลระบบงานที่เกิดเหตุต้องลงนามสรุปผลการทดสอบความปลอดภัยเพื่อเสนอขออนุมัติเปิดระบบจริงต่อ ผู้อำนวยการสำนักวิทยบริการฯ หรือผู้รับผิดชอบระบบนั้น ๆ เสมอ

๑๕.๓ มาตรการเฝ้าระวังและติดตามสถานการณ์เป็นพิเศษหลังการกู้คืน (Enhanced Post-Restore Monitoring)

ภายหลังจากการกู้ระบบและเปิดบริการใหม่ (Restore) ทีมปฏิบัติการเทคนิค (Technical Lead) จะต้องเปิดระบบเฝ้าระวังภัยคุกคามเป็นพิเศษ (Enhanced Monitoring) ต่อระบบดังกล่าวอย่างต่อเนื่องเป็นระยะเวลาอย่างน้อย ๑๔ ถึง ๓๐ วัน

การเฝ้าระวังจะเน้นการเฝ้าตรวจระบบตรวจจับและวิเคราะห์ เช่น การกรอง Log ผ่านระบบ SIEM การสังเกตการณ์ผ่าน Endpoint Detection and Response (EDR) และการสแกนหา IoC เดิม เพื่อยืนยันให้มั่นใจ ๑๐๐% ว่าผู้โจมตีหรือแฮกเกอร์ไม่ได้ลักลอบกลับเข้ามาในเครือข่ายของมหาวิทยาลัยฯ อีกครั้ง ผ่านช่องทางที่ตกสำรวจ

๑๕.๔ การประเมินเพื่อปรับปรุงและถอดบทเรียน BCP/DR (Post-Recovery Feedback Loop)

ทุกครั้งหลังเสร็จสิ้นกระบวนการกู้คืนระบบไอที ทีม CIRT และเจ้าของระบบสารสนเทศ จะต้องร่วมกันลงบันทึกข้อมูลผลลัพธ์การทำงานจริง ได้แก่

- ระยะเวลากู้คืนระบบที่ใช้จริง (Actual Recovery Time: ART) ระยะเวลาตั้งแต่ระบบเริ่มเกิดเหตุขัดข้องจนกู้คืนกลับมา Go-Live สำเร็จ
- ปริมาณข้อมูลสูญหายที่เกิดขึ้นจริง (Actual Data Loss: ADL) ระยะห่างของช่วงเวลาข้อมูลล่าสุดที่มีและสามารถกู้กลับคืนมาได้

นำข้อมูล ART และ ADL ที่วัดได้จริง ไปทำการเปรียบเทียบกับเป้าหมาย RTO และ RPO ที่มหาวิทยาลัยฯ กำหนดไว้ เพื่อวิเคราะห์หาช่องว่างข้อจำกัด (Performance Gap)

สรุปผลการวิเคราะห์และข้อเสนอแนะเชิงป้องกัน ส่งมอบให้แก่ผู้อำนวยการสำนักงานอธิการบดี (งานประกันคุณภาพการศึกษา) ในฐานะผู้บริหารจัดการความเสี่ยง เพื่อนำข้อมูลไปปรับปรุง พัฒนาประสิทธิภาพแผน BCP และแผน DR ของมหาวิทยาลัยฯ ให้มีความพร้อมและตอบสนองได้รวดเร็วยิ่งขึ้นในการซ้อมแผนปีถัดไป

๑๖. คู่มือรับมือเหตุเฉพาะประเภท (Incident Playbooks)

เพื่อให้ทีมปฏิบัติการรับมือภัยคุกคามไซเบอร์ (CIRT) และผู้ดูแลระบบคอมพิวเตอร์ สามารถดำเนินขั้นตอนตอบสนอง ระงับเหตุ และกู้คืนระบบได้อย่างรวดเร็ว ถูกต้อง และเป็นมาตรฐานเดียวกัน มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย จึงกำหนดรายชื่อคู่มือรับมือเหตุเฉพาะประเภท โครงสร้างของคู่มือ และคู่มือปฏิบัติการต้นแบบสำหรับการเผชิญเหตุวิกฤต ดังต่อไปนี้

๑๖.๑ รายชื่อคู่มือรับมือเหตุเฉพาะประเภท (Playbook Catalog)

- คู่มือภัยมัลแวร์เรียกค่าไถ่ (Ransomware Playbook)
- คู่มือการแพร่ระบาดของมัลแวร์ในระบบเครือข่าย (Malware Outbreak Playbook)
- คู่มือภัยวิศวกรรมสังคมและการลักลอบสวมรอยอีเมล (Phishing / Business Email Compromise Playbook)
- คู่มือการละเมิดบัญชีผู้ใช้งานและสิทธิระดับสูง (Account / Privilege Compromise Playbook)
- คู่มือเหตุข้อมูลรั่วไหลและการโจรกรรมข้อมูล (Data Breach / Data Exfiltration Playbook)
- คู่มือการโจมตีเพื่อปฏิเสธการให้บริการ (DDoS Playbook)
- คู่มือการลักลอบแก้ไขหน้าเว็บไซต์มหาวิทยาลัย (Web Defacement Playbook)
- คู่มือการโจมตีช่องโหว่ของระบบสารสนเทศสำคัญ (Vulnerability Exploitation Playbook)
- คู่มือภัยคุกคามจากระบบคลาวด์และผู้ให้บริการภายนอก (Cloud / Third-Party Incident Playbook)

๑๖.๒ โครงสร้างมาตรฐานของคู่มือเผชิญเหตุ (Standard Playbook Template)

คู่มือรับมือภัยคุกคามไซเบอร์ทุกประเภทของมหาวิทยาลัยฯ จะต้องถูกจัดทำขึ้นภายใต้โครงสร้างมาตรฐานเดียวกัน เพื่อป้องกันความสับสน โดยประกอบด้วยหัวข้อสำคัญ ๘ ส่วน ดังนี้

- เงื่อนไขการเปิดใช้งาน (Trigger Criteria): สัญญาณบ่งชี้เหตุคุกคาม (Indicators of Compromise: IoC) ที่ตรวจจับได้จากอุปกรณ์ SIEM หรือระบบ Endpoint เพื่อสั่งเปิดใช้คู่มือ
- รายการหลักฐานทางดิจิทัลที่ต้องจัดเก็บ (Evidence to Collect): รายชื่อ Log หรือพยานหลักฐานดิจิทัลที่ต้องรีบสำรองข้อมูลเก็บไว้
- ขั้นตอนการควบคุมจำกัดความเสียหาย (Containment Steps): มาตรการและวิธีทางเทคนิคเพื่อหยุดยั้งไม่ให้ความเสียหายกระจายตัว
- ขั้นตอนการกำจัดสาเหตุ (Eradication Steps): การอุดช่องโหว่ การถอนรากถอนโคนโปรแกรมประสงค์ร้าย และการเปลี่ยนข้อมูลสิทธิ์เข้าใช้งาน

- ขั้นตอนการฟื้นฟูระบบและเปิดบริการ (Recovery Steps): วิธีการนำระบบกลับมาใช้งานอย่างปลอดภัยและตรวจสอบความบริสุทธิ์ของข้อมูล
- ผู้มีอำนาจและจุดตัดสินใจ (Decision Points and Approver): ตัวบุคคลหลักและตัวสำรองตามตารางอำนาจภาวะฉุกเฉินในการดำเนินมาตรการสำคัญ
- การรายงานและการสื่อสาร (Reporting and Communication): สายงานรายงานภายในและการจัดทำรายงาน ก๑/ก๒ เพื่อส่งต่อ สกมช.
- เกณฑ์การปิดเหตุการณ์ (Closure Criteria): เงื่อนไขการประเมินว่าภัยคุกคามสิ้นสุดแล้วจริง ๆ เพื่อสรุปถอดบทเรียนหลังเหตุการณ์

๑๗. การจัดการหลักฐานและนิติวิทยาศาสตร์ดิจิทัลเพิ่มเติม

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดมาตรฐานการปฏิบัติงานและมาตรการควบคุมการจัดการพยานหลักฐานดิจิทัล (Digital Evidence) เพื่อให้พยานหลักฐานคงสภาพความสมบูรณ์ ไม่ถูกเปลี่ยนแปลงหรือถูกทำลายในระหว่างขั้นตอนการระงับเหตุ และสามารถใช้สนับสนุนกระบวนการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ตลอดจนใช้เป็นพยานหลักฐานที่ยอมรับได้ในชั้นศาลตามกฎหมาย โดยมีแนวทางปฏิบัติทางเทคนิคดังต่อไปนี้

๑๗.๑ ให้ใช้ Chain of Custody ทุกครั้งที่มีการยึด รับ ส่ง ทำสำเนา วิเคราะห์ หรือเคลื่อนย้ายหลักฐาน และบันทึกผู้ดำเนินการ วันเวลา สถานที่ วัตถุประสงค์ และค่า Hash

๑๗.๒ ให้จัดลำดับการเก็บข้อมูลตามความผันผวน (Order of Volatility) และหลีกเลี่ยงการกระทำที่เปลี่ยนแปลงหลักฐานโดยไม่จำเป็น

๑๗.๓ หลักฐานต้องเก็บในพื้นที่ที่ควบคุมสิทธิ์ มีบันทึกการเข้าถึง และกำหนดระยะเวลาการเก็บตามกฎหมาย ระเบียบ และความจำเป็นของคดี

๑๗.๔ การใช้เครื่องมือหรือผู้เชี่ยวชาญภายนอกต้องมีขอบเขตงาน การรักษาความลับ การส่งมอบหลักฐาน และข้อกำหนดด้าน Chain of Custody ที่ชัดเจน

๑๘. การฝึกซ้อม การทดสอบ และการสร้างความพร้อม

๑๘.๑ ความถี่และเงื่อนไขในการจัดการฝึกซ้อม (Exercise Frequency and Triggers)

มหาวิทยาลัยฯ กำหนดให้มีการฝึกซ้อมแผนรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง นอกจากการซ้อมแผนตามรอบวงรอบประจำปีแล้ว มหาวิทยาลัยฯ กำหนดให้ต้องจัดการฝึกซ้อมเพิ่มเติมทันทีเมื่อเกิดกรณีหรือเงื่อนไขสำคัญ ดังต่อไปนี้

- การเปลี่ยนแปลงระบบสารสนเทศสำคัญ (Major System Change) มีการเปลี่ยนแปลงโครงสร้างสถาปัตยกรรมระบบเครือข่ายหลักหรือระบบบริการสำคัญ เช่น การโยกย้ายฐานข้อมูลหลักไปสู่ระบบคลาวด์ (Cloud Migration) หรือการเปลี่ยนระบบบริหารจัดการ Active Directory
- การปรับปรุงโครงสร้างทีม (CIRT Restructuring) มีการปรับเปลี่ยนบทบาท โครงสร้าง หรือผู้ดำรงตำแหน่งหลักในทีม CIRT (ตามข้อ ๙.๒) มากกว่าร้อยละ ๕๐ ของทีม
- การเปิดให้บริการระบบงานใหม่ (New Core Service) มีการประกาศเปิดตัวระบบงานหรือช่องทางการให้บริการสารสนเทศใหม่ระดับองค์กรที่มีผลกระทบสูงต่อข้อมูลส่วนบุคคล

๑๘.๒ รูปแบบและวิธีการฝึกซ้อมเพื่อสร้างความพร้อม (Exercise Methodology and Formats)

เพื่อทดสอบขีดความสามารถรอบด้าน มหาวิทยาลัยฯ กำหนดให้เลือกใช้หรือผสมผสานรูปแบบการฝึกซ้อมอย่างน้อย ๔ รูปแบบหลัก ดังนี้

- การฝึกซ้อมบนโต๊ะจำลองสถานการณ์ (Tabletop Exercise - TTX) เป็นการประชุมอภิปรายโดยจำลองเหตุการณ์ภัยคุกคามไซเบอร์ (Scenario-based Discussion) เพื่อให้ผู้มีสิทธิ์ตัดสินใจและผู้แทนฝ่ายต่างๆ ได้ร่วมทดสอบขั้นตอนประสานงาน สายการรายงาน (Escalation Path) และการตัดสินใจตามกรอบเวลา (SLA) โดยเน้นความเข้าใจในบทบาทหน้าที่และข้อกฎหมาย
- การซ้อมเชิงเทคนิคจำลองเหตุการณ์จริง (Technical Simulation) เป็นการทดสอบภาคปฏิบัติของทีมเทคนิค (Technical Lead/System Admin) โดยอาจจัดทำการซ้อมในรูปแบบ Red-Blue Team (ทีมรุกและทีมรับ) เพื่อทดสอบประสิทธิภาพของเครื่องมือ ระบบป้องกันความปลอดภัย และระบบวิเคราะห์ Log/SIEM ในการตรวจจับและระงับภัยคุกคามเฉพาะหน้าทางเทคนิค
- การซ้อมสื่อสารและประสานงานในภาวะวิกฤต (Communication Exercise) จำลองการส่งรายงานข้อมูลแจ้งเหตุตามกฎหมาย เช่น การจำลองเขียนและส่งแบบรายงาน ก๑ และ ก๒ ให้แก่ สกมช. ภายใน ๒๔ ชั่วโมง รวมถึงการซ้อมร่างข้อความประชาสัมพันธ์เพื่อชี้แจงต่อนักศึกษา บุคลากร และสื่อมวลชนอย่างเหมาะสมโดยทีมประชาสัมพันธ์
- การทดสอบแผนร่วมกับแผนฟื้นฟูภัยพิบัติ (Joint BCP/DR and Cyber Drill) ดำเนินการทดสอบร่วมกับแผนการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) และแผนกู้คืนระบบคอมพิวเตอร์จากภัยพิบัติ

(DRP) ของมหาวิทยาลัยฯ เพื่อซ้อมขั้นตอนการ Restore ข้อมูลจากระบบ Backup ในสภาวะเครือข่ายล่ม หรือการสลับไปทำงานผ่านสิทธิสำรอง/ระบบแมนนวลจริง

๑๘.๓ ผู้ที่ระบุในแผน รวมถึงผู้บริหาร เจ้าของระบบ ทีมเทคนิค ทีมสื่อสาร กฎหมาย/PDPA และผู้ให้บริการสำคัญควรมีส่วนร่วมตามสถานการณ์จำลอง

๑๘.๔ กระบวนการประเมินผลและการจัดทำรายงาน AAR (After Action Review and Corrective Actions)

หลังเสร็จสิ้นกิจกรรมการฝึกซ้อมทุกครั้ง ทีม CIRT จะต้องปิดวงจรการประเมินผลตามขั้นตอนเพื่อนำไปปรับปรุงระบบอย่างแท้จริง ดังต่อไปนี้

การประชุมสรุปผลทันที (Hot Debrief) จัดประชุมสั้น ๆ ร่วมกับผู้เข้าร่วมซ้อมแผนทุกคนทันทีหลังการฝึกซ้อมสิ้นสุดลง เพื่อแลกเปลี่ยนความเห็นและข้อสังเกตเบื้องต้น

การจัดทำรายงานสรุปผลการซ้อมแผน (After Action Report: AAR) ทีม CIRT ต้องรวบรวมข้อมูลและจัดทำรายงาน AAR ภายในระยะเวลา ๑๔ วันหลังเสร็จสิ้นการซ้อมแผน โดยรายงานต้องระบุหัวข้อหลักดังนี้

- ข้อมูลสรุปของรูปแบบการซ้อม และสถานการณ์จำลอง (Scenario)
- ดัชนีชี้วัดที่วัดผลได้ เช่น เวลาแจ้งรายงาน (SLA) และความถูกต้องของการตรวจพบ
- ข้อค้นพบ (Key Findings) และช่องว่างในการทำงาน (Gaps) เช่น ข้อจำกัดทางเทคโนโลยี หรือจุดขัดข้องในการสื่อสารประสานงาน
- รายการข้อเสนอแนะทางนโยบายเพื่อปรับปรุงแก้ไข

การกำหนดมาตรการแก้ไขและติดตามผล (Corrective Action Tracking) ข้อบกพร่องที่พบในรายงาน AAR จะต้องถูกแปลงให้อยู่ในรูปแบบงานที่ต้องแก้ไข โดยต้องระบุรายละเอียด ประกอบด้วย

- ผู้รับผิดชอบการแก้ไขปัญหา (Action Owner): ระบุชื่อเจ้าหน้าที่หรือตำแหน่งรับผิดชอบชัดเจน
- กำหนดวันแล้วเสร็จ (Target Date): กำหนดเวลาการปรับปรุงแก้ไขอย่างสมเหตุสมผล
- หลักฐานการปิดประเด็น (Verification Evidence): มีขั้นตอนการตรวจสอบและติดตามผลงานโดยผู้ตรวจสอบความปลอดภัย (Auditor) เพื่ออนุมัติปิดประเด็นอย่างเป็นทางการ

๑๙. การทบทวนหลังเหตุและการปรับปรุงอย่างต่อเนื่อง

มหาวิทยาลัยฯ กำหนดให้กระบวนการเรียนรู้และถอดบทเรียนจากเหตุการณ์จริงเป็นกลไกสำคัญในการปิดช่องโหว่และยกระดับความมั่นคงปลอดภัยทางไซเบอร์อย่างยั่งยืน โดยเมื่อการสกัดกั้นภัยคุกคามเสร็จสิ้นและระบบบริการกลับคืนสู่สภาวะปกติที่มีเสถียรภาพแล้ว ให้ทีม CIRT และผู้เกี่ยวข้องดำเนินการตามมาตรการดังต่อไปนี้

๑๙.๑ การประชุมถอดบทเรียนหลังเกิดเหตุการณ์ (Lessons Learned Meeting)

ภัยคุกคามที่มีระดับความรุนแรงภายในระดับสูง หรือระดับวิกฤต (เทียบเท่าระดับร้ายแรงและระดับวิกฤตตามกฎหมาย สกมช.) ทีม CIRT จะต้องจัดประชุมถอดบทเรียน (Lessons Learned Meeting) หรือกระบวนการทบทวนหลังการปฏิบัติงาน (After-Action Review: AAR) ภายในระยะเวลา ๑๔ วันทำการ นับแต่วันที่ปิดเหตุการณ์ความมั่นคงปลอดภัยอย่างเป็นทางการ ที่ประชุมจะต้องวิเคราะห์สถานการณ์เพื่อค้นหาช่องว่างในการทำงาน โดยครอบคลุม ๕ ช่องว่างสำคัญ (๕ Gaps Assessment) ดังนี้

- ช่องว่างด้านสาเหตุที่แท้จริง (Root Cause Gap) ร่วมกันสืบค้นและวิเคราะห์เชิงลึกว่าผู้โจมตีบุกรุกเข้าสู่ระบบผ่านช่องทางใด ช่องโหว่ทางเทคนิคใดที่ถูกใช้งาน และแฮกเกอร์สามารถหลบเลี่ยงมาตรการป้องกันเดิมของมหาวิทยาลัยฯ ได้อย่างไร
- ช่องว่างด้านการตรวจจับ (Detection Gap) ประเมินว่าระบบป้องกันและเฝ้าระวัง เช่น ระบบ SIEM หรือ Anti-Malware สามารถตรวจจับสัญญาณแจ้งเตือน (Alert/Log) ได้รวดเร็วเพียงใด และเหตุใดจึงไม่สามารถตรวจพบได้ตั้งแต่ระยะเริ่มต้นของการโจมตี
- ช่องว่างด้านมาตรการควบคุมและระงับเหตุ (Control Gap) ทบทวนว่าเครื่องมือ ขั้นตอนทางปฏิบัติ และระบบกักกันภัยคุกคาม (Containment) ที่เลือกใช้ มีประสิทธิภาพและจำกัดวงความเสียหายได้ทันตามเกณฑ์เวลา SLA ภายในหรือไม่
- ช่องว่างด้านการสื่อสารและการประสานงาน (Communication Gap) ประเมินความราบรื่นในการติดต่อสื่อสารภายในทีม CIRT, การประสานงานกับผู้บริหาร, การประสานผู้มีส่วนได้ส่วนเสียภายนอก (สกมช. Thai-CERT และผู้ให้บริการ) และการชี้แจงประชาสัมพันธ์แก่ผู้ใช้งาน
- ช่องว่างด้านการกู้คืนระบบ (Recovery Gap) วิเคราะห์อุปสรรคและปัญหาทางเทคนิคในระหว่างกระบวนการติดตั้งและ Restore ข้อมูลกลับคืนสู่บริการจริง รวมถึงประเมินว่าระยะเวลากู้คืนที่ใช้จริงมีความล่าช้ากว่าเป้าหมาย RTO/RPO หรือไม่

๑๙.๒ ให้จัดทำ Corrective and Preventive Action (CAPA) พร้อมผู้รับผิดชอบ ระดับความสำคัญ วันครบกำหนด และหลักฐานการปิดประเด็น

๑๙.๓ การปรับปรุงแผนและมาตรการป้องกันเชิงรุกอย่างต่อเนื่อง (Continuous Improvement and Integration)

มหาวิทยาลัยฯ กำหนดกลไกสะท้อนกลับ (Feedback Loop) เพื่อนำข้อมูลอินพุตจากหลายช่องทางมาสอดรับและปรับปรุงประสิทธิภาพความปลอดภัยในภาพรวมอย่างสม่ำเสมอ โดยดำเนินกิจกรรมดังนี้

แหล่งข้อมูลในการประสานปรับปรุง: กำหนดให้นำผลลัพธ์ที่ได้จากการเผชิญเหตุจริง รายงานสรุปผลการฝึกซ้อมแผนประจำปี (AAR) รายงานผลการตรวจสอบและตรวจประเมินความเสี่ยงไซเบอร์ประจำปี ข้อมูลการสแกนตรวจหาช่องโหว่ของระบบสารสนเทศ และข้อมูลข่าวสารเตือนภัยคุกคามใหม่ ๆ (Threat Intelligence) มาร่วมวิเคราะห์อย่างเป็นระบบ

ขอบเขตการดำเนินการปรับปรุง ให้นำข้อมูลวิเคราะห์ข้างต้นไปประสานเพื่อปรับปรุงพิทักษ์ความปลอดภัยในมิติต่าง ๆ ประกอบด้วย

- การทบทวนและแก้ไขเนื้อหาของ แผนรับมือเหตุภัยคุกคามฯ (Incident Response Plan) และคู่มือเผชิญเหตุเฉพาะประเภท (Playbooks) ให้ทันสมัยและสอดรับกับเทคโนโลยีปัจจุบัน
- การปรับแต่งและปรับปรุงประสิทธิภาพเกณฑ์การวิเคราะห์ของ ระบบ SIEM หรือบันทึกสัญญาณบ่งชี้ของระบบป้องกันมัลแวร์ (EDR Agents) เพื่อเพิ่มประสิทธิภาพและสปีดในการดักจับภัยคุกคาม
- การปรับปรุงหรือจัดหาเครื่องมือและมาตรการป้องกันความปลอดภัยเชิงรุกเพิ่มเติมของมหาวิทยาลัยฯ
- การนำกรณีศึกษาหรือเหตุการณ์จริงที่เกิดขึ้น มาใช้ออกแบบและพัฒนาหลักสูตร การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านภัยไซเบอร์ (Security Awareness Training) ให้แก่บุคลากรและนักศึกษาอย่างตรงจุดเพื่อลดความเสี่ยงจากภัยคุกคามประเภทวิศวกรรมสังคม (Phishing)

การทำรายงานสถิติเสนอผู้บริหาร โดยทีม CIRT จะรวบรวมข้อมูลสถานการณ์และผลลัพธ์การแก้ไขเหตุการณ์ในภาพรวม มาจัดทำรายงานสถิติภัยคุกคามทางไซเบอร์เป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อคณะผู้บริหารที่มีหน้าที่ดูแลและรับผิดชอบภายในมหาวิทยาลัยฯ เพื่อใช้ประกอบการกำหนดนโยบายและแนวทางการจัดการงบประมาณป้องกันความปลอดภัยต่อไป

๒๐. ตัวชี้วัดและหลักฐานสำหรับการตรวจประเมิน

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดให้มีการรวบรวมตัวชี้วัดและจัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์อย่างเป็นระบบ เพื่อใช้ประเมินประสิทธิภาพการทำงานของทีม CIRT และใช้เป็นหลักฐานแสดงความสอดคล้องตามเกณฑ์การตรวจประเมินความมั่นคงปลอดภัยไซเบอร์ประจำปีของ สกมช. โดยมีรายละเอียดการดำเนินงานดังนี้

๒๐.๑ ตัวชี้วัดประสิทธิภาพการจัดการเหตุการณ์ความมั่นคงปลอดภัย (Incident Response Key Performance Indicators)

ทีม CIRT จะต้องทำการรวบรวมข้อมูลสถานการณ์จริงเพื่อนำมาคำนวณและประเมินผลตัวชี้วัดขั้นต่ำเป็นประจำทุกปี ดังต่อไปนี้

- สถิติจำนวนเหตุการณ์สะสม (Incident Volume) จำนวนเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจริงทั้งหมดในรอบปี โดยทำการจำแนกและจัดกลุ่มตามประเภทของภัยคุกคาม และจำแนกตามระดับความรุนแรงของภัยคุกคาม
- ระยะเวลาเฉลี่ยในการตรวจพบ (Mean Time to Detect: MTTD) ค่าเฉลี่ยของเวลาตั้งแต่วินาทีที่ระบบหรือบุคลากรเริ่มได้รับผลกระทบจากภัยคุกคาม จนถึงวินาทีที่ทีม CIRT ได้รับแจ้งเหตุและออกเลขตั๋วบันทึก (Incident ID)
- ระยะเวลาเฉลี่ยในการระงับเหตุ (Mean Time to Respond/Contain: MTTR/MTTC) ค่าเฉลี่ยของเวลาตั้งแต่ทีม CIRT เริ่มกระบวนการตรวจสอบจนกระทั่งสามารถดำเนินมาตรการกักกันควบคุมวงความเสียหาย (Containment) ได้สำเร็จ
- ระยะเวลาในการฟื้นคืนบริการ (Mean Time to Recover) ระยะเวลาเฉลี่ยที่ใช้ในการทำความสะอาดระบบ ตรวจสแกนช่องโหว่ และนำระบบหรือข้อมูลสำรองกลับมาเปิดให้บริการจริงตามปกติ (Go-Live)
- สถิติอัตราการเกิดเหตุซ้ำ (Incident Recurrence Rate) จำนวนครั้งของเหตุภัยคุกคามที่เกิดขึ้นซ้ำในระบบเดิม หรือจากช่องโหว่ลักษณะเดิมภายหลังการแก้ไขเสร็จสิ้น
- สัดส่วนการแจ้งเหตุตาม SLA กฎหมาย (SLA Compliance Rate) อัตราร้อยละของเหตุการณ์ภัยคุกคามที่มีนัยสำคัญที่ทีมงานสามารถจัดทำและจัดส่งแบบรายงาน ก๑ หรือ ก๒ ให้แก่ สกมช. ได้สำเร็จภายในกรอบเวลา ๒๔ ชั่วโมงที่กฎหมายกำหนด
- สถานะการจัดการตามตาราง CAPA (CAPA Resolution Rate) สัดส่วนเปรียบเทียบระหว่างรายการมาตรการแก้ไขป้องกัน (CAPA) ที่ได้รับการอนุมัติปิดประเด็นสำเร็จ กับรายการ CAPA ทั้งหมดที่ยังค้างดำเนินการ
- ผลประเมินการฝึกซ้อมแผนประจำปี (Exercise Evaluation) คะแนนสรุปผลการประเมินการตอบสนองและอุปสรรคที่พบจากรายงาน After Action Report (AAR) ของการฝึกซ้อมแผนรับมือประจำปี

๒๐.๒ ดัชนีความเชื่อมโยงเอกสารและพยานหลักฐาน (Evidence Index Matrix)

เพื่ออำนวยความสะดวกแก่ผู้ตรวจประเมินภายในและผู้ตรวจสอบอิสระจากภายนอก มหาวิทยาลัยฯ กำหนดตารางดัชนีความเชื่อมโยงข้อกำหนดของแผนเข้ากับเอกสารหลักฐานเชิงประจักษ์ (Evidence Index) แสดงดังตารางที่ ๑๑

ตารางที่ ๑๑ ดัชนีความเชื่อมโยงข้อกำหนดของแผน

ลำดับ	กิจกรรม / ข้อกำหนดในแผนงาน	รายการพยานเอกสารและหลักฐานทางเทคนิคที่ต้องจัดเก็บเพื่อการตรวจสอบ (Evidence Document)
๑	การรับแจ้งเหตุและการคัดกรอง	- ตั๋วบันทึกการรับแจ้งเหตุการณ์ (Incident Ticket) - ข้อมูลการแจ้งเตือนจากระบบตรวจจับความปลอดภัยและอุปกรณ์เครือข่าย (Alert/Log)
๒	การบันทึกและสืบสวนหาข้อเท็จจริง	- บันทึกประวัติเส้นเวลาของเหตุการณ์ที่มีการระบุเวลาแน่นอน (Time-stamped Incident Timeline) - ภาพบันทึกหน้าจอแสดงหลักฐานความเสียหายที่ตรวจพบ (Screenshot)
๓	การควบคุมจำกัดวงความเสียหาย	เอกสารการอนุมัติทางเทคนิคเพื่อสั่งการตัดระบบหรือปิดพอร์ตเครือข่ายชั่วคราว (Containment Approval)
๔	การรายงานเหตุตามกฎหมาย	- สำเนาแบบรายงานผลตรวจสอบเบื้องต้น (แบบรายงาน ก๑) - สำเนาแบบรายงานภัยคุกคามที่มีนัยสำคัญที่ส่งภายใน ๒๔ ชั่วโมง (แบบรายงาน ก๒) - สำเนาแบบรายงานสรุปสถิติจำนวนภัยคุกคามรอบปี (แบบรายงาน ก๓)
๕	การจัดการนิติวิทยาศาสตร์ดิจิทัล	- ใบลงประวัติและควบคุมห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody Form) - เอกสารรายงานผลสรุปเชิงนิติวิทยาศาสตร์จากผู้เชี่ยวชาญ (Forensic Report)
๖	การกู้คืนและเปิดให้บริการระบบ	บันทึกรายงานผลการทดสอบการสแกนความมั่นคงปลอดภัยและความสะอาดของข้อมูลสำรองก่อน Restore (Recovery Test Report)
๗	การถอดบทเรียนและการซ้อมแผน	รายงานสรุปผลการถอดบทเรียนหลังเหตุการณ์จริง หรือรายงานสรุปผลการซ้อมแผนประจำปี (After Action Report: AAR)
๘	มาตรการแก้ไขและป้องกันเกิดซ้ำ	ทะเบียนรายการมาตรการแก้ไขป้องกัน (CAPA Register) และพยานหลักฐานเชิงเทคนิคที่ใช้เพื่อขออนุมัติปิดประเด็นตาม CAPA

๒๐.๓ มาตรฐานการควบคุมและพิทักษ์เอกสารหลักฐาน (Document and Evidence Control Standard)

มหาวิทยาลัยฯ กำหนดมาตรฐานสำหรับพยานเอกสารและเอกสารพยานหลักฐานทุกรายการที่จัดเก็บตามดัชนีข้อ ๒๐.๒ เพื่อรักษาความน่าเชื่อถือและความพร้อมใช้งานเมื่อมีเหตุสืบสวนหรือตรวจประเมิน โดยต้องมีข้อมูลควบคุมขั้นต่ำดังนี้

หมายเลขอ้างอิงระบบ (Document / Incident ID) เอกสารหลักฐานทุกชิ้นต้องมีหมายเลขรหัสอ้างอิงเหตุการณ์ที่ชัดเจนและเป็นระบบเดียวกัน (เช่น INC-YYYY-XXXX-DOC-XX) เพื่อให้สอดคล้องกันทุกส่วน

การระบุเวลาจัดทำ (Date Identification) เอกสารหลักฐานต้องประทับระบุวันและเวลาที่มีการจัดทำอย่างชัดเจน

การระบุบทบาทผู้รับผิดชอบหลัก ต้องระบุรายชื่อตัวบุคคลในบทบาทต่าง ๆ ประกอบด้วย

- ระบุชื่อเจ้าหน้าที่ผู้ดำเนินการรวบรวมพยานหลักฐานและจัดทำเอกสาร
- ระบุชื่อผู้มีสิทธิ์ตรวจรับรองความถูกต้องของหลักฐานและลงนามอนุมัติ (ตามตารางอำนาจในข้อ ๑๑.๔)

การควบคุมเวอร์ชันเอกสาร (Version Control) ในกรณีที่พยานเอกสารหรือรายงานหลักฐานทางเทคนิคมีการปรับเปลี่ยนรายละเอียดเพิ่มเติมนับแต่วันที่ตรวจพบ ให้จัดทำระบบการควบคุมเวอร์ชัน (Version Control) ของเอกสารให้ชัดเจนและมีความเป็นปัจจุบันตามความเหมาะสม

๒๑.การรายงานตามกฎหมายและแนวทาง สกมช.

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย กำหนดขั้นตอนปฏิบัติ มาตรการควบคุม และช่องทางการแจ้งรายงานเหตุภัยคุกคามทางไซเบอร์ให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ อย่างเคร่งครัด เพื่อให้กระบวนการส่งต่อข้อมูลพยานหลักฐานและประสานความร่วมมือกับ สกมช. และกระทรวง อว. เป็นไปอย่างรวดเร็วและสมบูรณ์ ดังนี้

๒๑.๑ เกณฑ์การพิจารณาและแบบรายงานตามกฎหมาย สกมช.

มหาวิทยาลัยฯ กำหนดการแยกแยะและเลือกใช้แบบฟอร์มรายงานภัยคุกคามตามเกณฑ์และลักษณะของความรุนแรงที่กฎหมายกำหนดไว้ ๓ รูปแบบหลัก ได้แก่

- แบบรายงาน ก๑: ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

วัตถุประสงค์ในการใช้งาน: ใช้สำหรับรายงานข้อมูลการประสานงาน และผลการวิเคราะห์เพื่อตรวจหาช่องโหว่หรือตรวจสอบภัยคุกคามขั้นต้น เพื่อประสานงานขอคำแนะนำ ความช่วยเหลือ หรือแบ่งปันข้อมูลจราจรภัยคุกคาม (Threat Intelligence Sharing) จาก สกมช. หรือ Thai-CERT

เกณฑ์การใช้งาน: ใช้กับเหตุภัยคุกคามทั่วไปที่ไม่ส่งผลกระทบต่อเนื่องทางธุรกิจอย่างรุนแรง (ระดับ ๑ และ ๒ ตามเกณฑ์ความรุนแรงภายในมหาวิทยาลัยฯ) หรือเหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน

- แบบรายงาน ก๒: แบบรายงานเหตุภัยคุกคามทางไซเบอร์ (กรณีมีนัยสำคัญ/ร้ายแรง/วิกฤต)

วัตถุประสงค์ในการใช้งาน: ใช้สำหรับรายงานเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต่อเนื่อง หรือสร้างผลกระทบต่อระบบงาน โครงสร้างพื้นฐานสำคัญ และความพร้อมในการให้บริการสารสนเทศของมหาวิทยาลัยฯ

เกณฑ์การใช้งาน: ใช้กับภัยคุกคามที่มีความรุนแรงสูงและระดับวิกฤต (ระดับ ๓ และ ๔ ตามเกณฑ์ความรุนแรงภายในมหาวิทยาลัยฯ) เช่น กรณีมัลแวร์เรียกค่าไถ่บุกรุกระบบงานสำคัญ หรือตรวจพบเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach) รั่วไหลในปริมาณมาก

กรอบระยะเวลาบังคับทางกฎหมาย: ต้องดำเนินการรายงานส่งไปยัง สกมช. และกระทรวง อว. (ในฐานะหน่วยงานกำกับดูแล) ภายในระยะเวลา ๒๔ ชั่วโมง นับแต่มหาวิทยาลัยฯ ตรวจพบหรือทราบเหตุการณ์ภัยคุกคามนั้น ๆ

- แบบรายงาน ก๓: แบบรายงานสรุปสถิติจำนวนภัยคุกคามทางไซเบอร์ในรอบปี

วัตถุประสงค์ในการใช้งาน: มหาวิทยาลัยฯ ในฐานะหน่วยงานของรัฐ มีหน้าที่รวบรวมและนำส่งสถิติจำนวนเหตุภัยคุกคามทั้งหมดที่เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของมหาวิทยาลัยฯ ภายใต้การดูแลของตนในรอบปี โดยทำการคัดแยกและรวบรวมสถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคาม (หมวดหมู่ที่ ๐ ถึง ๙) และจำแนกตามทรัพย์สินสารสนเทศที่ได้รับผลกระทบ (เช่น เครื่องแม่ข่าย เครื่องผู้ใช้ เว็บไซต์ หรืออุปกรณ์เครือข่าย)

กรอบระยะเวลาบังคับทางกฎหมาย: ต้องจัดส่งรายงานสรุปสถิติประจำปี (แบบรายงาน ก๓) นำส่ง สกมช. ภายในวันที่ ๓๑ มกราคมของปีถัดไป เป็นประจำทุกปี

๒๑.๒ ขั้นตอนสายการรายงานและช่องทางการประสานงาน (Reporting Workflow and Channels)

เพื่อให้การรายงานเป็นไปอย่างถูกต้อง มีระบบ และได้รับการตรวจสอบความชอบด้วยกฎหมายก่อนจัดส่งจริง มหาวิทยาลัยฯ กำหนดลำดับขั้นตอนการประสานรายงานดังนี้

๑) การจัดเตรียมและยกร่างรายงาน: เมื่อเกิดภัยคุกคามที่ต้องรายงานตามกฎหมาย ทีม CIRT และผู้ปฏิบัติงานเทคนิคจะร่วมทำการรวบรวมข้อเท็จจริง และส่งต่อให้ ผู้แทน นิติกร สำนักงานนิติการ ดำเนินการตรวจสอบความถูกต้องทางข้อกฎหมายและยกร่างเขียนรายละเอียดในแบบฟอร์ม ก๑ หรือ ก๒

๒) การพิจารณาลงนามและอนุมัติ: นำเสนอเอกสารร่างรายงานแก่ ผู้อำนวยการสำนักวิทยบริการฯ (หัวหน้า CIRT) เพื่อตรวจสอบความเรียบร้อยทางเทคนิค ก่อนส่งเสนอต่อ อธิการบดี (หรือผู้บังคับบัญชาสูงสุดที่ได้รับมอบอำนาจ) เพื่อพิจารณาลงนามในเอกสารรายงานก่อนส่งมอบ

๓) ช่องทางการจัดส่งรายงานที่ได้รับการรับรอง: นำส่งรายงานไปยัง สกมช. และกระทรวง อว. ผ่านช่องทางอย่างเป็นทางการตามคู่มือปฏิบัติการล่าสุดของ สกมช. ประกอบด้วย

- ระบบแจ้งเหตุออนไลน์ (NCSA Portal/Incident Reporting System) ของ สกมช.
- จดหมายอิเล็กทรอนิกส์ (Email): thaicert@ncsa.or.th
- การแจ้งฉุกเฉินทางโทรศัพท์: ในกรณีที่เป็นภัยคุกคามระดับวิกฤตสูงสุด ให้เจ้าหน้าที่ดำเนินการโทรศัพท์แจ้งเหตุเพื่อรายงานสถานการณ์แก่เจ้าหน้าที่ สกมช. หรือ Thai-CERT ด้วยวาจาโดยทันที เพื่อประสานรับความช่วยเหลือฉุกเฉิน แล้วจึงรีบจัดส่งแบบรายงาน ก๒ เป็นลายลักษณ์อักษรตามไปทันที

๒๑.๓ แนวทางปฏิบัติการรายงานเมื่อข้อมูลไม่ครบถ้วน (Progressive Reporting Guidelines)

๑) กรณีเกิดเหตุภัยคุกคามที่มีความร้ายแรงหรือวิกฤต (SLA ๒๔ ชั่วโมง) หากข้อมูลเชิงเทคนิคหรือผลการตรวจสอบยังไม่ครบถ้วนสมบูรณ์ มหาวิทยาลัยฯ กำหนดห้ามชะลอการแจ้งรายงานไปยัง สกมช. และ อว. เพื่อรอข้อมูลสมบูรณ์เป็นอันขาด

๒) กระบวนการรายงานแบบแบ่งระยะ (Phase-based Reporting)

- ระยะแจ้งเหตุครั้งแรก (Initial Phase): ให้จัดส่งแบบรายงาน ก๒ ภายในช่วงเวลา ๒๔ ชั่วโมง โดยกรอกและรายงานเฉพาะรายละเอียดข้อเท็จจริงเท่าที่จะสามารถรวบรวมและสืบค้นได้ในขณะนั้น เพื่อให้เป็นไปตามกรอบกฎหมาย
- ระยะรายงานเพิ่มเติม (Update Phase): ทีม CIRT และสำนักงานนิติการ จะดำเนินการติดตามรวบรวมความคืบหน้าอย่างต่อเนื่อง และดำเนินการส่งข้อมูลทางเทคนิค พยานหลักฐานทางดิจิทัลเพิ่มเติม หรือค่าความเสียหายประเมินเพิ่มเติมให้แก่ สกมช. และ อว. เป็นระยะ ๆ เมื่อผลการตรวจสอบมีความเด่นชัด
- ระยะปิดรายงานเหตุ (Closing Phase): เมื่อสืบสวนหาสาเหตุที่แท้จริง (Root Cause) ดำเนินการระงับภัย และกู้ระบบเสร็จสิ้นจนเหตุการณ์สิ้นสุดอย่างมีเสถียรภาพ ให้จัดทำสรุปรายงานภาพรวมและบทเรียนที่ได้รับ (Lessons Learned) นำส่งเพื่อสรุปผลปิดเหตุการณ์ความปลอดภัยอย่างเป็นทางการ

๒๑.๔ การบันทึกและพิทักษ์หลักฐานการส่งรายงาน (Auditable Notification Log)

๑) การเก็บบันทึกประวัติ ทุกครั้งที่มีการส่งแบบรายงาน ก๑/ก๒/ก๓ ไปยังหน่วยงานภายนอก เจ้าหน้าที่รับผิดชอบจะต้องทำบันทึกประวัติการส่งรายงานและจัดเก็บพยานหลักฐานอย่างรัดกุมในคลังข้อมูลประวัติเหตุการณ์ความปลอดภัย (Incident Record)

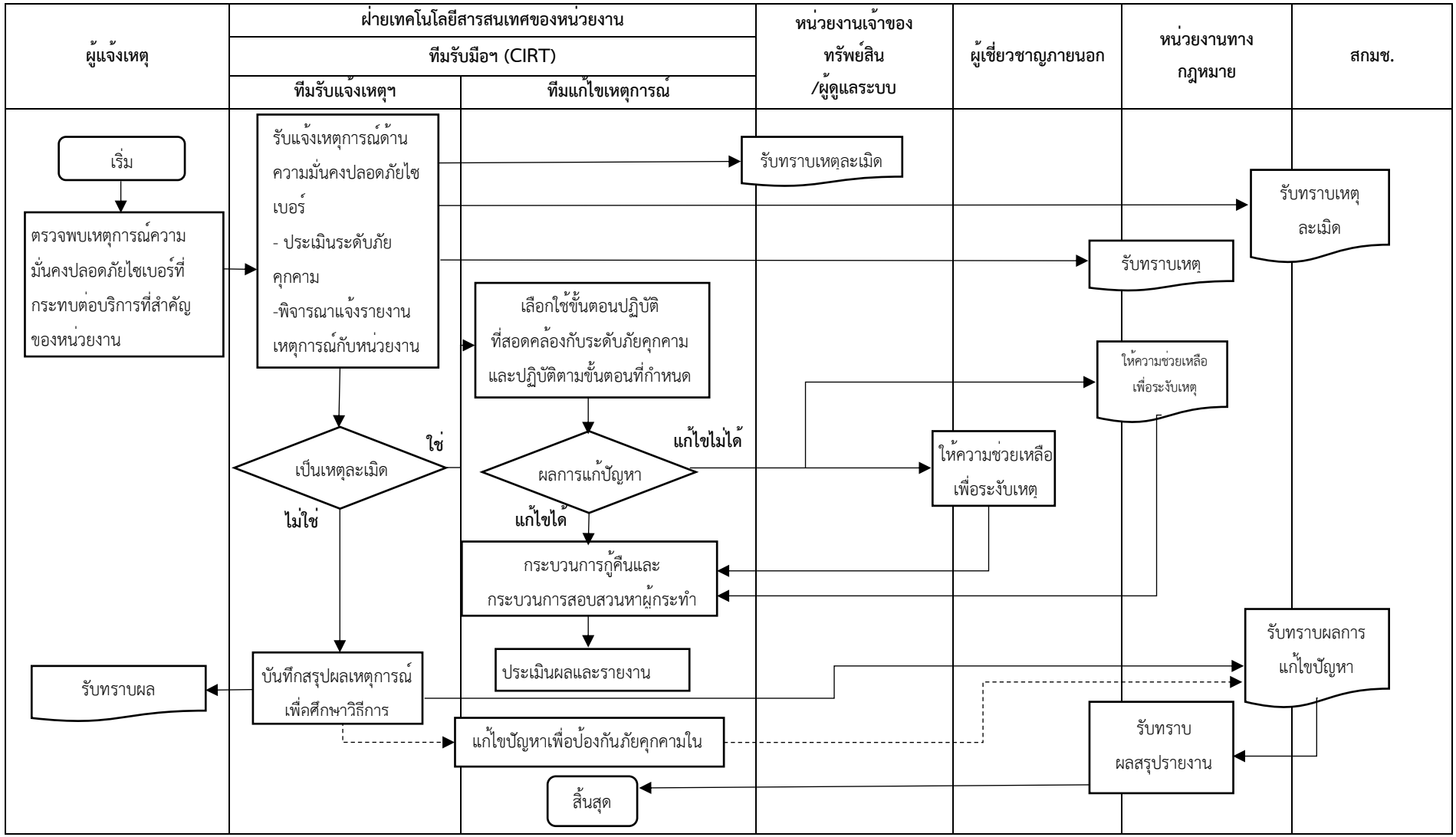
๒) รายการหลักฐานที่ต้องจัดเก็บขั้นต่ำ

- จดหมายอิเล็กทรอนิกส์ (Email) หรือไฟล์ตอบรับการแจ้งเหตุจากระบบออนไลน์ สกมช. พร้อมเลขรับเรื่อง (ถ้ามี)
- วันและเวลาที่มีการจัดส่งรายงานที่ระบุไว้อย่างชัดเจน (Time-stamped Receipt)
- รายชื่อเจ้าหน้าที่ผู้ดำเนินการส่งรายงาน และผู้ประสานงานหลัก
- สำเนาเอกสารแบบรายงาน ก๑/ก๒/ก๓ ฉบับที่ลงนามเรียบร้อย และเอกสารแนบทางเทคนิคทั้งหมด (เช่น ภาพบันทึกหน้าจอ และข้อมูล Log ประกอบ)

๓) ความสอดคล้องกับ Incident ID หลักฐานการส่งรายงานทั้งหมดจะต้องเชื่อมโยงและใช้รหัสหมายเลขเหตุการณ์ (Incident ID) เดียวกันกับประวัติการจัดการเหตุการณ์ และมีการควบคุมเวอร์ชันเอกสารให้ถูกต้อง เพื่อให้สอดประสานกันและตรวจสอบย้อนหลังได้โดยง่ายในกระบวนการประเมินความมั่นคงปลอดภัยประจำปี

ภาคผนวก ๑

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



ภาคผนวก ๒

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

ภาคผนวก ๓

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)
ตัวอย่าง ๑๒/๑/๖๖ – ๐๙.๐๐ น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

ภาคผนวก ๔

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
๑. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง
๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)
๔. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
๕. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[1] ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

[1] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ **วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[2] ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

[2] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม
ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ) ☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ
ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี) โปรดระบุ

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:

โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ) โปรดระบุ

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[3]

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตช์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[4]

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

[3] หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔

[4] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ภาคผนวก ๕

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
๑.๑	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
๑.๒	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
๑.๓	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
๑.๔	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
๗.๓	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	

๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

- NIST SP 800-61r2 Computer Security Incident Handling Guide

- ACSC Cyber Incident Response Plan Guidance

เอกสารอ้างอิงเพิ่มเติม (ฉบับปรับปรุง)

• ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๘

• คู่มือประกอบแนวทางการแจ้งรายงานเหตุภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๙ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน่วยงานของรัฐ

• ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

• ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔