**Security Document - CMPS‑480 Academic Support Hub**

**1. Purpose & Scope**

The purpose of this document is to define the security measures for the Academic Support Hub, a platform that enables students to find study groups, access approved materials, participate in peer Q&A, and use a built-in planner. The scope covers all application components, including the frontend, backend APIs, databases, and infrastructure supporting production and development environments.

**2. System Description**

* **Frontend:** Web application (e.g., React)
* **Backend API:** Node.js/Express (or similar framework)
* **Database:** PostgreSQL with encryption
* **Authentication:** OAuth 2.0 / OpenID Connect (Google/Microsoft) with optional local login
* **Infrastructure** (Render or university servers). (?)
* **Branches:**
  + main → stable production
  + dev → integration
  + feature branches → new development

**3. Data Classification**

**Level A - Restricted (Highest Sensitivity):**

* Personally identifiable information: name, email, student ID, authentication credentials
* Educational records (planner items, private notes, course data)

**Level B - Confidential:**

* Study group memberships, user activity, drafts, IP addresses

**Level C - Public:**

* Publicly posted Q&A content, shared study materials intended for public access

**4. Risk Assessment**

| **Threat** | **Impact** | **Mitigation** |
| --- | --- | --- |
| Unauthorized access | High | Auth/OIDC, role‑based access control (RBAC), multi‑factor authentication for admins |
| SQL injection | Medium | Parameterized queries, input validation, output encoding, CSRF tokens |
| Credential stuffing | Medium | Rate limiting, CAPTCHA, account lockouts |
| Data loss (ransomware, accidental deletion) | High | Encrypted backups, tested restore process, disaster recovery plan |
| Insider misuse | Medium | Least privilege access, audit logging, monitoring |

**5. Security Controls**

**5.1 Technical Controls**

* **Authentication:** (if local auth used)
* **Encryption:** database field encryption, encrypted backups
* **Web Security:** Content Security Policy (CSP), sanitized uploads, malware scanning for files
* **Access Control:** Role‑based access (student, moderator, instructor, admin), row‑level security in PostgreSQL
* **Rate Limiting & Logging:** API rate limiting on auth endpoints, centralized logging for anomaly detection

**5.2 Administrative Controls**

* **Code Reviews:** All merges require review; feature → dev → main workflow
* **Training:** Team members follow secure coding best practices
* **Incident Response Plan:** Steps for detection, reporting, and remediation of security incidents
* **Policies:** Clear rules for handling sensitive data and using production systems

**5.3 Physical & Infrastructure Controls**

* **Hosting Security:** Isolation of environments (dev, staging, prod)
* **Access Restrictions:** SSH key authentication, no password logins, secrets managed securely
* **Network Protections:** DDoS mitigation and IP filtering

**6. Monitoring & Incident Response**

* **Monitoring:** API metrics (latency, error rates), login anomalies, failed login attempts
* **Alerting:** Automated alerts for suspicious activities, backup failures, or unusual access patterns
* **Incident Response:** Documented procedures including identification, containment, eradication, recovery, and lessons learned

**7. Compliance Considerations**

* **FERPA:** Treat Level An educational record with strict confidentiality
* **Data Minimization:** Collect only necessary data; delete user data upon request
* **Retention Policy:** Retain sensitive data only for active accounts + 12 months, purge from backups as required
* **User Rights:** Export and deletion requests supported

**Summary:** This document establishes a structured, layered security approach for the Academic Support Hub. By combining technical, administrative, and infrastructure controls with strong compliance awareness, the project ensures confidentiality, integrity, and availability of student data.