ITSM Class: B

Class Activity Week 10

Individual

Nama : Komang Alit Pujangga
NRP : 5026231115

Information Systems Department
Institut Teknologi Sepuluh Nopember
August-December 2025

A.Manajemen Perubahan (*Change Management*)

Definisi dan Tujuan

Definisi: Manajemen Perubahan adalah proses yang bertujuan untuk mengontrol semua perubahan pada layanan dan infrastruktur TI secara efisien dan terorganisir. Ini meminimalkan dampak buruk dari insiden yang terkait dengan perubahan, memastikan bahwa perubahan dilakukan dengan cara yang terstandardisasi, dan memungkinkan perubahan yang bermanfaat untuk dibuat.

Tujuan: Tujuan utama Manajemen Perubahan adalah:

1. Memastikan Perubahan yang Berhasil: Memastikan bahwa semua perubahan diimplementasikan dengan benar dan terintegrasi, memenuhi kebutuhan bisnis.
2. Meminimalkan Risiko: Mengurangi risiko insiden dan gangguan layanan yang disebabkan oleh perubahan yang salah atau tidak terkelola.
3. Mendukung Bisnis: Memungkinkan organisasi untuk merespons kebutuhan bisnis yang berubah dengan cepat dan biaya yang efektif.

3 Tipe Perubahan (3 Types of Changes)

Manajemen Perubahan mengklasifikasikan perubahan menjadi tiga jenis utama, yang menentukan tingkat proses dan persetujuan yang diperlukan:

1. Perubahan Standar (Standard Change):
    - Perubahan berisiko rendah, umum, dan telah disetujui sebelumnya.
    - Mengikuti prosedur yang didokumentasikan dan disahkan.
    - Tidak memerlukan persetujuan CAB (Change Advisory Board) setiap kali dilakukan.
    - Contoh: Menambahkan port baru ke switch, upgrade patch software rutin yang telah diuji.
2. Perubahan Normal (Normal Change):
    - Perubahan yang tidak termasuk dalam kategori Standar atau Darurat.
    - Biasanya berisiko sedang hingga tinggi dan memerlukan evaluasi risiko dan dampak penuh.
    - Membutuhkan persetujuan dari Change Authority (biasanya CAB) sebelum implementasi.
    - Contoh: Pemasangan server baru, upgrade besar aplikasi inti, migrasi basis data.
3. Perubahan Darurat (Emergency Change - EC)*:*
    - Perubahan yang harus diimplementasikan secepat mungkin untuk memperbaiki kesalahan atau insiden yang berdampak sangat serius pada bisnis.

    - Memiliki proses yang disingkat atau dipercepat, seringkali dengan persetujuan oleh ECAB (Emergency Change Advisory Board) atau otoritas tunggal tertentu.
    - Evaluasi risiko dilakukan secara cepat, dan dokumentasi lengkap sering dilakukan setelah perubahan berhasil diterapkan.
    - Contoh: Memperbaiki bug kritis keamanan yang terekspos, mengembalikan layanan yang down karena kegagalan komponen.

Sub-proses

Proses Manajemen Perubahan (Normal) yang umum meliputi langkah-langkah berikut:

1. Permintaan Perubahan (Request for Change/RFC): Pengajuan resmi yang mendokumentasikan kebutuhan untuk perubahan.
2. Pencatatan dan Pemfilteran (Record and Filter): Mencatat RFC di sistem dan memfilter permintaan yang tidak valid.
3. Penilaian dan Evaluasi (Assess and Evaluate): Menganalisis dampak, risiko, dan manfaat perubahan. Ini termasuk pertemuan CAB.
4. Otorisasi (Authorize): Memberikan persetujuan resmi (oleh Change Authority/CAB) untuk melanjutkan ke tahap implementasi.
5. Perencanaan dan Penjadwalan (Plan and Schedule): Membuat rencana implementasi, back-out, dan pengujian; menjadwalkan jendela perubahan (Change Window).
6. Implementasi (Implement): Melaksanakan perubahan sesuai dengan rencana yang disetujui.
7. Tinjauan Pasca-Implementasi (Post Implementation Review/PIR): Meninjau keberhasilan perubahan, apakah tujuan tercapai, apakah ada efek samping yang tidak diinginkan, dan memastikan dokumentasi sudah diperbarui.

Contoh-Contoh KPI (Key Performance Indicators)

KPI digunakan untuk mengukur efektivitas proses Manajemen Perubahan:

- Persentase Perubahan yang Berhasil: Jumlah perubahan yang berhasil dibagi dengan total perubahan.
    - Tujuan: Menunjukkan kualitas perencanaan dan pelaksanaan.
- Jumlah Insiden yang Disebabkan oleh Perubahan: Jumlah insiden serius yang terjadi dalam 24-48 jam setelah perubahan diterapkan.
    - Tujuan: Mengukur risiko yang dimasukkan ke dalam lingkungan oleh proses perubahan.
- Waktu Siklus Perubahan (Change Cycle Time): Waktu rata-rata dari pengajuan RFC hingga penyelesaian PIR.
    - Tujuan: Mengukur efisiensi dan kecepatan proses.

- Jumlah Perubahan Darurat (Emergency Changes): Mengukur frekuensi perubahan mendesak yang harus melewati proses ringkas.
    - Tujuan: Menunjukkan kualitas perencanaan proaktif dan Manajemen Masalah.
- Kepatuhan terhadap Prosedur Perubahan: Persentase perubahan yang mengikuti prosedur yang disetujui (misalnya, semua perubahan disahkan oleh CAB).

Definisi, Tugas/Wewenang CAB (Change Advisory Board)

Definisi CAB: Dewan Penasihat Perubahan (Change Advisory Board disingkat CAB) adalah sekelompok orang yang terdiri dari perwakilan dari semua area bisnis TI (seperti tim teknis, operasional, keamanan, dan perwakilan bisnis) yang membantu Change Manager dalam mengevaluasi, memprioritaskan, dan mengotorisasi perubahan Normal.

Tugas/Wewenang CAB:

1. Menilai dan Mengevaluasi Risiko/Dampak: Meninjau setiap RFC yang kompleks, berisiko tinggi, atau signifikan untuk menilai potensi dampak negatif terhadap layanan dan bisnis.
2. Memverifikasi Sumber Daya: Memastikan bahwa semua sumber daya teknis dan finansial yang diperlukan tersedia untuk implementasi.
3. Mengotorisasi Perubahan: Memberikan persetujuan atau penolakan akhir untuk perubahan Normal, memastikan bahwa perubahan yang diusulkan adalah yang terbaik bagi organisasi.
4. Memfasilitasi Komunikasi: Memastikan bahwa semua pihak yang terkena dampak memiliki kesempatan untuk menyuarakan kekhawatiran dan memahami rencana perubahan.
5. Memantau Perubahan yang Sedang Berjalan: Terkadang meninjau status perubahan yang sedang berlangsung.

B.Manajemen Rilis dan Deployment (*Release & Deployment Management*)

Definisi dan Tujuan

Definisi: Manajemen Rilis dan Deployment adalah proses yang bertanggung jawab untuk memastikan bahwa semua perubahan, baik perangkat lunak maupun perangkat keras (yang disetujui melalui Manajemen Perubahan), diimplementasikan secara terstruktur dan terkoordinasi ke lingkungan live (produksi). Ini mencakup perencanaan, perancangan, build, konfigurasi, dan pengujian rilis perangkat keras dan perangkat lunak.

Tujuan: Tujuan utama Manajemen Rilis dan Deployment adalah:

1. Pengiriman Nilai: Memastikan pengiriman layanan baru atau perubahan pada layanan yang ada yang memenuhi persyaratan bisnis dan telah divalidasi.
2. Integritas Lingkungan Live: Melindungi integritas lingkungan live dan memastikan bahwa hanya komponen yang teruji dan diotorisasi yang dideploy.
3. Transisi yang Efisien: Mengelola transisi layanan ke lingkungan live dengan risiko minimum dan dampak minimum pada pengguna dan layanan yang ada.

Kaitan Antara Manajemen Perubahan dan Manajemen Rilis/Deployment (The Link between Change & Release/Deployment Management)

Manajemen Perubahan dan Manajemen Rilis/Deployment adalah dua proses yang sangat erat terkait dan saling bergantung dalam Manajemen Transisi Layanan (Service Transition):

1. Pengendalian (Kontrol): Setiap Rilis (baik baru maupun perubahan) harus dimulai dan disahkan oleh proses Manajemen Perubahan. Rilis mewakili pelaksanaan atau instalasi fisik dari satu atau lebih Perubahan (Change).
2. Satu ke Banyak: Sebuah Permintaan Perubahan (RFC) dapat menghasilkan satu atau lebih Rilis. Sebaliknya, satu Rilis sering kali mencakup banyak perubahan (Change), perbaikan (Bug Fix), dan peningkatan.
3. Otorisasi Kritis: Setelah Manajemen Perubahan menyetujui perubahan (melalui RFC), Manajemen Rilis dan Deployment bertanggung jawab untuk merencanakan waktu yang tepat, cara, dan prosedur untuk benar-benar membangun, menguji, dan memasukkan perubahan tersebut ke lingkungan live.
4. Umpan Balik: Manajemen Rilis memberikan informasi status kembali ke Manajemen Perubahan (misalnya, melaporkan keberhasilan atau kegagalan deployment) untuk keperluan Tinjauan Pasca-Implementasi (PIR).

Sub-proses

Proses Manajemen Rilis dan Deployment yang umum meliputi langkah-langkah berikut:

1. Perencanaan Rilis (Release Planning): Mendefinisikan cakupan rilis (apa saja yang termasuk) dan jenis rilis (misalnya, rilis mayor, minor, atau darurat).
2. Membangun dan Menguji Rilis (Release Build and Test): Mengumpulkan semua Configuration Item (CI) yang terkait (kode, hardware, dokumentasi) dan merakitnya menjadi paket rilis, kemudian mengujinya secara menyeluruh di lingkungan pengujian.
3. Rencana Deployment (Deployment Planning): Merancang strategi deployment yang terperinci, termasuk jadwal, prosedur back-out, dan koordinasi dengan pengguna.
4. Deployment: Melaksanakan instalasi paket rilis ke lingkungan live sesuai dengan jadwal dan rencana yang disetujui. Ini dapat berupa deployment bertahap, big bang, atau deployment otomatis.

5. Verifikasi dan Penutupan (Verification and Closure): Memastikan bahwa rilis telah berhasil dideploy, layanan berfungsi sebagaimana mestinya di lingkungan live, dan menyerahkan kontrol ke Manajemen Operasi Layanan.

Contoh-Contoh KPI (Key Performance Indicators)

KPI digunakan untuk mengukur kinerja dan kualitas proses Rilis dan Deployment:

- Tingkat Kegagalan Deployment (Deployment Failure Rate): Persentase rilis yang gagal atau yang harus dilakukan back-out segera.
    - Tujuan: Mengukur kualitas proses build dan test.
- Waktu Penyelesaian Rilis (Release Completion Time): Waktu rata-rata yang diperlukan untuk menyelesaikan deployment (misalnya, dari persetujuan hingga go-live).
    - Tujuan: Mengukur efisiensi proses transisi.
- Jumlah Gangguan Layanan Akibat Rilis: Jumlah insiden serius yang terjadi dalam periode tertentu setelah deployment.
    - Tujuan: Mengukur dampak negatif dan risiko yang dimasukkan ke lingkungan live.
- Cakupan Deployment Otomatis: Persentase deployment yang dilakukan menggunakan alat otomatis (vs. manual).
    - Tujuan: Mengukur efisiensi dan konsistensi.
- Kepatuhan Terhadap Jadwal: Persentase deployment yang selesai tepat waktu dan sesuai jadwal yang disetujui.

C.Configuration & Asset Management (Manajemen Aset dan Konfigurasi)

1. Definisi, Fungsi, dan Tujuan

Definisi: Manajemen Aset dan Konfigurasi Layanan (Service Asset and Configuration Management disingkat SACM) adalah proses yang bertujuan untuk mengidentifikasi, mengontrol, mencatat, dan memelihara informasi tentang semua Aset Layanan (termasuk aset finansial dan fisik) dan Item Konfigurasi (CI) yang mendukung penyediaan layanan TI.

Fungsi dan Tujuan: Fungsi utama SACM adalah menyediakan model logis atau pandangan hierarki dari layanan dan infrastruktur TI. Tujuannya adalah untuk:

- Memastikan bahwa informasi konfigurasi yang akurat dan dapat diandalkan tersedia bagi semua proses Manajemen Layanan TI lainnya, seperti Manajemen Perubahan, Manajemen Insiden, dan Manajemen Masalah.

- Mendukung akuntabilitas dengan mengetahui lokasi, status, dan versi setiap komponen infrastruktur.
- Mengontrol integritas aset dan CI sepanjang siklus hidupnya.

2. Sub-proses

SACM umumnya melibatkan sub-proses utama berikut untuk mengelola siklus hidup Item Konfigurasi (CI):

- Perencanaan dan Identifikasi: Menentukan kebijakan dan prosedur SACM, serta memutuskan tingkat detail yang dibutuhkan. Langkah ini mencakup identifikasi semua CI yang relevan, atributnya, dan hubungan logisnya.
- Kontrol Konfigurasi: Memastikan bahwa hanya CI yang telah diotorisasi dan diverifikasi yang diizinkan masuk ke dalam Sistem Manajemen Konfigurasi (CMS). Proses ini bekerja sangat erat dengan Manajemen Perubahan untuk mengontrol perubahan pada CI.
- Akuntansi Status Konfigurasi (Configuration Status Accounting): Mencatat dan melaporkan setiap perubahan status CI yang penting (misalnya, dari diuji menjadi aktif atau pensiun). Tujuannya adalah menyediakan riwayat konfigurasi yang lengkap.
- Verifikasi dan Audit: Melakukan audit fisik dan logis secara berkala untuk membandingkan informasi yang tercatat dalam CMS dengan kondisi aktual di lingkungan live. Setiap perbedaan yang ditemukan harus diselidiki dan dikoreksi.

3. Penjelasan CI, CMS, dan CMDB

a. CI (Configuration Item)

Configuration Item adalah setiap komponen yang perlu dikelola atau dikontrol untuk menyediakan layanan TI. CI bukan hanya perangkat keras atau perangkat lunak, tetapi juga dapat mencakup layanan, dokumentasi (seperti SLA), personel, atau arsitektur. Yang paling penting, CI mendefinisikan hubungan antar-komponen tersebut, yang memungkinkan analisis dampak yang cepat saat terjadi perubahan atau insiden.

b. CMDB (Configuration Management Database)

Configuration Management Database adalah basis data aktual tempat semua rekaman CI dan hubungannya disimpan secara fisik. CMDB berfungsi sebagai repositori sentral data konfigurasi. CMDB hanyalah sebuah database.

c. CMS (Configuration Management System)

Configuration Management System adalah kumpulan alat dan data yang komprehensif yang digunakan untuk mengelola data konfigurasi. CMS mencakup satu atau lebih CMDB bersama dengan alat lain seperti alat discovery (untuk menemukan aset), alat audit, dan alat pelaporan

yang membantu mengumpulkan, memelihara, dan menyajikan informasi konfigurasi. CMS memberikan pandangan logis dan lengkap tentang semua aset TI dan layanan di seluruh organisasi.

4. Contoh-Contoh KPI (Key Performance Indicators)

KPI digunakan untuk mengukur efektivitas dan kualitas proses SACM:

- Tingkat Akurasi CMDB: Diukur berdasarkan persentase Item Konfigurasi (CI) yang diverifikasi dan dianggap akurat (atribut dan hubungan) selama audit. Akurasi tinggi adalah indikator proses yang sehat.
- Waktu Penyelesaian Pembaruan CI: Waktu rata-rata yang diperlukan untuk memperbarui rekaman CI setelah adanya perubahan yang diimplementasikan.
- Pelanggaran Kontrol Konfigurasi: Jumlah insiden di mana perubahan dilakukan pada CI tanpa otorisasi formal atau tanpa tercatat dalam CMS.
- Cakupan CMS/CMDB: Persentase total aset penting organisasi yang berhasil diidentifikasi dan dikelola sebagai CI.
- Jumlah Perbedaan yang Ditemukan: Jumlah ketidaksesuaian yang ditemukan antara CMDB dan lingkungan fisik selama audit

Tugas Kelompok

Part 1

Request for Change (RFC) Checklist

Field	**Detail**
Unique ID	CHG-2025-WIFI-01
Date of Submission	October 28, 2025
Proposed Priority	High (Time-sensitive, but not an emergency)

Priority Assigned by Change Mgmt	High
Reference to Change Proposal	"IT Security Improvement Plan 2025"

General Information

Field	**Detail**
Change Owner	Network Infrastructure Manager
Initiator of RFC	IT Security Analyst
Summary Description	Upgrade campus Wi-Fi authentication from the local student ID/password system to a centralized Single Sign-On (SSO) solution integrated with Microsoft Azure AD.
Reason for Change	Current system is unstable under high load (e.g., midterms/finals) and has inconsistent password synchronization, leading to repeated login failures.

Business Justification and Impact

Field	**Detail**
Business Case	1. Reduce login failures and improve user experience during peak periods. 2. Enhance security via centralized password management (Azure AD). 3. Prepare the environment for

	integration with future university applications (specifically, the upcoming Online Course Registration Portal - OCRP).
Benefits	Improved login reliability and availability; stronger, centralized password management; easier integration with future systems.
Consequences if Not Implemented	Continued and frequent login failures for students; delayed or blocked rollout of the new Online Course Registration Portal (OCRP) and other SSO-dependent initiatives.
Business Areas Affected	Students, Faculty, Library, IT Services (Helpdesk/Networking)
Services Affected	Campus Wi-Fi Service; Authentication Service
References	Problem Record #NET-452 (Repeated login failures during peak times)

Technical & Implementation Details

Field	**Detail**
Configuration Items (CIs) Affected	Authentication Gateway (CI-2025-AUTH-01); Application Server (CI-2025-APP-01)

Technology Aspects	Introduction of Single Sign-On (SSO) and Microsoft Azure AD federation for wireless authentication.
Time Schedule	Pilot Test: November 10 (Engineering Faculty only). Full Rollout: November 15–16 (scheduled after working hours).
Restrictions	Maintenance window for all changes is restricted to 22:00–05:00 (local time).
Resources Required	2 Network Engineers, 1 Security Admin, 1 Helpdesk Representative.
Costs	Software license for the integration module; estimated 30 hours of network configuration labor.
Budget	Within approved FY 2025 IT security budget.
Supporting Documentation	Network change plan, test results from the lab environment, user communication draft.

Risk and Contingency Planning

Field	**Detail**

Risks During Implementation	1. Temporary total or partial Wi-Fi outage. 2. Certificate and trust errors preventing authentication. 3. Synchronization delays with Azure AD causing login issues.
Counter-Measures	1. Implement a staged rollout by building. 2. Test thoroughly with a smaller, contained group (Engineering Faculty) first. 3. Have a Network Engineer and Security Admin on-site/on-call during the deployment window.
Back-Out Strategy	Revert configuration on the Authentication Gateway and Application Server back to the legacy local password authentication system configuration files.

CAB Decision

Approval / Reject / Defer: Approve

Justification: The RFC addresses a critical, recorded problem (NET-452), significantly improves security and reliability, and is a mandatory prerequisite for the major Online Course Registration Portal (OCRP) initiative, with a clear, low-risk staged rollout and back-out plan.

Part 2

1. Tujuan Rilis

Tujuan dari rilis ini adalah untuk menerapkan aplikasi web Online Course Registration Portal (OCRP) yang terintegrasi dengan Azure AD Single Sign-On (SSO), sebagai pengganti proses manual registrasi mata kuliah. Implementasi ini bertujuan untuk:

- Meningkatkan efisiensi proses pendaftaran mata kuliah.
- Mengurangi kesalahan input dan antrian manual.
- Memberikan pengalaman pengguna yang lebih baik bagi mahasiswa dan staf akademik.

2. Lingkup Rilis

Rilis mencakup:

- Aplikasi OCRP (web-based) dengan fitur add/drop mata kuliah, sinkronisasi jadwal real-time, dan tampilan ketersediaan kursi.
- Integrasi autentikasi menggunakan Azure AD SSO (reused dari RFC-2025-WIFI-01).
- Update konfigurasi pada Application Server, Database Server, dan Authentication Gateway.

Lingkup tidak mencakup pengembangan sistem akademik baru di luar fungsi registrasi.

3. Jadwal Implementasi

Fase	Periode	Kegiatan Utama
Development	Sept – Oct 2025	Pengembangan modul dan integrasi SSO
Testing	1–7 Nov 2025	UAT (User Acceptance Testing), perbaikan bug minor
Rollout (Pilot)	10–12 Nov 2025	Uji coba terbatas ke 1 fakultas
Full Deployment	13 Nov 2025	Rilis penuh ke seluruh fakultas dan mahasiswa

4. Sumber Daya dan Tim Pelaksana

Peran	Nama/Jabatan
Release Manager	IT Applications Lead
Change Owner	Head of Registrar’s Office
Database Support	Database Administrator
Infrastructure Support	Network Engineer
Quality Assurance	QA Tester
Communication & Training	IT Helpdesk Coordinator

5. Risiko dan Mitigasi

Risiko	Dampak	Mitigasi
Integrasi SSO gagal	Pengguna tidak dapat login	Validasi koneksi ke Azure AD sebelum rollout
Database error saat sinkronisasi jadwal	Data kursus tidak tersimpan	Backup database penuh sebelum implementasi

Pengguna belum familiar dengan sistem baru	Penurunan efisiensi awal	Distribusi User Guide dan pelatihan online

6. Rencana Rollback

Jika implementasi gagal atau gangguan besar terjadi:

1. Rollback akan dilakukan dengan mengembalikan koneksi ke sistem registrasi manual (legacy system).
2. Restore database dari backup sebelum tanggal rollout.
3. Tim QA dan DBA akan memverifikasi data integritas sebelum sistem dinonaktifkan.
4. Komunikasi akan dikirimkan melalui email universitas dan portal ITS.

7. Rencana Komunikasi

- Sebelum rilis: Pengumuman melalui email dan portal mahasiswa (H-7).
- Selama rollout: Notifikasi status sistem melalui dashboard ITS Status Page.
- Setelah rilis: Laporan hasil rilis dan feedback survey ke mahasiswa & staf.

Dokumen pendukung:

- Test Plan
- User Training Guide
- Communication Plan

8. Uji dan Validasi

- Status Pengembangan: 90% selesai.

- Tahapan Saat Ini: User Acceptance Testing (UAT) sedang berlangsung.
- Kriteria Keberhasilan:
    - Autentikasi SSO berfungsi normal untuk semua akun mahasiswa.
    - Sinkronisasi data kursus dengan sistem akademik berjalan tanpa error.
    - Minimal 95% peserta UAT menyatakan sistem berjalan baik.

9. Persetujuan (Sign-Off Sequence)

1. QA Tester – Konfirmasi hasil UAT
2. IT Applications Lead – Persetujuan teknis implementasi
3. Head of Registrar's Office – Persetujuan bisnis
4. Change Manager – Persetujuan final untuk rilis ke produksi

10. Catatan Tambahan

- Rilis ini bergantung penuh pada keberhasilan RFC-2025-WIFI-01 (Wi-Fi Authentication Upgrade) untuk fungsi SSO.

Part 3

✅ Part 3 : Configuration Management

CI Record: Authentication Gateway (SSO)

Field	**Detail**
Identifier (CI ID)	CI-2025-AUTH-01
Name	Authentication Gateway
Description	Central authentication service providing SSO for Wi-Fi, Student Portal, and OCRP.
CI Owner	IT Security Engineer

CI Type	Network Service
Manufacturer / Vendor	Microsoft Azure AD
Serial / License Reference	Azure AD Tenant #UNIV-2025-SSO
Version Information	v2.0 (SSO Enabled)
Location	Logical: auth.university.ac.id; Physical: Cloud tenant (Azure Southeast Asia)
Modification History	2025-11-16 – Upgraded from v1.4 to v2.0 under RFC-2025-WIFI-01
Status History	Deployed, Under Maintenance, Active (Post-Release)
Present Status	Active
Relationships to Other CIs	Supports OCRP (CI-2025-REG-01); Supports Student Portal (CI-2024-WEB-01)
Licensing Info	Azure AD enterprise license FY-2025
Document References	Network Change Plan v2.0; SSO Integration Manual; CAB Approval Minutes
Emergency Docs	Rollback Procedure #DR-AUTH-01

CI Record: Application Server

Field	**Detail**
Identifier (CI ID)	CI-2025-APP-01
Name	Application Server
Description	Virtual machine hosting Student Portal backend and OCRP modules.
CI Owner	Infrastructure Manager
CI Type	Virtual Server (Hardware/Platform)
Manufacturer / Vendor	AWS EC2 (Ubuntu 22.04)
Serial / License Instance ID	i-043a8f00abcd
Version Info	Server Image v3.5
Location	Logical: app-srv01.university.ac.id; Physical: AWS Region ap-southeast-1
Modification History	2025-11-10 – Configuration optimized for OCRP deployment (REL-2025-01)
Status History	Active since 2023; Patch applied 2025-11
Present Status	Active
Relationships	Hosts OCRP (CI-2025-REG-01); Uses Authentication Gateway (CI-2025-AUTH-01)
Documentation	Server Configuration Manual; OCRP Deployment Log
Change / Release	RFC-2025-WIFI-01; REL-2025-01

References	

CI Record: Online Course Registration Portal (OCRP)

Field	**Detail**
Identifier (CI ID)	CI-2025-REG-01
Name	Online Course Registration Portal (OCRP)
Description	Web application allowing students to add/drop courses and sync with academic database.
CI Owner	Applications Development Lead
CI Type	Software Application / Service
Manufacturer / Developer	ITS Applications Team
Version Info	v1.0 (Initial Release)
Location	Logical: ocrp.university.ac.id; Deployed on Application Server (CI-2025-APP-01)
Modification History	2025-11-12 – First deployment under REL-2025-01
Status History	Tested, Piloted, Active
Present Status	Active
Relationships	Runs on Application Server (CI-2025-APP-01); Uses Authentication Gateway (CI-2025-AUTH-01)
License / Contract	Internal university software; No external license
Documentation	User Guide v1.0; Training Materials; Release Plan REL-2025-01
Change / Release References	Depends on RFC-2025-WIFI-01; Implemented via REL-2025-01