ครอบคลุม
ทุกความปลอดภัย
ทางไซเบอร์

nt โทรคมนาคม แห่งชาติ

ที่พร้อมดูแลความปลอดภัย
จากผู้เชี่ยวชาญมืออาชีพ

Agenda

- เกณฑ์การประเมิน CO-CSIRT โรงพยาบาล โรงพยาบาลโดนประเมินอะไร
- ใครสามารถประเมิน รพ. ได้บ้าง
- Solution ที่สามารถนำเสนอโรงพยาบาลตามเกณฑ์การประเมิน
- การตรวจประเมินตามเกณฑ์การประเมิน CO-CSIRT
- Flow ในการดำเนินงาน

โรงพยาบาล โดนประเมินอะไร

แนวทางการดำเนินงาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับโรงพยาบาลของรัฐ

พ.ศ. 2567

หัวข้อความเสี่ยงสูง	รายละเอียดหัวข้อการประเมิน	ISO 27001 Reference	ข้อบังคับประเมิน
(1.1) Backup : การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย	มีการสำรองข้อมูลอย่างน้อย 1 วัน และย้อนหลังได้ 7 วันเป็นอย่างน้อยตามมาตรฐานโดยจัดเก็บบนระบบ Logical HDD หรือ Physical HDD **คำแนะนำ:** ในการสำรองข้อมูลเพิ่มเติม: จัดเก็บ Backup ในรูปแบบ 3-2-1 (1) สำเนาข้อมูลไว้บนระบบ 3 ชุด (2) สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน 2 ชุด (3) สำเนาข้อมูลไว้แบบ Offsite หรือ Cloud 1 ชุด โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.13 Information backup	บังคับการดำเนินการ (Mandatory)
(1.2) Antivirus Software : โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับ ป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์	มีการติดตั้ง Next-gen Anti-virus หรือ EDR หรือ XDR ที่เครื่องฝั่ง Server ทุกเครื่องและอัปเดต Signature ทุกวัน และมีเอกสารแนบระบุ Product และ version อย่างละเอียดชัดเจน โดย Anti-virus จะต้อง Active ตลอดเวลา ในการดำเนินการ Phase1 จะตรวจสอบติดตั้งเฉพาะกลุ่ม Server ก่อนเท่านั้น โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.7 Protection againts malware	บังคับการดำเนินการ (Mandatory)
(1.3) Access Control (Public และ Private) : การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายในประเทศ และต่างประเทศ	มีระบบ Security ในการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private โดยมีรายละเอียดดังนี้ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน (1) ดำเนินการกำหนด Whitelist Port และไม่เปิด Port ที่มีความเสี่ยงต่อการโดนโจมตีปัจจุบันได้แก่ 7, 19, 20, 21, 22, 23, 25, 37, 53, 69, 79, 80, 110, 111, 135, 137, 138, 139, 445, 161, 443, 512, 513, 514, 1433, 1434, 1723,3 389, 8080 (หากมีความจำเป็นในการเปิดจะต้องทำการกำหนด Source และ Destination ให้ชัดเจน) (กรณีใช้งาน Port 80, 443 จะต้องมี WAF ในหัวข้อความเสี่ยงที่ 2.5) (2) มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และ อุปกรณ์ลูกข่าย (Client) (3) มีการใช้งาน VPN ในการเข้าถึงเครื่องอุปกรณ์แม่ข่าย (Server) แทนการเข้าใช้งานผ่าน Public (4) มีการ Block การใช้งาน International Traffic กรณีไม่มีความจำเป็นในใช้งาน (Optional ตามการใช้งาน) (5) มีการใช้งาน Terminal server ในการเข้าถึงระบบ Server แทนที่คอมพิวเตอร์ต้นทาง	8.20 Network Security 8.21 Security of network services 8.22 Segregation of network 8.23 Web filtering	บังคับการดำเนินการ (Mandatory)
(1.4) Privileged Access Management (PAM) : โซลูชันการรักษาความปลอดภัยของข้อมูลประจำตัวที่ช่วยปกป้องค์กรจากภัยคุกคามทางไซเบอร์ด้วยการติดตาม ตรวจหา และป้องกันการใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูง	มีการควบคุมการเข้าถึงระบบโดยใช้งานสิทธิ์ระดับ High privileged ดังนี้ (1) ดำเนินการ Disable Administrator / Root / Admin บนระบบเพื่อป้องกันการโจมตี ในรูปแบบ Brute Force (2) มี Policy การเปลี่ยน Password อย่างน้อยทุก 3 เดือน (3) มีการกำหนด Role-base access ในการเข้าถึงระบบ (4) มีการสร้าง Account ตาม User ที่ใช้งานในระบบ (5) มีการตั้ง Password ให้ Complex ตามมาตรฐานอย่างน้อย 10 Digi ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.20 Network Security 8.21 Security of network services 8.22 Segregation of network 8.23 Web filtering	บังคับการดำเนินการ (Mandatory)

หัวข้อความเสี่ยงปานกลาง	รายละเอียดหัวข้อการประเมิน	ISO 27001 Reference	ข้อบังคับประเมิน
(2.1) Business Continuity Plan (BCP) : แผนที่กำหนดแนวทางการดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ส่งผลให้กระบวนการทำงานของหน่วยงานหยุดชะงัก เพื่อให้สามารถกลับมาดำเนินการได้อย่างต่อเนื่อง	มีการทดสอบ Business Continuity Plan (BCP) อย่างน้อย ปีละ 1 ครั้ง และ มีการจัดทำรายงานถึงขั้นตอนการดำเนินการที่ชัดเจนรวมถึงระยะเวลาดำเนินการและผู้ที่เกี่ยวข้องในการดำเนินการงานดังนี้ (1) การบริหารจัดการความเสี่ยง (Risk Management) (2) การบริการจัดการด้าน Resource (Resource Management) (3) การวางแผนความต่อเนื่องจากธุรกิจที่เกิดขึ้น (Business Continuity Planning) (4) การทดสอบ (Testing) (5) การปรับปรุงและแก้ไข (Review & Update) โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	5.30 ICT readiness for business continuity	บังคับการดำเนินการ (Mandatory)
(2.2) Disaster Recovery site (DR) : ศูนย์สำรองข้อมูล สำหรับแก้ไขปัญหาระบบสารสนเทศ ที่เกิดขึ้นจากภัยพิบัติต่างๆ ให้สามารถทำงานได้อย่างต่อเนื่อง	มีระบบ Disaster Recovery site (DR) ในกรณีฉุกเฉินที่ระบบหลักมีปัญหาและไม่สามารถใช้งานได้ โดยจะต้องมี DR-Site โดยยึดจากมาตรฐาน ISO27001 และนำมาปรับใช้งานดังนี้ (1) ระยะห่างระหว่าง DC-Site กับ DR-Site ต้องไม่น้อยกว่า 60 กิโลเมตร (2) ต้องมีระบบฐานข้อมูลที่สำคัญอย่างน้อย 1 ระบบขึ้นบน DR-site (3) RTO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง หรือขึ้นอยู่กับ Solution (4) RPO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง (5) ต้องมีเอกสารสรุปผลการทดสอบการดำเนินการ DR-Site (6) ระบบต้องมีมาตรฐาน ISO ดังนี้เป็นอย่างน้อย - ISO27001: Information Security Management System - ISO27799 : Health Informatics-Information Security Management โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	5.30 ICT readiness for business continuity	ตัวเลือกในการดำเนินการ (Optional)
(2.3) OS Patching : การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น	มีการอัปเดต Security Patching ในระดับ Operating System ทั้ง Windows / Linux ทุกๆ 6 เดือน หรือทันทีหากมี Critical security patching โดยการตรวจสอบจะต้องไม่มี Security Patch ระดับ Critical , High เกิดขึ้น โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.8 Management of technical vulnerabilities	บังคับการดำเนินการ (Mandatory)

หัวข้อความเสี่ยงปานกลาง	รายละเอียดหัวข้อการประเมิน	ISO 27001 Reference	ข้อบังคับประเมิน
(2.4) Multi-Factor Authentication (2FA) : การยืนยันตัวตน 2 ชั้น เป็นการเข้าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน	มีการใช้งานระบบ Multi-Factor Authentication (2FA) เพื่อยืนยันตัวตน 2 ชั้นในการเข้าถึงระบบต่างๆ สำหรับ Admin ที่ใช้งานระบบดังนี้ (1) การ Login แบบ Multi-factor ไปยังระบบ VPN Access (2) การ Login แบบ Multi-factor ไปยังอุปกรณ์ Network (3) การ Login แบบ Multi-factor ไปยังอุปกรณ์ Security (4) การ Login แบบ Multi-factor ไปยัง Hypervisor (5) การ Login แบบ Multi-factor ไปยัง Operating system โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.5 Secure authentication	บังคับการดำเนินการ (Mandatory)
(2.5) Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชันโดยเฉพาะ เพื่อป้องกันการโจมตีไปยังระบบเว็บแอพพลิเคชั่นขององค์กร	มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application ในรูปแบบCloud security เพื่อป้องกันการโจมตีตามมาตรฐาน OWASP Top 10 ได้เป็นอย่างน้อยตามรายละเอียดดังนี้ (1) Broken Access Control (2) Cryptographic Failures (3) Injection (4) Insecure Design (5) Security Misconfiguration (6) Vulnerable and Outdated Components (7) Identification and Authentication Failures (8) Software and Data Integrity Failures (9) Security Logging and Monitoring Failures (10) Server-Side Request Forgery (SSRF) Reference : https://owasp.org/www-project-top-ten/ และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.23 Web filtering	บังคับการดำเนินการ (Mandatory)
(2.6) Log Management : การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	มีระบบการจัดเก็บ Log อินเตอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ.ฯ อย่างน้อย 90 วัน โดยรายละเอียดทั้งหมดจะต้องมีเอกสารแนบอย่างละเอียดและชัดเจน	8.15 Logging	บังคับการดำเนินการ (Mandatory)

ปานกลาง	รายละเอียดหัวข้อการประเมิน	ISO 27001 Reference	ข้อบังคับประเมิน
tion & Event Log และ Event ต่าง ๆ วามเชื่อมโยงของ วามปลอดภัยทั้งหมด น่งของภัยคุกคามให้ ทำให้สามารถป้องกัน ย่างรวดเร็ว	มีระบบ SIEM เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OS) โดยจะต้องคลอบคลุมการตรวจจับพื้นฐานดังนี้ **(2.7.1) <u>Common Alert Trigge</u>** 2.7.1.1 ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้าระบบและการ Scan Port (Port Scanning) 2.7.1.2 Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่าง ๆ ที่เกิดขึ้น หรือจาก Signature 2.7.1.3 Blacklist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ที่เป็น Blacklist และระบุการเปิด Connection ได้ 2.7.1.4 Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต หรือไม่มีสิทธิ์เข้าถึงระบบ 2.7.1.5 DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ทั้งภายนอกและภายใน 2.7.1.6 Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลที่สำคัญของระบบที่ไม่อนุญาต ให้เข้าถึง **(2.7.2) <u>Alert & Notification</u>** 2.7.2.1 สามารถแจ้งเตือนภัยคุมคามต่าง ๆ ที่เกิดขึ้นได้ผ่านทาง Email และ Chat 2.7.2.2 สามารถแจ้งเตือนผ่าน IOC ไปยังหน่วยงานอื่น ๆ ได้ **(2.7.3) <u>Dashboard & Report</u>** 2.7.3.1 มี Dashboard เพื่อควบคุมและตรวจสอบพฤติกรรมผิดปกติที่เกิดขึ้นกับระบบโดยสามารถแบ่งตาม Severity ได้ชัดเจนรวมถึงมี Timestamp 2.7.3.2 มีการสรุป Report ประจำเดือนเพื่อรายงานเหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.16 Monitoring Activities	บังคับการดำเนินการ (Mandatory)
sessment (VA ระบบ เพื่อให้ทราบถึง บความรุนแรง ของ การถูกโจรกรรมข้อมูล	มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีละ 1 ครั้ง ในระดับ Operating system (OS) โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ต่างๆที่เกิดขึ้นโดยจะต้องไม่มีความเสี่ยงระดับ Critical , High ในระบบที่ตรวจสอบ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.8 Management of technical vulnerabilities	บังคับการดำเนินการ (Mandatory)

หัวข้อความเสี่ยงต่ำ	รายละเอียดหัวข้อการประเมิน	ISO 27001 Reference	ข้อบังคับประเมิน
(3.1) Software Update : การตรวจสอบ Version ของ Software ให้เป็น Version Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้นใน Software Version ก่อนหน้า	มีการอัปเดต Software Patching ของระบบ HIS และมีการทำ Penetration Testing อย่างน้อยปีละ 1 ครั้ง หรือ มีการออก Major version โดยจะต้องดำเนินการแก้ไขช่องโหว่ใน **ระดับ Severity Critical และ High** เป็นอย่างน้อย โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.19 Installation of software on operation systems software on operation systems	บังคับการดำเนินการ (Mandatory)
(3.2) Penetration Testing : การทดสอบการเจาะระบบ	มีการทำ Penetration Testing ของ Web Application ในรูปแบบของ Graybox หรือ Blockbox อย่างน้อยปีละ 1 ครั้ง และดำเนินการแก้ไขโดยจะต้องไม่มีช่องโหว่ระดับ Severity Critical , High เกิดขึ้นและไม่มีช่องโหว่ที่เกิดขึ้นตามมาตรฐาน OWASP TOP10 และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน	8.8 Management of technical vulnerabilities	บังคับการดำเนินการ (Mandatory)

ใครสามารถประเมินได้บ้าง

Dashboard การยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานปลัดกระทรวงสาธารณสุข

แนวทางการประเมิน Cybersecurity สำหรับ รพ.

แนวทางการประเมิน cybersecurity dashboard

- คณะกรรมการ/คณะทำงาน CISO ระดับเขตสุขภาพ เป็นหน่วยงานประเมิน Cybersecurity Dashboard
- ระยะเวลา ก.ค. - ก.ย. 67 ให้คณะกรรมการ/คณะทำงาน CISO ระดับเขต ใช้เกณฑ์การประเมิน Cybersecurity Assessment Matrix โดยจะใช้ผลประเมินจากบริษัทเอกชน หรือตรวจประเมินกันเองผ่านคณะกรรมการ/คณะทำงาน CISO ระดับเขต ก็ได้
- ศทส. รับข้อมูลผลประเมิน (เขียว/ต่ำ, เหลือง/กลาง, แดง/สูง) จาก คณะกรรมการ/คณะทำงาน CISO ระดับเขตสุขภาพ
- โดยจัดส่งมาที่ health-cirt@moph.go.th ทุกวันพฤหัสบดี ศทส.จะ Update ข้อมูลทุกวันศุกร์นำขึ้น Dashboard (https://ict.moph.go.th/th/extension/1524)
- ตั้งแต่ ต.ค.67 เป็นต้นไปจะใช้เกณฑ์ใหม่ที่ทำการตกลงกับเขตสุขภาพทั้ง 12 เขตสุขภาพ

Partner/บริษัทเอกชน ที่กระทรวงสาธารณสุขได้ประสาน ให้ช่วยดำเนินการประเมินโดยไม่คิดค่าใช้จ่าย เบื้องต้น

บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)

บริษัท พาโล อัลโต เน็ตเวิร์กส์ (ประเทศไทย) จำกัด

บริษัท อี-ซี.โอ.พี (ประเทศไทย) จำกัด/บริษัท เบย์ คอมพิวติ้ง จำกัด (BAYCOMS)

บริษัท ซีเคียวอินโฟ จำกัด

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

บริษัท พีทีที ดิจิตอล โซลูชั่น จำกัด

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สารบัญ (ต่อ)

หน้า

NT สามารถเสนออะไรได้?

1

เสี่ยงสูง

ทำทันที

- 1.1 BACKUP
- 1.2 Antivirus Software
- 1.3 Access Control (Public และ Private)
- 1.4 Privileged Access Management (PAM)

2

เสี่ยงกลาง

ควรต้องทำ

- 2.1 Business Continuity Plan (BCP)
- 2.2 Disaster Recovery Site (DR)
- 2.3 OS Patching
- 2.4 Multi-Factor Authentication
- 2.5 Web Application Firewall
- 2.6 Log Management
- 2.7 Secruity Information & Event Mnt
- 2.8 Vulnerbility Assessment

3

เสี่ยงต่ำ

เพิ่มความมั่นคง

- 3.1 Software Update
- 3.2 Penetration Testing
- 3.3 Dashboard
- 3.4 Cybersecurity Operations Center (CSOC)

บริการของ NT ด้านการปรับปรุงระบบความปลอดภัยไซเบอร์

CYFENCE

เสี่ยงสูง

ทำทันที

1

- 1.1 BACKUP
- 1.2 Antivirus Software
- 1.3 Access Control (Public และ Private)
- 1.4 Privileged Access Management (PAM)

บริการ NT Backup

มีการสำรองข้อมูลอย่างน้อย 1 วัน
และย้อนหลังได้ 7 วันเป็นอย่างน้อย
ตามมาตรฐาน ผ่านระบบ NT cloud

File อัปขึ้น Cloud

S : 500 GB	ราคา 2,200 บาท
M : 1,000 GB	ราคา 4,200 บาท
L : 2,000 GB	ราคา 8,200 บาท

บริการ Antivirus

มีบริการให้ทั้งแบบติดตั้งบน Server
และมีบริการสำหรับ Client
โดยสามารถเลือกใช้ได้ตามความต้องการ

1 Server	2,900
10 Client	19,200

บริการ All@Secure

มีระบบ Security ในการควบคุม Policy
การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private
โดยมี สามารถเปิดปิด Portที่มีความเสี่ยงโดนโจมตีได้
แบ่ง Zone, VPN และ Block Connection
รวมถึงให้คำแนะนำในการกำหนด Policy และ การตั้งค่าการเข้าถึงต่าง ๆ

เริ่มต้น 4,400 บาท (Concurrent Device 100)

บริการของ NT ด้านการปรับปรุงระบบความปลอดภัยไซเบอร์

CYFENCE

เสี่ยงกลาง 2 ควรต้องทำ

- 2.1 Business Continuity Plan (BCP)
- 2.2 Disaster Recovery Site (DR)
- 2.3 OS Patching
- 2.4 Multi-Factor Authentication
- 2.5 Web Application Firewall
- 2.6 Log Management
- 2.7 Secruity Information & Event Mnt
- 2.8 Vulnerbility Assessment

บริการ Business Resiliency

บริการบริหารความต่อเนื่องแบบครบวงจร
เพื่อให้ธุรกิจสามารถดำเนินต่อได้
แม้เกิดเหตุการณ์ไม่คาดฝัน เช่น โรคระบาด
น้ำท่วม ไฟไหม้ ประท้วง ก่อการร้าย ฯลฯ

CALL

บริการ All@Secure

เป็นอุปกรณ์ด้านการรักษาความปลอดภัยระบบ IT
สามารถทำ MFA ก่อนเข้าถึง
อุปกรณ์ Firwalle และเครือข่าย

เริ่มต้น 4,400 บาท (Concurrent Device 100)

บริการ Vulnerbility Assessment

บริการตรวจสอบช่องโหว่ของระบบ
ตั้งแต่ช่องโหว่ในกระบวนการทำงานของระบบ
เซิร์ฟเวอร์ และเครือข่าย ไปจนถึงอุปกรณ์รักษาความปลอดภัย

เริ่มต้น 21,000 บาท/ ครั้ง ไม่เกิน 5 IP

บริการ DR-SITE

บริการพื้นที่ DR SITE (Warm Site)

CALL

บริการ WAF

ปกป้องระบบ Web Application ตาม OWASP Top 10 : 2021
เริ่มต้น Bandwidth 10 Mbps

ราคา 3,500 บาท/เดือน

บริการ Mini SIEM | บริการ CSM

เก็บล็อกตาม พ.ร.บ. รวมถึงทำการเฝ้าระวัง
และแจ้งเตือนยามเกิดเหตุภัยคุกคาม

MINI SIEM	200 EPS ราคา 21,200 ต่อเดือน
CSM	110 EPS ราคา 23,900 ต่อเดือน

* ราคายังไม่รวม Event Collector

บริการของ NT ด้านการปรับปรุงระบบความปลอดภัยไซเบอร์

CYFENCE

เสี่ยงต่ำ 3

เพิ่มความมั่นคง

3.1 Software Update

3.2 Penetration Testing

Dashboard

Cybersecurity Operations Center (CSOC)

บริการ Penetration Testing

บริการทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว่ และแก้ไขปรับปรุงจุดอ่อน

1 ระบบ เริ่มต้น 80,000 บาท

บริการ Mini SIEM

จัดเก็บล็อกเป็นศูนย์กลาง และมีหน้าจอ Dashboard โดยตั้งศูนย์ไว้ที่ Data Center ของตัวเอง

MINI SIEM 200 EPS ราคา 21,200 ต่อเดือน

บริการ Cybersecurity Monitoring

บริการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ และความปลอดภัยของระบบเทคโนโลยีสารสนเทศผ่านศูนย์ปฏิบัติการ Cybersecurity Operations Center (CSOC)

CSM 110 EPS ราคา 23,900 ต่อเดือน

* ราคายังไม่รวม Event Collector

ข้อแตกระหว่าง
Mini SIEM กับ
Cybersecurity Monitoring

Mini SIEM

1. Dashboard
2. Log management
3. Smart Report & Alert
4. Standard Warranty 5x8xNBD (Remote Only)
5. ผู้ใช้บริการ Monitor ด้วยเอง

Cybersecurity Monitoring

1. Monitoring 24x7
2. Log 90 วัน
3. Log แบบ off-line ระยะเวลา 1 ปี
4. บริการแจ้งเตือน (Incident Notification)
5. จัดทำ Use Case ให้จำนวน 17 use cases/ปี (ครั้งแรก)
6. จัดทำ Customize Use Case (Advance Analytic & Threat Intelligence) ให้จำนวน 12 use cases/ปี
7. จัดทำ SIEM portal access ให้ จำนวน 1 account
8. บริการ Web Monitoring 1 Webpages
9. จัดทำ Monthly Report

Cybersecurity Services Certified


TÜV NORD

CERTIFICATE

Management system as per
ISO/IEC 27001 : 2013

National Telecom Public Company Limited
Security Operation Center (SOC) Included the Disaster Recovery Site
53/58 Moo 8 Tiwanon Rd., Bang Krasor, Muaang
Nonthaburi 11000
Thailand

Scope

Provision for the management, operation and maintenance of Security Operation Center providing Managed Security Service and Secure Log Mangement including the infrastructure required to supporting the provision of stated services

As per the Statement of Applicability, V.7.3, Date 15.06.2018

TUV NORD CERT GmbH


FROST & SULLIVAN

2017 BEST PRACTICES AWARD

THAILAND
MANAGED SECURITY
SERVICE PROVIDER OF THE YEAR


FROST & SULLIVAN

2016 BEST PRACTICES AWARD

THAILAND
MANAGED SECURITY SERVICE
PROVIDER OF THE YEAR

ได้รับมอบใบรับรองมาตรฐาน

ISO/IEC 27001:2013

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ของศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามระบบเทคโนโลยีสารสนเทศ (SOC)
จากบริษัท บริษัท ทูฟ นอร์ด (ประเทศไทย) จำกัด (TUV NORD)

Managed Security Service Provider Award

Frost & Sullivan Thailand Excellence Awards 2016–2017

บริการของ NT ด้านการปรับปรุงระบบความปลอดภัยไซเบอร์

CYFENCE

เสี่ยงต่ำ 3

เพิ่มความมั่นคง

3.1 Software Update

3.2 Penetration Testing

3.3 Dashboard

3.4 Cybersecurity Operations Center (CSOC)

บริการ Vulnerbility Assessment

นอกจากบริการตรวจสอบช่องโหว่ของระบบแล้ว จะมีการรายงานคำแนะนำในการตรวจสอบ software Version จากผลการการ Scan ช่องโหว่

เริ่มต้น 21,000 บาท/ ครั้ง ไม่เกิน 5 IP

บริการ Mini SIEM

จัดเก็บล็อกเป็นศูนย์กลาง และมีหน้าจอ Dashboard โดยตั้งศูนย์ไว้ที่ Data Center ของตัวเอง

MINI SIEM 200 EPS ราคา 21,200 ต่อเดือน

บริการ Penetration Testing

บริการทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว่ และแก้ไขปรับปรุงจุดอ่อน

1 ระบบ เริ่มต้น 80,000 บาท

บริการ Cybersecurity Monitoring

บริการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ และความปลอดภัยของระบบเทคโนโลยีสารสนเทศผ่านศูนย์ปฏิบัติการ Cybersecurity Operations Center (CSOC)

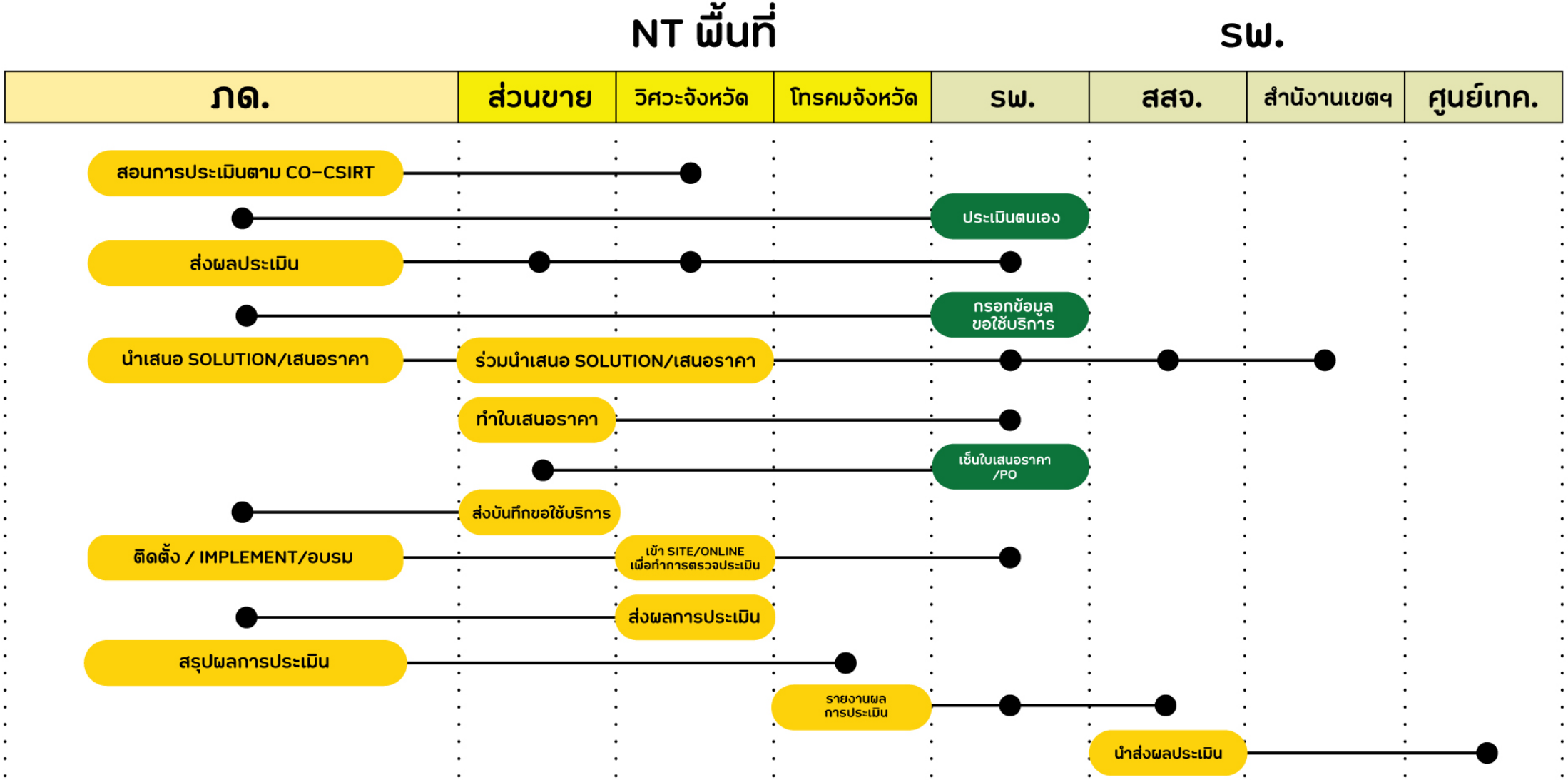
CSM 110 EPS ราคา 23,900 ต่อเดือน

* ราคายังไม่รวม Event Collector

การตรวจประเมินตามเกณฑ์ CO-CIRT

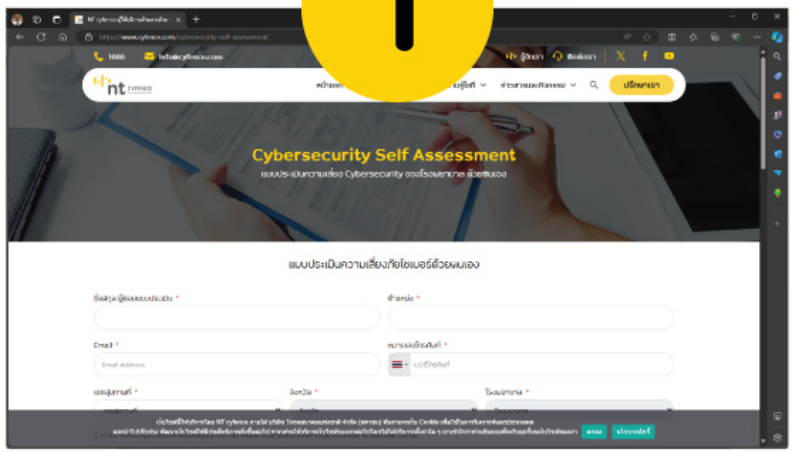
NT Process

FLOW | กระบวนการทำงาน ทั้งหมดในการให้บริการกับ รพ.



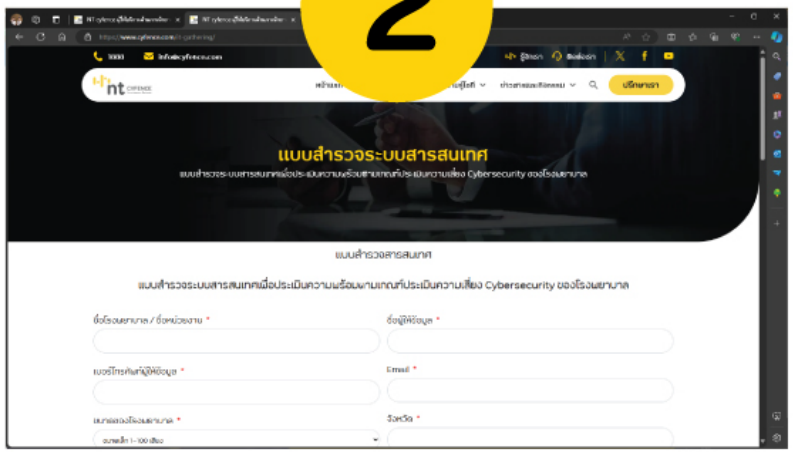
FORM | ฟอร์มออไลน์ทั้ง 3 ฟอร์ม ในการให้บริการกับ รพ.

1



ฟอร์ม 1
แบบประเมินความเสี่ยง
ภัยไซเบอร์ด้วยตนเอง

2

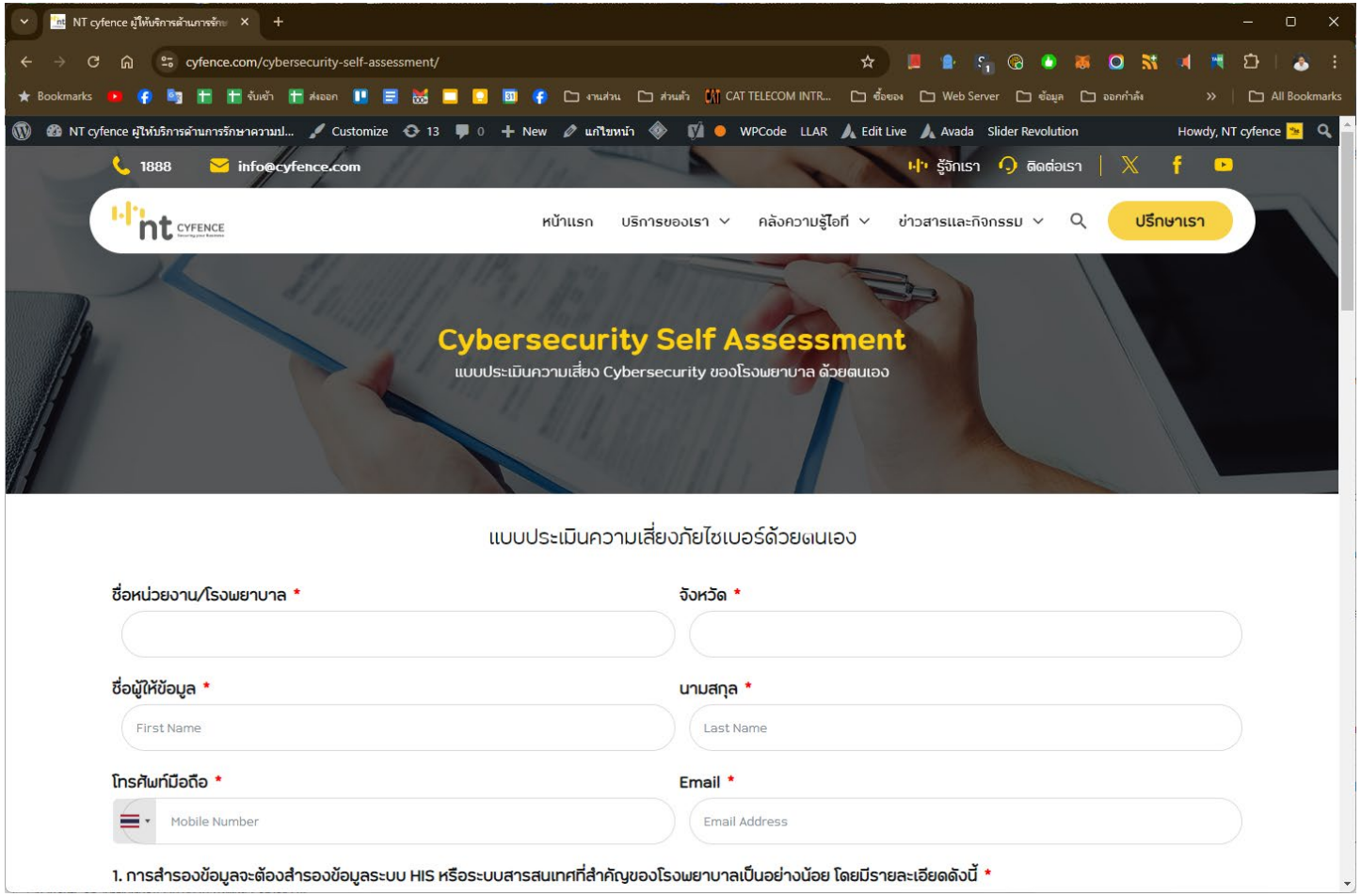


ฟอร์ม 2
แบบสำรวจความต้องการ
ทางสารสนเทศโรงพยาบาล

3

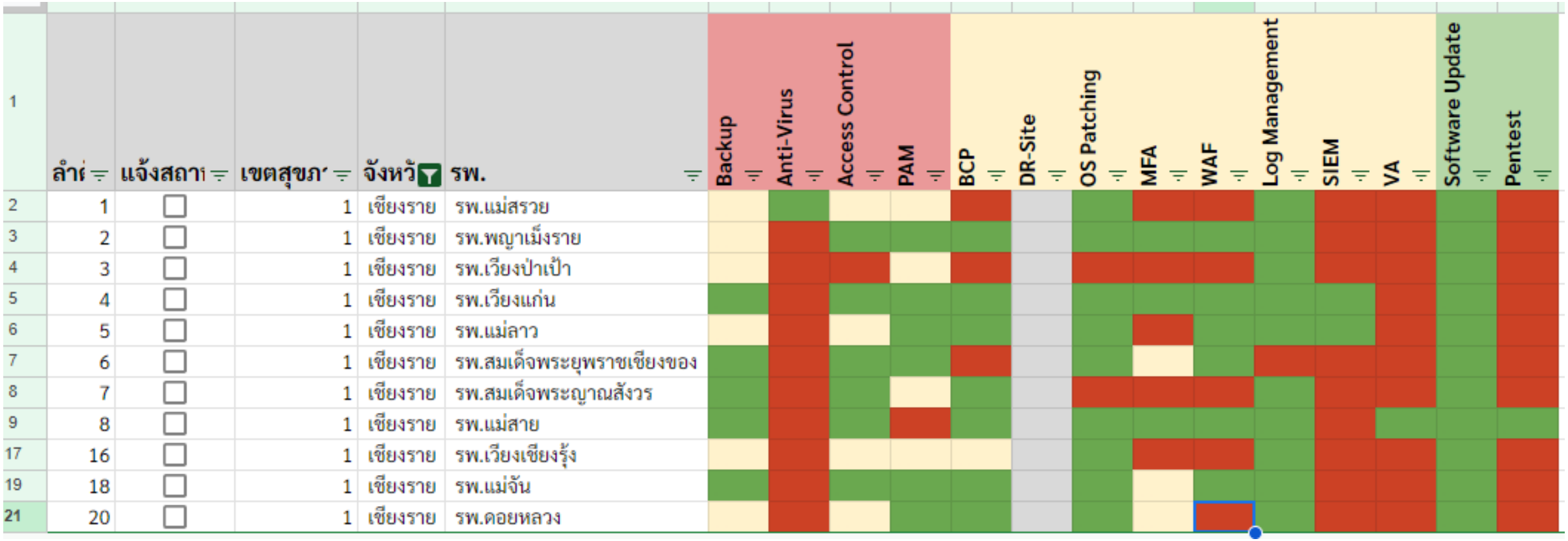
ฟอร์ม 3
แบบประเมินภัยคุกคามไซเบอร์
สำหรับโรงพยาบาลและหน่วยงานสาธารณสุข

แบบฟอร์มประเมินตนเองเบื้องต้น



www.cyfence.com/cybersecurity-self-assessment

แสดงรายงานของ พื้นที่



1	ลำดั	แจ้งสถา	เขตสุขภ	จังหวั	รพ.	Backup	Anti-Virus	Access Control	PAM	BCP	DR-Site	OS Patching	MFA	WAF	Log Management	SIEM	VA	Software Update	Pentest
2	1	☐	1	เชียงราย	รพ.แม่สรวย														
3	2	☐	1	เชียงราย	รพ.พญาเม็งราย														
4	3	☐	1	เชียงราย	รพ.เวียงป่าเป้า														
5	4	☐	1	เชียงราย	รพ.เวียงแก่น														
6	5	☐	1	เชียงราย	รพ.แม่ลาว														
7	6	☐	1	เชียงราย	รพ.สมเด็จพระยุพราชเชียงของ														
8	7	☐	1	เชียงราย	รพ.สมเด็จพระญาณสังวร														
9	8	☐	1	เชียงราย	รพ.แม่สาย														
17	16	☐	1	เชียงราย	รพ.เวียงเชียงรุ้ง														
19	18	☐	1	เชียงราย	รพ.แม่จัน														
21	20	☐	1	เชียงราย	รพ.ดอยหลวง														

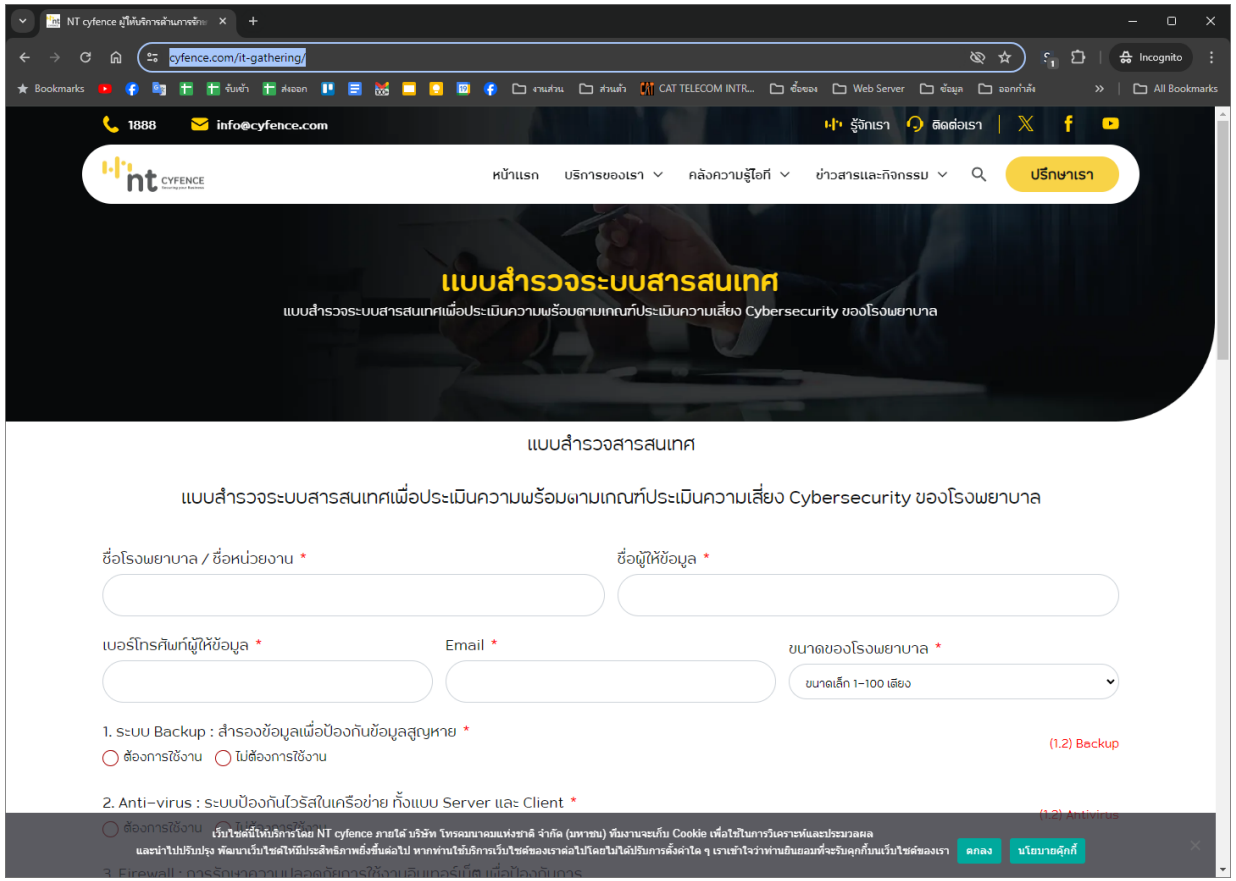
รายงานประเมินตนเองส่ง ให้ รพ.

การประเมินตนเองตามเกณฑ์ CO-CERT ของโรงพยาบาล/หน่วยงาน

รพ.แม่สาย จังหวัด เชียงราย

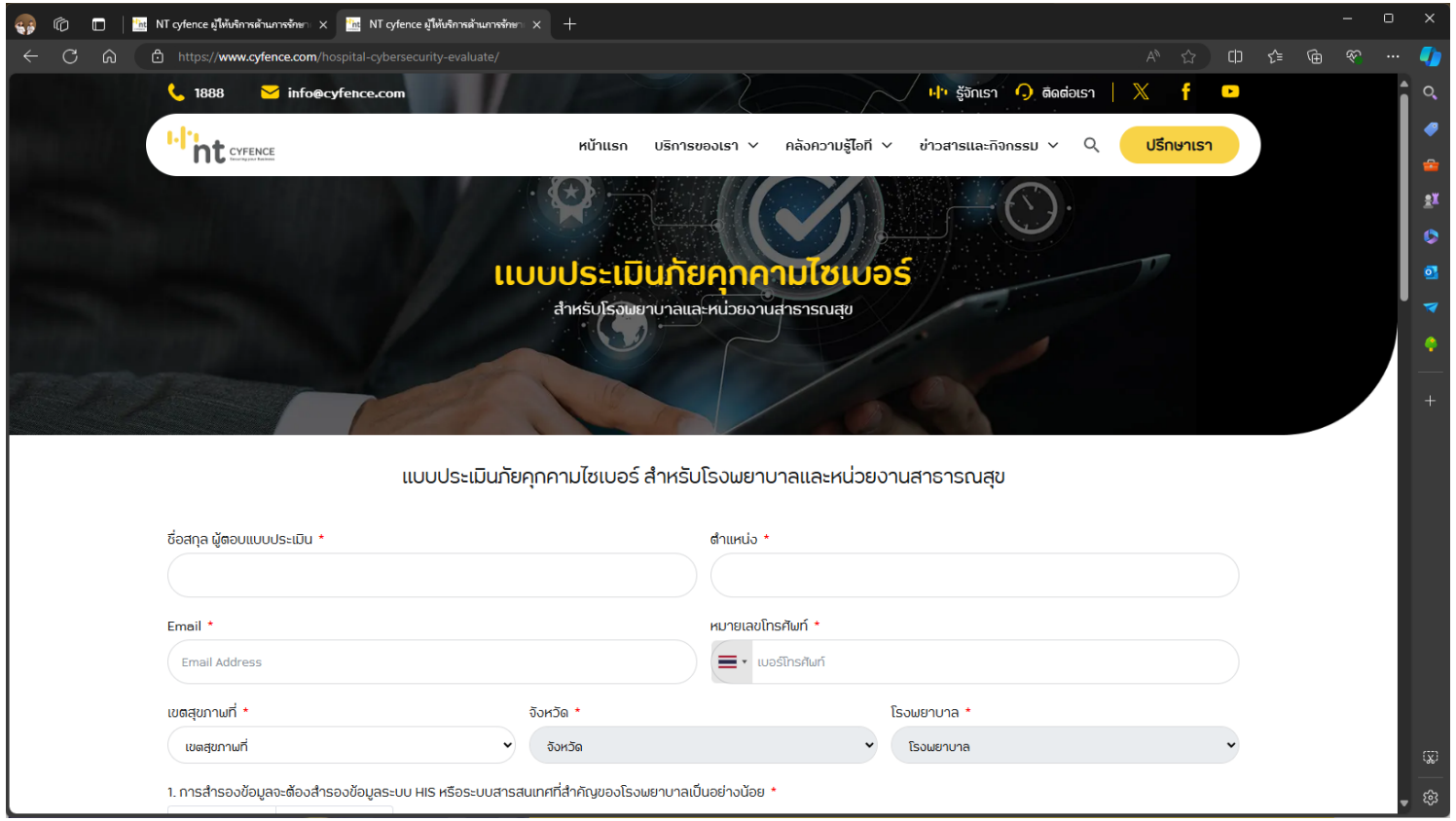
ลำดับ	เกณฑ์ประเมิน	สถานะ	ผลการประเมิน	รายละเอียด	ข้อแนะนำ
1	Backup		ผ่านการประเมิน	มีการสำรองข้อมูล 3 Copy: มี มีการใช้ 2 เทคโนโลยีในการจัดเก็บ HDD / Tape / External / Cloud: มี มีการ Backup OS / Backup Software HIS: มี มีการสำรองข้อมูลวันละครั้ง ย้อนหลังได้ 7 วัน: มี มีการสำรองข้อมูลแบบ Offsite หรือ Cloud 1 ชุด: มี	-
2	Anti-Virus		ไม่ผ่านการประเมิน		ควรดำเนินการแก้ไขโดยเร่งด่วน
3	Access Control		ผ่านการประเมิน	องค์กรมีการใช้ Firewall หรืออุปกรณ์ควบคุมการเข้าถึงระบบสารสนเทศภายในเครือข่าย: มี องค์กรมีการกำหนด White list Port และไม่เปิด Port ที่มีความเสี่ยงโดนโจมตี: มี องค์กรมีการแบ่งโซน Network ระหว่าง Server และ Client : มี ในกรณีที่ต้องการ Access เข้า Server จาก Public ได้ทำการเข้าผ่าน VPN: มี องค์กรมีการใช้ Terminal server ในการเข้าถึง Server แทนที่ใช้ Computer ต้นทาง: มี	-
4	PAM		ไม่ผ่านการประเมิน		ควรดำเนินการแก้ไขโดยเร่งด่วน
5	BCP		ผ่านการประเมิน	องค์กรมีการจัดทำรายงานขั้นตอนการดำเนินการแผนความต่อเนื่องทางธุรกิจ (แผน BCP) ที่ชัดเจนรวมถึงระยะเวลาและผู้เกี่ยวข้อง: มี การทำ BCP ครอบคลุม OS ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย: มี องค์กรมีการทดสอบ BCP อย่างน้อยปีละ 1 ครั้ง: มี	-
6	DR-Site			ยังไม่บังคับในเกณฑ์ CO-CERT	ควรวางแผนในการจัดหา DR Site เพื่อใช้ในยามฉุกเฉิน
7	OS Patching		ผ่านการประเมิน	องค์กรมีการ update Security Patch สำหรับ OS ของระบบ HIS อย่างน้อย 6 เดือนครั้งหรือทันทีหากมี Critical patch	-
8	MFA		ผ่านการประเมิน	หากองค์กรมีการใช้ VPN ได้ทำการเปิด 2FA แล้ว: มี องค์กรมีการใช้ 2FA ครอบคลุม OS ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย: มี	-

แบบฟอร์มความต้องการสารสนเทศ รพ.



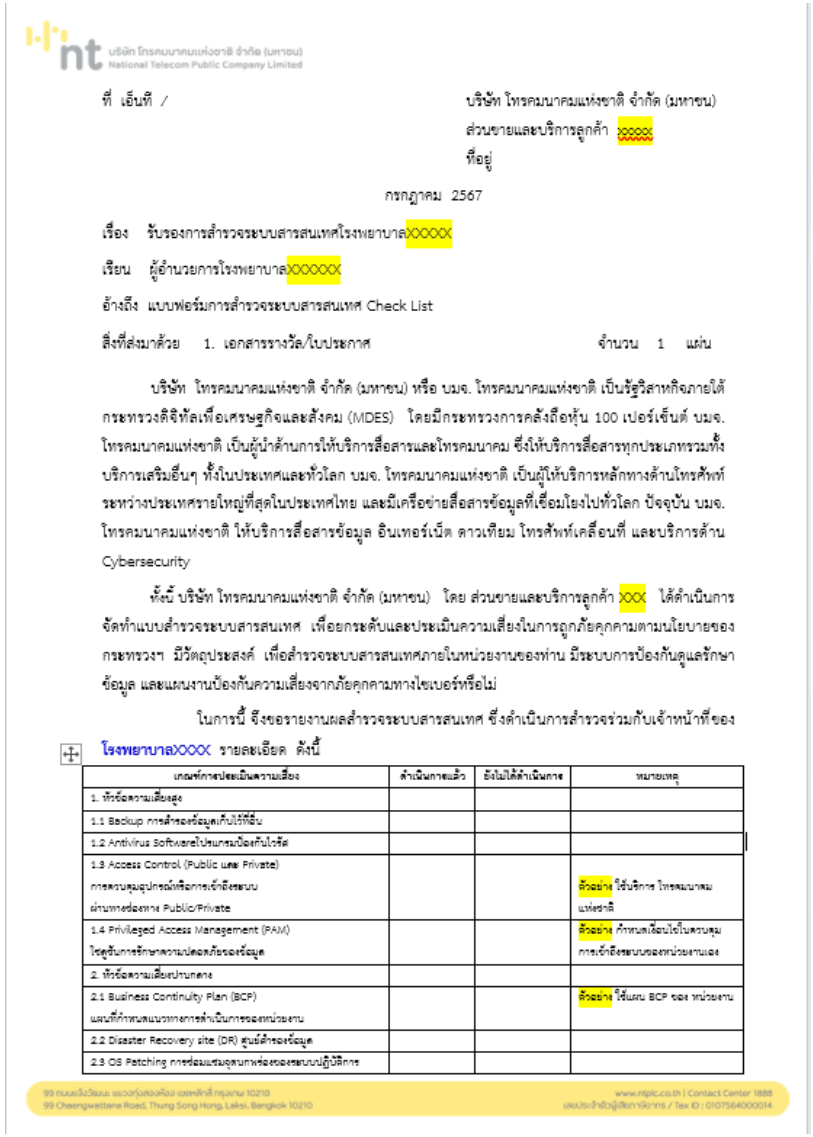
www.cyfence.com/it-gathering

แบบฟอร์มประเมินรพ. ของทีมพื้นที่



https://www.cyfence.com/hospital-cybersecurity-evaluate/

ตัวอย่าง บันทึกรับรองการสำรวจระบบสารสนเทศโรงพยาบาล



บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

ที่ เอ็นที /

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
ส่วนขายและบริการลูกค้า xxxxx
ที่อยู่

กรกฎาคม 2567

เรื่อง รับรองการสำรวจระบบสารสนเทศโรงพยาบาลXXXXX

เรียน ผู้อำนวยการโรงพยาบาลXXXXX

อ้างถึง แบบฟอร์มการสำรวจระบบสารสนเทศ Check List

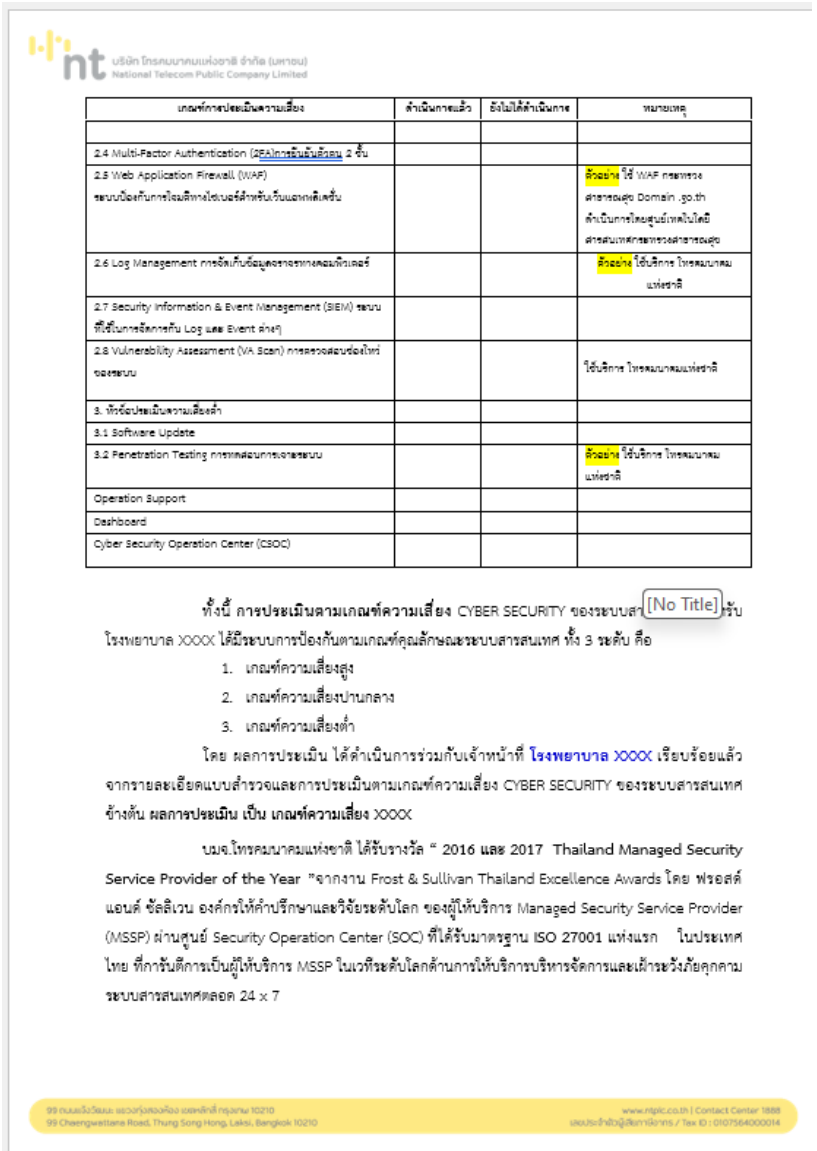
สิ่งที่ส่งมาด้วย 1. เอกสารรางวัล/ใบประกาศ จำนวน 1 แผ่น

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) หรือ บมจ. โทรคมนาคมแห่งชาติ เป็นรัฐวิสาหกิจภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) โดยมีกระทรวงการคลังถือหุ้น 100 เปอร์เซ็นต์ บมจ. โทรคมนาคมแห่งชาติ เป็นผู้นำด้านการให้บริการสื่อสารและโทรคมนาคม ซึ่งให้บริการสื่อสารทุกประเภทรวมทั้งบริการเสริมอื่นๆ ทั้งในประเทศและทั่วโลก บมจ. โทรคมนาคมแห่งชาติ เป็นผู้ให้บริการหลักทางด้านโทรศัพท์ระหว่างประเทศรายใหญ่ที่สุดในประเทศไทย และมีเครือข่ายสื่อสารข้อมูลที่เชื่อมโยงไปทั่วโลก ปัจจุบัน บมจ. โทรคมนาคมแห่งชาติ ให้บริการสื่อสารข้อมูล อินเทอร์เน็ต ดาวเทียม โทรศัพท์เคลื่อนที่ และบริการด้าน Cybersecurity

ทั้งนี้ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) โดย ส่วนขายและบริการลูกค้า XXX ได้ดำเนินการจัดทำแบบสำรวจระบบสารสนเทศ เพื่อยกระดับและประเมินความเสี่ยงในการถูกภัยคุกคามตามนโยบายของกระทรวงฯ มีวัตถุประสงค์ เพื่อสำรวจระบบสารสนเทศภายในหน่วยงานของท่าน มีระบบการป้องกันดูแลรักษาข้อมูล และแผนงานป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือไม่

ในการนี้ จึงขอรายงานผลสำรวจระบบสารสนเทศ ซึ่งดำเนินการสำรวจร่วมกับเจ้าหน้าที่ของโรงพยาบาลXXXX รายละเอียด ดังนี้

เกณฑ์การประเมินความเสี่ยง	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ	หมายเหตุ
1. ทิศร้อความเสี่ยงสูง			
1.1 Backup การสำรองข้อมูลเก็บไว้ที่อื่น			
1.2 Antivirus Softwareโปรแกรมป้องกันไวรัส			
1.3 Access Control (Public และ Private) การควบคุมอุปกรณ์เพื่อการเข้าถึงระบบผ่านทางช่องทาง Public/Private			ตัวอย่าง ใช้บริการ โทรคมนาคมแห่งชาติ
1.4 Privileged Access Management (PAM) ใช้ดูสิทธิการรักษาความปลอดภัยของข้อมูล			ตัวอย่าง กำหนดเงื่อนไขในควบคุมการเข้าถึงระบบของหน่วยงานเอง
2. ทิศร้อความเสี่ยงปานกลาง			
2.1 Business Continuity Plan (BCP) แผนที่กำหนดแนวทางการดำเนินการของหน่วยงาน			ตัวอย่าง ใช้แผน BCP ของ หน่วยงาน
2.2 Disaster Recovery site (DR) ศูนย์สำรองข้อมูล			
2.3 OS Patching การซ่อมแซมอุดมการพ่องของระบบปฏิบัติการ			



บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

เกณฑ์การประเมินความเสี่ยง	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ	หมายเหตุ
2.4 Multi-Factor Authentication (2FAการยืนยันตัวตน 2 ชั้น			
2.5 Web Application Firewall (WAF) ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่น			ตัวอย่าง ใช้ WAF กระทรวงศาธารณสุข Domain .go.th ดำเนินการโดยศูนย์เทคโนโลยีสารสนเทศกระทรวงสาธารณสุข
2.6 Log Management การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์			ตัวอย่าง ใช้บริการ โทรคมนาคมแห่งชาติ
2.7 Security Information & Event Management (SIEM) ระบบที่ใช้ในการจัดการกับ Log และ Event ต่างๆ			
2.8 Vulnerability Assessment (VA Scan) การตรวจสอบช่องโหว่ของระบบ			ใช้บริการ โทรคมนาคมแห่งชาติ
3. ทิศร้อประเมินความเสี่ยงต่ำ			
3.1 Software Update			
3.2 Penetration Testing การทดสอบการเจาะระบบ			ตัวอย่าง ใช้บริการ โทรคมนาคมแห่งชาติ
Operation Support			
Dashboard			
Cyber Security Operation Center (CSOC)			

ทั้งนี้ การประเมินตามเกณฑ์ความเสี่ยง CYBER SECURITY ของระบบสา[No Title]รับโรงพยาบาล XXXX ได้มีระบบการป้องกันตามเกณฑ์คุณลักษณะระบบสารสนเทศ ทั้ง 3 ระดับ คือ

1. เกณฑ์ความเสี่ยงสูง
2. เกณฑ์ความเสี่ยงปานกลาง
3. เกณฑ์ความเสี่ยงต่ำ

โดย ผลการประเมิน ได้ดำเนินการร่วมกับเจ้าหน้าที่ โรงพยาบาล XXXX เรียบร้อยแล้ว จากรายละเอียดแบบสำรวจและการประเมินตามเกณฑ์ความเสี่ยง CYBER SECURITY ของระบบสารสนเทศข้างต้น ผลการประเมิน เป็น เกณฑ์ความเสี่ยง XXXX

บมจ.โทรคมนาคมแห่งชาติ ได้รับรางวัล " 2016 และ 2017 Thailand Managed Security Service Provider of the Year "จากงาน Frost & Sullivan Thailand Excellence Awards โดย ฟรอสต์ แอนด์ ซัลลิเวน องค์กรให้คำปรึกษาและวิจัยระดับโลก ของผู้ให้บริการ Managed Security Service Provider (MSSP) ผ่านศูนย์ Security Operation Center (SOC) ที่ได้รับมาตรฐาน ISO 27001 แห่งแรก ในประเทศไทย ที่การันตีการเป็นผู้ให้บริการ MSSP ในเวทีระดับโลกด้านการให้บริการบริหารจัดการและเฝ้าระวังภัยคุกคามระบบสารสนเทศตลอด 24 x 7

ขอบคุณผู้ร่วมฟังบรรยายทุกท่าน

@cyfence

www.cyfence.com