ประกาศโรงพยาบาลปราสาท
เรื่อง มาตรฐานสถาปัตยกรรมเครือข่ายคอมพิวเตอร์ที่มั่นคงปลอดภัย
(Network Security Architecture Standard)

โรงพยาบาลปราสาท ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ตระหนักและให้ความสำคัญอย่างยิ่งต่อการรักษาความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินงานสอดคล้องตามเจตนารมณ์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ตลอดจนมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๒๒ และ NIST Cybersecurity Framework (CSF) v๒.๐

โรงพยาบาลมุ่งเน้นการสร้างระบบนิเวศดิจิทัลที่มีความมั่นคงปลอดภัย เชื่อถือได้ และพร้อมให้บริการแก่ประชาชนอย่างต่อเนื่อง จึงพิจารณาจัดทำมาตรฐานสถาปัตยกรรมเครือข่ายคอมพิวเตอร์ที่มั่นคงปลอดภัยฉบับนี้ขึ้น เพื่อใช้เป็นกรอบแนวทางและมาตรการในการออกแบบ ติดตั้ง ดำเนินงาน และบำรุงรักษาโครงสร้างพื้นฐานเครือข่ายคอมพิวเตอร์ของโรงพยาบาลให้เป็นไปอย่างมีประสิทธิภาพ มีมาตรฐานเทียบเท่าระดับสากล และบูรณาการร่วมกันเป็นเอกภาพทั่วทั้งองค์กร จึงกำหนดหลักเกณฑ์ดังต่อไปนี้

๑. วัตถุประสงค์

มาตรฐานฉบับนี้จัดทำขึ้นเพื่อ

๑.๑ กำหนดกรอบแนวทางการออกแบบ ติดตั้ง และบำรุงรักษาสถาปัตยกรรมเครือข่ายคอมพิวเตอร์ของโรงพยาบาลปราสาทให้มีความมั่นคงปลอดภัย สอดคล้องกับหลักการ CIA Triad (Confidentiality, Integrity, Availability)

๑.๒ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยบังคับใช้มาตรการควบคุมเชิงป้องกัน (Preventive Controls) มาตรการตรวจจับ (Detective Controls) และมาตรการตอบสนอง (Responsive Controls) อย่างเป็นระบบ

๑.๓ รับรองว่าโครงสร้างพื้นฐานเครือข่ายเป็นไปตามข้อกำหนดของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑.๔ สร้างมาตรฐานเดียวกันทั่วทั้งองค์กร เพื่อให้การบริหารจัดการเครือข่ายเป็นไปอย่างมีเอกภาพ โปร่งใส และตรวจสอบได้

๑.๕ สนับสนุนการเปลี่ยนผ่านสู่โรงพยาบาลดิจิทัล (Digital Hospital) โดยรักษาความพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่สำคัญยิ่ง (Critical Information Systems) อย่างต่อเนื่อง

๑.๖ เพื่อปฏิบัติตามข้อกำหนดมาตรฐาน ด้านโครงสร้างพื้นฐานสารสนเทศสำหรับโรงพยาบาล

๒. ขอบเขตการบังคับใช้

๒.๑ มาตรฐานฉบับนี้มีผลบังคับใช้ครอบคลุมสถาปัตยกรรมเครือข่ายคอมพิวเตอร์ทั้งหมดของโรงพยาบาลปราสาท ประกอบด้วย

๒.๑.๑ อุปกรณ์เครือข่ายทุกประเภท ได้แก่ Next-Generation Firewall (FortiGate

๒๐๐E), Core Switch (Cisco C๙๓๐๐L), Distribution Switch (Ruijie S๖๒๑๐), Access Switch ทั้งหมด รวมถึงอุปกรณ์เครือข่ายไร้สาย (Wireless Access Point)

๒.๑.๒ ระบบเซิร์ฟเวอร์ทุกประเภท ได้แก่ HCI Cluster, VMware ESXi Server และ Physical Server

๒.๑.๓ ระบบสารสนเทศโรงพยาบาล (Hospital Information System-HIS) และระบบสนับสนุนอื่นๆ

๒.๑.๔ โครงสร้างพื้นฐานเครือข่าย LAN, VLAN, WAN และระบบเชื่อมต่ออินเทอร์เน็ตกับหน่วยงานภายนอก

๒.๒ บุคลากรที่อยู่ภายใต้ขอบเขตการบังคับใช้

๒.๒.๑ ผู้บริหารเทคโนโลยีสารสนเทศ (CIO/CISO)

๒.๒.๒ เจ้าหน้าที่ผู้ดูแลระบบเครือข่ายและระบบเซิร์ฟเวอร์

๒.๒.๓ ผู้ใช้งานทั่วไปทุกหน่วยงานภายในโรงพยาบาล

๒.๒.๔ ผู้ให้บริการภายนอก (Outsource/Vendor) ที่ต้องเข้าถึงระบบเครือข่ายของโรงพยาบาล

๓. หลักการออกแบบสถาปัตยกรรมเครือข่าย (Architecture Design Principles)

โรงพยาบาลปราสาทใช้หลักการออกแบบสถาปัตยกรรมเครือข่ายที่สอดคล้องกับแนวปฏิบัติสากล โดยยึดหลักการสำคัญดังต่อไปนี้

๓.๑ หลักการป้องกันเชิงลึก (Defense-in-Depth) จัดวางมาตรการความปลอดภัยแบบหลายชั้น (Layered Security) ตั้งแต่ระดับ Perimeter (FortiGate ๒๐๐E) ผ่าน Core/Distribution Layer (Cisco C๙๓๐๐L / Ruijie S๖๒๑๐) ไปจนถึง Endpoint (EDR) เพื่อไม่ให้ Single Point of Failure ใด ๆ ส่งผลกระทบต่อทั้งระบบ

๓.๒ หลักการ Zero Trust Architecture ไม่เชื่อถือทราฟฟิกใด ๆ โดยปริยาย (Never Trust, Always Verify) ทุก Session ต้องผ่านการตรวจสอบ Policy Check ก่อนอนุญาตให้เข้าถึงทรัพยากร โดยเฉพาะทราฟฟิกที่ข้ามระหว่าง Security Zone

๓.๓ หลักสิทธิ์น้อยที่สุด (Least Privilege) ให้สิทธิ์การเข้าถึงเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงาน ทั้งในระดับเครือข่าย (ACL/Firewall Rule) และระดับระบบ (PAM — Privileged Access Management)

๓.๔ หลักการแบ่งส่วนเครือข่าย (Network Segmentation) แยกเครือข่ายออกเป็นเขต (Zone) ตามระดับความเสี่ยงและหน้าที่ โดยใช้ VLAN เป็นกลไกหลักในการแบ่งส่วน และใช้ Firewall/ACL ควบคุมทราฟฟิกระหว่าง Zone

๓.๕ หลักความพร้อมใช้งานสูง (High Availability & Redundancy) ออกแบบให้มีช่องทางเชื่อมต่อสำรอง (Dual WAN, AGG-PORT, ๑๐Gbps Uplink) เพื่อลด Downtime และรองรับ Business Continuity Zone

๔. การแบ่งเขตเครือข่าย (Network Zone Architecture)

๔.๑ Security Zone (Gateway: FortiGate ๒๐๐E)

ทราฟฟิกทุก Session ที่เข้า-ออก Security Zone ต้องผ่านการตรวจสอบโดย FortiGate ๒๐๐E (Next-Generation Firewall) ซึ่งทำหน้าที่กรอง Policy, IPS, Application Control และ SSL Inspection

VLAN ID	ชื่อเขต	Subnet	ประกอบด้วย	Security Controls
VLAN ๓	HIS Server Zone	๑๙๒.๑๖๘.๓.x	ระบบสารสนเทศโรงพยาบาล (HIS)	Access Control, EDR, PAM, VASCAN
VLAN ๒๔	Outsource Zone	๑๙๒.๑๖๘.๒๔.x	เซิร์ฟเวอร์สำหรับผู้ให้บริการภายนอก	Access Control, EDR, VASCAN

VLAN ID	ชื่อเขต	Subnet	ประกอบด้วย	Security Controls
VLAN ๒๕	Server Other Zone	๑๙๒.๑๖๘.๒๕.x	เซิร์ฟเวอร์สนับสนุนอื่น ๆ	Access Control, EDR, PAM, VASCAN

๔.๒ LAN Zone (Gateway: Cisco C๙๓๐๐L)

เขตเครือข่ายสำหรับผู้ใช้งานภายในองค์กร ใช้ Cisco C๙๓๐๐L เป็น L๓ Gateway ทำ Fast Switching (ไม่ผ่าน Firewall) เพื่อประสิทธิภาพสูงสุดในการสื่อสารภายใน Zone เดียวกัน

VLAN ID	ชื่อเขต	ประกอบด้วย	Security Controls
VLAN ๑๐–๒๓	Client Subnets Zone	เครื่องคอมพิวเตอร์ผู้ใช้งานแต่ละหน่วยงาน	NAC, ๘๐๒.๑X

๔.๒.๑ Access Switch เชื่อมต่อกับ Core Switch ผ่าน Distribution Switch (Ruijie S๖๒๑๐) ด้วย ๑๐Gbps Uplink

๔.๒.๒ ใช้ Network Access Control (NAC) จัดกลุ่มเครื่อง Client (Client Group NAC) ก่อนอนุญาตเข้าใช้งาน

๔.๓ Management Zone

VLAN ID	ชื่อเขต	วัตถุประสงค์
VLAN ๔๙ ๙๙	MGMT (Management Zone)	การบริหารจัดการอุปกรณ์เครือข่ายเท่านั้น

๔.๓.๑ แยกออกจาก Data Plane โดยสิ้นเชิง

๔.๓.๒ อนุญาตเฉพาะโปรโตคอล SSH, HTTPS, SNMP จาก IP ที่ได้รับอนุญาตเท่านั้น

๔.๔ Routing Architecture (Logical Segmentation & Routing Flow)

๔.๔.๑ Default Route: ทราฟฟิกจาก LAN Zone ส่งผ่าน Cisco C๙๓๐๐L ⟶ FortiGate ๒๐๐E ⟶ Internet (Dual WAN)

๔.๔.๒ Inter-VLAN Routing (Security Zone): ทราฟฟิกระหว่าง VLAN ๓, ๒๔, ๒๕ ต้องผ่าน FortiGate ๒๐๐E ทุก Session (Policy Check / Zero Trust)

๔.๔.๓ Inter-VLAN Routing (LAN Zone): ทราฟฟิกภายใน VLAN ๑๐–๒๓ ใช้ Fast Switching บน Cisco C๙๓๐๐L (ไม่ผ่าน Firewall)

๔.๔.๔ AGG-PORT: ใช้ Link Aggregation เพื่อเพิ่ม Throughput และ Redundancy ระหว่าง Core Switch กับ FortiGate

๕. การควบคุมการเข้าออกของทราฟฟิก (Traffic Control and Filtering)

๕.๑ นโยบาย Firewall (FortiGate ๒๐๐E)

ใช้หลัก Default Deny — ปิดกั้นทราฟฟิกทั้งหมดเป็นค่าเริ่มต้น เปิดอนุญาตเฉพาะที่จำเป็น

๕.๑.๑ กำหนด Firewall Policy แยกตาม Zone (Security Zone LAN Zone Internet)

๕.๑.๒ เปิดใช้ SSL/TLS Inspection สำหรับทราฟฟิกที่ออกอินเทอร์เน็ต

๕.๑.๓ บังคับ Application Control เพื่อควบคุมแอปพลิเคชันที่อนุญาตให้ใช้งานเก็บ Log ตาม พ.ร.บ.คอมพิวเตอร์

๕.๒ Access Control List (ACL) บน Core/Distribution Switch

๕.๒.๑ Cisco C๙๓๐๐L และRuijie S๖๒๑๐ ต้องกำหนด ACL เพื่อกรองทราฟฟิกระหว่าง VLAN

๕.๒.๒ จำกัดการเข้าถึง VLAN ๓ (HIS) เฉพาะ IP/Port ที่ได้รับอนุญาต

๕.๒.๓ ห้ามทราฟฟิก VLAN ๒๔ (Outsource) เข้าถึง VLAN อื่นโดยตรงต้องผ่าน FortiGate เท่านั้น

๕.๓ Network Access Control (NAC)

๕.๓.๑ ใช้ NAC ตรวจสอบสถานะเครื่อง Client ก่อนอนุญาตเข้าใช้งานเครือข่าย (VLAN ๑๐–๒๓)

๕.๓.๒ เครื่องที่ไม่ผ่านการตรวจ (Non-Compliant) จะถูกกักกันไว้ใน Quarantine VLAN

๕.๓.๓ จัดกลุ่มเครื่อง Client ตามหน่วยงาน (Client Group NAC) เพื่อบังคับ Policy ที่แตกต่างกัน

๕.๔ การควบคุมทราฟฟิกขาออก (Egress Filtering)

๕.๔.๑ กรอง Outbound Traffic ผ่าน FortiGate เพื่อป้องกัน Data Exfiltration

๕.๔.๒ บล็อก Outbound Connection ไปยัง Known Malicious IP/Domain (Threat Intelligence Feed)

๖. มาตรการความปลอดภัยเครือข่าย (Network Security Controls)

๖.๑ Intrusion Prevention System (IPS)

๖.๑.๑ FortiGate ๒๐๐E เปิดใช้งาน IPS Engine สำหรับทราฟฟิกทุก Zone

๖.๑.๒ VLAN ๒๕ (Server Other) มี IPS เพิ่มเติมในระดับ Host-based

๖.๒ Endpoint Detection and Response (EDR)

๖.๒.๑ ติดตั้ง EDR Agent บนเซิร์ฟเวอร์ทุกเครื่องใน Security Zone (VLAN ๓, ๒๔, ๒๕)

๖.๒.๒ EDR ทำหน้าที่ตรวจจับพฤติกรรมผิดปกติ (Behavioral Analysis) และตอบสนองอัตโนมัติ

๖.๓ Privileged Access Management (PAM)

๖.๓.๑ บังคับใช้ PAM สำหรับการเข้าถึง VLAN ๓ (HIS Server) ซึ่งมีข้อมูลผู้ป่วยที่ละเอียดอ่อน

๖.๓.๒ ทุก Session การเข้าถึงระบบ HIS ต้องผ่าน PAM Gateway พร้อมบันทึก Session Recording

๖.๔ การเข้ารหัสข้อมูล (Encryption)

๖.๔.๑ บังคับใช้ TLS ๑.๒ ขึ้นไปสำหรับทราฟฟิกทุกประเภทที่ข้ามระหว่าง Zone

๖.๔.๒ ข้อมูลผู้ป่วย (PHI) ที่ส่งผ่านเครือข่ายต้องเข้ารหัส End-to-End

๖.๔.๓ การ Remote Access ต้องใช้ VPN (IPsec/SSL) ผ่าน FortiGate เท่านั้น

๖.๕ การป้องกัน DDoS

๖.๕.๑ FortiGate ๒๐๐E เปิดใช้ DoS Policy สำหรับทราฟฟิกขาเข้าจากอินเทอร์เน็ต

๖.๕.๒ กำหนด Rate Limiting บน WAN Interface

๗. มาตรฐานเครือข่ายไร้สาย (Wireless Network Security)

๗.๑ การเข้ารหัสและการพิสูจน์ตัวตน

๗.๑.๑ ใช้ WPA๓-Enterprise หรือ WPA๒-Enterprise เป็นอย่างน้อย

๗.๑.๒ พิสูจน์ตัวตนด้วย ๘๐๒.๑X ร่วมกับ RADIUS Server

๘. การเฝ้าระวังและการบันทึก Log (Monitoring and Logging)

๘.๑ เฝ้าระวังความปลอดภัย (CSOC Monitor)

๘.๑.๑ CSOC Monitor บริการเฝ้าระวังความปลอดภัยทางไซเบอร์แบบเรียลไทม์ตลอด ๒๔ ชั่วโมง โดยผู้เชี่ยวชาญเพื่อตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามที่ผิดปกติในระบบเครือข่ายขององค์กร (ใช้บริการ INET)

๘.๑.๒ เชื่อมต่อ Log จากทุกอุปกรณ์ (FortiGate, Cisco C๙๓๐๐L, Ruijie S๖๒๑๐, Servers) เข้าสู่ระบบ SIEM

๘.๒ การบันทึกและจัดเก็บ Log

๘.๒.๑ จัดเก็บ Log ไม่น้อยกว่า ๙๐ วัน ตามข้อกำหนดของ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๘.๒.๒ ประเภท Log ที่ต้องจัดเก็บ:

๘.๒.๒.๑ Log Firewall (FortiGate): Traffic Log, Threat Log, Web Filter Log

๘.๒.๒.๒ Log Switch: Authentication Log, Port Security Log

๘.๒.๒.๓ Log Server: Access Log, System Event Log

๘.๒.๒.๔ Log NAC: Authentication Success/Failure

๙. การบริหารจัดการอุปกรณ์เครือข่าย (Network Device Management)

๙.๑ การบริหารจัดการอุปกรณ์ทุกชนิดต้องเข้าถึงผ่าน VLAN ๙๙ (MGMT) เท่านั้น

๙.๒ ใช้ SSH (ปิด Telnet) และ HTTPS สำหรับ Web GUI

๙.๓ บังคับ Multi-Factor Authentication (MFA) สำหรับ Admin Access

๑๐.การรักษาความปลอดภัยทางกายภาพของอุปกรณ์เครือข่าย (Physical Security)

๑๐.๑ ห้องเซิร์ฟเวอร์และห้องอุปกรณ์เครือข่าย

๑๐.๑.๑ ติดตั้งระบบควบคุมการเข้าออก (Access Control System) เช่น Key Card, Biometric

๑๐.๑.๒ ติดตั้งกล้อง CCTV บันทึกภาพตลอด ๒๔ ชั่วโมง จัดเก็บไม่น้อยกว่า ๙๐ วัน

๑๐.๑.๓ จัดทำบันทึกผู้เข้า-ออกห้อง (Visitor Log)

๑๐.๒ สภาพแวดล้อม

๑๐.๒.๑ ควบคุมอุณหภูมิ ๑๘–๒๗ องศาเซลเซียส ความชื้นสัมพัทธ์ ๔๐–๖๐%

๑๐.๒.๒. ติดตั้งระบบดับเพลิงอัตโนมัติที่เหมาะสมกับอุปกรณ์ไฟฟ้า (FM-๒๐๐ หรือเทียบเท่า)

๑๐.๒.๓ ติดตั้ง UPS และ Generator สำรองไฟฟ้า

๑๐.๓ ระบบสาย Cabling

๑๐.๓.๑ ใช้สาย Cabling ที่ได้มาตรฐาน (Cat๖A ขึ้นไปสำหรับ Copper)

๑๐.๓.๒ จัดระเบียบสายในตู้ Rack ด้วย Cable Management อย่างเป็นระบบ

๑๐.๓.๓ ติด Label ทุกเส้นทั้งปลายต้นทางและปลายทาง

๑๑.แผนเผชิญเหตุด้านเครือข่าย (Network Incident Response)

๑๑.๑ การจำแนกระดับเหตุการณ์

ระดับ	คำอธิบาย	ตัวอย่าง	เวลาตอบสนอง
Critical	ระบบ HIS หรือเครือข่ายหลักใช้งานไม่ได้	Core Switch ล่ม, Ransomware	ทันที (≤ ๑๕ นาที)

ระดับ	คำอธิบาย	ตัวอย่าง	เวลาตอบสนอง
High	ระบบบางส่วนได้รับผลกระทบ	VLAN ใดใช้งานไม่ได้, Malware Outbreak	≤ ๓๐ นาที
Medium	เหตุการณ์ผิดปกติแต่ไม่กระทบบริการ	Brute-Force Attempt, Rogue Device	≤ ๒ ชั่วโมง
Low	เหตุการณ์ทั่วไป	Port Down เดี่ยว, Policy Violation	≤ ๒๔ ชั่วโมง

๑๑.๒ ขั้นตอนการตอบสนอง

๑๑.๒.๑ Detection & Identification ตรวจจับผ่าน SOC Monitor / SIEM Alert

๑๑.๒.๒ Containment แยกส่วนที่ได้รับผลกระทบออกจากเครือข่าย (Isolate VLAN/Port)

๑๑.๒.๓ Eradication กำจัดภัยคุกคามและ Patch ช่องโหว่

๑๑.๒.๔ Recovery กู้คืนระบบจาก Backup และทดสอบก่อนเปิดให้บริการ

๑๑.๒.๕ Lessons Learned จัดทำรายงานหลังเหตุการณ์ (Post-Incident Report) ภายใน ๗ วัน

๑๑.๓ การสื่อสารและรายงาน

๑๑.๓.๑ รายงานเหตุการณ์ระดับ Critical/High ต่อผู้บริหารภายใน ๑ ชั่วโมง

๑๑.๓.๒ แจ้ง สกมช. (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ) ตามระเบียบที่กำหนด

๑๑.๓.๓ แจ้งเจ้าของข้อมูล (Data Subject) กรณีมี Data Breach ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

๑๒.บทบาทและหน้าที่ความรับผิดชอบ

บทบาท	หน้าที่ความรับผิดชอบ
ผู้อำนวยการโรงพยาบาล / CIO	อนุมัตินโยบาย กำกับดูแลการปฏิบัติตามมาตรฐาน จัดสรรงบประมาณ
CISO / หัวหน้างานเทคโนโลยีสารสนเทศ	บริหารจัดการความมั่นคงปลอดภัยโดยรวม ทบทวนมาตรฐานอย่างน้อยปีละ ๑ ครั้ง
ผู้ดูแลระบบเครือข่าย (Network Admin)	ออกแบบ ติดตั้ง ดูแลอุปกรณ์เครือข่าย บังคับใช้ Firewall/ACL Policy ตอบสนองเหตุการณ์
ผู้ดูแลระบบเซิร์ฟเวอร์ (Server Admin)	บริหารจัดการ HCI/ESXi/Physical Server ติดตั้ง EDR/PAM ดูแล Patch Management
เจ้าหน้าที่ CSOC (ใช้บริการ INET)	เฝ้าระวัง Log/SIEM วิเคราะห์เหตุการณ์ผิดปกติ แจ้งเตือนและรายงาน
ผู้ใช้งานทั่วไป	ปฏิบัติตามนโยบาย ไม่เชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาต รายงานเหตุการณ์ผิดปกติ
ผู้ให้บริการภายนอก (Outsource/Vendor)	ปฏิบัติตาม SLA และนโยบายความปลอดภัย เข้าถึงเฉพาะ VLAN ๒๔ ที่ได้รับอนุญาต

ประกาศ ณ วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๙

(นางสาวชูหงส์ มหรรทัศนพงศ์)
ผู้อำนวยการโรงพยาบาลปราสาท