# Module Nine

# Final Project

# Law, Ethics, and Security Plan and Database Management System

# Grandfield College

Andrew Robinson

IT 650: Principles of Database Design

Southern New Hampshire University

September 28, 2024

Daniel Foster

## Introduction

In selecting the ideal Database Management System (DBMS) for the Grandfield College project, our primary objective is to provide a solution that not only addresses the college's current operational demands but also has the flexibility to scale as the institution expands. The selected DBMS must support an efficient software tracking system, ensure data integrity, facilitate secure data management, and offer reliable retrieval and reporting capabilities that will improve decision-making processes across the institution. To achieve this, our project will compare and analyze several leading DBMS options, evaluating their strengths, weaknesses, and overall suitability for Grandfield College’s evolving needs.

A key aspect of this project is the creation of a comprehensive data model. Data modeling is an essential process that allows us to conceptualize the relationships between various types of information within the organization, independent of its structure, processes, or personnel. By defining these relationships, we can ensure that the system supports efficient storage, management, and interaction with data, offering streamlined access to critical information. This will not only help Grandfield College improve its operational efficiency but also facilitate long-term scalability and adaptability to future challenges.

In addition to identifying the most suitable DBMS and developing a data model, the project will explore important legal, ethical, and security considerations. As Grandfield College handles sensitive student, faculty, and institutional data, it is crucial to ensure compliance with relevant legal standards, such as FERPA (Family Educational Rights and Privacy Act), as well as ethical best practices in data use and storage.

Our solution design will emphasize the protection of privacy, data integrity, and system security while considering the unique needs of different departments within the college.

For this project, we will focus on a particular department, constructing an enterprise data model tailored to its specific workflow and data relationships. This model will be compared with the broader security needs of the entire organization to provide a comprehensive, high-level security management plan. The plan will ensure that data is securely managed at both the departmental and organizational levels, aligning with Grandfield College's operational goals and safeguarding its critical information assets.

This introduction sets the stage for a detailed exploration of the DBMS selection process, data modeling, and security planning, as well as the implementation of best practices that will help Grandfield College maintain operational efficiency, legal compliance, and ethical standards.

## Organization Analysis

**Problem/Challenge**

Grandfield College currently relies on multiple spreadsheets to manage and track software across the institution. This approach is inefficient, prone to errors, and lacks the necessary functionality to meet the school's growing needs. The primary problems with the current system include:

**Inefficiency and Time-Consuming Processes**

The use of spreadsheets for tracking software installations, licenses, and requests is cumbersome and time-consuming.

**Inaccuracy and Error-Prone Data Management**

Manual data entry increases the risk of errors. Inaccurate records can lead to over-licensing or under-licensing, both of which have financial and legal repercussions.

**Lack of Centralized Data**

With data spread across multiple spreadsheets, there is no centralized repository for software information. This makes it difficult to get a comprehensive view of the software landscape, manage licenses effectively, and generate reports.

**Limited Tracking Capabilities**

The current system lacks the ability to track detailed information about software installations, such as specific machine assignments, user access, and software removal dates.

**Inadequate Request Management**

The process for handling software requests is not integrated with the tracking system. This leads to delays in fulfilling requests and difficulty in assessing software needs and availability.

## Business Requirements

To address these challenges, the software tracking system must meet the following business requirements:

**Centralized Database**

Implement a centralized database to store all software-related information, including licenses, versions, installations, and user assignments.

**Accurate and Automated Data Entry**

Automate data entry processes to reduce errors and ensure accurate, up-to-date records.

**Comprehensive Tracking and Reporting**

Provide robust tracking capabilities for software installations, license compliance, and machine assignments. Generate detailed reports for management and compliance purposes.

**Integrated Request Management**

Integrate the software request process with the tracking system to streamline approvals, fulfillments, and assessments of software needs.

**User-Friendly Interface**

Design an intuitive and user-friendly interface for staff to easily input, update, and retrieve software information.

**Security and Access Control**

Implement security measures to protect sensitive data and ensure only authorized personnel can access and modify the database.

## Limitations of Current Systems

The existing spreadsheet-based system has several limitations:

**Manual Data Entry**

Manual entry is time-consuming and prone to human error.

**Fragmented Data**

Data is fragmented across multiple spreadsheets, making it difficult to obtain a unified view of the software inventory.

**Limited Functionality**

Spreadsheets lack advanced functionalities such as automated tracking, integrated request management, and detailed reporting.

**Scalability Issues**

The current system cannot scale to accommodate the growing number of software licenses, installations, and requests.

**Inadequate Security**

Spreadsheets do not provide robust security features, posing risks to data integrity and confidentiality.

## Impact on Departments and Operations

**Information Technology (IT) Department**

The IT department bears the brunt of inefficiencies in software management. Staff spend excessive time on manual data entry, troubleshooting errors, and managing software requests. This diverts resources from more strategic IT initiatives and projects.

**Administrative and Finance Departments**

Accurate software tracking is crucial for financial planning and budgeting. Inaccurate records can lead to financial mismanagement, such as overspending on unnecessary licenses or facing penalties for under-licensing.

**Faculty and Staff**

Faculty and staff experience delays in software requests and installations due to the cumbersome request process. This impacts their ability to effectively use technology for teaching, research, and administrative tasks.

**Compliance and Legal**

The college risks non-compliance with software licensing agreements, which can result in legal and financial penalties. Accurate tracking is essential to ensure compliance and avoid costly audits.

**Overall Operations**

Inefficiencies in software management affect the overall operational efficiency of the college. Delays, errors, and lack of centralized information hinder effective decision-making and resource allocation.

## Conceptual Model

Preliminary Entities and Attributes

**Software**

SoftwareID (PK)

SoftwareTypeID (FK)

**SoftwareType**

SoftwareTypeID (PK)

**License**

LicenseID (PK)

SoftwareID (FK)

**Installation**

InstallationID (PK)

SoftwareID (FK)

UserID (FK)

**Request**

RequestID (PK)

UserID (FK)

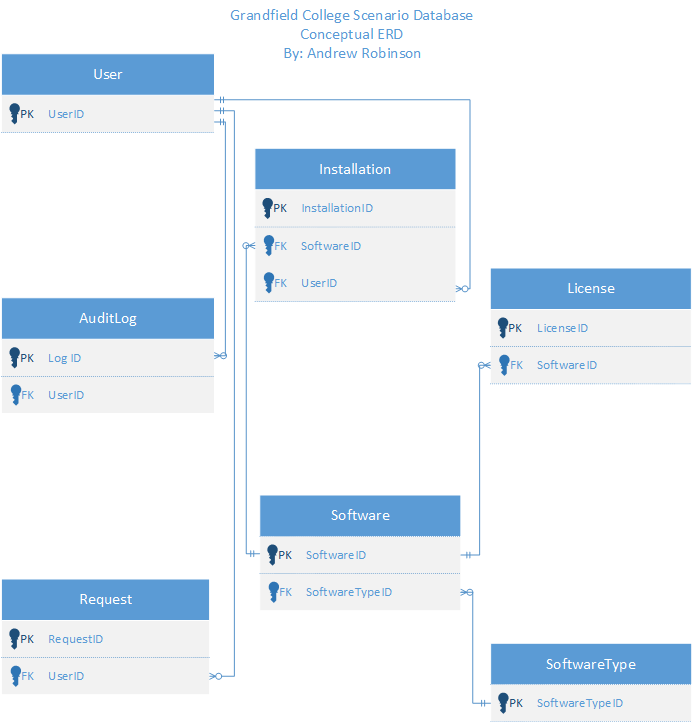
**User**

UserID (PK)

**AuditLog**

LogID (PK)

UserID (FK)



## Logical Model

Preliminary Entities and Attributes

**Software**

SoftwareID (PK)

SoftwareTypeID (FK)

Name

Version

Company

**SoftwareType**

SoftwareTypeID (PK)

Type

**License**

LicenseID (PK)

SoftwareID (FK)

LicenseType

StartDate

EndDate

Terms

Pricing

PricingUnit

**Installation**

InstallationID (PK)

SoftwareID (FK)

UserID (FK)

Location

InstallDate

RemovalDate

**Request**

RequestID (PK)

UserID (FK)

Software

RequestDate

Software

Reason

Response

ResponseDate

Status

**User**

UserID (PK)

Name

Location

Role

**AuditLog**

LogID (PK)

UserID (FK)

Action

Timestamp

Details

## 

## 

## 

## 

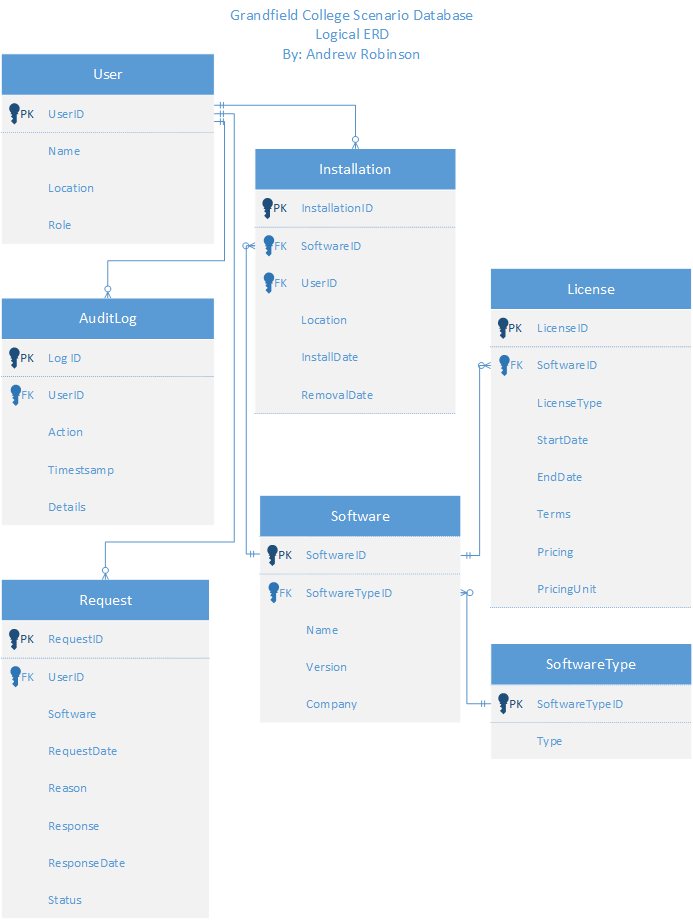
## 

## 

## 

## 

## 



## Physical Model

Preliminary Entities and Attributes

**Software**

SoftwareID (PK) | nvarchar(50)

SoftwareTypeID (FK) | varchar(50)

Name | varchar(50)

Version | varchar(50)

Company | varchar(50)

**SoftwareType**

SoftwareTypeID (PK) | nvarchar(50)

Type | varchar(50)

**License**

LicenseID (PK) | nvarchar(50)

SoftwareID (FK) | nvarchar(50)

LicenseType | nvarchar(50)

StartDate | date

EndDate | date

Terms | varchar(MAX)

Pricing | float

PricingUnit | nvarchar(50)

**Installation**

InstallationID (PK) | nvarchar(50)

SoftwareID (FK) | nvarchar(50)

UserID (FK) | nvarchar(50)

Location | varchar(50)

InstallDate | date

RemovalDate | date

**Request**

RequestID (PK) | nvarchar(50)

UserID (FK) | nvarchar(50)

Software | varchar(50)

RequestDate | date

Reason | varchar(50)

Response | varchar(50)

ResponseDate | date

Status | varchar(50)

**User**

UserID (PK) | nvarchar(50)

Name | varchar(50)

Location | varchar(50)

Role | varchar(50)

**AuditLog**

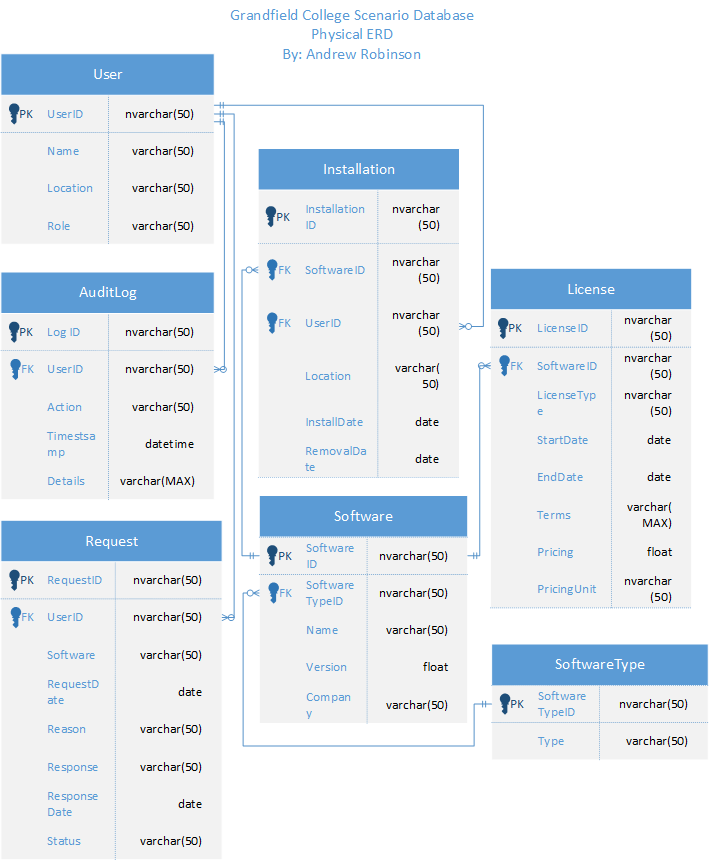
LogID (PK) | nvarchar(50)

UserID (FK) | nvarchar(50)

Action | varchar(50)

Timestamp | datetime

Details | varchar(MAX)



## Top DBMS Contenders

The following DBMS products are considered top contenders for this scenario:

1. Microsoft SQL Server

2. MySQL

3. PostgreSQL

4. Oracle Database

#### Microsoft SQL Server

Microsoft SQL Server is a powerful, enterprise-grade DBMS known for its comprehensive feature set, including robust security, scalability, and integration with other Microsoft products.

##### Strengths

**Ease of Integration**

SQL Server integrates seamlessly with Microsoft technologies such as Azure, .NET, and Power BI, making it an excellent choice for organizations heavily invested in the Microsoft ecosystem.

**Security**

Advanced security features, including encryption and auditing, make SQL Server a strong candidate for environments requiring high levels of data protection.

**Scalability**

SQL Server supports large-scale databases, making it suitable for both small and large organizations.

**Performance Tuning**

Features like indexing, in-memory processing, and query optimization help ensure high performance even with large datasets.

##### Weaknesses

**Cost**

SQL Server's licensing can be expensive, particularly for larger implementations, which may be a concern for budget-conscious organizations.

**Windows-Centric**

Although SQL Server can run on Linux, its full feature set is optimized for Windows environments.

#### MySQL

MySQL is an open-source DBMS known for its speed, reliability, and ease of use. It is widely used for web applications and is a common choice for small to medium-sized businesses.

##### Strengths

**Cost-Effective**

Being open-source, MySQL is free to use, which makes it an attractive option for organizations with limited budgets.

**Flexibility**

MySQL supports a variety of storage engines, allowing for flexibility in how data is stored and managed.

**Community Support**

A large community of developers and extensive documentation make MySQL easy to learn and troubleshoot.

##### Weaknesses

**Feature Set**

MySQL lacks some advanced features found in enterprise-grade DBMS products, such as full-text indexing and advanced security options.

**Scalability**

While MySQL can scale, it may not perform as well as other DBMS products in extremely large, complex environments.

#### PostgreSQL

PostgreSQL is an open-source, object-relational DBMS known for its standards compliance, extensibility, and advanced features.

##### Strengths

**Extensibility**

PostgreSQL allows users to define custom data types, operators, and functions, providing a high level of flexibility.

**Advanced Features**

PostgreSQL supports complex queries, full-text search, and advanced indexing techniques, making it suitable for complex data environments.

**ACID Compliance**

PostgreSQL ensures data integrity through strong adherence to ACID (Atomicity, Consistency, Isolation, Durability) principles.

##### Weaknesses

**Performance**

PostgreSQL's advanced features can sometimes lead to slower performance compared to other DBMS products, particularly in read-heavy applications.

**Complexity**

The richness of features can make PostgreSQL more challenging to configure and manage, particularly for less experienced users.

#### Oracle Database

Oracle Database is a highly robust, enterprise-grade DBMS known for its high performance, scalability, and comprehensive feature set.

##### Strengths

**High Performance**

Oracle offers exceptional performance for both OLTP (Online Transaction Processing) and OLAP (Online Analytical Processing) workloads.

**Scalability**

Oracle is designed to handle very large databases and can scale horizontally and vertically with ease.

**Comprehensive Feature Set**

Oracle provides a wide range of features, including advanced security, analytics, and data warehousing capabilities.

##### Weaknesses

**Cost**

Oracle is one of the most expensive DBMS products on the market, with significant licensing and maintenance costs.

**Complexity**

The richness of features and configuration options can make Oracle challenging to implement and manage.

## Recommendation for Grandfield College

For Grandfield College, Microsoft SQL Server is recommended as the best DBMS product. This recommendation is based on several factors:

#### Integration

Given the likelihood of existing Microsoft technologies in use at Grandfield College, SQL Server's seamless integration with Microsoft tools would be beneficial.

#### Scalability and Security

SQL Server's scalability and robust security features align well with the college's need to manage sensitive student and faculty data effectively.

#### Ease of Use

SQL Server's user-friendly management tools and strong support infrastructure make it accessible for database administrators at various skill levels.

## Software and Hardware Recommendations

#### Software

* Microsoft SQL Server Standard Edition
* Windows Server 2022 (for hosting SQL Server)
* Power BI (for reporting and data visualization)

#### Hardware

* Server: A dedicated server with at least 32 GB of RAM, a multi-core processor (e.g., Intel Xeon), and SSD storage for optimal performance.
* Backup Solutions: Implement a robust backup solution using Microsoft Azure Backup or similar cloud-based services to ensure data integrity and disaster recovery.
* Networking: Ensure high-speed network infrastructure to support real-time data access.

## Enterprise Data Model

We'll design the enterprise data model that shows their relationships within the IT Department.

**Software: Contains information about all the software managed by the IT Department.**

SoftwareID >SoftwareName

SoftwareID >Version

Version>LicenseID

**Installation: Records installations performed by the IT department.**

InstallationID>SoftwareID

InstallationID>MachineID

InstallationID>InstallDate

InstallDate>InstalledBy

**Request: Tracks software requests made by faculty or other departments.**

RequestID>UserID

RequestID>RequestDate

RequestDate>Status

**AuditLog: Tracks activities performed by the IT Admin, ensuring traceability.**

AuditID>ActionType

ActionType>ActionDate

ActionDate>Details

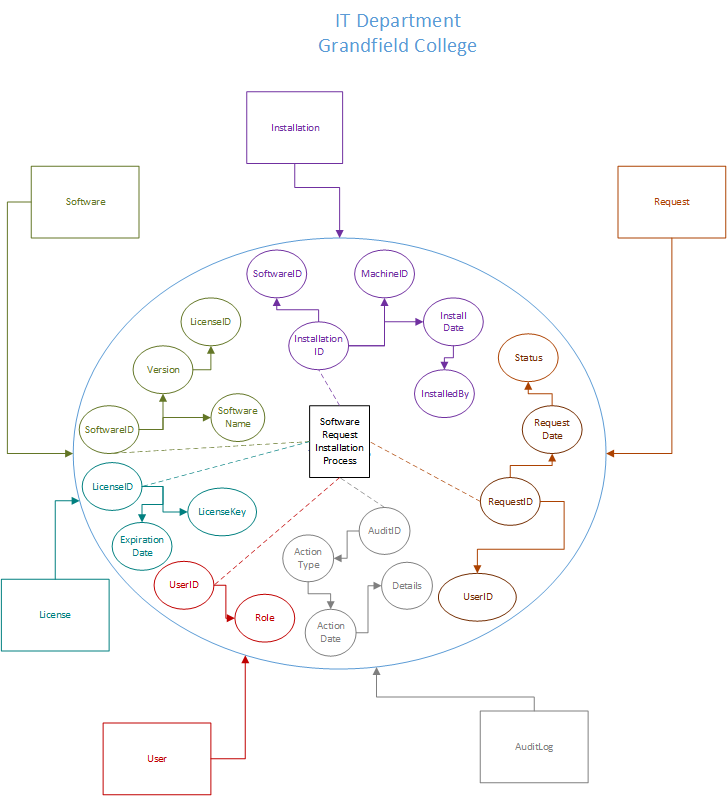
**User: Stores details about individuals, whether IT staff, faculty, or other users.**

UserID>Role

**License: Manages software licenses, their expiration dates, and restrictions.**

LicenseID>LicenseKey

LicenseID>ExpirationDate



## Operating Rules

The IT Department has the following operating rules:

#### Request and Approval Workflow

Faculty and other departments can submit requests for new software. Only IT Admins have the authority to approve and process these requests.

#### Installation Authorization

Software can only be installed after it is approved, and only by authorized IT staff. The installation is then recorded in the Installation table.

#### License Management

Every software entry must be tied to a valid license, which is stored and managed in the License table. Any expired licenses are flagged for renewal.

#### Auditing and Traceability

All actions by IT Admins (e.g., approving requests, installing software) are logged in the AuditLog table to ensure full traceability during audits.

#### Data Integrity

Requests, installations, and licenses are cross-referenced to maintain data integrity, ensuring that faculty do not receive unlicensed or outdated software.

## Rule Reflection

The data model directly reflects these operating rules:

#### Request and Approval Workflow

The relationship between the Request and Software tables ensures that no software is installed without being properly requested and tracked. The Status field in the Request table reflects the approval process.

#### Installation Authorization

The Installation table maintains a detailed record of who installed which software and when, ensuring only authorized personnel can complete installations.

#### License Management

The relationship between the Software and License tables ensures that each software package is tied to a valid, active license, preventing any licensing issues.

#### Auditing and Traceability

The AuditLog table captures every action performed by the IT team, allowing for full transparency in software management activities.

## Legal and Ethical Standards in Solution Design and Future Implementation

In designing and implementing database management solutions for Grandfield College, legal and ethical standards must be considered to ensure compliance and responsible data management.

#### Legal Standards

##### FERPA (Family Educational Rights and Privacy Act)

As an educational institution, Grandfield College must comply with FERPA, which protects the privacy of student education records. The DBMS must be designed to ensure that only authorized personnel can access sensitive student information and that such data is stored securely.

##### GDPR (General Data Protection Regulation)

If Grandfield College deals with students or faculty from the European Union, compliance with GDPR is mandatory. This regulation emphasizes the rights of individuals over their data and requires transparent data collection, storage, and usage policies. The solution should provide mechanisms for data portability, the right to erasure, and proper consent management.

##### HIPAA (Health Insurance Portability and Accountability Act)

If the institution handles sensitive health data (e.g., student health records), the DBMS must comply with HIPAA regulations to protect the privacy and security of health information.

##### State and Local Regulations

Different states may have specific regulations regarding data privacy and protection. For example, the California Consumer Privacy Act (CCPA) gives California residents specific rights over their personal information, including the right to know what data is collected and the ability to opt out of data sales.

#### Ethical Standards

##### Data Minimization

The DBMS design should adhere to the principle of collecting and storing only the necessary data to meet operational requirements. Minimizing data collection reduces the risk of misuse or exposure of sensitive information.

##### Transparency

Ethical handling of data requires transparency with users about how their data will be used, stored, and shared. Policies should be communicated clearly, ensuring that students, staff, and faculty are aware of the institution’s data practices.

##### Data Ownership and Access Rights

Individuals should have control over their data, including access, correction, and deletion rights. The DBMS design must account for user requests to manage their own data in compliance with privacy laws.

##### Informed Consent

Ethical data practices should involve obtaining informed consent from users before collecting, processing, or sharing their personal information. Consent should be easily revocable if necessary.

## Best Practices in Design, Data Use, and Storage

#### Design Best Practices

##### Security by Design

The DBMS should be built with security in mind from the start. Incorporating encryption, multi-factor authentication, and access controls are key strategies to protect sensitive data.

##### Modular Architecture

A modular system that separates sensitive information (such as student records) from less critical data helps reduce risk by limiting access to the most sensitive data.

##### Role-Based Access Control (RBAC)

Implement RBAC to restrict access to data based on the roles of individual users. Faculty, administrative staff, and students should have different access privileges depending on their roles.

#### 

#### Data Use Best Practices

##### Data Anonymization

Where possible, anonymize data to protect individuals’ identities, especially for research purposes or data analysis. This minimizes the risk of exposing sensitive information.

##### Data Lifecycle Management

Establish clear policies for data retention and deletion. This ensures that data is not kept longer than necessary and reduces the likelihood of breaches.

#### Storage Best Practices

##### Data Encryption

Encrypt sensitive data both at rest and in transit. This ensures that even if data is intercepted or accessed by unauthorized parties, it remains protected.

##### Backup and Disaster Recovery

Implement a robust backup strategy that includes frequent backups and off-site storage. This ensures data is recoverable in case of a disaster or system failure.

##### Auditing and Logging

Regularly audit data access and usage to detect unauthorized activity. Maintaining logs of access to sensitive data is important for both legal compliance and ethical accountability.

## Security Needs for the DBMS Solution

#### General Security Needs for Grandfield College

##### Confidentiality

Protecting the confidentiality of student records, grades, and personal information is essential. Role-based access, data encryption, and proper data governance policies are critical.

##### Integrity

Ensuring the integrity of data is paramount. The DBMS should include measures such as transaction logging and data validation to prevent unauthorized data manipulation or corruption.

##### Availability

High availability of the DBMS is necessary for faculty, staff, and students. Implementing redundancy and load balancing will ensure that the system remains operational even during peak usage or in the event of hardware failures.

#### Security Needs at the Department Level

For specific departments, such as Admissions or IT, the security needs might vary:

##### Admissions Department

Requires heightened security for sensitive applicant data. Only authorized personnel should have access to such records, and additional monitoring to prevent unauthorized access.

##### IT Department

Needs broader access for system maintenance and troubleshooting but must still adhere to strict guidelines for handling sensitive data. Enhanced security controls, such as logging and regular audits, are crucial.

#### Comprehensive Security Management Plan

Based on the considerations above, the following security management plan is recommended:

##### Access Control

Implement role-based access control (RBAC) to limit access to sensitive data based on the user’s role within the organization. Use multi-factor authentication (MFA) for enhanced security, especially for access to administrative functions.

##### Data Encryption

Use strong encryption protocols (such as AES-256) for sensitive data at rest and in transit. This protects data from unauthorized access in the event of a breach.

##### Regular Security Audits

Perform regular security audits and penetration testing to identify vulnerabilities. Logs should be continuously monitored for any suspicious activity, with alerts for potential security breaches.

##### Incident Response Plan

Develop a comprehensive incident response plan to quickly address data breaches or security incidents. This plan should include roles, responsibilities, and communication protocols.

##### Data Retention and Deletion Policies

Implement strict data retention policies to ensure that data is not kept longer than necessary. Automated deletion or archiving processes should be put in place to reduce exposure.

##### Disaster Recovery and Backup

Establish a disaster recovery plan that includes regular backups and off-site storage. Ensure that backups are encrypted and regularly tested for integrity and recoverability.

## Conclusion

In conclusion, selecting the right Database Management System (DBMS) is a critical decision for the success of the Grandfield College project. After careful evaluation, Microsoft SQL Server stands out as the most suitable solution, offering a strong balance of performance, security, scalability, and seamless integration with the college's existing infrastructure. Its ability to handle the growing demands of the institution ensures that Grandfield College will be well-prepared to manage its data efficiently, meet its operational needs, and support future expansion.

The comprehensive data model we developed for the IT department provides a structured and efficient framework for managing software installations, addressing faculty requests, and maintaining compliance with software licensing agreements. Additionally, the model supports rigorous auditing processes, enhancing transparency and accountability in software management. This tailored solution not only streamlines day-to-day operations but also aligns with the college’s broader goals of data integrity, compliance, and long-term scalability.

By implementing the recommended DBMS and data model, Grandfield College is positioned to optimize its data management practices and support the continued growth of its academic and administrative functions. The combination of robust technology, careful planning, and attention to legal and ethical considerations ensures that the college can operate securely and efficiently in an increasingly data-driven environment.

## References

Hernandez, M. J., & Hernandez, M. J. (2020). Database Design for Mere Mortals (4th ed.). Pearson Technology Group. https://mbsdirect.vitalsource.com/books/9780136788171

Conger, S. (2014). Hands-On Database (2nd ed.). Pearson Education (US). https://mbsdirect.vitalsource.com/books/9780133927078

AltexSoft. (2023, May 16). *Database Management Systems (DBMS) comparison: Mysql, postgr*. https://www.altexsoft.com/blog/comparing-database-management-systems-mysql-postgresql-mssql-server-mongodb-elasticsearch-and-others/

*System properties comparison mysql vs. Oracle vs. PostgreSQL*. MySQL vs. Oracle vs. PostgreSQL Comparison. (n.d.). https://db-engines.com/en/system/MySQL%3BOracle%3BPostgreSQL

Admin. (2019, January 7). *Oracle vs. SQL server vs. MySQL vs. postgresql comparison*. JanbaskTraining. https://www.janbasktraining.com/blog/oracle-sql-server-mysql-and-postgresql/

GmbH, L. (n.d.). Enterprise data modeling - techniques and best practices. https://www.leanix.net/en/wiki/it-architecture/enterprise-data-model