ليـــوا للتعليم
Liwa Education

Cybersecurity Incident Response Plan Policy

Policy Document

2024-2025

Policy Reference	IT-01
Version	V1
Date of Creation	01082024
Policy Owner	IT Manager
Date of Approval	01082024
Effective Date	01082024
Date of Review	01082026
Reviewed by	Director of Schools
	Deputy CEO
Approved by	CEO

Cybersecurity Incident Response Plan Policy

A. Rationale

Liwa Education is a K-12 educational institution located in Abu Dhabi and Al Ain serving students from KG1 to Grade 12. This document outlines Liwa School data and cybersecurity Incident Response plan policy to ensure compliance with ADEK (Abu Dhabi Department of Education and Knowledge) requirements and to maintain a secure digital environment for students, staff, and stakeholders.

B. Purpose

The purpose of this policy is to establish a clear, structured approach for responding to cybersecurity incidents that may impact Liwa Education School's technology systems, student and staff data, or daily operations. This plan outlines procedures to identify, contain, eradicate, and recover from cybersecurity incidents to protect our community and ensure compliance with applicable regulations.

C. Scope

This policy applies to all information systems, networks, data, and devices used by Liwa Education Schools. It encompasses all grades, from KG1 to Grade 12, and includes all school personnel, contractors, and third-party vendors who have access to our systems.

D. Definitions

1. **Cybersecurity Incident**: An event that may compromise the confidentiality, integrity, or availability of school information systems or data, including unauthorized access, malware infections, data breaches, or any other security violation.

2. **Incident Response Team (IRT)**: The designated team responsible for managing and coordinating the response to cybersecurity incidents. This team is led by the IT Manager.

E. Incident Response Phases

Liwa Education School's Cybersecurity Incident Response Plan consists of five key phases:

1. Preparation

1.1 Develop and maintain cybersecurity policies and procedures.
1.2 Train school personnel on cybersecurity best practices and awareness.
1.3 Conduct regular backups, updates, and maintenance of systems to reduce vulnerabilities.

2. Identification

2.1 Detect cybersecurity incidents by monitoring network activity, user reports, or security alerts.
2.2 Classify incidents based on severity and potential impact.
2.3 Notify the IT Manager and IRT immediately if a cybersecurity threat is detected.

3. Containment

3.1 Implement containment strategies to prevent the spread of the incident (e.g., isolating affected devices, disabling compromised accounts).
3.2 Determine whether containment should be short-term (e.g., immediate response) or long-term (e.g., sustained containment).

4. Eradication

4.1 Identify and remove the root cause of the incident (e.g., malware removal, patching vulnerabilities).

4.2 Ensure that all traces of the threat are eliminated before returning systems to normal operations.

5. Recovery

5.1 Restore affected systems and verify their functionality and integrity.
5.2 Monitor systems for any signs of lingering issues or vulnerabilities.
5.3 Document the incident and recovery process, noting lessons learned.

F. Incident Reporting and Documentation

All cybersecurity incidents must be documented with detailed reports, including the nature of the incident, actions taken, and follow-up measures. This documentation will be securely stored and reviewed by the IRT to improve response efforts for future incidents.

G. Communication

In the event of a cybersecurity incident, the IT Manager, in consultation with the school administration, will determine the appropriate communication plan. For incidents involving sensitive information or significant operational impact, parents, staff, and ADEK will be notified as necessary and in compliance with privacy regulations.

H. Roles and Responsibilities

1. **IT Manager**: Leads the Incident Response Team, coordinates all incident response actions, and communicates with school leadership and stakeholders.
2. **Incident Response Team (IRT)**: Supports incident response activities, conducts investigations, and provides technical expertise.
3. **School Leadership**: Collaborates with the IT Manager to determine the necessary level of communication and strategic response.

I. Policy Review and Maintenance

This policy will be reviewed annually or after any significant cybersecurity incident. Updates will be made as needed to reflect changes in technology, threats, or regulations.

References:

UAE National Cybersecurity Strategy (NCS)
ADEK ICT Guidelines
UAE Cybercrime Law (Federal Law No. 5 of 2012)

Policy Owner Department

IT Department

Key Stakeholders		
Policy Owner:	Hari Devicharan	IT Manager
Reviewed by:	Margaret Haynes	Director of Schools
	Kevin Wallis	Deputy CEO
Approved by:	Dr. Shereen Gobran	Chief Executive Officer