System Requirements Document

**LINK TO SYSML -** [**SysML System Requirements draft.pptx**](https://gmuedu-my.sharepoint.com/:p:/g/personal/asanch57_gmu_edu/EdNlDX_mUiFGk8NhQ3K-0LkBAUnP_HeEBxEaINTgFgu39w?e=vhzN9t)

**LINK TO UML DIAGRAM -** [**lucid.app**](https://lucid.app/lucidchart/82558ade-b247-4625-bf5a-10693564789e/edit?viewport_loc=-2571%2C-477%2C4352%2C2420%2C.Q4MUjXso07N&invitationId=inv_d429ee7f-288e-4f03-b49d-aacd8c74cc2a)

Requirement 1: ACCESS CONTROL

Requirement 1.1 - User Authentication

Requirement 1.1.1 - Passwords

Requirement 1.1.1.1 - Local password policies

Requirement 1.1.2 - Biometrics

Requirement 1.2 - Authorization

Requirement 1.2.1 - Permissions based on roles, attributes, or policies

Requirement 1.2.2 - Role-based-access control, attribute-based access control, etc.

Requirement 1.3 - Policy Management

Requirement 1.3.1 - Access Control policies

Requirement 1.3.1.1 - Policies for granting, modifying, and revoking access

Requirement 1.3.1.2 - Context-based access controls

Requirement 1.4 - Audit & logging

Requirement 1.4.1 - Logs of attempted login/access

Requirement 1.4.2 - Reports for compliance and auditing

Requirement 1.5 - Session Management

Requirement 1.5.1 - Control user sessions

Requirement 1.5.2 - Users can securely log out

Requirement 1.6 - Data Protection

Requirement 1.6.1 - Encrypt sensitive data

Requirement 1.6.2 - Secure communication protocols for data transmission

Requirement 1.7 - Intrusion detection

Requirement 1.7.1 - Monitor suspicious activity

Requirement 1.7.2 - Alert administration of potential breaches

Requirement 1.8 - Disaster Recovery

Requirement 1.8.1 - Mechanism for data backup/recovery

Requirement 1.x - Scalability

Requirement 2: INCIDENT DETECTION / RESPONSE

Requirement 2.1 - Incident Logging Report

Requirement 2.1.1 -

Requirement 2.2 - IDS (Intrusion Detection System)

Requirement 2.2.1 - Detection Methods

Requirement 2.2.1.1 - Signature-based detection

Requirement 2.2.1.2 - Anomaly detection

Requirement 2.2.1.3 - Network traffic monitoring

Requirement 2.2.2 - Alerting

Requirement 2.2.2.1 - Real-time alerts for detected threats

Requirement 2.2.2.2 - Detailed incident information

Requirement 2.2.3 - Data Collection & Analysis

Requirement 2.2.3.1 - Log collection

Requirement 2.2.3.2 - Historical data for trend analysis

Requirement 2.2.4 - Response Mechanism

Requirement 2.2.4.1 - Response systems for automated responses

Requirement 2.2.4.2 - Manual intervention

Requirement 2.2.4.3 - Investigation workflows

Requirement 2.2.5 - Security

Requirement 2.2.5.1 - Data Integrity

Requirement 2.2.5.2 - Access Control

Requirement 2.2.5.3 - Encryption

Requirement 2.2.x - Network based firewall

Requirement 2.2.x - Machine learning model to analyze data

Requirement 2.3 - IPS (Intrusion Prevention System)

Requirement 2.3.1 - Traffic monitoring

Requirement 2.3.1.1 - Monitor network traffic

Requirement 2.3.1.2 - Detect malicious activity in real-time

Requirement 2.3.2 - Threat Prevention

Requirement 2.3.2.1 - Block identified threats

Requirement 2.3.2.1.1 - Drop malicious packets

Requirement 2.3.2.1.2 - Terminate harmful connections

Requirement 2.3.3 - Policy Enforcement

Requirement 2.3.3.1 - Security policies

Requirement 2.3.3.1.1 - Dictate permissible actions

Requirement 2.3.3.1.2 - Prevent unauthorized access

Requirement 2.3.4 - Reporting

Requirement 2.3.4.1 - Real-time alerts

Requirement 2.3.4.1.1 - Blocked threats

Requirement 2.3.4.1.2 - Detailed incident reports

Requirement 2.3.5 - Data collection

Requirement 2.3.5.1 - Log traffic

Requirement 2.3.6 - Security

Requirement 2.3.6.1 - Data integrity

Requirement 2.3.6.2 - Access control

Requirement 2.3.6.3 - Encryption

Requirement 2.3.x - Block users using firewall

Requirement 2.3.x - Close open ports

Requirement 3: SECURE DEVOPS (DevSecOps)

Requirement 3.1 - Continuous Integration and continuous deployment (CI/CD)

Requirement 3.1.1 - Automate build, test, and deployment w/ integrated sec check

Requirement 3.2 - Security testing

Requirement 3.2.1 - Automated security testing tools

Requirement 3.2.2 - Vulnerability scanning

Requirement 3.3 - Configuration management

Requirement 3.3.1 - Infrastructure as Code (IaC) practices

Requirement 3.4 - Access Control

Requirement 3.4.1 - Role-based access control

Requirement 3.5 - Incident Response

Requirement 3.5.1 - Processes for detect, report, & response integrated into dvpmt workflow

Requirement 3.6 - Security

Requirement 3.6.1 - Data protection

Requirement 3.6.2 - Secrets management

Requirement 3.6.3 - Audit logging

Requirement 3.6.4 - Compliance adherence

Requirement 4: MACHINE LEARNING

Requirement 4.1 - Data Acquisition

Requirement 4.1.1 - Support mechanisms for collecting + preprocessing data from sources

Requirement 4.2 - Model training

Requirement 4.2.1 - Capabilities for training various types of machine learning models

Requirement 4.3 - Model Evaluation

Requirement 4.3.1 - Tools for evaluating model performance via metrics

Requirement 4.4 - Inference

Requirement 4.4.1 - Real-time or batch inference

Requirement 4.4.1.1 - Predictions based on trained models

Requirement 4.5 - Model Versioning

Requirement 4.5.1 - Support version control for models (allows rollback to prev versions)

Requirement 4.6 - Automated Machine Learning (AutoML)

Requirement 4.6.1 - AutoML features for automation

Requirement 4.7 - Security

Requirement 4.7.1 - Data Protection

Requirement 4.7.2 - Access Control

Requirement 4.7.3 - Model Integrity

Requirement 4.7.4 - Compliance