

# **Learning Management System**

## **(EduFlex School)**

**Group: 4**

**Group Member:**

- |                           |                  |
|---------------------------|------------------|
| <b>1. Yash Kachhadiya</b> | <b>(2543707)</b> |
| <b>2. Tushar Solanki</b>  | <b>(2536692)</b> |
| <b>3. Devang Zala</b>     | <b>(2534443)</b> |
| <b>4. Akash Luhariya</b>  | <b>(2535266)</b> |

# **EduFlex School – Analysing Security Needs**

## **1: Introduction**

### **EduFlex School**

EduFlex School uses an online Learning Management System (LMS) to:

- Manage courses
- Store student information
- Track student progress
- Upload learning materials
- Conduct online assessments

### **Objective**

Identify security threats, analyse their impact, and recommend ways to protect the LMS.

## **2: Key Users and Data**

### **Users**

- Students
- Teachers
- School Administrators
- IT Staff

## **Data Stored**

- Student personal information
- Grades and assessment results
- Attendance records
- Learning materials
- Teacher information
- Login credentials

## **Why Security Matters**

The LMS contains sensitive information that must be protected from unauthorized access and misuse.

## **3: Internal Threats**

### **Threat 1: Unauthorized Access by Employees**

#### **Example:**

- A teacher accesses records that they are not allowed to view.

### **Security Tenets Affected**

- Confidentiality
- Accountability

### **Consequences**

- Privacy violations
- Loss of trust
- Possible legal action

## **Threat 2: Incorrect System Configuration**

### **Example:**

- An administrator accidentally gives students access to confidential files.

### **Security Tenets Affected**

- Confidentiality
- Integrity

### **Consequences**

- Data exposure
- Incorrect information being accessed

## **4: External Threats**

### **Threat 3: Phishing Attacks**

#### **Example:**

- Students or teachers receive fake emails asking for login details.

### **Security Tenets Affected**

- Confidentiality
- Accountability

### **Consequences**

- Stolen accounts
- Unauthorized access to LMS data
- Data breaches

## **Threat 4: Malware or Ransomware**

### **Example:**

- Malicious software infects the LMS server.

### **Security Tenets Affected**

- Availability
- Integrity

### **Consequences**

- System downtime
- Loss of educational services
- Data corruption

## **5: Cyber Attacks**

### **Threat 5: Password Attacks**

### **Example:**

- Hackers guess weak passwords.

### **Security Tenets Affected**

- Confidentiality
- Accountability

### **Consequences**

- Account compromise
- Unauthorized changes to records

## **Threat 6: Denial of Service (DoS) Attack**

### **Example:**

- Attackers overload the LMS with traffic.

### **Security Tenets Affected**

- Availability

### **Consequences**

- Students cannot access lessons
- Teachers cannot upload materials
- Disruption of learning

## **6: Incidental Threats**

### **Threat 7: Human Error**

### **Example:**

- A teacher accidentally deletes student grades.

### **Security Tenets Affected**

- Integrity
- Availability

### **Consequences**

- Loss of important records
- Time required for recovery

## Threat 8: System Failure

### Example:

- Server hardware crashes.

### Security Tenets Affected

- Availability

### Consequences

- LMS becomes unavailable
- Learning activities are interrupted

## 7: Threat Summary Table

| Threat              | Category   | Security Tenets Affected        | Consequences        |
|---------------------|------------|---------------------------------|---------------------|
| Unauthorized Access | Internal   | Confidentiality, Accountability | Privacy breach      |
| Misconfiguration    | Internal   | Confidentiality, Integrity      | Data exposure       |
| Phishing            | External   | Confidentiality, Accountability | Account theft       |
| Malware/Ransomware  | External   | Availability, Integrity         | System disruption   |
| Password Attacks    | External   | Confidentiality, Accountability | Unauthorized access |
| DoS Attack          | External   | Availability                    | Service outage      |
| Human Error         | Incidental | Integrity, Availability         | Data loss           |
| System Failure      | Incidental | Availability                    | Downtime            |

## **8: Security Recommendations**

To improve security, EduFlex School should:

- Use Multi-Factor Authentication (MFA)
- Enforce strong password policies
- Provide cybersecurity awareness training
- Regularly back up data
- Install antivirus and anti-malware software
- Apply security updates and patches
- Monitor user activities through audit logs
- Restrict access using role-based permissions

## **9: Conclusion**

### **Key Findings**

- EduFlex LMS faces internal, external, and incidental threats.
- The most critical assets are student records, grades, and login credentials.
- Confidentiality, Integrity, Availability, Accountability, and Non-Repudiation must be protected.

### **Final Statement**

By implementing strong security controls, EduFlex School can protect sensitive information, maintain trust, and ensure uninterrupted learning services.