

เอกสารแนบท้ายประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์  
เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖  
ว่าด้วยข้อมูลที่ต้องแจ้งและแบบการรายงานภัยคุกคามทางไซเบอร์

## บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ และให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นั้น

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานการดำเนินมาตรการตามที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ จึงกำหนดให้หน่วยงานดังกล่าวจัดทำรายงานเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานตามรายการที่กำหนดไว้ในแนบท้ายนี้ ผ่านการส่งทางอีเมล โทรสาร หรือด้วยวิธีการทางอิเล็กทรอนิกส์อื่นใดที่มีความปลอดภัย เช่น การส่งรายงานที่เข้ารหัสด้วย PGP มาทางอีเมล (เป็นอย่างน้อย)

เนื่องด้วยการส่งรายงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ทันการณ์ เป็นเรื่องที่สำคัญ<sup>๑</sup> ในกรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศยังไม่สามารถแจ้งข้อมูลตามแบบรายงานได้อย่างครบถ้วนภายในระยะเวลา ๒๔ ชั่วโมง ให้หน่วยงานดังกล่าวจัดส่งรายงานด้วยข้อมูลเท่าที่มี และเมื่อมีความคืบหน้าหรือมีข้อมูลเพิ่มเติมในการดำเนินการรับมือ ให้แจ้งต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นระยะ และรีบจัดทำและส่งรายงานที่สมบูรณ์ให้แก่สำนักงานโดยเร็ว ทั้งนี้ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศพิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายการรักษาความลับของหน่วยงาน

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่สามารถดำเนินการจัดเตรียมข้อมูลในรายงานได้ด้วยเหตุผลบางประการ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งหน่วยงานควบคุมหรือกำกับดูแลของตนและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ทราบโดยเร็ว

<sup>๑</sup> การรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต่อรายงานภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

<sup>๒</sup> มาตรา ๓๓ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

ทั้งนี้ เพื่อให้หน่วยงานของรัฐ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานเหตุภัยคุกคามทางไซเบอร์ กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐ จึงให้นำหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศดังกล่าวข้างต้น มาบังคับใช้แก่หน่วยงานของรัฐโดยอนุโลม

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น																	
<b>๑. ข้อมูลการประสานงาน</b> ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง																	
<b>๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม</b> ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม																	
<b>๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม</b> ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)																	
<b>๔. ความต่อเนื่องของเหตุภัยคุกคาม</b> <input type="checkbox"/> เหตุภัยคุกคามใหม่ <input type="checkbox"/> การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม																	
<b>๕. ลักษณะภัยคุกคามทางไซเบอร์</b> ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ <sup>๓</sup> ในระดับใด (มาตรา ๖๐) <input type="checkbox"/> ไม่ร้ายแรง <input type="checkbox"/> ร้ายแรง <input type="checkbox"/> วิกฤต (ก) <input type="checkbox"/> วิกฤต (ข) <input type="checkbox"/> ยังไม่สามารถระบุได้																	
<b>๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)</b> <table border="1"> <thead> <tr> <th>หมวดหมู่*</th> <th>คำอธิบาย</th> </tr> </thead> <tbody> <tr> <td>หมวดหมู่ที่ ๒</td> <td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td> </tr> <tr> <td>หมวดหมู่ที่ ๓</td> <td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)</td> </tr> <tr> <td>หมวดหมู่ที่ ๔</td> <td>การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)</td> </tr> <tr> <td>หมวดหมู่ที่ ๕</td> <td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ ๖</td> <td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ ๗</td> <td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td> </tr> <tr> <td>หมวดหมู่ที่ ๘</td> <td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td> </tr> </tbody> </table>		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)
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)																

<sup>๓</sup> พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

\* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

<b>ส่วนที่ ๑</b>
<b>หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น</b>
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรตระบุ หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรตระบุ วันที่: เลือกวันที่ เวลา: โปรตระบุ
<b>ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม</b> ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรตระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรตระบุ
<b>ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม</b> ชื่อ-นามสกุล: โปรตระบุ ตำแหน่งงาน: โปรตระบุ ชื่อหน่วยงาน: โปรตระบุ อีเมล: โปรตระบุ โทรศัพท์ (ที่ทำงาน / มือถือ): โปรตระบุ
<b>ก๓. ความต่อเนื่องของเหตุภัยคุกคาม</b> <input type="checkbox"/> เหตุภัยคุกคามใหม่ <input type="checkbox"/> การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
<b>ก๔. ลักษณะภัยคุกคามทางไซเบอร์</b> ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน <input type="checkbox"/> ใช่ <input type="checkbox"/> ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ <sup>๔</sup> ในระดับใด (มาตรา ๖๐) <input type="checkbox"/> ไม่ร้ายแรง <input type="checkbox"/> ร้ายแรง <input type="checkbox"/> วิกฤต (ก) <input type="checkbox"/> วิกฤต (ข) <input type="checkbox"/> ยังไม่สามารถระบุได้

<sup>๔</sup> พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์	
ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ  วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ	
ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ <input type="checkbox"/> ยังไม่ได้แจ้ง <input type="checkbox"/> แจ้งแล้ว _____	
ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)	
หมวดหมู่*	คำอธิบาย
<input type="checkbox"/> หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
<input type="checkbox"/> หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
<input type="checkbox"/> หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
<input type="checkbox"/> หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
<input type="checkbox"/> หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
<input type="checkbox"/> หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
<input type="checkbox"/> หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
<input type="checkbox"/> อื่น ๆ	โปรดระบุ
* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามที่ต้องรายงาน)	
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	
<b>ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)</b>	
<input type="checkbox"/> เพิ่งพบเหตุการณ์	<input type="checkbox"/> อยู่ในขั้นตอนการขอความช่วยเหลือ
<input type="checkbox"/> อยู่ในขั้นตอนการสอบสวน	<input type="checkbox"/> กำลังถูกลาม
<input type="checkbox"/> อยู่ในขั้นตอนการระงับภัย	<input type="checkbox"/> สามารถระงับภัยได้แล้ว
<input type="checkbox"/> รายงานปิดเหตุการณ์ภัยคุกคามแล้ว	<input type="checkbox"/> อื่น ๆ: โปรดระบุ
<b>ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว</b>	
<input type="checkbox"/> ยังไม่ได้ดำเนินการแก้ไขใด ๆ	<input type="checkbox"/> ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว
<input type="checkbox"/> ตรวจสอบข้อมูลจราจร (Log) แล้ว	<input type="checkbox"/> ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว
<input type="checkbox"/> กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว	
<input type="checkbox"/> รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ	
<b>ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)</b>	
โปรดระบุ	

<b>ส่วนที่ ๒</b>										
<b>หมวด ง : รายละเอียดภัยคุกคาม</b>										
<b>ง๑. ข้อมูลการตรวจจับและการวิเคราะห์</b>										
<b>ง๑.๑ วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)</b> วันที่:   เลือกวันที่    เวลา:   โปรดระบุ    ไม่ทราบ: <input type="checkbox"/>										
<b>ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์</b> 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										
<b>ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)</b> จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย): จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ ชนิดของข้อมูล (เลือกทุกข้อที่ใช้): <table style="width: 100%;"><tr><td><input type="checkbox"/> ข้อมูลไบโอเมตริกซ์</td><td><input type="checkbox"/> ข้อมูลการติดต่อ</td></tr><tr><td><input type="checkbox"/> ข้อมูลการเงิน</td><td><input type="checkbox"/> ข้อมูลบุคลากรของรัฐ</td></tr><tr><td><input type="checkbox"/> หมายเลขบัตรประชาชน</td><td><input type="checkbox"/> ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ</td></tr><tr><td><input type="checkbox"/> ข้อมูลทางการแพทย์</td><td></td></tr><tr><td><input type="checkbox"/> อื่น ๆ : โปรดระบุ</td><td></td></tr></table> จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ	<input type="checkbox"/> ข้อมูลไบโอเมตริกซ์	<input type="checkbox"/> ข้อมูลการติดต่อ	<input type="checkbox"/> ข้อมูลการเงิน	<input type="checkbox"/> ข้อมูลบุคลากรของรัฐ	<input type="checkbox"/> หมายเลขบัตรประชาชน	<input type="checkbox"/> ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ	<input type="checkbox"/> ข้อมูลทางการแพทย์		<input type="checkbox"/> อื่น ๆ : โปรดระบุ	
<input type="checkbox"/> ข้อมูลไบโอเมตริกซ์	<input type="checkbox"/> ข้อมูลการติดต่อ									
<input type="checkbox"/> ข้อมูลการเงิน	<input type="checkbox"/> ข้อมูลบุคลากรของรัฐ									
<input type="checkbox"/> หมายเลขบัตรประชาชน	<input type="checkbox"/> ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ									
<input type="checkbox"/> ข้อมูลทางการแพทย์										
<input type="checkbox"/> อื่น ๆ : โปรดระบุ										

<p><b>๑๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</b></p> <p>หมายเลข CVE: โปรตระบบ ช่องโหว่ที่ถูกใช้โจมตี: โปรตระบบ การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น: โปตระบบ</p> <p>อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)</p> <p><input type="checkbox"/> ระบบล่ม <input type="checkbox"/> รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ</p> <p><input type="checkbox"/> บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ</p> <p><input type="checkbox"/> การโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ</p> <p><input type="checkbox"/> ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและไม่รู้สาเหตุ)</p> <p><input type="checkbox"/> การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ</p> <p><input type="checkbox"/> การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ</p> <p><input type="checkbox"/> การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย</p> <p><input type="checkbox"/> การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง</p> <p><input type="checkbox"/> การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก</p> <p><input type="checkbox"/> การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย</p> <p><input type="checkbox"/> รูปแบบการใช้งานที่ผิดปกติ <input type="checkbox"/> การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ</p> <p><input type="checkbox"/> ความพยายามที่จะเขียนไฟล์ของระบบ <input type="checkbox"/> การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ</p> <p><input type="checkbox"/> การแก้ไขหรือลบข้อมูลที่ผิดปกติ <input type="checkbox"/> การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)</p> <p><input type="checkbox"/> ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ <input type="checkbox"/> การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ไม่ปกติ</p> <p><input type="checkbox"/> การแก้ไขหน้าเว็บ <input type="checkbox"/> การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น</p> <p><input type="checkbox"/> การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ</p> <p><input type="checkbox"/> การตรวจพบโปรแกรมเจาะระบบ (Crack utility)</p> <p><input type="checkbox"/> สิ่งผิดปกติไปจากเดิมอื่น ๆ: โปตระบบ</p>
<p><b>๑๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ)</b></p> <p>โปตระบบ</p>
<p><b>๑๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องข้อกับเหตุภัยคุกคาม:</b> โปตระบบ</p>
<p><b>๑๒. ข้อมูลการระงับ ปรามปราม และฟื้นฟู</b></p>
<p><b>๑๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม:</b> โปตระบบ</p>
<p><b>๑๒.๒ การคาดการณ์ความสามารถฟื้นฟู</b> โปตระบบรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู</p>
<p><b>๑๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)</b></p>
<p><b>๑๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด</b> วันที่: เลือกวันที่ เวลา: โปตระบบ</p>
<p><b>๑๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน:</b> โปตระบบ</p>

ง๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรรระบุ