# Academic Support Hub Security Document

* Ensuring System Security and Data Safety
  + Authentication / Authorization: Oauth 2.0 provides strong user authentication and role-based access ensures that users can view only their own data in the hub
  + Data Encryption: AES-256 & TLS 1.3 will ensure that data at rest and in transit is secure
  + Audits: Regular security audits and periodic penetration testing will help identify and correct vulneraibilities
* Identifying Sensitive Data
  + Personally Identifiable Information (PII): Names, email address, phone numbers, student IDs, and login credentials.
  + Academic Records: Assignments, feedback, course enrollment details
  + Communication Logs: Messages between users
  + Payment Information: Payment card details and billing information
  + Behavioral Data: Usage information and performance analytics
* Data Protection Measures
  + Data Minimization: Only collect necessary data and retain it only as long as it is needed
  + Access Controls: Limit access to sensitive data
  + Anonymization: Obscure personal identifiers in analytics and reporting
  + Secure Backups: Maintain encrypted backups in geographically distributed locations
* Technologies Used
  + HTTPS (TLS): Encrypt data in transit
  + AES-256: Encrypt data at rest
  + Oauth 2.0: User Authentication
  + JWT: Session Management