



# K&I Exam Software Enterprise

## Information Security Policy

**D**ocument Version: 1.0 Effective Date: October 30, 2025 Purpose: This policy establishes the requirements and procedures for maintaining the confidentiality, integrity, and availability of all data and systems within K&I Exam software Enterprise. It ensures compliance with the Uganda Data Protection and Privacy Act and safeguards the data of all users, particularly minors.

### Governance and Responsibility

#### Designated Roles

The responsibility for information security is assigned according to the EMS user roles:

Role	Primary Security Responsibility
Admin	<b>Data Controller &amp; System Security Coordinator.</b> Oversees all security procedures, manages user accounts, performs database backups, and leads incident response.
Exam Master	<b>Assessment Integrity Officer.</b> Monitors proctoring logs, investigates malpractice flags, and manages security settings for exams (e.g., setting the complexity of the security check).

<b>Teacher</b>	<b>Data Integrity Officer.</b> Responsible for the security of their own accounts, managing submitted student work, and ensuring the accurate entry of grades.
----------------	--

### **Policy Review and Training**

- The **Admin** must review and update this policy at least annually or immediately following any significant system change or security incident.
- All new staff requiring access must undergo mandatory training on this policy during induction.

## **Access Control and User Accounts**

### **Principle of Least Privilege (Responsibility-Based Access)**

User access is strictly restricted based on the duties required by their role:

- **Admin:** Full read/write access to user management, system configuration, and database maintenance functions.
- **Teacher:** Read/write access to their assigned exams, question banks, and student submissions. **No access** to system settings or other teachers' exams.
- **Finance:** Access restricted entirely to the financial module (secret code generation, eligibility). **No access** to academic scores or question content.
- **Student:** Access restricted to their own current and past exam records and the secure exam environment.

### **Password Requirements and Management**

- **Unique Identifiers:** All staff must use unique user accounts; generic or shared accounts are strictly prohibited.
- **Complexity:** Passwords must be a minimum of **8 characters** and include a mix of uppercase letters, lowercase letters, numbers, and special characters.
- **Rotation:** Passwords must be changed every **90 days** or immediately if a compromise is suspected.
- **Storage:** Passwords must **not** be stored in plain text (written notes, digital files).

- **Lockout:** Accounts will be locked after **three** unsuccessful login attempts.

### **Screen and Session Confidentiality**

- **Automatic Timeout:** The EMS system enforces an **automatic session time-out** (e.g., 15 minutes) to log users out and prevent unauthorized access when the workstation is unattended.
- **Logout Procedure:** Administrative staff must close any confidential electronic file (e.g., student lists) before leaving the computer area.

### **Data Protection and Integrity**

#### **Data Storage and Processing**

- **On-Premises Security:** All sensitive data is stored locally on the school's **dedicated server**, granting the institution full physical control over the data.
- **Encryption:** All data transmitted for the online (university) version must be secured using **HTTPS (SSL/TLS encryption)**.

#### **Backup and Recovery**

- **Frequency:** The **Admin** must conduct backups of the database and application files at least **daily**.
- **Offsite Storage:** Backup media (e.g., encrypted external drive) must be stored **offsite** in a secure location separate from the server location to protect against environmental risks (fire, flood).
- **Testing:** Data restoration procedures must be tested **quarterly** to ensure data can be recovered promptly in the event of hardware failure.

#### **Protection of Minors' Data**

- **Data Minimization:** The EMS collects only data **strictly necessary** for the educational functions (assessment and security).
- **Purpose Limitation:** Proctoring data (webcam snapshots, audio logs) is used *exclusively* for **exam integrity verification** and **malpractice auditing**. It must never be used for general surveillance, marketing, or external profiling.

# Anti-Malpractice and System Monitoring

## Malpractice Logging

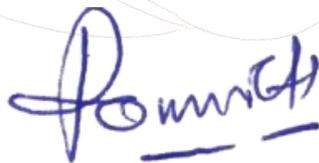
The system maintains a comprehensive audit trail to detect and log security violations:

- **Proctoring Logs:** Continuous recording of system events (audio spikes, webcam snapshots, browser exits) is stored in the *ProctoringLog* model for forensic review by the Exam Master.
- **QR Code Sealing:** All final student submissions (PDFs) are digitally sealed with a traceable QR code to confirm the document's authenticity during offline grading.

## Incident Response

- In the event of a suspected cybersecurity incident (e.g., unauthorized access, data alteration), the **Admin** must immediately **isolate the affected system** (disconnect from the network) and initiate the recovery procedures outlined in the disaster recovery plan.
- The **Admin** is responsible for assessing the incident and complying with mandatory reporting laws to the PDPO if a data breach is confirmed.

*Signed By:*



.....  
*Muyinda Ronnie Pius*  
*Founder and CEO*