

คู่มือการใช้งานระบบติดตามการแก้ไขช่องโหว่

ระบบสารสนเทศ

Vulnerability Tracking System



ฝ่ายความมั่นคงปลอดภัยไซเบอร์ สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25 มิถุนายน 2568		
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ລບັບປรັບປรຸง	ครั้งที่ 1	
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 1/13		
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	เสารสนเทศ (CM	U VTS)	

สารบัญ

ขั้นตอนการใช้งานระบบ	2
การเข้าสู่ระบบของส่วนงาน	3
การจัดการข้อมูล	4
้การจัดการผู้ดูแลระบบของส่วนงาน	4
ผลการตรวจสอบช่องโหว่และการรายงานผล	6
การจัดการทรัพย์สินสารสนเทศ	9



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่	25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ລບັບປรັບປรຸง	ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 2/13	
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CM	iu vts)

ขั้นตอนการใช้งานระบบ

ระบบติดตามการแก้ไขช่องโหว่ของระบบสารสนเทศ มหาวิทยาลัยเชียงใหม่ (CMU VTS) เป็นระบบ ติดตามการรายงานผลการดำเนินงานแก้ไขช่องโหว่ของระบบสารสนเทศของส่วนงาน หลังจากการตรวจสอบ ช่องโหว่ (VA) ประจำปีโดยสำนักบริการเทคโนโลยีสารสนเทศ โดยมีขั้นตอนการใช้งานที่ผู้ดูแลระบบสารสนเทศ ของส่วนงานต้องดำเนินการดังนี้ (กล่องสีฟ้า หมายถึง ดำเนินการในระบบ CMU VTS)





รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่	25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง	ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 3/13	
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CM	U VTS)

การเข้าสู่ระบบของส่วนงาน

เริ่มใช้งานระบบ CMU VTS ในรูปแบบ Web Application ผ่าน URL: <u>https://vts.csd.itsc.cmu.ac.th</u> และเข้าสู่ระบบด้วย IT Account ที่เมนู "สำหรับส่วนงาน" ดังภาพที่ 1



บริการตรวจสอบช่องโหว่ของระบบ

แลย์สารสนเทศ ให้บริการตรวจสอบช่องไหว่ของระบบ ตั้งแต่ช่องไหว่ในกระบวนการทำงานของระบบเครื่องแม่ข่าย ระบบเร็กษาความปลอดภัยเครือข่าย รวมถึงระบบอื่นๆ ที่เกี่ยวข้อง ทำให้ส่วนงานได้รับรุ้ถึงช่องไหว่ของระบบที่ติดตั้งใช้งานะ การแก้ไขปรับปรุงได้อย่างถูกต้องในอนาคตต่อไป ทั้งนี้เพื่อลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้น ซึ่งกระบวนการตรวจสอบช่องไหว่นี้เป็นหนึ่งในมาตรการ การรักษาความปลอดภัยของระบบแทคโนโลยีสารสนเทศที่ดี ที่ควรมีการดำเนินการอย่างเป็นระเ ละ 1 ครั้ง ซึ่งหากองค์กรใดไปมีกระบวนการดำเนินการดังกล่าว ก็ย่อมมีความเสี่ยงที่อาจเกิดเหตุการณ์ที่ไปคาดคิดขึ้นได้

ภาพที่ 1 การคลิกเข้าสู่ระบบสำหรับส่วนงาน

หลังจากยืนยันตัวตนเข้าสู่ระบบเรียบร้อยแล้ว จะปรากฎเมนูจัดการข้อมูลด้านซ้ายมือ ประกอบด้วย

- ผู้ดูแลระบบของส่วนงาน
- ผลการสแกนช่องโหว่
- จัดการทรัพย์สินสารสนเทศ
- หน้าหลัก
 ดังภาพที่ 2



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 4/13
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CMU VTS)



ภาพที่ 2 เมนูจัดการข้อมูลสำหรับส่วนงาน หลังจากยืนยันตัวตนเข้าสู่ระบบแล้ว

การจัดการข้อมูล

ผู้ดูแลระบบสารสนเทศของส่วนงาน สามารถจัดการข้อมูลในระบบ CMU VTS ได้ตามสิทธิของส่วนงานที่ สังกัด ใน 3 หัวข้อหลัก ดังนี้

- การจัดการผู้ดูแลระบบของส่วนงาน
- ผลการตรวจสอบช่องโหว่และการรายงานผล
- จัดการทรัพย์สินสารสนเทศ

โดยมีลำดับขั้นตอนการดำเนินงานตามหัวข้อ "ขั้นตอนการใช้งานระบบ" อธิบายเมนูจัดการข้อมูลในแต่ ละหัวข้อได้ดังนี้

การจัดการผู้ดูแลระบบของส่วนงาน

เป็นการจัดการรายชื่อผู้ดูแลระบบของส่วนงาน ผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนงาน จะเป็นผู้มีสิทธิ สูงสุดของส่วนงาน และสามารถเพิ่มรายชื่อผู้ดูแลระบบท่านอื่นภายหลังได้ แต่ผู้ที่ได้รับการเพิ่มจะสามารถ ดูรายงานผลการตรวจสอบช่องโหว่ได้เพียงอย่างเดียว ไม่สามารถรายงานผลการแก้ไขช่องโหว่ได้ เหมาะ สำหรับผู้บริหาร หรือหัวหน้างาน ที่มีความประสงค์ดูข้อมูลในระบบ แต่การรายงาน จะเป็นหน้าที่ของผู้ที่ ได้รับมอบหมายจากหัวหน้าส่วนงาน (ผู้ดูแลระบบหลัก) (* หากต้องการเพิ่มผู้ดูแลระบบหลัก สามารถแจ้ง ความประสงค์ผ่านหัวหน้าส่วนงานในรูปแบบบันทึกข้อความ) หน้าจอการจัดการรายชื่อผู้ดูแลระบบของ ส่วนงาน แสดงดังภาพที่ 3

รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25	5 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง ค	รั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 5/13	
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CMU \	VTS)

จัดการรายชื่อผู้ดูแลระบบของส่วนงาน

							+ ผู้ดูแลระบบ
รายชื่อผู้ด	ูแลระบบของส่วนง	วาน		Search			Q
ชื่อ	นามสกุล	อีเมล	ส่วนงาน	โทรศัพท์	ดำแหน่ง	วันที่ลงทะเบียน	จัดการข้อมูล
_			สำนักบริการเทคโนโลยีสารสนเทศ			2022-09-29T00:00:00	
_			สำนักบริการเทคโนโลยีสารสนเทศ			2022-10-12T00:00:00	
			สำนักบริการเทคโนโลยีสารสนเทศ			2022-10-21T07:13:04:043	
			สำนักบริการเทคโนโลยีสารสนเทศ			2022-11-07T03:51:35.463	แก้ไข ลบ
			สำนักบริการเทคโนโลยีสารสนเทศ			2022-11-07T09:04:01:36	ແກ້ໄข ລບ
-			สำนักบริการเทคโนโลยีสารสนเทศ			2022-11-08T08:49:41.063	ແກ້ໄข au
-			สำนักบริการเทคโนโลยีสารสนเทศ		· · · · · ·	2022-12-06T10:05:47.003	ແກ້ໄບ ລບ
_			สำนักบริการเทคโนโลยีสารสนเทศ			2022-12-06T10:06:29.76	แก้ไข ลบ
			สำนักบริการเทคโนโลยีสารสนเทศ			2022-12-06T10:07:40.447	แก้ไข ลม
						Rows per page 10 👻	1-9 of 9 < >

ภาพที่ 3 หน้าจอการจัดการรายชื่อผู้ดูแลระบบของส่วนงาน

จากภาพที่ 3 รายชื่อผู้ดูแลระบบหลัก ที่ได้รับมอบหมายจากหัวหน้าส่วนงาน จะไม่สามารถแก้ไขหรือลบ ได้ (ต้องแจ้งทางสำนักบริการเทคโนโลยีสารสนเทศ) แต่ถ้าเป็นผู้ดูแลระบบสารสนเทศที่เพิ่มเติมภายหลัง จึงจะสามารถเปลี่ยนแปลงแก้ไข/ลบข้อมูลได้ ส่วนการเพิ่มผู้ดูแลระบบสารสนเทศของส่วนงาน (ดูผลอย่าง

เดียว) สามารถทำได้ด้วยการคลิกปุ่ม + พั**ดูแลระบบ** และบันทึกข้อมูล ประกอบด้วย

- o ชื่อ นามสกุล (* บังคับบันทึก)
- O IT Account ในรูปแบบ <u>name.surname@cmu.ac.th</u> (* บังคับบันทึก)
- หมายเลขโทรศัพท์สำหรับติดต่อ (ไม่บังคับ)
- ดำแหน่ง (ไม่บังคับ)

ดังภาพที่ 4 หลังจากนั้นให้คลิกปุ่ม "บันทึกข้อมูล" รายชื่อจะถูกเพิ่มในหน้าจัดการผู้ดูแลระบบของ ส่วนงานทันที ถ้าหากไม่ต้องการบันทึก ให้คลิกปุ่ม "ปิดหน้าต่าง"



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 6/13
ชื่อเอกสาร คู่มือการ	สารสนเทศ (CMU VTS)	

เพิ่มข้อมูลผู้ดูแลระบบของส่วนงาน

ชื่อ*

นามสกุล*

CMU IT Account (@cmu)*

หมายเลขโทรศัพท์ (ที่ทำงาน)

ตำแหน่ง

* จำเป็นต้องระบุข้อมูล

ปิดหน้าต่าง บันทึกข้อมูล

ภาพที่ 4 การเพิ่มผู้ดูแลระบบของส่วนงาน (* หมายถึง จำเป็นต้องระบุ)

ผลการตรวจสอบช่องโหว่และการรายงานผล

ผู้ดูแลระบบสารสนเทศของส่วนงานสามารถดูผลการตรวจสอบช่องโหว่ (VA) ของทรัพย์สินสารสนเทศได้ ที่เมนูนี้ รายงานผลการสแกนช่องโหว่ของส่วนงาน ประกอบด้วย ดังภาพที่ 5

- O Host หมายถึง ip หรือ domain ของทรัพย์สินสารสนเทศ
- Name หมายถึง ชื่อของช่องโหว่ที่ตรวจพบ
- O Detail หมายถึง เลขรหัสของช่องโหว่ สามารถคลิกเพื่อเปิดเว็บแสดงรายละเอียดได้
- O Port หมายถึง Port ของ Host ที่ตรวจพบช่องโหว่



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25 มิถุนายน 2568			
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง ครั้งที่ 1			
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 7/13			
ชื่อเอกสาร คู่มือการใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบสารสนเทศ (CMU VTS)					

- O Risk หมายถึง ระดับความเสี่ยงของช่องโหว่ ประกอบด้วย Critical, High, Medium,
 Low และ None (ให้ส่วนงานรายงานผลเฉพาะความเสี่ยงระดับ Critical
 เท่านั้น)
- O CVE หมายถึง Common Vulnerabilities and Exposures ซึ่งเป็นระบบมาตรฐาน ที่ใช้ในการระบุและติดตามช่องโหว่
- O CVSS v.3.0 หมายถึง Common Vulnerability Scoring System เวอร์ชัน 3.0 ใช้ในการ ประเมินความรุนแรงของช่องโหว่ คะแนนตั้งแต่ 0.0 ถึง 10.0
- O วันที่สแกน หมายถึง วันที่ทำการตรวจสอบช่องโหว่
- ด สถานะ หมายถึง สถานะการดำเนินการของการรายงานผลการแก้ไขช่องโหว่ ดังนี้
 - ยังไม่ได้ดำเนินการ
 หมายถึง ยังไม่มีการรายงานผลการ
 ดำเนินงานของส่วนงาน
 อยู่ระหว่างดำเนินการ
 หมายถึง ส่วนงานรับทราบแล้ว และอยู่ใน ระหว่างการตรวจสอบแก้ไขปัญหา
 ดำเนินการแล้ว
 หมายถึง ส่วนงานตรวจสอบและแก้ไข ช่องโหว่แล้ว
- ๑ รายงานผล หมายถึง การคลิก เพื่อรายงานผลการดำเนินงาน และปรับปรุงสถานะของ รายการช่องโหว่นั้น ๆ มีผลต่อคอลัมภ์สถานะ

CMU Vulnerability Tracking System

รายงานผลการสแกนช่องโหว่

รายงาเ	มผลเป็นกลุ่ม									
ผลการสแกนช่องโหว่ของส่วนงาน				Sear	ch				Q	
เลือก	Host	Name	Detail	Port	Risk	CVE	CVSS v.3.0	วันที่สแกน	สถานะ	รายงานผลการแก้ไข
		PHP Unsupported Version Detection		443	Critical		10	11/1/2022,	ยังไม่ดำเนินการ	รายงานพล
		Dropbear SSH Server < Multiple Vulnerabilities		22	Critical	CVE-	9.8	11/1/2022,	ยังไม่ดำเนินการ	รายงานพล
		Dropbear SSH Server < 4ultiple Vulnerabilities	-	22	Critical	CVE-	9.8	11/1/2022,	ยังไม่ดำเนินการ	รายงานผล
		Dropbear SSH Server < 4ultiple Vulnerabilities	-	22	Critical	CVE-	9.8	11/1/2022,	ยังไม่ดำเนินการ	รายงานผล
		Dropbear SSH Server < Multiple Vulnerabilities		22	Critical	CVE-	9.8	11/1/2022,	ยังไม่ดำเนินการ	รายงานผล

ภาพที่ 5 รายงานผลการสแกนช่องโหว่ของส่วนงาน



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 8/13
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	เสารสนเทศ (CMU VTS)

สามารถดูรายละเอียดของช่องโหว่ได้จากคอลัมน์ "Detail" ด้วยการคลิก link ที่เลขรหัส เพื่อเปิดหน้า เว็บแสดงรายละเอียดของช่องโหว่ แสดงดังภาพที่ 6



ภาพที่ 6 รายละเอียดของช่องโหว่ของแต่ละรายการทรัพย์สินสารสนเทศ อ้างอิงจากเลขรหัส

การรายงานผลการตรวจสอบแก้ไขช่องโหว่ สามารถทำได้ 2 วิธี คือ

- การรายงานผลที่ละรายการ
- การรายงานผลเป็นกลุ่ม

<u>การรายงานผลที่ละรายการ</u>

สามารถทำได้โดยการคลิกปุ่ม "รายงานผล" ด้านท้ายสุดของตาราง (ดูภาพที่ 5 ประกอบ) ของ รายการที่ต้องการรายงานผลการแก้ไข จะปรากฏหน้าต่างการรายงานผลขึ้นมา ประกอบด้วย ผลการ ดำเนินงาน และสถานการณ์ดำเนินงาน (ดังภาพที่ 7) ให้บันทึกรายละเอียดเกี่ยวกับการดำเนินงาน (พอ สังเขป) และสถานะปัจจุบัน หลังจากนั้นคลิกปุ่ม "**บันทึกข้อมูล**" (* แนะนำให้ท่านเปลี่ยนสถานะเป็น<u>อยู่</u> <u>ระหว่างดำเนินการ</u> หากท่านทราบผลการรายงานแล้ว และอยู่ในระหว่างการดำเนินการแก้ไข)



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่	25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ລບັບປรັບປรຸง	ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 9/13	
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CM	U VTS)

ผลการแก้ไขช่องโหว่

ผลการดำเนินงาน*	
	0 / 250
สถานะการดำเนินงาน*	
รอดำเนินการ	Ŧ

* จำเป็นต้องระบุข้อมูล

ปิดหน้าต่าง บันทึกข้อมูล

ภาพที่ 7 หน้าต่างรายงานผลการแก้ไขช่องโหว่

<u>การรายงานผลเป็นกลุ่ม</u>

เป็นการรายงานผลการแก้ไขช่องโหว่เป็นกลุ่ม หรือการรายงานผลการแก้ไขช่องโหว่หัวข้อ เดียวกันแต่แยก CVE หรือ Port เป็นต้น เป็นการรายงานหลาย ๆ รายการพร้อมกัน ด้วยการคลิกช่อง สี่เหลี่ยมหน้ารายการที่ต้องการรายงาน (ดูภาพที่ 5 ประกอบ) หลังจากเลือกครบแล้ว ให้คลิกปุ่ม "รายงานผลเป็นกลุ่ม" จะปรากฏหน้าต่างผลการแก้ไขช่องโหว่ คล้ายกับการรายงานผลทีละรายการ แต่ เป็นการรายงานที่มีผลกับทุกรายการที่เลือก ให้ระบุผลการดำเนินงานที่เกี่ยวข้อง พร้อมทั้งสถานะการ ดำเนินงาน และคลิกปุ่ม "บันทึกข้อมูล"

การจัดการทรัพย์สินสารสนเทศ

รายการทรัพย์สินสารสนเทศของส่วนงาน ในที่นี้ หมายถึง ชื่อโดเมนของระบบสารสนเทศ หรือหมายเลข ไอพีเครื่องแม่ข่าย (IP Address) ที่ติดตั้งระบบสารสนเทศที่ต้องการประเมินช่องโหว่ด้านความปลอดภัย โดยรายการต่าง ๆ เหล่านี้ต้องผ่านการประเมินผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ด้านความมั่นคง ปลอดภัยไซเบอร์ หรือ Business Impact Analysis (BIA) ซึ่งประกอบด้วย ลำดับความสำคัญ โอกาสถูก โจมตี (Likelihood) และผลกระทบ (Impact) ซึ่งจะถูกคำนวณให้เป็นระดับความเสี่ยง (Risk Score) ของ



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25 ม์	มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง ครั้ง	เที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 10/13	
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CMU VT	⁻S)

แต่ละรายการทรัพย์สินสารสนเทศ (Asset) รายการทรัพย์สินสารสนเทศของส่วนงานที่ปรากฏในระบบมา จากการแจ้งตรวจสอบช่องโหว่ในปี 2567 และการประเมิน BIA ของส่วนงานประจำปี

ส่วนงานสามารถปรับปรุง หรือ เพิ่มข้อมูลให้เป็นปัจจุบันได้ โดยมีขั้นตอนดังต่อไปนี้ (ดูภาพที่ 8 ประกอบ)

จัดการทรัพย์สินสารสนเทศของส่วนงาน

+ เพิ่มทรัพย์สินส			การตรวจสอบ	* ยังไม่ได้ยืนยัเ	มรายการทรัพย์สิเ	มสารสนเทศ!							
ทรัพย์สินสารส	สนเทศของ	ส่วนงาน					Searc	h					Q
Host	ลำดับควาเ	มสำคัญ	โอกาสถูกโจมตี	i i	พลกระทบ	ระดับความเสี่ยง		ข้อมูลส่วนบุคคล	VA Package	ปรับปรุงล่า	สุด	จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
								No				จัดการข้อมูล	
										Rows per page:	10 💌	1-10 of 192 <	>

ภาพที่ 8 การจัดการทรัพย์สินสารสนเทศของส่วนงาน

 การปรับปรุงรายการทรัพย์สินสารสนเทศ ด้วยการคลิกปุ่ม "จัดการข้อมูล" ท้ายรายการ ทรัพย์สินสารสนเทศนั้น ๆ หลังจากคลิกแล้วจะปรากฏหน้าต่างบันทึกข้อมูล ดังภาพที่ 9

			10 / 1
ลำดับความสำคัญ *	•	ไอกาสถูกโจมตี *	
Wans:nu *	•	ระดับความเสี่ยง *	
. มีป้อมูลส่วนบุคคล *			
No	*	VA Package *	

ภาพที่ 9 การบันทึก/ปรับปรุงข้อมูลทรัพย์สินสารสนเทศ



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่ 25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 11/13
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	เสารสนเทศ (CMU VTS)

มีขั้นตอนการบันทึก/ปรับปรุงรายการทรัพย์สินสารสนเทศ ดังนี้

- ระบุ<u>ลำดับความสำคัญ</u>ของทรัพย์สินสารสนเทศ (ระดับ 1 5) โดย 5 หมายถึง สำคัญที่สุด
- ระบุโอกาสถูกโจมตีทางไซเบอร์ของทรัพย์สินสารสนเทศ (ระดับ 1 5) โดย 5 หมายถึง มาก

ที่สุด

- ระบุ<u>ผลกระทบ</u>จากการถูกโจมตีของทรัพย์สินสารสนเทศนั้น ๆ ต่อการดำเนินงานที่เกี่ยวข้อง
 (ระดับ 1 5) โดย 5 หมายถึง มีผลกระทบสูงสุด
- ระดับความเสี่ยง (โอกาสถูกโจมตี x ผลกระทบ) จะถูกคำนวณอัตโนมัติ หากมีระดับคะแนน ตั้งแต่ 15 ขึ้นไป ตัวเลือกของ VA Package จะถูกกำหนดเป็น Credential Scan โดยอัตโนมัติ
- ระบุว่าทรัพย์สินสารสนเทศนั้น ๆ มีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล หรือไม่
 (Yes/No) หากมีทรัพย์สินสารสนเทศมีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล ตัวเลือก

ของ VA Package จะถูกกำหนดเป็น Credential Scan โดยอัตโนมัติ

- VA Package เป็นการเลือกประเภทของการตรวจสอบช่องโหว่ทรัพย์สินสารสนเทศ มีให้เลือก
 3 ประเภท ได้แก่

Basic Scan	เป็นการตรวจสอบจากมุมมองภายนอกโดยไม่ต้องอนุญาต
	อะไรเพิ่มเติม
Open Firewall Scan	เป็นการตรวจสอบช่องโหว่ในมุมมองที่เสมือนเชื่อมต่อภายใน
	ระบบเครือข่ายของส่วนงาน

Credential Scan เป็นการตรวจสอบช่องโหว่ในเชิงลึก เหมาะกับทรัพย์สิน สารสนเทศที่มีความสำคัญสูงมาก และทรัพย์สินสารสนเทศที่ มีข้อมูลส่วนบุคคล

เมื่อกำหนดค่าทุกรายการเสร็จสิ้นแล้ว ให้คลิกปุ่ม "บันทึกข้อมูล" หรือ "ปิดหน้าต่าง" หาก ต้องการยกเลิกการบันทึก/ปรับปรุงข้อมูล

 การลบรายการทรัพย์สินสารสนเทศ หรือ ไม่ประสงค์จะตรวจสอบช่องโหว่ของรายการ สารสนเทศนั้น ๆ ให้ทำการแจ้งความประสงค์ด้วยการ คลิกเลือกกล่องสี่เหลี่ยม "ไม่ต้องการ สแกนช่องโหว่" ก่อนการบันทึกข้อมูล จะเป็นการลบรายการดังกล่าว ดังภาพที่ 10



รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่	25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ລບັບປรັບປรຸง	ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 12/13	
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CM	IU VTS)



ภาพที่ 10 การแจ้งลบรายการทรัพย์สินสารสนเทศนั้น ๆ (อ้างอิงจากภาพที่ 9)

การเพิ่มรายการทรัพย์สินสารสนเทศ จากหน้าจอในภาพที่ 8 คลิกปุ่ม

+ เพิ่มทรัพย์สินสารสนเทศ เพื่อเพิ่มรายการทรัพย์สินสารสนเทศ จะปรากฏหน้าต่างเพิ่ม

ข้อมูลดังภาพที่ 11

เพิ่มทรัพย์สินสารสนเทศของส่วนงาน

			0 / 10
ลำดับความสำคัญ *	•	โอกาสถูกโจมตี *	-
ผลกระทบ *	•	ระดับความเสี่ยง *	
มีข้อมูลส่วนบุคคล *	•	VA Package *	

ปิดหน้าต่าง บันทึกข้อมูล

ภาพที่ 11 การเพิ่มรายการทรัพย์สินสารสนเทศ

รายละเอียดของการบันทึกข้อมูล อยู่ในหัวข้อ<u>การปรับปรุงรายการทรัพย์สินสารสนเทศ</u> หน้า 10

 การยืนยันรายการทรัพย์สินสารสนเทศ หลังจากการเพิ่ม แก้ไข/ปรับปรุงรายการทรัพย์สิน สารสนเทศของส่วนงานเสร็จสิ้นแล้ว ต้องทำการยืนยันเพื่อแจ้งความประสงค์ตรวจสอบช่องโหว่

ด้วยการคลิกปุ่ม ด้วยการคลิกปุ่ม <u>แก้ไขข้อมูล</u>ได้ หากต้องการแก้ไขข้อมูลหลังจากยืนยันแล้ว ให้แจ้งความประสงค์ได้ที่อีเมล security@cmu.ac.th

|--|

รหัสเอกสาร	CSD_OM_001	วันที่เผยแพร่	25 มิถุนายน 2568
ประเภทเอกสาร	คู่มือการใช้งานระบบสารสนเทศ	ฉบับปรับปรุง	ครั้งที่ 1
ประเภทชั้นความลับ	เอกสารเผยแพร่ (ภายในมหาวิทยาลัย)	หน้า 13/13	
ชื่อเอกสาร คู่มือการ	ใช้งานระบบติดตามการแก้ไขช่องโหว่ระบบ	สารสนเทศ (CM	U VTS)

หากท่านมีคำถาม หรือข้อเสนอแนะใด ๆ นอกเหนือจากคู่มือฉบับนี้ สามารถติดต่อสอบถามได้ที่อีเมล security@cmu.ac.th ฝ่ายความมั่นคงปลอดภัยไซเบอร์ สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่