มาตรการด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานสังกัด สำนักงานสาธารณสุขจังหวัดสงขลา

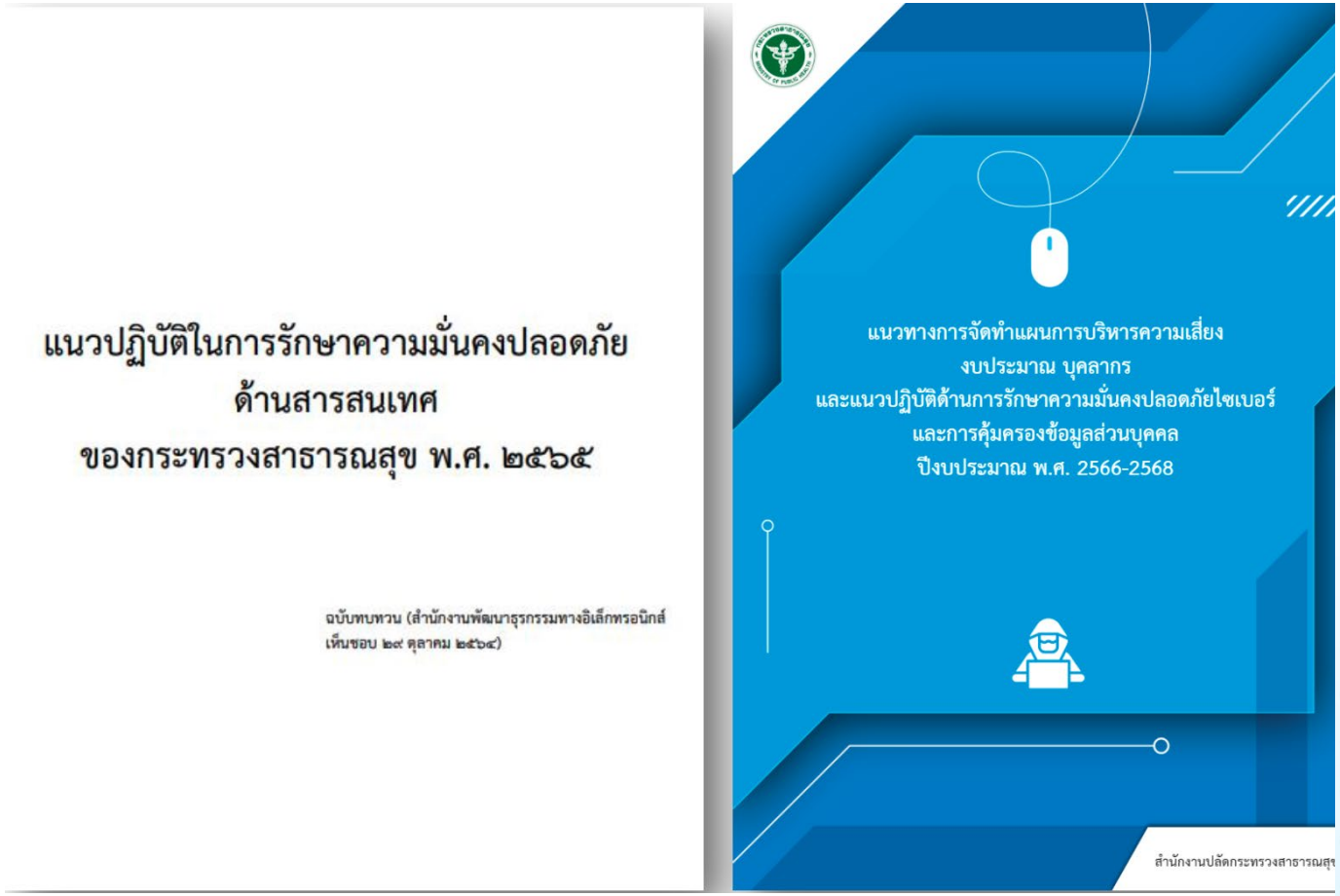
นายสุทธิพงค์ อยู่หนู
หัวหน้าฝ่ายดิจิทัลและข้อมูลสุขภาพ
4 เมษายน 2567

มาตรการยกระดับความมั่นคงปลอดภัย

ข้อสั่งการ

- หนังสือ สธ. 0212/ว4968 เรื่อง เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์
- หนังสือ สธ.0212/ว1908 เรื่อง มาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์
- หนังสือ สธ.0212/ว8584 เรื่อง ประกาศย้ำเตือนให้ปฏิบัติตาม "มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์กระทรวงสาธารณสุข ฉบับที่ 1"
- หนังสือสธ.0212/ว20268 เรื่องย้ำเตือนให้ทุกหน่วยงานใช้ซอฟต์แวร์ที่ถูกกฎหมาย
- หนังสือ สธ.0212/ว22582 เรื่อง สั่งการให้ดำเนินการมาตรการความมั่นคงปลอดภัยไซเบอร์และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- หนังสือ สธ 0212/ว34399 เรื่อง ข้อสั่งการยกระดับมาตรการไซเบอร์ประเด็นการสำรองข้อมูลและซอฟต์แวร์ลิขสิทธิ์
- หนังสือ สธ. 0212.07/ว4914 เรื่อง เครื่องมือสำหรับทดสอบความมั่นคงปลอดภัยเว็บแอปพลิเคชัน
- หนังสือ สธ. 0212/ว9097 เรื่อง ข้อสั่งการมาตรการยกระดับความมั่นคงปลอดภัยไซเบอร์ของกระทรวงสาธารณสุข

แนวทางปฏิบัติของระบบเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์



ที่มา https://cyber.moph.go.th/

ข้อปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ สำนักงานสาธารณสุขจังหวัดสงขลา

1. ตั้งค่า Login ก่อนเข้าใช้งาน โดยกำหนดบัญชีผู้ใช้งาน Username และ รหัสผ่าน Password เพื่อใช้ในการพิสูจน์ตัวตน
   - ประกอบด้วยตัวเลข ตัวอักษร และตัวอักขระพิเศษ ไม่น้อยกว่า 8 ตัวอักษร
   - คาดเดายาก (แต่ต้องจำได้)
2. ไม่เปิดเผย Username และ Password ให้แก่บุคคลอื่นทราบ
3. ลงชื่อเข้าใช้งานคอมพิวเตอร์ด้วยชื่อบัญชีผู้ใช้ของตัวเองเท่านั้น
4. เปลี่ยนรหัสผ่าน (Password) ไม่เกิน 180 วัน หรือทุกครั้งที่มีการแจ้งเตือน
5. ตั้งค่า Screen Saver Log out หลังจากไม่ใช้งานภายใน 10 นาที
6. Log Out หน้าจอทุกครั้งเมื่อไม่ใช้งาน
7. เปิดการทำงาน Scan Virus
8. สแกนไวรัสทุกครั้งเมื่อมีการเชื่อมต่อกับอุปกรณ์ภายนอก
9. ห้ามนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงออกนอกหน่วยงาน
10. ห้ามนำอุปกรณ์ภายนอกเชื่อมต่อเครือข่ายโดยไม่ได้รับอนุญาต
11. ไม่นำเข้า ส่งต่อ เผยแพร่ข้อมูลอันเป็นเท็จ ลามก อนาจาร หรือที่มีผลกระทบต่อผู้อื่น
12. สำรองข้อมูลไว้กับอุปกรณ์สำรองข้อมูลภายนอก (External Storage) อย่างสม่ำเสมอ
13. ไม่ดาวน์โหลดและติดตั้งโปรแกรมที่มาจากแหล่งข้อมูลที่ไม่น่าเชื่อถือหรือไม่ปลอดภัย
14. หากจำเป็นต้องติดตั้งโปรแกรมเพิ่มเติม ให้แจ้งฝ่ายดิจิทัลและข้อมูลสุขภาพทราบเพื่อพิจารณา
15. มีปัญหาการใช้งาน/พบเจอเครื่องคอมพิวเตอร์มีอาการผิดปกติ ให้รีบแจ้งฝ่ายดิจิทัลและข้อมูลสุขภาพเพื่อตรวจสอบทันที
16. กรณีมีเจ้าหน้าที่ในกลุ่มงาน/ฝ่าย ลาออก/ย้าย ไปจาก สสจ. ให้แจ้งฝ่ายดิจิทัลและข้อมูลสุขภาพทันที เพื่อดำเนินการปิดการใช้งานบัญชีผู้ใช้อินเตอร์เน็ต
17. ห้ามถอดถอนโปรแกรม GLPI ซึ่งใช้สำหรับบริหารจัดการสินทรัพย์

หมายเหตุ : หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ username และรหัสผ่าน Password ของบุคคลใด บุคคลนั้นต้องรับผิดชอบต่อการกระทำความผิดนั้นตามกฎหมายข้อบังคับที่เกี่ยวข้อง

ศึกษารายละเอียดเพิ่มเติมได้ที่

แนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานสาธารณสุขจังหวัดสงขลา พ.ศ. 2567

มาตรการการยกระดับด้านความมั่นคงปลอดภัยไซเบอร์

- ตรวจสอบความปลอดภัยและทบทวนสิทธิ์ในการเข้าถึงจากระยะไกล(Remote) และการใช้งานเครือข่ายส่วนตัวแบบเสมือน (VPN)
- ปิดการใช้งาน Service Port ที่ไม่ได้ใช้งานและมีความเสี่ยง หากจำเป็นควรใช้งาน VPN
- ปิดกั้น หมายเลข IP Address จากต่างประเทศหรือในประเทศ/มีพฤติกรรมที่น่าสงสัย โดยทันที
- เตรียมเจ้าหน้าที่ เฝ้าระวังภัยคุกคามทางไซเบอร์ โดยสามารถเข้าถึงห้อง SERVER ได้โดยเร็ว
- หากเกิดสถานการณ์ฉุกเฉินด้านภัยคุกคามทางไซเบอร์ ให้การตัดการเชื่อมต่อกับเครือข่ายในทันที
- สำรองข้อมูลแบบ Full Backup และสำเนาไว้ในสื่อบันทึกข้อมูลแบบ Offline นำไปจัดเก็บไว้ในที่ปลอดภัยและ ไม่เชื่อมต่อกับระบบเครือข่าย เพื่อใช้ในกรณีฉุกเฉินอย่างน้อย 2 ชุด

สถิติเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

ปีงบประมาณ 2567

ประเภทหน่วยงาน	เหตุการณ์
สำนักงานสาธารณสุขจังหวัด	2
โรงพยาบาล	4
สาธารณสุขอำเภอ	0

แหล่งข้อมูล HealthCERT สธ. และ สกมช. ข้อมูล ณ เดือน มีนาคม 2567

ข้อสั่งการ/มาตรการสำหรับหน่วยงานสังกัดสำนักงานสาธารณสุขจังหวัดสงขลา

- ปิดระบบข้อมูล Datacenter สสจ./อำเภอ และระบบอื่น ๆ ที่มีการจัดเก็บข้อมูลส่วนบุคคล ยกเว้น HIS
- ระงับการส่งข้อมูลไปยัง R12 Network (หมอรู้จักคุณ)
- ให้หน่วยบริการนำส่งข้อมูล HDC ผ่านทางเว็บไซต์ HDC โดยตรง
- รพ.สต.ส่งข้อมูลเบิกจ่าย OPPP นำส่งผ่านเว็บไซต์ สปสช. โดยตรง

ผลกระทบ

ระบบข้อมูล

- ระบบ Songkhla Health Alert (งานอนามัยแม่และเด็ก)
- ระบบ Smart Bone (งานผู้สูงอายุ)
- ระบบการคืนข้อมูล Data Exchange รายงานที่ไม่มีใน HDC
- ระบบรายงานตัวชี้วัด ประเมินผลงาน / นิเทศงาน / ตรวจราชการ
- ระบบบริหารเตียง
- ระบบติดตามผู้ป่วย DMHT
- ระบบรายงาน Smart4D เขตสุขภาพที่ 12
- ระบบรายงานสาเหตุการตาย
- ระบบรายงานสนับสนุนกลุ่มงาน / ฝ่าย / รพ / สสอ / รพ.สต (Songkhla SIS)

การส่งต่อข้อมูล

- ระบบรายงานการส่งวัคซีน DTP ประจำสัปดาห์ สคร.สงขลา
- ระบบรายงานและตัวชี้วัด
- การส่งข้อมูลเบิกชดเชยบริการ ระบบ OPPP สปสช.
- การส่งข้อมูล summary smart 4D เขตสุขภาพที่ 12

มาตรการยกระดับด้านความมั่นคงปลอดภัยไซเบอร์
CO-CSIRT

ระดับความเสี่ยง		หัวข้อการประเมิน
ความเสี่ยงสูง		(1.1) Backup
	**	(1.2) Antivirus Software
		(1.3) Access Control (Public และ Private)
		(1.4) Privileged Access Management (PAM)
ความเสี่ยงปานกลาง		(2.1) Business Continuity Plan (BCP)
		(2.2) Disaster Recovery site (DR)
		(2.3) OS Patching
	**	(2.4) Multi-Factor Authentication (2FA)
	**	(2.5) Web Application Firewall (WAF)
	**	(2.6) Log Management
	**	(2.7) Security Information & Event Management (SIEM)
	**	(2.8) Vulnerability Assessment (VA Scan)
ความเสี่ยงต่ำ		(3.1) Software Update
	**	(3.2) Penetration Testing

1 22 มีนาคม 67

จัดตั้ง line กลุ่ม CO-CSIRT เพื่อเป็นช่องทางการสื่อสาร

2 25 มีนาคม 67

ประชุมชี้แจงแนวทางการดำเนินงาน การประเมิน และยกระดับความมั่นคงปลอดภัยไซเบอร์

3 3 เมษายน 67

หน่วยบริการประเมินตนเอง ตามเกณฑ์ และแนวทาง CO-CSIRT INET

4 4-9 เมษายน 67

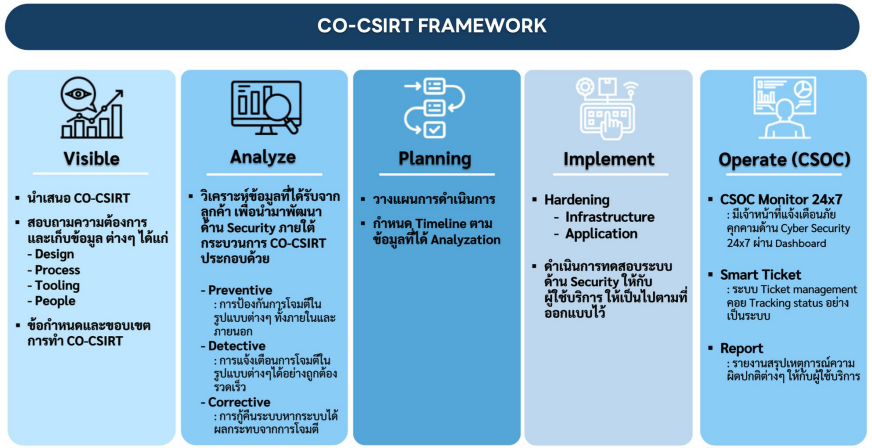
INET ประสานงานขอนัดหมายประเมินความเสี่ยงด้าน Cyber security ตามหลักเกณฑ์ในการประเมิน

5 11-15 เมษายน 67

INET ตรวจสอบยืนยันผลที่ หน่วยบริการประเมินตนเอง และ INET ประเมิน พร้อมให้คำแนะนำเพื่อการปรับปรุง

6 17-26 พฤษภาคม 67

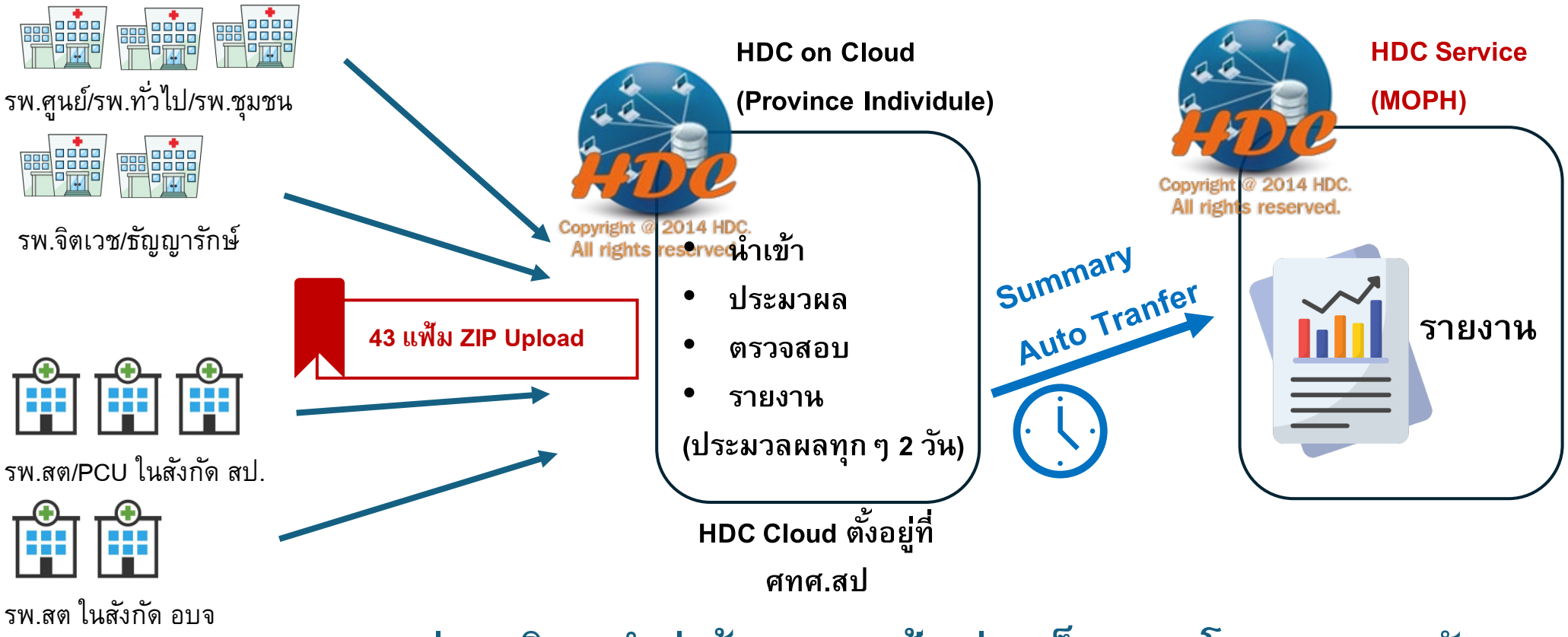
หน่วยบริการปรับปรุง และพัฒนายกระดับความมั่นคงปลอดภัยไซเบอร์ และให้ทาง INET ตรวจสอบและยืนยัน ปรับปรุงสถานะและระดับความเสี่ยง



ทีมา INET

แนวทางแก้ไขและการดำเนินการ

ข้อมูลรายงาน ตัวชี้วัด และการคืนข้อมูล Date Exchange



- หน่วยบริการนำส่งข้อมูล 43 แฟ้ม ผ่านเว็บ HDC โดยตรงทุก 3 วัน
- ปฏิบัติตามแนวทางและมาตรการความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด

ขอบคุณครับ