IT Requirements for Cognia Accreditation

Policy

1. Cybersecurity Policy

The Cybersecurity Policy aims to protect school networks, systems, and data from digital threats and ensure confidentiality, integrity, and availability.

Policy Objectives:

- Protect information from unauthorized access.
- Ensure business continuity.
- Reduce risks associated with cyber threats.

Scope:

Applies to all staff, students, contractors, and visitors using school systems.

Core Rules:

- MFA must be enabled.
- Systems must be regularly updated.
- Continuous monitoring of servers and networks.
- Strong password enforcement.
- No software installations without IT approval.

2. Acceptable Use Policy (AUP)

Defines guidelines for the safe and responsible use of school devices, networks, and internet services.

Allowed:

- Educational use of school devices.
- Accessing approved learning platforms.

Not Allowed:

- Accessing inappropriate websites.
- Installing software without approval.
- Sharing passwords.

User Responsibilities:

- Handle devices carefully.
- Report any security issues immediately.

3. Backup & Disaster Recovery Policy

Purpose:

Ensure data can be restored in cases of loss, corruption, or system failure.

Backup Types:

- Full Backup
- Incremental Backup

Schedule:

- Daily: Incremental
- Weekly: Full
- Monthly: Off-site backup

Responsibilities:

- IT Manager supervises implementation.
- Weekly reports are submitted to school leadership.

4. Business Continuity Plan

Purpose:

Enable uninterrupted school operations during emergencies such as internet outage, server failure, or cyberattack.

Core Elements:

- Backup internet (4G Router)
- Cloud or secondary server failover
- Manual SIS operation procedure
- Communication plan during downtime

---

5. Device Management Policy

Purpose:

Ensure proper management, usage, and maintenance of all school devices.

Key Sections:

- All devices must be recorded in the Inventory List.
- Personal devices cannot access school data.
- Regular software updates.
- Scheduled maintenance cycles.

6. IT Annual Training Plan

Includes:

- Cybersecurity awareness training
- Google Workspace / Microsoft 365 training
- SIS training
- Teacher digital tools training