School Security Breach Policy

1. Purpose

The purpose of this policy is to ensure that all schools have a clear, coordinated, and effective system for **preventing, identifying, and responding to security breaches**. A "security breach" refers to any unauthorized access, activity, or event that threatens the safety of **students, staff, visitors, information, or property** within school premises.

This policy aims to protect lives, prevent damage or theft, and maintain a secure learning environment.

2. Scope

This policy applies to all individuals on school property, including:

- Students, teachers, and administrative staff
- Contractors, suppliers, and service providers
- Parents and visitors
- After-hours personnel and security guards

It covers **all school facilities**, including classrooms, playgrounds, parking areas, sports fields, ICT systems, and school buses.

3. Policy Statement

The school is committed to maintaining a **safe and secure educational environment** by ensuring that:

- All access to school property is controlled and monitored.
- Any breach in physical, digital, or operational security is immediately detected, reported, and addressed.
- Clear procedures are established for lockdown, evacuation, or police notification if required.
- All staff and students are trained to recognize and respond appropriately to potential security threats.

No unauthorized person should be allowed entry to any restricted area, and all suspicious activities must be reported immediately.

4. Legal and Regulatory Framework

This policy aligns with the following standards and requirements:

- **ADEK Health, Safety & Environment Framework (2024)**
- **ADOSH 4.0 – Security and Emergency Preparedness**
- **NCEMA 6000 – Emergency, Crisis, and Disaster Management Standard**
- **Abu Dhabi Monitoring and Control Center (MCC) Security Guidelines (2017)**
- **UAE Civil Defence Fire and Safety Code**
- **Federal Law No. 12 of 2016 – School Safety and Security**
- **ISO 45001:2018 – Occupational Health and Safety Management Systems**

5. Definitions

- **Security Breach:** Any event that results in unauthorized access, loss, or damage to people, property, or information.
- **Unauthorized Access:** Entry to school premises or restricted areas without permission or identification.
- **Incident Commander:** The designated staff member responsible for leading emergency response during a security event.
- **Lockdown:** Protective action taken to keep occupants safe when an external or internal threat exists.

6. Roles and Responsibilities

6.1 School Principal / Management

- Ensure the full implementation of this policy.
- Approve and periodically review the **School Security Plan (OSH-R-38A)**.
- Maintain coordination with local authorities such as **Police**, **Civil Defence**, and **MCC**.

- Lead the school's response during any major breach or intrusion.
- Ensure all security systems (CCTV, access control, alarms) are functional.

6.2 OSH Department / Safety Officer

- Conduct **security risk assessments** at least annually.
- Maintain records of all security breaches and corrective actions.
- Train all staff in **security awareness and response procedures**.
- Liaise with authorities and submit reports to ADEK when required.
- Ensure signage, emergency communication tools, and access systems are properly installed and maintained.

6.3 Security Guards

- Monitor entry and exit points throughout the day.
- Verify identity of all visitors and issue **visitor badges**.
- Prevent unauthorized access and report suspicious activity immediately.
- Maintain a **Security Logbook** for all incidents and visitors.
- Support emergency lockdown or evacuation procedures.

6.4 Staff and Teachers

- Challenge any unknown or unbegged person within school premises.
- Keep classroom and office doors secured when not in use.
- Report immediately any theft, vandalism, or suspicious behavior.
- Cooperate fully with security personnel during investigations or drills.

6.5 Students

- Follow school security and emergency procedures.
- Never open doors or gates to strangers.
- Report suspicious behavior, online threats, or bullying to teachers or the OSH Officer.

7. Types of Security Breaches

- **Unauthorized entry** by outsiders or intruders.
- **Theft or vandalism** of school property or personal belongings.
- **Cybersecurity breach**, such as hacking, phishing, or data theft.

- **Violence or threats** from students, staff, or visitors.
- **Tampering with fire alarms or CCTV systems.**
- **Suspicious packages or unidentified vehicles** near the school.

8. Security Breach Response Procedure

Step 1: Detection and Reporting

- Any staff or student identifying a security breach must report it **immediately** to the Principal, OSH Officer, or Security Team.
- The incident should be recorded in the **Security Incident Log**

Step 2: Immediate Action

Depending on the nature of the threat:

- **Intrusion or threat present:** Initiate **Lockdown Procedure**
- **Fire-related or hazardous material threat:** Initiate **Evacuation Plan (**
- **Cyber or information breach:** Disconnect affected systems and inform IT support.
-

Step 3: Communication

- Notify the **Principal, OSH Officer, and local police** immediately.
- The **Communication Tree** should be activated, ensuring that all staff are informed quickly and calmly.
- Parents and ADEK will be notified only after safety has been secured and verified.

Step 4: Investigation

- The OSH Officer, along with the Principal and Security Team, investigates the cause of the breach.
- CCTV footage, visitor logs, and access records are reviewed.
- Findings are documented in the **Security Breach Investigation Report**

Step 5: Corrective Actions

- Implement corrective and preventive measures (e.g., gate reinforcement, staff retraining).
- Review and update the **School Security Plan** to prevent recurrence.

9. Communication and Information Security

- Access to CCTV footage is limited to authorize personnel only.
- All visitor and contractor data shall be kept confidential and stored securely.
- Any loss or compromise of digital information must be reported to IT and the OSH Officer immediately.
- School staff shall not share sensitive school information via personal devices or social media.
-

10. Training and Awareness

- All employees must undergo **annual Security Awareness Training**, covering:
  - Identifying suspicious behavior.
  - Lockdown and evacuation procedures.
  - Emergency communication and reporting.
- Security guards shall receive additional training on **conflict management and intruder response**.
- Students will be educated through **age-appropriate awareness sessions** about safety and security.
-

11. Drills and Testing

- **Security breach or lockdown drills** must be conducted **twice per academic year**.
- Each drill must be documented using the **Drill Record**
- Findings from drills must be reviewed and used to improve future response.

12. Monitoring and Review

- The OSH Department shall monitor compliance through inspections, CCTV reviews, and access audits.
- The policy shall be reviewed annually or following any significant security event.
- Improvements or recommendations must be approved by the principal and communicated to all staff.

13. References

- **ADEK Health, Safety & Environment Framework (2024)**
- **ADOSH 4.0 – Emergency Preparedness and Security Management**
- **NCEMA 6000 – National Emergency and Crisis Management Standard**
- **Abu Dhabi Monitoring and Control Center (MCC) Security Guidelines (2017)**
- **UAE Civil Defence Code of Practice**
- **ISO 45001:2018 – Occupational Health and Safety Management Systems**

Principal		OSH officer
Sister Claudette Dababneh		Marwah Aljammali