TechArch Solutions
235 Sycamore Street
Santa Clara, CA 95054
+1 408.555.3840

info@techarch.domain
techarch.domain
Company Representative
Eddie J. Stevens

System Design Specification

Design Specifications
for Night Veil University Student Portal

Prepared for:

Deborah Marples

Night Veil University
1412 Horseshoe Lane
Philadelphia, PA 19108
+1 484.555.0368
d.marples@nvu.edu

Version:
Version 3

Date Published:
06.10.2021

Table of Contents

1. Document Version Control

Document Version Information	
Title:	NVU Portal System Design Specification (SDS)
System Name:	NVU Portal
Version:	1.0
Date:	June 2021
Author:	Eddie J. Stevens
Status:	Published

2. Executive Summary

The NVU Portal is a web-based academic management platform designed to streamline administrative and academic operations for the fictional Northern Valley University (NVU). It provides unified access for students, faculty, and administrators to manage courses, view announcements, and oversee research projects — including sensitive, classified initiatives.

This System Design Specification (SDS) describes the architectural design, database schema, relationships, and security considerations of the NVU Portal. It aims to guide developers, database administrators, and security teams through the system's foundational data model and design rationale. Point of Contact

1.1. Points of Contact

Specific points of contact may be reached throughout the development of the system. Information for these contacts is provided in the table below.

Points of Contact

Name:	Melvin K. Sailsbury
Position:	Software Development Manager
Phone Number:	(715) 555-4703
E-mail:	msalisbury@techarch.domain

3. Purpose

The purpose of this document is to define the data model and design principles for the NVU Portal's database subsystem. It provides a clear and detailed technical reference that ensures:

- Consistent understanding of data entities, relationships, and constraints.
- Alignment between application logic and database design.
- Security and scalability for both academic and research use cases.
- Future extensibility for role-based access, reporting, and analytics.

This document is intended for system architects, developers, cybersecurity personnel, and stakeholders responsible for implementing or maintaining the NVU Portal.

4. Scope

The SDS focuses on the database and logical data layer of the NVU Portal. Specifically, it covers:

- Database structure, entity relationships, and data integrity rules.
- Security and privacy controls for user and research data.
- Design considerations for scalability and role-based access.
- Recommendations for future database enhancements.

4.1. Out of scope:

Frontend UI design, API implementation, and network deployment architecture are not covered in this version.

5. System Overview

The NVU Portal integrates multiple academic and administrative functions into one cohesive system. It enables:

- Students to view courses and announcements.
- Professors to post announcements, manage course listings, and lead research projects.
- Administrators to oversee portal activity, user management, and data access.

5.1. Core Components:

User Management Module – Authentication and authorization.

- Course Management Module – Course creation, updates, and catalog listings.
- Announcement System – Internal bulletin and notification framework.
- Research Management Module – Repository for academic and classified research data.

6. Design Considerations

6.1. Architectural Principles

- Modular Design: Each table represents a self-contained domain (users, courses, announcements, research).
- Scalability: Prepared for expansion with additional tables (enrollments, assignments, grades).
- Normalization: Minimizes redundancy; future versions may introduce foreign keys for referential integrity.
- Security First: Sensitive tables (e.g., research projects) include access control and encryption considerations.
- Extensibility: Designed to integrate easily with APIs or ORM frameworks (Flask, Django, or Express.js).

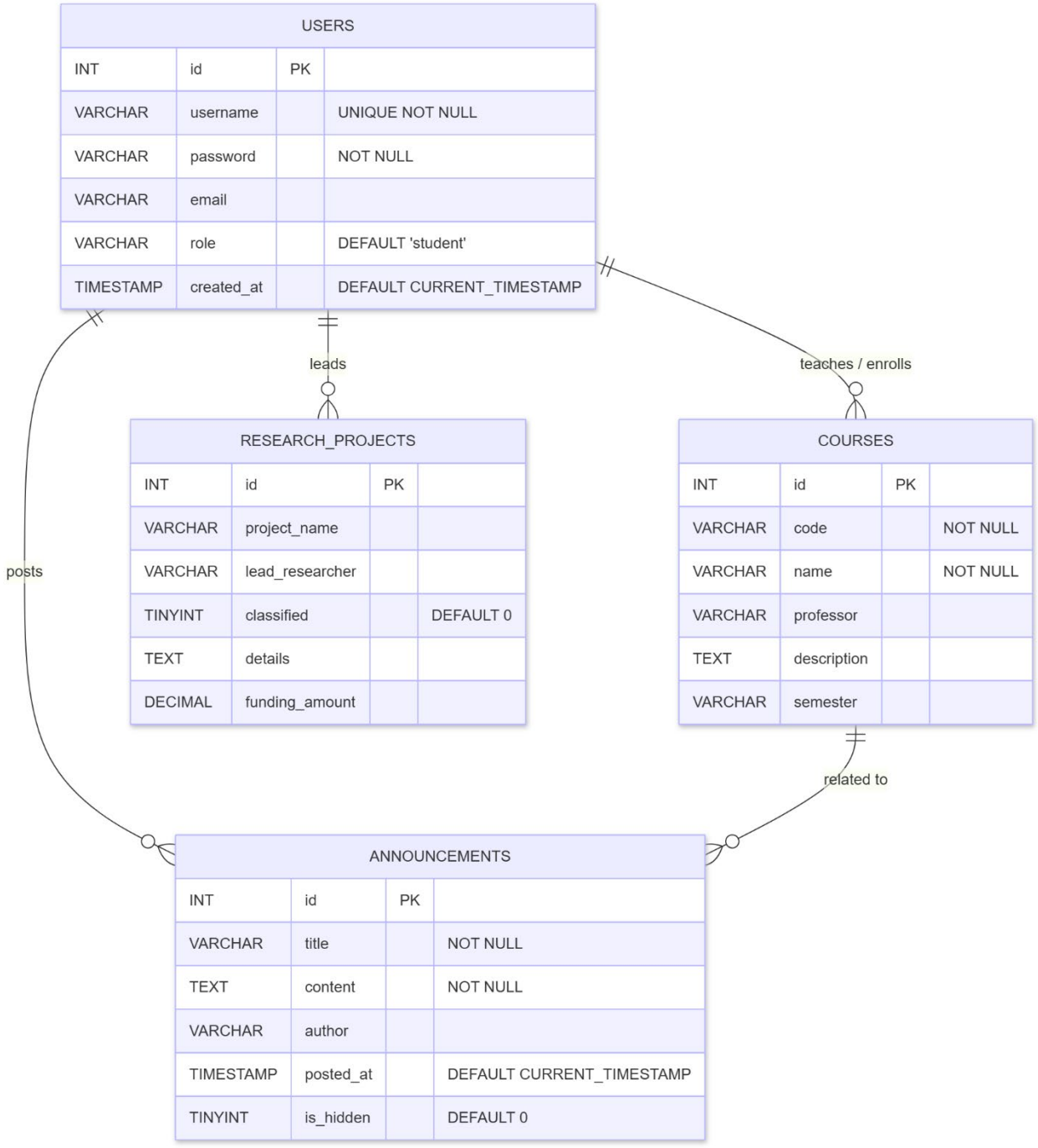
6.2. Constraints

- Passwords must be stored using modern cryptographic hashing (bcrypt, Argon2).
- Classified data must be restricted to authorized roles only.
- All tables must maintain audit logs for security compliance.

7. Data Model Design

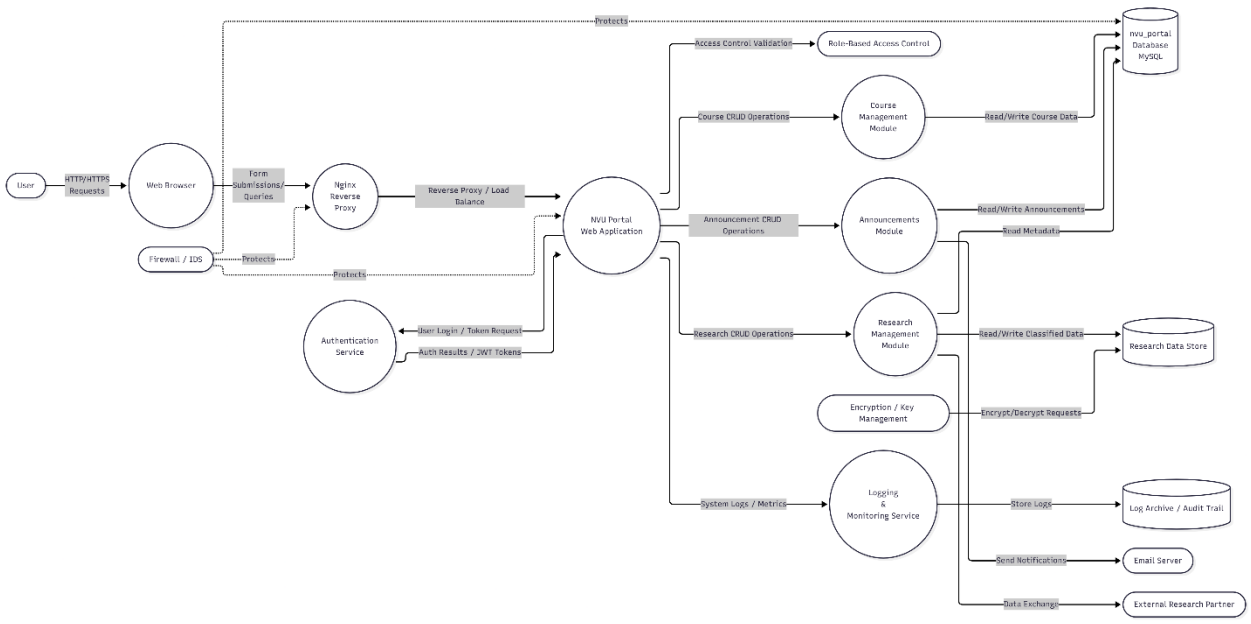
7.1. Entity Relationship Diagram

Figure 1: Database ER Diagram



8. Data Flow Diagram (DFD3) Model

Figure 2: Data Flow Diagram



External Entities

- Users (Students, Faculty, Admins): Access the portal via browser or mobile interface.
- Email Server / Notification Service: Used for announcements and alerts (SMTP or third-party API).
- External Research Partner: Optional integration for sharing non-classified research data.

Web Layer

- Web Browser / Client UI: Frontend interface for all roles.
- Nginx Reverse Proxy / Load Balancer: Routes HTTPS traffic to the appropriate backend application instance, handling SSL termination and rate limiting.

Application Layer

- NVU Portal Web Application: Central application server (Flask, Django, or Node.js) implementing business logic.
- Authentication Service: Handles user login, session management, JWT issuance, and password hashing.
- Course Management Module: Manages CRUD (Create, Read, Update, Delete) operations for courses.
- Announcements Module: Handles message posting, editing, and visibility settings.
- Research Management Module: Manages classified/unclassified research data, applying encryption policies.

- Logging & Monitoring Service: Centralized collection of audit logs, metrics, and application performance data.

Data Stores

- nvu_portal Database:
- Stores all normalized data tables:
    - users
    - courses
    - announcements
    - research_projects
- Encrypted Research Data Store:
    - Dedicated repository for encrypted research content using AES-256 and controlled access.
- Log Archive:
    - Stores audit and event logs for system monitoring, intrusion detection, and compliance.

Security Components

RBAC (Role-Based Access Control):

- Controls user access levels (student, professor, admin).

Encryption & Key Management:

- Protects classified data in the research_projects table and research data store.

Firewall / Intrusion Detection System:

- Monitors network traffic, filters malicious packets, and prevents unauthorized access to the application and database layers.

Data Flow Summary

FLOW	DIRECTION	DESCRIPTION
1	User → Web UI	HTTP(S) requests for login, announcements, courses
2	Web UI → App Server	Application logic requests routed via reverse proxy
3	App Server ↔ Auth Service	Authentication requests and session validation

Flow	Direction	Description
4	App Server ↔ DB	CRUD operations for user, course, and announcement data
5	App Server ↔ Encrypted Store	Secure access to classified research data
6	App Server ↔ Notification Service	Sends announcements via email
7	App Server ↔ Log Archive	Writes audit and activity logs
8	External Research Partner ↔ Research Module	Authorized data exchange (non-classified only)

Security Boundaries

All internal components (Application Server, Authentication Service, Database) reside within the trusted network segment protected by:

- Layer 7 firewall (WAF)
- Intrusion Detection System (IDS)
- Encrypted data transport (TLS 1.3)

External access is limited to the web front-end (port 443), with strict network ACLs protecting database and storage layers.

9. Sequence Diagram

9.1. User Authentication

- The user logs into the NVU Portal through the web UI over HTTPS.
- The credentials are securely transmitted through the Nginx reverse proxy to the application server.
- The Auth Service verifies credentials by querying the users table in the nvu_portal database.
- A JWT (JSON Web Token) or secure session cookie is issued, containing the user's role and permissions.

9.2. Authorization and Role Validation

- Before fulfilling any request, the application layer consults the Auth Service to validate the token and role permissions.
- Access control rules (RBAC) ensure:
    - Students can only read course and announcement data.
    - Professors can post announcements and access their own research projects.
    - Admins can manage users, courses, and all research data.

9.3. Data Retrieval

- The Web App queries the nvu_portal database for user-related records:
    - courses (based on user enrollment or teaching role)
    - announcements (where is_hidden = 0)
- If the user has clearance (e.g., a lead researcher), the Research Module requests decrypted data from the Encrypted Store, leveraging AES-256 decryption via the Key Management Service.

9.4. Logging and Notifications

- Each operation (login, data fetch, or error) is logged into the Audit / Log Archive with a timestamp, user ID, and IP address.
- The system may trigger an email notification or internal event for session tracking, successful login alerts, or announcements.

Figure 3: Sequence Diagram