	กระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	KSC MOPH-Identify -03
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นเอกสารของความลับ	1 ธ.ค. 68 ใช้ภายในเท่านั้น

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นางสาวศิรดา สว่างสุข	นายชัพ ธิราขันธ์	นายภูจิตต์ ตรีบำเพ็ญ
ตำแหน่ง	นักสาธารณสุขปฏิบัติการ	นักจัดการงานทั่วไปชำนาญการ	ผู้อำนวยการโรงพยาบาลเกาะสีชัง
วันเดือนปี	24 พฤศจิกายน 2568	28 พฤศจิกายน 2568	28 พฤศจิกายน 2568

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	1 ธ.ค. 68	จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์

	กระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	KSC MOPH-Identify -03
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นเอกสารของความลับ	1 ธ.ค. 68 ใช้ภายในเท่านั้น

สารบัญ

1. วัตถุประสงค์ 3
2. ขอบเขต 3
3. คำจำกัดความ/นิยามศัพท์เฉพาะ 4
4. ผู้รับผิดชอบและความรับผิดชอบ 4
5. ขั้นตอนปฏิบัติ 5
6. การติดตามและจัดการช่องโหว่ (Vulnerability Management) 7
7. การรายงานผลการทดสอบเจาะระบบไปยังหน่วยควบคุมกำกับหรือกำกับดูแล 7
8. การทบทวนกระบวนการดำเนินการ 7
9. เอกสารอ้างอิง 8

	กระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	KSC MOPH-Identify -03
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นเอกสารของความลับ	1 ธ.ค. 68 ใช้ภายในเท่านั้น

การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.3.1, ข้อ 21.3.3, ข้อ 21.3.4, ข้อ 21.3.5, ข้อ 21.3.6, ข้อ 21.3.7, ข้อ 21.3.8, ข้อ 21.3.9, ข้อ 21.3.10]

1. วัตถุประสงค์

เอกสารฉบับนี้จัดทำขึ้นเพื่อให้มีกระบวนการและขั้นตอนการประเมินช่องโหว่ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับบริการที่สำคัญ รวมถึงการดำเนินการทดสอบเจาะระบบเพื่อประเมินความเสี่ยงและการควบคุมความปลอดภัย

2. ขอบเขต

กระบวนการนี้ครอบคลุมการประเมินช่องโหว่และการทดสอบเจาะระบบเทคโนโลยีสารสนเทศและระบบควบคุมเครื่องจักรในอุตสาหกรรม (ถ้ามี) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน โดยรวมถึงการตรวจสอบความมั่นคงปลอดภัยของโฮสต์ เครือข่าย สถาปัตยกรรม และแอปพลิเคชัน

3. คำจำกัดความ/นิยามศัพท์เฉพาะ

ลำดับ	คำศัพท์	คำจำกัดความ
1	Vulnerability Assessment	การประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศและ/หรือระบบควบคุมเครื่องจักรในอุตสาหกรรม
2	Penetration Testing	การทดสอบเจาะระบบเทคโนโลยีสารสนเทศและ/หรือระบบควบคุมเครื่องจักรในอุตสาหกรรม
3	Vulnerability Assessment and Penetration Testing Service Providers	ผู้ให้บริการประเมินช่องโหว่และทดสอบเจาะระบบเทคโนโลยีสารสนเทศและ/หรือระบบควบคุมเครื่องจักรในอุตสาหกรรม

4. ผู้รับผิดชอบและความรับผิดชอบ

ลำดับ	ผู้รับผิดชอบ	ความรับผิดชอบ
1	IT Security Team / IST	• ดำเนินการให้มีการประเมินช่องโหว่และการทดสอบเจาะระบบ รวมถึงการติดตามและแก้ไขช่องโหว่ที่พบ
	Penetration Testing Service Providers	• ดำเนินการทดสอบเจาะระบบตามขอบเขตที่กำหนดจาก IT Security Team / IST โดยผู้ให้บริการต้องมีการรับรองและได้รับประกาศนียบัตรที่เป็นที่ยอมรับในอุตสาหกรรม
2	Top Management / ISM	• รับทราบผลการดำเนินการ • รับผิดชอบในการอนุมัติและสนับสนุนการดำเนินการตามกระบวนการ รวมถึงการตรวจสอบและประเมินผล

5. ขั้นตอนปฏิบัติ

5.1 การประเมินช่องโหว่ (Vulnerability Assessment)

1) การประเมินช่องโหว่ตามหลักการบริหารความเสี่ยง

ขั้นตอน: ดำเนินการประเมินช่องโหว่ของระบบเทคโนโลยีสารสนเทศและระบบควบคุมเครื่องจักรในอุตสาหกรรม (ถ้ามี) ตามหลักการบริหารความเสี่ยงที่หน่วยงานกำหนด เพื่อระบุจุดอ่อนและการควบคุมที่จำเป็น โดยการประเมินความเสี่ยงความมั่นคงปลอดภัยเพื่อหาช่องโหว่ที่อาจถูกโจมตีได้

2) การตรวจสอบขอบเขตของการประเมินช่องโหว่

ขั้นตอน: ตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่ครอบคลุมถึงการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม โดยการตรวจสอบว่าได้ทำการประเมินความมั่นคงปลอดภัยของเครือข่ายทั้งหมดที่เชื่อมต่อกับระบบที่สำคัญ

3) การประเมินช่องโหว่ก่อนดำเนินการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ

ขั้นตอน: ดำเนินการประเมินช่องโหว่ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ หรือเชื่อมต่อระบบใหม่ รวมถึงการเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ และการปรับเปลี่ยน เทคโนโลยี

4) การรับรองผู้ทำการประเมินช่องโหว่

ขั้นตอน: ตรวจสอบให้แน่ใจว่าผู้ทำการประเมินช่องโหว่มีการรับรองและมีประกาศนียบัตรที่เป็นที่ ยอมรับในอุตสาหกรรม และผู้ดำเนินการต้องเป็นอิสระจากระบบที่ทำการประเมิน

5) การควบคุมการประเมินช่องโหว่โดยหน่วยงานที่รับผิดชอบ

ขั้นตอน: ตรวจสอบให้แน่ใจว่าการประเมินช่องโหว่ระบบทั้งหมดดำเนินการภายใต้การดูแลของ หน่วยงานที่รับผิดชอบ โดยต้องมีทีมงานภายในหน่วยงานควบคุมและตรวจสอบการประเมินช่องโหว่ระบบที่ดำเนินการโดยผู้ให้บริการภายนอก

5.2 การทดสอบเจาะระบบ (Penetration Testing)

1) การดำเนินการทดสอบเจาะระบบตามความเสี่ยง

ขั้นตอน: พิจารณาดำเนินการทดสอบเจาะระบบสำหรับบริการที่สำคัญ โดยเฉพาะอย่างยิ่งระบบที่เชื่อมต่อกับอินเทอร์เน็ต ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบ ที่อาจเกิดขึ้นจากการทดสอบ โดยเฉพาะการทดสอบเจาะระบบของแอปพลิเคชันที่มีการเข้าถึง จากภายนอกผ่านอินเทอร์เน็ต

2) การตรวจสอบขอบเขตของการทดสอบเจาะระบบ

ขั้นตอน: ตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบครอบคลุมถึงโฮสต์ เครือข่าย และแอปพลิเคชันของระบบที่เป็นบริการที่สำคัญ โดยเฉพาะระบบที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง

3) ความถี่ในการทดสอบเจาะระบบ

ขั้นตอน: พิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ เพื่อประเมินความถูกต้องของระบบรักษาความมั่นคงปลอดภัย ตัวเช่น การทดสอบเจาะระบบสารสนเทศเมื่อมีการปรับปรุงเทคโนโลยีใหม่

4) การรับรองผู้ทดสอบเจาะระบบ

ขั้นตอน: ตรวจสอบให้แน่ใจว่าผู้ทดสอบเจาะระบบมีการรับรองและมีประกาศนียบัตรที่เป็นที่ ยอมรับในอุตสาหกรรม และผู้ทดสอบต้องเป็นอิสระจากระบบที่ทำการทดสอบ เช่น การใช้ผู้ทดสอบเจาะระบบที่ได้รับการรับรองจากองค์กรมาตรฐานสากล เช่น CEH – Certificated Ethical Hacker, OSCP – Offensive Security Certificated Professional

5) การควบคุมการทดสอบเจาะระบบโดยหน่วยงานที่รับผิดชอบ

ขั้นตอน: ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดดำเนินการภายใต้การดูแลของหน่วยงานที่รับผิดชอบ โดยต้องมีทีมงานภายในหน่วยงานควบคุมและตรวจสอบการทดสอบเจาะระบบที่ดำเนินการโดยผู้ให้บริการภายนอก

6. การติดตามและจัดการช่องโหว่ (Vulnerability Management)

ขั้นตอน: สร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ทั้งหมดได้รับการแก้ไขอย่าง เพียงพอ ซึ่งมีการใช้ระบบ/กระบวนการติดตามการแก้ไขช่องโหว่ (Vulnerability Management System) เพื่อรับประกันว่าช่องโหว่ทั้งหมดถูกแก้ไขตามกำหนดเวลา

7. การรายงานผลการทดสอบเจาะระบบไปยังหน่วยควบคุมกำกับหรือกำกับดูแล

ขั้นตอน: หากได้รับการร้องขอจากหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ หน่วยงานภายใต้การควบคุมกำกับหรือดูแล ต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบภายใน 30 วันหลังจากได้รับการร้องขอ โดยรูปแบบของรายงานให้เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนด

8. การทบทวนกระบวนการดำเนินการ

กระบวนการดำเนินการนี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงกระบวนการดำเนินการนี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

	กระบวนการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing Procedure)	รหัสเอกสาร	KSC MOPH-Identify -03
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ ชั้นเอกสารของความลับ	1 ธ.ค. 68 ใช้ภายในเท่านั้น

เอกสารอ้างอิง

ลำดับ	ชื่อเอกสาร
1	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 - กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify) - การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)
2	รายงาน/ผลการทดสอบเจาะระบบ
3	รายงาน/ผลการประเมินช่องโหว่
4	เอกสารการประเมินความเสี่ยง ทั้ง 3 ด้าน (Host Security, Network Security, Architecture Security)
5	สัญญาจ้างบริการทดสอบเจาะระบบ

	กระบวนการทดสอบเจาะระบบ (Penetration Testing Procedure)	**รหัสเอกสาร**	KSC MOPH-Identify -04
		แก้ไขครั้งที่	00
		วันที่บังคับใช้ **ชั้นความลับของเอกสาร**	1 ธ.ค. 2568 **ใช้ภายในเท่านั้น**

การอนุมัติเอกสาร

ลงนาม	ผู้เรียบเรียง/จัดทำโดย	ผู้ตรวจทาน/ผู้ทบทวน	ผู้อนุมัติ
ลายเซ็นต์			
ชื่อ-สกุล	นางสาวศิรดา สว่างสุข	นายชัพ ธิราขันธ์	นายภูจิตต์ ตรีบำเพ็ญ
ตำแหน่ง	นักสาธารณสุขปฏิบัติการ	นักจัดการงานทั่วไปชำนาญการ	ผู้อำนวยการโรงพยาบาลเกาะสีชัง
วันเดือนปี	24 พฤศจิกายน 2568	28 พฤศจิกายน 2568	28 พฤศจิกายน 2568

ประวัติการแก้ไข

ครั้งที่	วันที่ประกาศใช้	รายละเอียดการแก้ไข
00	1 ธ.ค. 2568	**จัดทำเอกสารครั้งแรก พร้อมขึ้นระบบ พรบ ไซเบอร์**

ขั้นตอนการทดสอบเจาะระบบ (Penetration Testing Procedure)

อ้างอิง : ประมวลและกรอบ [ข้อ 21.3.1, ข้อ 21.3.3, ข้อ 21.3.4, ข้อ 21.3.5, ข้อ 21.3.6, ข้อ 21.3.7, ข้อ 21.3.8, ข้อ 21.3.9, ข้อ 21.3.10]

1. วัตถุประสงค์ (Objective)

การทดสอบเจาะระบบมีวัตถุประสงค์เพื่อระบุและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT System) และระบบควบคุมเครื่องจักรในอุตสาหกรรม (ICS) เพื่อให้สามารถดำเนินการแก้ไขปัญหาเหล่านั้นได้ก่อนที่จะถูกโจมตีจริง

2. ขอบเขตของการทดสอบ (Scope of Testing)

การทดสอบจะครอบคลุมระบบและส่วนประกอบต่อไปนี้

- ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) Systems)
- ระบบควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control Systems: ICS)
- โครงสร้างพื้นฐานทางเครือข่าย (Network Infrastructure)
- แอปพลิเคชันและบริการที่เชื่อมต่ออินเทอร์เน็ต (Internet-facing Applications and Services)
- ฐานข้อมูล (Database)
- ระบบควบคุมการเข้าถึง (Access Control System)

3. ทีมที่รับผิดชอบ (Responsibility)

- **ผู้ทดสอบเจาะระบบ (Penetration Tester):** ทีมความมั่นคงปลอดภัยหรือผู้ให้บริการภายนอกที่ได้รับการรับรอง
- **ผู้ประสานงาน (Coordinator):** ผู้จัดการหรือหัวหน้าทีมที่มีหน้าที่ดูแลและประสานงานกับทีมต่าง ๆ
- **เจ้าของระบบ (System Owner):** เจ้าของหรือผู้ดูแลระบบที่ได้รับการทดสอบ

4. ขั้นตอนการทดสอบ (Testing Procedure)

4.1 การวางแผนและการเตรียมการ (Planning and Preparation)

- **กำหนดขอบเขตการทดสอบ (Define Scope):** ระบุระบบและส่วนประกอบที่ต้องการทดสอบ เช่น ระบบฐานข้อมูล, ระบบควบคุมเครื่องจักร, หรือระบบเครือข่าย โดยในการทดสอบนี้ขอบเขตครอบคลุมถึงระบบฐานข้อมูลของลูกค้า ระบบเครือข่ายที่ใช้ในการสื่อสาร และแอปพลิเคชันที่เชื่อมต่อกับอินเทอร์เน็ต
- **จัดทำเอกสารการอนุญาต (Obtain Authorization):** ขอกำหนดการอนุญาตจากเจ้าของระบบหรือผู้บริหารที่เกี่ยวข้องเพื่อดำเนินการทดสอบ ซึ่งต้องได้รับอนุญาตจากฝ่าย IT และผู้จัดการฝ่ายความมั่นคงสารสนเทศในการดำเนินการทดสอบเจาะระบบ
- **เตรียมเครื่องมือและทรัพยากร (Prepare Tools and Resources):**ตรวจสอบเครื่องมือที่จะใช้ในการทดสอบให้มีความพร้อมใช้ เช่น เครื่องมือสำหรับการสแกนช่องโหว่ (Nessus) และเครื่องมือสำหรับการทดสอบการเจาะระบบ (Metasploit)

4.2 การสแกนและการรวบรวมข้อมูล (Scanning and Information Gathering)

- **สแกนหาช่องโหว่ (Vulnerability Scanning):** ใช้เครื่องมือสแกนหาช่องโหว่ (Nessus) ในระบบเครือข่ายหรือเซิร์ฟเวอร์ฐานข้อมูลเพื่อหาช่องโหว่ การตั้งค่าการเข้าถึง
- **รวบรวมข้อมูลเกี่ยวกับระบบเป้าหมาย (Information Gathering):** รวบรวมข้อมูลที่จำเป็นเกี่ยวกับระบบที่กำลังทดสอบ เช่น ที่อยู่ IP, โดเมน, และบริการที่เปิดใช้งาน รวมถึงพอร์ตที่เปิดใช้งาน

4.3 การวิเคราะห์และการทดสอบช่องโหว่ (Analysis and Exploitation)

- **วิเคราะห์ผลการสแกน (Analyze Scan Results):** ตรวจสอบผลการสแกนเพื่อระบุช่องโหว่ที่ควรดำเนินการทดสอบเพิ่มเติม เช่น มีช่องโหว่ในระบบฐานข้อมูลที่เปิดให้เข้าถึงได้หรือไม่ โดยไม่ได้รับอนุญาตผ่านพอร์ตที่ไม่ได้เข้ารหัส
- **ทดสอบการเจาะระบบ (Exploitation Testing):** ดำเนินการทดสอบเจาะระบบโดยใช้เครื่องมือเฉพาะเพื่อยืนยันและประเมินความรุนแรงของช่องโหว่ที่พบ โดยใช้เครื่องมือ Metasploit ในการเจาะระบบฐานข้อมูลผ่านช่องโหว่ที่พบ และดูว่าสามารถเข้าถึงข้อมูลสำคัญได้หรือไม่

4.4 การรายงานและการสรุปผล (Reporting and Conclusion)

- **จัดทำรายงานผลการทดสอบ (Create Testing Report):** สรุปผลการทดสอบที่ดำเนินการช่องโหว่ที่พบ ความรุนแรง และแนวทางการแก้ไข ซึ่งการจัดทำรายงานนั้นต้องระบุว่าได้พบช่องโหว่ที่รุนแรงในระบบฐานข้อมูลหรืออื่นๆและพร้อมการนำเสนอการปรับปรุง ด้วย เช่น การตั้งค่าไฟร์วอลล์และการเข้ารหัสข้อมูล เป็นต้น
- **เสนอแนะการแก้ไข (Provide Remediation Recommendations):** ให้คำแนะนำเกี่ยวกับวิธีการแก้ไขช่องโหว่ที่พบในการทดสอบ
- **สรุปผลการทดสอบกับผู้เกี่ยวข้อง (Conclude Testing with Stakeholders):** สรุปผลการทดสอบและข้อเสนอแนะให้กับทีมงานที่เกี่ยวข้องและเจ้าของระบบรับทราบ หรืออาจจัดประชุมสรุปผลการทดสอบกับทีม IT และผู้จัดการฝ่ายความมั่นคงสารสนเทศ ก็ได้ เพื่อดำเนินการแก้ไขช่องโหว่ตามข้อเสนอแนะ

4.5 การติดตามผลการแก้ไข (Follow-Up on Remediation)

1. **ตรวจสอบการแก้ไขช่องโหว่ (Verify Remediation):** ทดสอบช่องโหว่ที่ได้รับการแก้ไขแล้วอีกครั้ง เพื่อยืนยันว่าได้ทำการแก้ไขอย่างถูกต้องและไม่มีความเสี่ยงอีกต่อไป

5. สรุปและการปิดโครงการ (Summary and Closure)

1. **ปิดโครงการทดสอบเจาะระบบ (Project Closure):** สรุปโครงการและปิดโครงการหลังจากได้ดำเนินการทดสอบเจาะระบบและแก้ไขช่องโหว่ทั้งหมดแล้ว
2. **จัดเก็บเอกสาร (Documentation Storage):** จัดเก็บรายงานผลการทดสอบและเอกสารที่เกี่ยวข้องอย่างปลอดภัย เพื่อใช้เป็นข้อมูลอ้างอิงในอนาคต

การทบทวนระเบียบกระบวนการดำเนินการ (Procedure Review)

ระเบียบกระบวนการดำเนินการ นี้จะได้รับการทบทวนเป็นประจำทุกปีหรือตามความจำเป็นเพื่อให้มั่นใจในประสิทธิภาพและและถ้ามีการเปลี่ยนแปลงระเบียบกระบวนการดำเนินการ นี้จะต้องมีการสื่อสารไปยังทุกฝ่ายที่ได้รับผลกระทบหรือทุกฝ่ายที่เกี่ยวข้องทราบ

เอกสารอ้างอิง

1. แผนรวมถึงขอบเขตการทดสอบเจาะระบบ
2. เอกสารที่ได้รับการอนุญาตในการเจาะระบบ
3. ผลการทดสอบช่องโหว่
4. รายงานผลการทดสอบ
5. รายงานผลการติดตามการแก้ไข
6. เอกสารสรุปปิดโครงการ