Naskah Akademik Pendirian Laboratorium

Network and Cyber Security

Penyusun:

Erfan Rohadi, S.T., M.Eng., Ph.D

Ade Ismail, S.Kom., M.TI

Sofyan Noor Arief

Usman Nurhasan

Vipkas Al Hadid Firdaus

Meyti Eka Apriyani

Septian Enggar Sukmana

Jurusan Teknologi Informasi

Politeknik Negeri Malang

2025

DAFTAR ISI

1 PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi yang masif telah menempatkan Jaringan Komputer sebagai infrastruktur vital bagi seluruh aspek kehidupan modern. Penguasaan kapabilitas dalam merancang, mengimplementasikan, dan mengelola jaringan yang tangguh (resilient) merupakan fondasi utama. Namun, seiring dengan kompleksitas jaringan, ancaman siber (cyber threats) telah berkembang menjadi risiko strategis. Laboratorium Network and Cyber Security (NCS) didirikan dengan tujuan ganda: untuk melatih mahasiswa menjadi ahli dalam infrastruktur jaringan tingkat lanjut sekaligus ahli dalam melindungi aset digital yang mengalir di dalamnya.

Sebagai institusi pendidikan tinggi, terutama di bidang teknologi, memiliki tanggung jawab fundamental untuk membekali mahasiswa dengan keahlian praktis dan teoritis yang relevan dengan kebutuhan industri. Kurikulum saja tidak cukup untuk menghadapi dinamika ancaman siber yang berubah cepat. Oleh karena itu, diperlukan sebuah sarana **praktikum dan riset yang terisolasi (*isolated*) dan realistis** yang dapat mereplikasi lingkungan jaringan dan serangan siber nyata tanpa membahayakan infrastruktur utama kampus.

Pendirian **Laboratorium Network and Cyber Security (NCS)** menjadi sangat penting dengan alasan sebagai berikut:

1. **Peningkatan Kualitas Pembelajaran Infrastruktur dan Keamanan:** Lab sebagai sarana untuk praktik implementasi kurikulum, menyediakan fasilitas perangkat keras (*hardware*) untuk konfigurasi **router, switch, dan *High Availability***, serta perangkat keamanan spesifik (IDS/IPS, *forensics*).
2. **Dukungan Penelitian Dua Arah:** Lab ini akan menjadi *enabler* bagi riset mendalam di topik-topik **optimasi dan desain jaringan (*SDN, Cloud Networking*)** maupun topik **keamanan siber (*incident response, malware analysis*)**.
3. **Penguatan Kompetensi Lulusan:** Dengan fasilitas lab yang memadai, lulusan akan memiliki **kompetensi unggul** yang siap bersaing sebagai **Spesialis Keamanan Jaringan, *Ethical Hacker*, atau *Cyber Security Analyst***, serta siap mengikuti sertifikasi profesional berskala internasional (seperti CCNA, CompTIA Security+, atau CEH) yang sangat dicari oleh industri.

4. **Mendukung Visi dan Misi Institusi:** Laboratorium NCS secara langsung mendukung visi institusi untuk menjadi pusat unggulan teknologi dan inovasi, khususnya dalam menyiapkan sumber daya manusia yang mampu menjaga kedaulatan siber nasional dan regional.

1.2. Urgensi Pendirian Laboratorium

Urgensi pendirian Laboratorium Network and Cyber Security (NCS) didasarkan pada kesenjangan (gap) antara tuntutan keahlian profesional di dunia kerja dengan ketersediaan fasilitas praktik yang representatif, serta kebutuhan untuk meningkatkan kualitas akademik institusi secara keseluruhan.

1.2.1. Alasan Pentingnya Laboratorium

Laboratorium NCS memiliki peran krusial sebagai pilar pendukung utama:

1. **Dukungan Kurikulum Berbasis Praktik:** Laboratorium ini berfungsi sebagai wadah utama untuk mengimplementasikan mata kuliah yang membutuhkan praktik langsung, seperti Jaringan Komputer Lanjut, Keamanan Jaringan, Kriptografi, *Ethical Hacking*, *Penetration Testing*, dan *Digital Forensics*. Tanpa lab khusus, materi-materi ini hanya dapat disampaikan melalui simulasi teoritis yang kurang efektif, menghambat pemahaman mahasiswa terhadap skenario serangan dan pertahanan dunia nyata.
2. **Pemenuhan Standar Akreditasi:** Ketersediaan fasilitas laboratorium yang spesifik dan terkini di bidang Keamanan Siber merupakan salah satu indikator penting dalam penilaian akreditasi program studi dan institusi. Lab NCS akan memenuhi standar infrastruktur dan peralatan yang diwajibkan, menunjukkan komitmen institusi terhadap kualitas pendidikan di bidang *high-demand*.
3. **Respons terhadap Kebutuhan Industri:** Dunia industri, khususnya sektor finansial dan teknologi, menuntut lulusan yang memiliki keahlian *hands-on* dalam mengamankan sistem dan merespons insiden siber. Laboratorium NCS akan melahirkan SDM yang mampu mengoperasikan dan mengelola perangkat keamanan tingkat *enterprise* (seperti *firewall*, IDS/IPS, *SIEM*), sehingga secara langsung menjawab kebutuhan mendesak pasar kerja akan tenaga profesional keamanan siber.

1.2.2. Peran Laboratorium dalam Pencapaian Kompetensi Lulusan

Laboratorium NCS secara spesifik dirancang untuk memastikan pencapaian kompetensi inti lulusan, yaitu:

- **Keunggulan Teknis:** Mahasiswa mampu merancang, mengimplementasikan, dan mengelola infrastruktur jaringan yang tangguh dan aman, serta menguasai teknik mitigasi serangan siber.
- **Keterampilan *Red Team* dan *Blue Team*:** Memberikan kesempatan praktik simulasi serangan (*red team*) dan praktik pertahanan, deteksi, serta respons insiden (*blue team*) dalam lingkungan yang aman dan terkontrol.
- **Kesiapan Sertifikasi Profesional:** Fasilitas lab yang mendekati standar industri akan mempermudah mahasiswa dalam mempersiapkan diri dan lulus ujian sertifikasi profesional NCS yang diakui secara global (misalnya, CCNA Security, CompTIA Security+, CEH).

1.2.3. Kondisi Fasilitas Saat Ini

Fasilitas praktik di bidang Network and Cyber Security saat ini masih menghadapi keterbatasan:

- **Keterbatasan Perangkat Keras:** Praktikum Keamanan Jaringan masih sangat bergantung pada perangkat lunak simulasi (misalnya Cisco Packet Tracer, GNS3) yang tidak dapat mereplikasi kompleksitas performa dan konfigurasi sistem operasi keamanan industri (misalnya *firewall* Palo Alto/Fortinet, *router* Cisco seri lanjutan).
- **Ketiadaan Lingkungan Terisolasi:** Belum tersedianya **Lab Terisolasi (*Isolated Security Range*)** yang memungkinkan mahasiswa melakukan praktik *live hacking* atau *malware analysis* tanpa risiko mengganggu atau merusak jaringan utama kampus.

1.2.4. Manfaat bagi Peningkatan Mutu dan Daya Saing Institusi

Pendirian Laboratorium NCS akan memberikan dampak positif yang luas bagi institusi:

1. **Peningkatan Mutu Pendidikan:** Mendukung penerapan *outcome-based education* (OBE) melalui praktik yang terukur dan relevan, menjamin kualitas capaian pembelajaran lulusan (CPL) di bidang NCS.
2. **Peningkatan Mutu Penelitian dan Tri Dharma:** Menyediakan *platform* riset yang canggih, mendorong peningkatan jumlah penelitian terapan dan publikasi ilmiah di jurnal bereputasi, serta memperluas peluang pengabdian masyarakat melalui program audit keamanan dan edukasi siber.
3. **Peningkatan Daya Saing Institusi:** Memosisikan institusi sebagai **pusat keunggulan (Center of Excellence)** di bidang Network and Cyber Security, menarik minat calon mahasiswa unggulan, dan memperkuat kemitraan strategis dengan industri teknologi dan keamanan nasional.

2 IDENTIFIKASI MASALAH DAN TUJUAN

2.1. Permasalahan yang Dihadapi

Permasalahan yang dihadapi oleh Jurusan/Program Studi dalam memenuhi tuntutan kualitas pendidikan dan riset di bidang Network and Cyber Security (NCS) dapat diringkas sebagai **kesenjangan infrastruktur praktik** yang tidak sebanding dengan pesatnya perkembangan ancaman siber dan teknologi pertahanan industri. Kesenjangan ini menciptakan hambatan nyata yang berdampak langsung pada kualitas lulusan, penelitian, dan kontribusi jurusan.

2.1.1. Kondisi Nyata yang Menjadi Hambatan di Jurusan

Terdapat beberapa kondisi aktual yang menjadi hambatan utama dalam pelaksanaan Tri Dharma Perguruan Tinggi yang optimal di bidang NCS:

1. **Keterbatasan Perangkat Keras Keamanan *Enterprise*:**
    - **Kondisi Aktual:** Jurusan masih mengandalkan simulasi perangkat lunak (seperti Cisco Packet Tracer) dan infrastruktur *server* umum untuk praktikum Jaringan dan Keamanan.
    - **Hambatan:** Kurangnya ketersediaan perangkat keras khusus berstandar industri (misalnya: *Next-Generation Firewall*, *Load Balancer*, *Hardware Security Module* - HSM, dan *Switch/Router* level 3 lanjutan). Hal ini membatasi mahasiswa dalam memahami **performa, *troubleshooting* level mendalam, dan *Command Line Interface* (CLI)** dari produk keamanan riil, sehingga menciptakan *gap* besar ketika mereka memasuki dunia kerja.
2. **Ketiadaan Lingkungan *Security Testing* yang Terisolasi:**
    - **Kondisi Aktual:** Praktikum yang melibatkan simulasi serangan siber (*ethical hacking*, *penetration testing*) harus dilakukan dengan sangat hati-hati dan dibatasi secara ketat demi keamanan jaringan kampus.
    - **Hambatan:** Jurusan tidak memiliki **Laboratorium *Sandbox* atau *Cyber Range*** yang sepenuhnya terisolasi. Dampaknya, mahasiswa tidak dapat melakukan praktik **simulasi serangan siber yang agresif** (misalnya,

live malware analysis, *Distributed Denial of Service* - DDoS testing) yang merupakan inti dari kompetensi *Red Team* dan *Blue Team*.

3. **Keterbatasan Sumber Daya untuk *Digital Forensics* dan *Incident Response* (DFIR):**
    - **Kondisi Aktual:** Praktikum *Digital Forensics* umumnya hanya menggunakan data statis dan *software* dasar.
    - **Hambatan:** Tidak tersedianya stasiun kerja spesialis (*forensic workstations*) dan perangkat lunak *forensics* berlisensi (misalnya EnCase, FTK Imager) yang memadai. Akibatnya, mahasiswa tidak terlatih dalam teknik **mengamankan barang bukti digital (*chain of custody*)** dan **analisis *live incident***, yang merupakan keahlian krusial dalam penanganan kasus kejahatan siber.

2.1.2. Dampak Permasalahan terhadap Kualitas Tri Dharma

Kesenjangan infrastruktur di atas berdampak signifikan terhadap tiga pilar utama Perguruan Tinggi:

Pilar Tri Dharma	Dampak Permasalahan (Kondisi Aktual)
Pendidikan & Pembelajaran	Penurunan Kualitas Kompetensi Lulusan: Mahasiswa hanya menguasai konsep teoritis dan simulasi sederhana. Kemampuan hands-on dan problem-solving mereka dalam menghadapi kasus keamanan siber nyata di industri menjadi rendah.
Penelitian	Hambatan Riset Terapan: Dosen dan mahasiswa kesulitan melaksanakan penelitian terapan di bidang NCS yang membutuhkan lingkungan pengujian berisiko tinggi (misalnya, menguji kerentanan protokol IoT atau mengembangkan honeypot). Ini menghambat kontribusi jurusan pada publikasi ilmiah berkualitas dan solusi industri.
Pengabdian Masyarakat	Keterbatasan Kontribusi Solusi: Kurangnya infrastruktur nyata membatasi kemampuan jurusan untuk menawarkan layanan pengabdian yang bernilai tinggi, seperti audit keamanan jaringan untuk instansi pemerintah atau UMKM, sehingga mengurangi daya saing institusi dalam memberikan solusi praktis.

2.2. Tujuan Pendirian Laboratorium

Tujuan pendirian Laboratorium Network and Cyber Security (NCS) adalah untuk menjadi pusat keunggulan (*center of excellence*) dalam pendidikan, penelitian, dan

penerapan solusi keamanan siber dan infrastruktur jaringan yang relevan dengan kebutuhan industri dan masyarakat. Secara rinci, sasaran utama yang ingin dicapai melalui pendirian laboratorium ini meliputi:

1. Peningkatan Kualitas Pembelajaran dan Fasilitas

- Menyediakan **infrastruktur praktikum** yang memadai, terisolasi (*sandbox*), dan mereplikasi lingkungan jaringan serta ancaman siber yang sesungguhnya di dunia industri.
- Mengintegrasikan fasilitas lab ke dalam kurikulum mata kuliah Network and Cyber Security, memastikan **Capaian Pembelajaran Lulusan (CPL)** dapat dicapai melalui praktik *hands-on* yang terukur.
- Memfasilitasi dosen untuk mengembangkan modul praktikum yang inovatif, relevan dengan teknologi terbaru, dan sejalan dengan **skema sertifikasi profesional** global.

2. Dukungan terhadap Riset, Inovasi, dan Publikasi

- Menjadi *platform* utama untuk melaksanakan **penelitian terapan** di bidang NCS, seperti *Intrusion Detection*, *Malware Analysis*, *Security Orchestration, Automation, and Response* (SOAR), dan *Cloud Security*.
- Meningkatkan kuantitas dan kualitas **publikasi ilmiah** dosen dan mahasiswa di jurnal bereputasi tinggi melalui hasil-hasil riset yang didukung oleh fasilitas lab yang canggih.
- Mendorong lahirnya **inovasi dan paten** yang berorientasi pada solusi keamanan siber, serta prototipe teknologi pertahanan siber yang dapat dikomersialkan.

3. Pemenuhan Kompetensi Lulusan Sesuai Standar Industri

- Melatih mahasiswa untuk menguasai **kompetensi teknis inti** di bidang NCS, termasuk konfigurasi perangkat keras keamanan, *vulnerability assessment*, *penetration testing*, dan *digital forensics*.

- Meningkatkan **daya saing lulusan** dengan membekali mereka keterampilan praktis yang sangat dicari di industri (misalnya, kemampuan *Blue Team* dalam *incident response* dan *Security Information and Event Management* - SIEM).
- Memfasilitasi mahasiswa dalam meraih **sertifikasi kompetensi profesional** di bidang jaringan dan keamanan siber, sesuai dengan standar Kerangka Kualifikasi Nasional Indonesia (KKNI) dan kebutuhan global.

4. Kontribusi Jurusan bagi Industri dan Masyarakat

- Menjadi mitra strategis bagi **industri, pemerintah, dan komunitas** dalam menyediakan layanan konsultasi, audit keamanan, dan pelatihan di bidang NCS.
- Melaksanakan kegiatan **Pengabdian kepada Masyarakat** (PkM) secara berkala, menggunakan fasilitas lab untuk memberikan edukasi dan solusi praktis dalam rangka meningkatkan literasi dan ketahanan siber masyarakat.
- Mendukung **Visi dan Misi Institusi** untuk menjadi institusi pendidikan unggulan yang responsif terhadap tantangan era digital, khususnya dalam menjaga kedaulatan dan keamanan siber nasional.

3 PERENCANAAN KEGIATAN DAN PENGEMBANGAN

3.1. Rencana Kegiatan

Rencana kegiatan Laboratorium NCS dirancang sebagai kerangka kerja *multi-stakeholder* yang memastikan pemanfaatan optimal fasilitas untuk mendukung **Tri Dharma Perguruan Tinggi** dan berkontribusi pada peningkatan kualitas SDM di bidang Keamanan Siber.

3.1.1. Dukungan Praktikum Mata Kuliah

Laboratorium NCS akan digunakan secara terjadwal untuk mendukung praktik mata kuliah inti, dengan fokus pada *hands-on experience* menggunakan infrastruktur yang mendekati standar industri. Pemanfaatan lab ini mencakup simulasi skenario jaringan, konfigurasi perangkat keamanan, dan respons insiden siber.

Mata Kuliah Pendukung	Jenis Praktikum yang Difasilitasi	Output Pembelajaran Utama
Jaringan Komputer Lanjut	Implementasi Virtual Private Network (VPN) site-to-site dan remote-access, konfigurasi Load Balancing, dan setup High Availability (HA) pada perangkat riil.	Mahasiswa mampu membangun, menguji, dan mengelola infrastruktur jaringan yang tangguh, terukur, dan memiliki redundansi.
Keamanan Jaringan	Konfigurasi Next-Generation Firewall (NGFW), instalasi dan analisis log Intrusion Detection/Prevention System (IDS/IPS), serta perancangan Access Control List (ACL) kompleks.	Mahasiswa mampu menerapkan lapisan pertahanan jaringan (Defense-in-Depth) dan memitigasi serangan tingkat layer 3 hingga 7.
Administrasi dan Keamanan Jaringan	Praktik Hardening Sistem Operasi Server (Linux/Windows), implementasi Autentikasi Terpusat (misalnya, RADIUS/TACACS+), dan setup serta monitoring Security Information and Event Management (SIEM) sederhana.	Mahasiswa mampu mengelola sistem server dan network services dengan prinsip keamanan zero-trust dan melakukan log analysis insiden.

3.1.2. Dukungan Penelitian dan Inovasi

Laboratorium NCS akan menyediakan *platform* dan *tools* canggih untuk memfasilitasi penelitian dosen dan mahasiswa sesuai dengan bidang keahlian di *track* keamanan siber:

- **Riset Keamanan Khusus:** Penelitian di bidang **Keamanan *Cloud Computing***, **Keamanan IoT (Internet of Things)**, **Keamanan Sistem Kontrol Industri (ICS/SCADA)**, dan pengembangan *malware sandbox* lokal.
- **Pengembangan Sistem Pertahanan:** Pengembangan dan pengujian prototipe ***Honeypot* cerdas** dan sistem *Intrusion Detection* berbasis *Machine Learning* (*AI-based Intrusion Detection*) yang dapat mendeteksi pola serangan baru.
- **Fasilitasi Skripsi/Tesis:** Menyediakan *workstation* dengan spesifikasi tinggi dan *software* berlisensi untuk menyelesaikan tugas akhir yang membutuhkan pemrosesan data besar atau simulasi keamanan tingkat lanjut.

3.1.3. Program Pengembangan Kompetensi dan Sertifikasi

Untuk memastikan *transfer knowledge* dan peningkatan kualitas SDM, Lab NCS secara rutin akan mengadakan program pengembangan kompetensi:

1. **Pelatihan dan *Workshop* Teknis:** Penyelenggaraan pelatihan berkala (misalnya, *Cloud Security Fundamentals*, *Cyber Threat Intelligence*, *Wireless Hacking*) bagi mahasiswa, dosen, dan praktisi industri.
2. **Fasilitasi Sertifikasi Profesional:** Menjadi lokasi *training center* dan/atau *testing center* untuk sertifikasi industri terkemuka, seperti **Cisco CCNA/CCNP, CompTIA Security+, CEH (Certified Ethical Hacker)**, atau sertifikasi lain yang relevan. Lab akan menyediakan fasilitas infrastruktur dan simulator ujian.
3. **Kompetisi dan *Event* Siber:** Mengorganisir kompetisi **CTF (*Capture The Flag*)** internal maupun regional secara rutin untuk mengasah keterampilan praktis mahasiswa dalam situasi kompetitif.

3.1.4. Pengelolaan dan Evaluasi Keberlanjutan

Agar Laboratorium NCS dapat berfungsi optimal dan berkelanjutan, akan diterapkan mekanisme pengelolaan dan evaluasi:

- **Standard Operating Procedure (SOP):** Penyusunan SOP peminjaman, penggunaan perangkat, dan **SOP Keamanan Laboratorium** yang ketat, terutama untuk lingkungan *sandbox* guna menjaga integritas dan keamanan fasilitas.
- **Pemeliharaan dan *Upgrade* Rutin:** Melakukan pemeliharaan perangkat keras dan pembaruan lisensi perangkat lunak keamanan secara berkala, minimal dua kali setahun, untuk menjaga **relevansi fasilitas** dengan teknologi dan tren ancaman siber terkini.
- **Evaluasi Kinerja:** Melakukan evaluasi tahunan terhadap kinerja lab berdasarkan tiga metrik utama: **1) Tingkat Pemanfaatan Praktikum (Jumlah SKS yang didukung), 2) Jumlah Publikasi Riset dan Inovasi yang dihasilkan, dan 3) Tingkat Kelulusan Sertifikasi Profesional Mahasiswa/Dosen.** Hasil evaluasi menjadi dasar untuk menyusun rencana anggaran dan pengembangan tahun berikutnya.

3.2. Tahapan Pengembangan

Pengembangan Laboratorium NCS akan dilaksanakan secara bertahap dan terencana dalam horizon waktu lima tahun (dapat disesuaikan) yang terbagi menjadi tiga fase utama: Fase Inisiasi (Tahun 1), Fase Konsolidasi (Tahun 2-3), dan Fase Penguatan/Keunggulan (Tahun 4-5).

Fase Pengembangan	Periode	Fokus Utama Kegiatan
I. Fase Inisiasi	Tahun 1	Perencanaan, Pengadaan Sarana Prasarana Dasar, dan Implementasi Praktikum Awal.
II. Fase Konsolidasi	Tahun 2–3	Penguatan Infrastruktur Riset, Pengembangan Modul Praktikum Lanjut, dan Pilot Project Sertifikasi.
III. Fase Penguatan & Keunggulan	Tahun 4–5	Optimalisasi Fasilitas, Pengakuan Pusat Riset, dan Penguatan Kolaborasi Industri.

I. Fase Inisiasi (Tahun 1: Perencanaan dan Pengadaan Dasar)

Fokus pada peletakan dasar infrastruktur fisik dan teknis yang penting untuk memulai operasional praktikum NCS:

1. ***Perencanaan Kebutuhan dan Desain:***
    - *Menyusun **Bill of Quantity (BOQ)** terperinci untuk perangkat keras (router/switch dasar, server virtualisasi) dan perangkat lunak keamanan (OS, tool forensics dasar).*
    - *Menentukan **Desain Tata Letak (Layout)** Laboratorium NCS, termasuk isolasi jaringan (sandbox) dan kebutuhan Uninterruptible Power Supply (UPS) khusus.*
2. ***Pengadaan Sarana dan Prasarana:***
    - *Pengadaan peralatan jaringan dan server dasar sesuai BOQ.*
    - *Instalasi dan konfigurasi **Jaringan Laboratorium yang Terpisah (Isolated Network)** dari jaringan utama institusi.*
    - *Penyusunan dan penetapan **Standard Operating Procedure (SOP)** penggunaan fasilitas dan SOP Keamanan Lab.*
3. ***Awal Pelaksanaan Kegiatan:***
    - *Integrasi Lab ke dalam modul praktikum mata kuliah **Jaringan Komputer Lanjut** dan **Keamanan Jaringan** (fase konfigurasi dasar).*

II. Fase Konsolidasi (Tahun 2–3: Penguatan dan Pengembangan Riset)

Fokus pada peningkatan kapabilitas Lab untuk mendukung riset dan praktikum lanjutan, serta memulai program pengembangan kompetensi formal:

1. ***Penguatan Infrastruktur:***
    - ***Pengadaan Perangkat Keamanan Lanjut:** Pembelian Next-Generation Firewall (NGFW) dan appliance IDS/IPS tingkat menengah.*
    - ***Pengembangan Cyber Range:** Pembangunan platform virtualized cyber range dan CTF server untuk simulasi serangan siber.*

2. ***Pengembangan Modul dan SDM:***
    - *Pengembangan modul praktikum **Administrasi dan Keamanan Jaringan** serta Digital Forensics lanjutan.*
    - *Peningkatan kompetensi dosen dan teknisi lab melalui pelatihan dan persiapan sertifikasi profesional (misalnya CCNA Security atau CompTIA Security+).*
3. ***Aktivitas Riset dan Pengembangan:***
    - *Pelaksanaan **riset pilot project** di bidang IoT Security atau AI-based Intrusion Detection.*
    - *Penyelenggaraan workshop internal berskala kecil untuk mahasiswa dan alumni.*

III. Fase Penguatan & Keunggulan (Tahun 4–5: Optimalisasi dan Keberlanjutan)

Fokus pada pengakuan Lab sebagai pusat rujukan regional dan menjamin keberlanjutan fungsi Lab:

1. ***Optimalisasi Fasilitas:***
    - ***Pembaruan dan Upgrade Perangkat:** Penggantian atau upgrade perangkat keras yang sudah usang dan pembaruan lisensi software keamanan.*
    - ***Penyediaan Workstation Spesialis:** Pengadaan stasiun kerja khusus untuk Digital Forensics dan Malware Analysis.*
2. ***Penguatan Status dan Kolaborasi:***
    - *Pengajuan Lab NCS sebagai **Pusat Riset Keamanan Siber Institusi** atau **Tempat Uji Kompetensi (TUK)** untuk skema sertifikasi NCS.*
    - *Peningkatan kolaborasi dengan industri dan lembaga keamanan siber nasional melalui Memorandum of Understanding (MoU) untuk penelitian dan penyerapan lulusan.*
3. ***Evaluasi dan Keberlanjutan:***

- *Melakukan **Evaluasi Kinerja Laboratorium** secara menyeluruh berdasarkan metrik tahunan (publikasi, sertifikasi, dan tingkat pemanfaatan).*
- *Menyusun **Rencana Pengembangan Jangka Panjang (Roadmap Jilid II)** untuk menyesuaikan Lab dengan ancaman siber yang diprediksi di masa depan (misalnya, Post-Quantum Cryptography atau Zero Trust Architecture).*

4 POSISI LABORATORIUM DALAM PETA KOMPETENSI KURIKULUM

4.1. Pemosisian Diri Laboratorium NCS

Laboratorium NCS memosisikan diri sebagai fasilitas utama yang berfokus pada **Domain Keamanan Siber (SEC)** dan **Domain Infrastruktur Teknologi (INF)** sesuai dengan Peta Okupasi Nasional dan standar industri global.

Fokus Kompetensi Utama yang Didukung Lab NCS:

- **Network Administration & Engineering:** Kemampuan merancang, mengimplementasikan, dan mengelola infrastruktur jaringan yang kompleks dan *highly available*.
- **Cyber Defense (Blue Team):** Kemampuan mendeteksi, menganalisis, dan merespons insiden keamanan siber (DFIR - *Digital Forensics and Incident Response*).
- **Offensive Security (Red Team):** Kemampuan melakukan pengujian penetrasi (*penetration testing*) dan penilaian kerentanan (*vulnerability assessment*) secara etis.

4.2. Keterkaitan Mata Kuliah, Kompetensi Lulusan, dan Peran Lab

Peran Laboratorium NCS sangat terintegrasi dalam alur pembelajaran kurikulum. Setiap fasilitas dan *toolset* di Lab dirancang untuk secara spesifik mendukung pencapaian luaran (*outcome*) pembelajaran dari mata kuliah kunci:

Mata Kuliah	Capaian Pembelajaran Lulusan (CPL) Terkait	Peran Laboratorium NCS dalam Mendukung CPL
Jaringan Komputer Lanjut	Mahasiswa mampu mengimplementasikan teknologi jaringan modern yang menjamin konektivitas dan ketersediaan tinggi.	Menyediakan perangkat keras riil (router/switch enterprise) dan Virtual Private Network (VPN) Server untuk praktik konfigurasi redundansi dan high availability.
Keamanan Jaringan	Mahasiswa mampu menganalisis risiko jaringan dan menerapkan mekanisme	Menyediakan Next-Generation Firewall (NGFW) dan IDS/IPS Appliance untuk praktik konfigurasi,

	pertahanan menggunakan perangkat keamanan khusus.	policy enforcement, dan log analysis pertahanan jaringan.
Administrasi & Keamanan Jaringan	Mahasiswa mampu mengelola sistem server dan layanan jaringan dengan mengutamakan aspek keamanan (hardening).	Menyediakan SIEM Server dan lingkungan server terisolasi untuk praktik system hardening, monitoring, dan incident log correlation.

4.3. Peran Laboratorium dalam Evaluasi dan Pengembangan Kurikulum

Laboratorium NCS tidak hanya berfungsi sebagai fasilitas praktik, tetapi juga sebagai alat evaluasi dan pengembangan kurikulum:

1. **Evaluasi Kompetensi *Hands-On*:** Lab digunakan untuk mengukur kompetensi praktis mahasiswa secara objektif, sering kali melalui skenario *live Capture The Flag* (CTF) atau simulasi insiden siber. Hasil praktik ini menjadi *feedback* langsung terhadap efektivitas metode pengajaran dan kesenjangan kompetensi yang harus segera diatasi.
2. **Inkubator Kurikulum Baru:** Fasilitas Lab yang fleksibel memungkinkan dosen untuk menguji coba dan mengembangkan modul praktikum untuk mata kuliah pilihan/baru (misalnya Keamanan IoT, *Threat Intelligence*) sebelum diintegrasikan secara penuh ke dalam kurikulum reguler.
3. **Memastikan Relevansi Industri:** Melalui fasilitas dan *toolset* yang diselaraskan dengan tren ancaman siber terbaru, Lab NCS memastikan bahwa konten kurikulum tetap relevan dan lulusan menguasai teknologi keamanan yang sedang digunakan di lapangan.

5 LANDASAN HUKUM DAN KEBIJAKAN

5.1. Dasar Hukum dan Regulasi Nasional

Dasar hukum yang melandasi urgensi dan pendirian Laboratorium NCS meliputi, namun tidak terbatas pada:

1. **Undang-Undang Nomor 12 Tahun 2012** tentang Pendidikan Tinggi, yang mengamanatkan penyelenggaraan Tri Dharma Perguruan Tinggi (Pendidikan, Penelitian, dan Pengabdian kepada Masyarakat). Lab NCS adalah sarana esensial untuk mendukung pelaksanaan Tri Dharma di bidang teknologi terkini.
2. **Peraturan Pemerintah Nomor 4 Tahun 2014** tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi, yang menekankan perlunya fasilitas memadai untuk mencapai mutu pendidikan.
3. **Kebijakan Strategis Nasional (Sesuai Konteks):** Merujuk pada payung hukum yang berhubungan dengan keamanan siber dan infrastruktur, seperti **Undang-Undang Nomor 11 Tahun 2008** tentang Informasi dan Transaksi Elektronik (UU ITE) dan **Kebijakan Strategis Badan Siber dan Sandi Negara (BSSN)**, yang menunjukkan bahwa keamanan siber adalah isu strategis nasional.
4. **Kebijakan Merdeka Belajar Kampus Merdeka (MBKM):** Program ini mendorong kolaborasi dengan dunia industri dan pengalaman praktik riil. Lab NCS berfungsi sebagai *platform* internal yang mereplikasi lingkungan kerja profesional di bidang keamanan siber, mendukung kesuksesan program MBKM.

5.2. Regulasi Internal Perguruan Tinggi

Pendirian Lab NCS sejalan dan didukung oleh peraturan dan kebijakan internal institusi (disesuaikan dengan nama dan aturan Perguruan Tinggi Anda), seperti:

1. **Statuta Institusi:** Yang menjadi landasan utama bagi pengembangan unit pendukung akademik, termasuk laboratorium.
2. **Rencana Strategis (Renstra) Institusi:** Lab NCS secara eksplisit mendukung tujuan dalam Renstra yang berkaitan dengan **peningkatan kualitas riset dan inovasi**, serta **pencapaian status institusi unggulan** di bidang teknologi.
3. **Peraturan Organisasi dan Tata Kerja (POTK):** Yang mengatur pembentukan dan operasional unit pelaksana teknis (UPT) dan unit pendukung akademik di lingkungan Jurusan/Program Studi.

5.3. Kesesuaian Visi-Misi dan Kebutuhan Industri

Laboratorium NCS dirancang untuk memastikan kesesuaian antara luaran akademik dengan tuntutan pasar kerja, memberikan legitimasi pengembangan yang jelas:

- **Visi dan Misi Institusi:** Lab NCS mendukung visi institusi untuk menjadi lembaga pendidikan vokasi/teknologi terkemuka dengan berfokus pada keahlian *hands-on* yang **tahan banting terhadap ancaman siber** dan mampu mengelola infrastruktur digital secara aman.
- **Kebutuhan Industri dan Kompetensi Lulusan:** Dengan fokus pada praktik **Jaringan, *Firewall*, IDS/IPS, dan *Digital Forensics***, Lab ini menjamin bahwa kompetensi lulusan telah diselaraskan dengan **standar profesional industri** (seperti yang didefinisikan oleh NIST, ISO 27001, atau sertifikasi seperti CCNA Security dan CEH).

6 ANALISIS SWOT LABORATORIUM

6.1. Faktor Internal

A. Strengths (Kekuatan)

Kekuatan merupakan keunggulan internal yang dimiliki oleh institusi/jurusan dalam mendirikan dan mengoperasikan Lab NCS.

1. **Dukungan SDM Dosen Berkualitas:** Adanya staf pengajar (dosen) yang memiliki **sertifikasi profesional di bidang jaringan dan keamanan siber** (seperti CCNA, CEH, Mikrotik MTCNA, dll.) dan berpengalaman dalam riset terkait.
2. **Kurikulum yang Relevan:** Kurikulum Program Studi sudah memiliki mata kuliah spesifik di bidang NCS (*Jaringan Komputer Lanjut, Keamanan Jaringan, Administrasi & Keamanan Jaringan*), sehingga integrasi Lab ke dalam pembelajaran menjadi mudah.
3. **Potensi Integrasi Multidisiplin:** Laboratorium memiliki potensi untuk berintegrasi dengan bidang ilmu lain (seperti *IoT* dan *Machine Learning*) yang membutuhkan lingkungan jaringan aman untuk pengujian (*sandbox*).
4. **Komitmen Institusi:** Adanya komitmen manajemen puncak dan Jurusan untuk memprioritaskan keamanan siber sebagai area keunggulan riset dan pendidikan.

B. Weaknesses (Kelemahan)

Kelemahan adalah keterbatasan internal yang dapat menjadi hambatan dalam pengembangan Lab NCS.

1. **Biaya Pengadaan dan Lisensi Tinggi:** Peralatan dan perangkat lunak keamanan siber kelas industri (*Next-Generation Firewall, SIEM system, Digital Forensics tool*) seringkali memerlukan **biaya investasi awal dan biaya lisensi tahunan** yang sangat tinggi.
2. **Keterbatasan Ruang Fisik:** Keterbatasan alokasi ruangan fisik yang memadai untuk menampung infrastruktur *server* dan *workstation* keamanan yang memiliki spesifikasi tinggi.

3. **Ketergantungan pada Teknisi Spesialis:** Operasional dan pemeliharaan Lab NCS membutuhkan **teknisi dengan keahlian khusus** dalam mengelola perangkat keras dan lingkungan *virtualized cyber range*, yang sulit didapatkan atau dipertahankan.
4. **Umur Ekonomis Peralatan Pendek:** Teknologi keamanan siber dan *hacker tools* berkembang sangat cepat, menyebabkan **perangkat keras cepat usang** dan harus di-*upgrade* atau diganti secara berkala.

6.2. Faktor Eksternal

C. Opportunities (Peluang)

Peluang adalah faktor eksternal yang dapat dimanfaatkan untuk mengembangkan dan memajukan Lab NCS.

1. **Permintaan Pasar Kerja Tinggi:** Adanya **permintaan yang sangat tinggi** dari industri (perbankan, *fintech*, BUMN) terhadap lulusan dengan kompetensi *hands-on* di bidang *Cyber Security Analyst* dan *Network Security Engineer*.
2. **Dukungan Program Sertifikasi Nasional/Global:** Banyak program sertifikasi dan pelatihan (seperti BNSP, Cisco, CompTIA) yang mendorong kerjasama dalam penyediaan *Authorized Training Center* atau *Testing Center*.
3. **Prioritas Isu Keamanan Siber Nasional:** Pemerintah (melalui BSSN) dan institusi strategis lainnya sangat memprioritaskan **ketahanan siber nasional**, membuka peluang pendanaan riset dan pengabdian masyarakat.
4. **Tren *Cloud Security* dan *DevSecOps*:** Pergeseran industri ke *cloud computing* dan *DevSecOps* membuka peluang untuk mengembangkan modul praktikum dan riset baru yang relevan.

D. Threats (Ancaman)

Ancaman adalah faktor eksternal yang dapat menghambat pencapaian tujuan dan fungsi Lab NCS.

1. **Dinamika Ancaman Siber yang Cepat: Perubahan metode serangan dan *tools* peretasan** yang sangat cepat membuat modul praktikum dan

infrastruktur yang sudah dibangun menjadi rentan dan memerlukan pembaruan terus-menerus.

2. **Persaingan dengan Institusi Lain:** Institusi pendidikan lain, terutama yang berdekatan, mungkin juga mendirikan Lab serupa dengan investasi yang lebih besar, menciptakan **persaingan dalam kualitas dan daya tarik**.
3. **Ancaman Regulasi Lisensi:** Kebijakan lisensi perangkat lunak keamanan siber oleh vendor global yang bisa berubah sewaktu-waktu, berpotensi menaikkan biaya operasional secara drastis.
4. ***Brain Drain* SDM Laboratorium:** Teknisi atau asisten laboratorium yang sudah terlatih seringkali **diambil oleh industri** dengan tawaran gaji yang jauh lebih tinggi, menyebabkan hilangnya SDM operasional inti Lab.

6.3. Strategi Pengembangan Berdasarkan SWOT

Berdasarkan analisis di atas, strategi pengembangan Laboratorium NCS dapat difokuskan pada penguatan Kekuatan untuk memanfaatkan Peluang (**Strategi SO**) dan penggunaan Kekuatan untuk menanggulangi Ancaman (**Strategi ST**).

- **Strategi SO (Kekuatan-Peluang):** Memanfaatkan **Kekuatan Dosen Tersertifikasi (S1)** untuk menjadi **Penyelenggara Resmi Sertifikasi (O2)**, sehingga Lab NCS menjadi sumber pendapatan dan pusat pelatihan regional.
- **Strategi ST (Kekuatan-Ancaman):** Menggunakan **Kekuatan Kurikulum yang Relevan (S2)** untuk secara cepat menyusun **modul *quick-response*** terhadap **Dinamika Ancaman Siber yang Cepat (T1)**, memastikan materi ajar selalu *up-to-date* dan relevan.

7 ROADMAP LABORATORIUM

Roadmap ini berfungsi sebagai panduan strategis yang menetapkan tujuan dan target terukur bagi Laboratorium NCS dalam kurun waktu lima tahun (2025–2029). Implementasi bertahap ini dirancang untuk memastikan Lab NCS mampu berkontribusi secara berkelanjutan terhadap peningkatan kualitas lulusan, riset, dan pemecahan masalah nyata di industri keamanan siber.

7.1. Jangka Pendek (Tahun 1 – 2: Inisiasi dan Fungsional Dasar)

Fokus utama pada peletakan dasar infrastruktur dan integrasi Lab ke dalam kegiatan akademik wajib.

Fokus Utama	Target Pencapaian	Indikator Kinerja Utama (IKU)
Infrastruktur Jaringan (Networking)	Pengadaan dan instalasi perangkat keras enterprise dasar (router/switch Level 3) untuk praktik VPN dan Redundansi Jaringan.	100% mata kuliah Jaringan Komputer Lanjut terintegrasi menggunakan perangkat keras riil Lab NCS.
Keamanan Siber (Cyber Security)	Instalasi Jaringan Praktikum Terisolasi (Sandbox) dan konfigurasi firewall dasar. Pengembangan modul praktik Keamanan Jaringan (konfigurasi dasar NGFW).	Rata-rata nilai praktik CPL Keamanan Jaringan meningkat 10% dan SOP Keamanan Lab tervalidasi.
Pendidikan & SDM	Dosen dan teknisi Lab minimal memiliki sertifikasi dasar (misalnya, CCNA/MTCNA). Modul praktikum Jaringan Komputer Lanjut dan Keamanan Jaringan selesai direvisi.	80% modul praktikum diawaki oleh SDM yang memiliki sertifikasi relevan.

7.2. Jangka Menengah (Tahun 3 – 4: Konsolidasi dan Keahlian Lanjut)

Fokus utama pada pengembangan infrastruktur riset lanjutan, spesialisasi, dan penguatan *branding* Lab NCS di tingkat regional.

Fokus Utama	Target Pencapaian	Indikator Kinerja Utama (IKU)
Infrastruktur Jaringan (Networking)	Pengembangan platform Cloud Networking lokal dan praktik implementasi SDN (Software Defined Networking). Peningkatan workstation untuk praktik administrasi sistem.	Implementasi dan testing sistem jaringan virtual yang kompleks untuk riset dan skripsi.

Keamanan Siber (Cyber Security)	Pembelian dan instalasi SIEM dan perangkat lunak Digital Forensics berlisensi. Pengembangan modul praktik Ethical Hacking / DFIR dalam lingkungan Cyber Range.	Minimal 50% mahasiswa tingkat akhir mengikuti kompetisi siber (CTF) atau ujian sertifikasi internal Lab NCS.
Riset & Sertifikasi	Lab NCS diakui sebagai Pusat Pelatihan Non-Formal atau TUK untuk 1 skema sertifikasi NCS. Minimal 5 riset terapan kolaboratif didanai eksternal.	Minimal 3 publikasi ilmiah terakreditasi/internasional dari riset yang didukung Lab.

7.3. Jangka Panjang (Tahun 5 ke Atas: Keunggulan dan Keberlanjutan)

Fokus utama pada pengakuan Lab NCS sebagai pusat rujukan nasional, inovasi berkelanjutan, dan kemandirian operasional.

Fokus Utama	Target Pencapaian	Indikator Kinerja Utama (IKU)
Pusat Keunggulan (Center of Excellence)	Lab NCS diakui sebagai Pusat Rujukan Jaringan Aman & Cyber Range regional. Menjadi mitra utama industri untuk pengujian keamanan.	Pendapatan Lab NCS dari layanan training dan audit keamanan minimal 10% dari biaya operasional tahunan.
Riset & Inovasi Berkelanjutan	Pengadaan GPU Server untuk mendukung riset AI-based Intrusion Detection dan Malware Analysis tingkat lanjut.	Minimal 1 Paten/HAKI atau kerjasama industrial research yang bernilai komersial.
SDM & Kurikulum	Minimal 10 dosen memiliki sertifikasi keamanan tingkat lanjut (misalnya CCNP Security, CISSP, OSCP). Kurikulum dan fasilitas Lab senantiasa relevan dengan teknologi Post-Quantum Cryptography.	Skor kepuasan industri terhadap kompetensi lulusan (yang didukung Lab) mencapai > 90%.

8 PENUTUP

Pendirian Lab NCS bukan sekadar penambahan fasilitas fisik, melainkan **investasi strategis** dalam kualitas pendidikan, riset, dan kesiapan lulusan menghadapi tantangan keamanan siber. Dengan dukungan penuh dari institusi dan implementasi *roadmap* yang terencana, Lab NCS akan berperan vital dalam mewujudkan visi Jurusan/Program Studi sebagai pusat unggulan yang mencetak sumber daya manusia kompeten dan berintegritas di bidang Network and Cyber Security.

9 LAMPIRAN

Lampiran 9.1. Matriks Mata Kuliah Pendukung dan Kebutuhan Praktikum

Tabel ini menunjukkan pemetaan antara mata kuliah yang ada dalam Kurikulum Program Studi dengan kebutuhan praktikum spesifik yang hanya dapat difasilitasi oleh Laboratorium NCS.

No.	Mata Kuliah	SKS Praktikum	Kompetensi Praktis yang Dicapai di Lab NCS	Keterangan/Hubungan ke Bidang NCS
1.	Jaringan Komputer Lanjut	2	Konfigurasi Lanjut & Redundansi: VPN, HA (High Availability), Load Balancing pada perangkat riil.	Network Engineering, Resilience.
2.	Keamanan Jaringan	2	Penerapan Pertahanan: Konfigurasi Next-Generation Firewall, IDS/IPS, dan policy enforcement.	Network Defense, Perimeter Security.
3.	Administrasi & Keamanan Jaringan	2	Pengelolaan Sistem Aman: Server Hardening, Log Management dengan SIEM, User Authentication (RADIUS/TACACS+).	System Hardening, Incident Monitoring.
4.	Ethical Hacking & Penetration Testing	2	Pengujian Sistem: Vulnerability Assessment, Exploit dalam lingkungan Cyber Range/Sandbox.	Offensive Security, Threat Simulation.
5.	Digital Forensics & Incident Response	2	Investigasi Insiden: Live Acquisition, Malware Analysis, Analisis Bukti Digital dengan Tool Forensik.	Blue Team, Cyber Crime Investigation.
6.	Cloud Computing (Pilihan)	1	Keamanan Cloud: Konfigurasi Virtual Private Cloud (VPC) dan Security Group pada platform cloud (misalnya AWS/Azure).	Cloud Security, Infrastructure as Code.

Lampiran 9.2. Daftar Kebutuhan Sarana dan Prasarana Laboratorium NCS (Contoh BOQ Singkat)

Daftar ini memuat kebutuhan infrastruktur utama yang diperlukan untuk operasional Laboratorium NCS, dikelompokkan berdasarkan fungsinya dalam Tri Dharma Perguruan Tinggi.

A. Infrastruktur Jaringan dan Keamanan Inti

No.	Nama Peralatan / Lisensi	Kuantitas (Unit)	Fungsi Utama	Keterangan
1.	Server Virtualisasi/Compute Node	3	Hosting Cyber Range, SIEM, Honeypot, dan Virtual Machine Praktikum.	Server spesifikasi tinggi (CPU Multi-core, RAM > 128GB, SSD)
2.	Next-Generation Firewall (NGFW)	1	Perangkat keras untuk praktik policy enforcement dan Application Layer Filtering.	Minimal 1 Unit NGFW entry-level industri (misalnya Fortinet/Palo Alto).
3.	Switch Layer 3 Managed (PoE)	2	Membangun jaringan kampus dan praktik VLAN, Access Control List (ACL), dan Network Segmentation.	Cisco/Juniper/HPE (minimal 48 port).
4.	Rack Server & Kabinet Pendingin	1	Penyimpanan dan pengamanan seluruh perangkat aktif Lab.	42U Rack Cabinet dengan sistem pendingin dan UPS terpisah.

B. Perangkat Lunak dan Platform Uji Coba

No.	Nama Perangkat Lunak / Platform	Kuantitas (Lisensi/Tahun)	Fungsi Utama	Keterangan
1.	Platform Virtualisasi (VMware/Hyper-V)	Sesuai Kebutuhan	Dasar untuk membangun lingkungan Cyber Range dan Sandbox.	Lisensi Akademik/Enterprise.
2.	SIEM (Security Information and Event Management)	1	Praktik Log Analysis, Incident Monitoring, dan Threat Correlation.	Lisensi Akademik/Community Edition.

3.	Digital Forensics Tools	5	Praktik Data Acquisition, Malware Analysis, dan Incident Response.	Lisensi perangkat lunak forensik industri (misalnya FTK Imager, Autopsy).
4.	Sistem Operasi Server	Sesuai Kebutuhan	Lisensi sistem operasi server untuk praktik System Hardening.	Lisensi Windows Server/Red Hat Enterprise Linux.

C. Sarana Penunjang Lain

No.	Nama Sarana	Kuantitas (Unit)	Fungsi Utama	Keterangan
1.	Workstation Praktikum	20	Komputer dengan spesifikasi tinggi untuk menjalankan VM praktik.	Min. Core i5/Ryzen 5, RAM 16GB, SSD 512GB.
2.	Meja dan Kursi Ergonomis	20	Penunjang kenyamanan praktik jangka panjang.	Disesuaikan dengan kapasitas ruangan.
3.	Papan Tulis Interaktif/Proyektor	1	Dukungan pengajaran dan debriefing praktik.	Dilengkapi koneksi jaringan ke Lab.

Lampiran 9.3. Visi, Misi, dan Struktur Organisasi Laboratorium NCS

A. Visi Laboratorium NCS

"Menjadi Pusat Keunggulan (Center of Excellence) Nasional dalam Pendidikan Vokasi dan Riset Terapan di Bidang Infrastruktur Jaringan Aman dan Mitigasi Ancaman Siber, yang selaras dengan kebutuhan industri 4.0."

B. Misi Laboratorium NCS

1. Menyelenggarakan praktikum berbasis *hands-on* yang adaptif terhadap dinamika ancaman siber dan teknologi jaringan terbaru.
2. Mendukung riset dan inovasi yang berfokus pada solusi keamanan siber terapan untuk memecahkan masalah industri dan masyarakat.
3. Meningkatkan kompetensi profesional lulusan melalui fasilitas yang mendukung sertifikasi NCS berskala global.
4. Menjalin kemitraan strategis dengan industri, pemerintah, dan komunitas dalam transfer pengetahuan dan teknologi keamanan siber.

C. Struktur Organisasi Laboratorium NCS

(Sertakan diagram struktur organisasi di sini. Contoh strukturnya adalah sebagai berikut):

- **Kepala Laboratorium NCS:** (Penanggung Jawab Utama dan Koordinator Strategis)
    - **Koordinator Praktikum & Kurikulum:** (Bertanggung jawab atas modul praktik dan jadwal harian)
    - **Koordinator Riset & Inovasi:** (Bertanggung jawab atas riset, publikasi, dan kerjasama PkM)
    - **Tenaga Laboran/Teknisi Jaringan:** (Bertanggung jawab atas pemeliharaan infrastruktur dan *troubleshooting* teknis)
    - **Asisten Laboratorium:** (Bertanggung jawab atas asistensi praktikum harian)