Aldar Education

Aldar Education Information Security Policy Manual

Instrument Information	
Name	Aldar Education Information Security Policy Manual
Reference	ALDED-EDT-GEN-PL-00004

Instrument Version Control		
Version	**Date**	**Change Summary**
Version 1	September 02, 2025	Initial Version

Contents

A. INTRODUCTION 4
1. TITLE 4
2. PURPOSE 4
3. GOVERNING INSTRUMENT 4
4. SCOPE 4
5. COMPLIANCE 5

B. POLICY STATEMENTS 6
1. INFORMATION SECURITY – GENERAL 7
2. RISK MANAGEMENT 7
3. INFORMATION PROCESSING SYSTEMS OR FACILITIES 7
4. CONTACT WITH AUTHORITIES / OTHER GROUPS 8
5. ASSET MANAGEMENT 8
6. IDENTITY AND ACCESS CONTROL 9
7. THIRD PARTY SERVICE MANAGEMENT 10
8. INFORMATION SECURITY INCIDENT & THREAT MANAGEMENT 13
9. DISASTER RECOVERY MANAGEMENT 14
10. HUMAN RESOURCE SECURITY 14
11. REMOTE WORKING 15
12. PHYSICAL AND ENVIRONMENTAL SECURITY 15
13. ENDPOINT DEVICE SECURITY 16
14. PASSWORD MANAGEMENT 16
15. ANTI-VIRUS MANAGEMENT 17
16. SYSTEM LOGGING 17
17. SOFTWARE USAGES 17
18. CRYPTOGRAPHY 17

C. DEFINITIONS 19

D. APPENDIX 21
1. RELATED ISO CERTIFICATIONS 21

A. INTRODUCTION

1. TITLE

1.1. This Instrument is entitled the Aldar Education Information Security Policy Manual ("the Policy").

2. PURPOSE

2.1. This Policy establishes the controls for an efficient governance and better management of information security within Aldar Education. It emphasises on the people, process and technology related information security controls.

3. GOVERNING INSTRUMENT

3.1. This Policy Manual must be read in conjunction with the following documents:

3.1.1. ADEK Digital Policy,

3.1.2. ADEK Records Policy,

3.1.3. COBIT 2019, and

3.1.4. ISO 27001:2022.

4. SCOPE

4.1. This Policy binds and applies to all Employees across the Aldar Education HQ, Aldar Training Academy (ATA), its Operated Schools (hereafter referred to as AE) and contractors and vendors, who handle AE's information assets including but not limited to information created, processed, stored, or retained by AE as part of its functions and services regardless of geographical location. For Managed Schools, this Policy will be referred to areas where the responsibility is given to Aldar Education as per the respective legal agreement.

4.2. Nothing in this Policy has the effect of invalidating past acts validly performed under previous Instruments.

4.3. The Policy addresses the following areas:

4.3.1. Information Security – General,

4.3.2. Risk Management,

4.3.3. Information Processing Systems or Facilities,

4.3.4. Contact with Authorities / Other Groups,

4.3.5. Asset Management,

4.3.6. Identity and Access Control,

4.3.7. Third Party Service Management,

4.3.8. Information Security Incident & Threat Management,

4.3.9. Disaster Recovery Management,

4.3.10. Human Resource Security,

4.3.11. Remote Working,

4.3.12. Physical and Environmental Security,

4.3.13. Endpoint Device Security,

4.3.14. Password Management,

4.3.15. Anti-Virus Management,

4.3.16. System Logging,

4.3.17. Software Usages, and

4.3.18. Cryptography.

5. COMPLIANCE

5.1. Compliance with local and international data protection regulations and standards must be ensured.

5.2. Violations of this Policy and supporting Instruments may result in corrective action by the relevant management authorities. Disciplinary investigation will be consistent with the severity of the incident as determined by the investigation.

5.3. Any instance of non-compliance or breaches of this Policy must be reported immediately to Aldar Education Service Desk at sd@aldareducation.com for immediate action and resolution.

5.4. All queries regarding interpretation of this Policy Manual must be addressed to Aldar Education Service Desk at sd@aldareducation.com.

5.5. Once the approved version of this Policy Manual must be used. The printed copies are uncontrolled and will not be considered valid.

B. POLICY STATEMENTS

1. INFORMATION SECURITY – GENERAL

1.1. Responsibilities

1.1.1. Users are responsible for:

- Adhering to the Information Security Policies and Procedures.
- Participating in security awareness and training activities.
- Knowing assets or parts of assets they are directly responsible for (e.g., printer, desktop, specific support service, etc.).
- Reporting incidents to Aldar Education.

2. RISK MANAGEMENT

2.1. To manage information security, AE adopts a risk-based approach. This approach mandates:

2.1.1. The identification of all critical information assets.

2.1.2. The identification of security vulnerabilities in these information assets.

2.1.3. The identification of threats and threat probabilities that may result in exploitation of the vulnerabilities.

2.1.4. The identification of the proper set of controls to protect these assets from the identified threats. Controls must also be identified in line with any client guidelines or contractual clauses on information security, if any.

2.1.5. Periodical assessment of risk management and identified risk closure.

3. INFORMATION PROCESSING SYSTEMS OR FACILITIES

3.1. When formally approving the acquisition, development, deployment or implementation of a new information processing system or facility, Aldar Education considers the following:

3.1.1. The information processing system or facility's compliance with AE's Information Security Policy, standards and criteria specifically developed for the system or facility.

3.1.2. The extent of technical compatibility of the new system with existing system components.

3.2. Users must ensure only approved processing systems or facilities are used to acquire or process AE's data.

3.3. The use of personal equipment, such as laptops or remote / mobile devices, for processing AE's data is strictly prohibited, unless expressly authorised by AE.

3.4. Web Filtering

3.4.1. Access to web resources is governed by centrally managed controls that prevent access to content that is inappropriate, malicious, or not aligned with the Company's operational and educational objectives. These controls include:

- Automated mechanisms to categorize and block websites that fall under predefined restricted categories (e.g., adult content, gambling, hate speech, known malware sources).
- Configuration of DNS (Domain Name System) or secure web gateways to enforce these web filters across HQ and school-managed networks and devices.
- Periodic review and adjustment of web filters and exceptions to reflect changing risk landscapes and operational needs.

- Logging and monitoring of web filtering to detect violations or potential threats.

3.5. Aldar Education has deployed and maintained identity-based firewall solutions that enable user-level visibility and control over web usage.

4. CONTACT WITH AUTHORITIES / OTHER GROUPS

4.1. AE recognizes that the maintenance of the desired level of information security may require the cooperation, support, and assistance of certain external agencies (authorities and other organisations).

4.2. The extent of cooperation and transfer of security-related information between AE and external parties or agencies must be formalized and in accordance with the agencies' legal authority.

4.3. This cooperation must be in the interest of AE and must not result in a violation of this Policy, including the unsanctioned transfer of confidential / classified information to unauthorized external organisations.

4.4. External parties' agreements and access requirements must be processed in accordance with the Third-Party Service Management controls defined in this Policy.

4.5. AE will not outsource any activity in respect of information or data processing functions or DTS services to third-party organisations without approval. In such cases, formal service level agreements will be signed between both parties to ensure compliance with this Policy and periodic auditing of the third-party services must be performed.

5. ASSET MANAGEMENT

5.1. The identification, classification, maintenance, and disposal of AE's information assets must be secure, ensuring information system related assets are accounted and have a nominated owner.

5.2. Asset classification

5.2.1. The classification, treatment and handling of AE's information system assets are key to the protection of critical and sensitive information. Asset management must consider the CIA needs of all information system assets to ensure the appropriate implementation and management of security processes and controls.

5.2.2. Asset classification guidelines

- Information owner must classify its information assets on three different parameters:

Criteria	Description
Confidentiality	The level of confidentiality to be accorded to the information system assets and consequently the level of accessibility to the information it contains or represents.
Integrity	Impact of unauthorised modification to an information system asset or loss of the information system asset or data contained therein.
Availability	Impact of an information systems asset being unavailable. Availability criteria are further subdivided into long-term unavailability and short-term unavailability.

- The asset classification guidelines consider the following:
  - The type of asset (data or information systems),
  - The criticality of the asset,
  - The information systems asset value and its sensitivity,

- The impact of a security breach, and
- The basis on which access to the information systems asset will be provided and the extent of access (read, modify, delete) that will be provided to different Users.

- Assets may be classified by one or more of the CIA criteria depending on the applicability.
- The classification categories dictate the level of protection applied to the information asset.
- Classification and associated controls for information access, sharing or handling must consider the business needs for sharing or restricting information and the business impact associated with such needs.

5.3. In line with the Aldar Group Technology Clear Desk Clear Screen Policy, Users must ensure that:

5.3.1. Documents are not to be left on the desk after the office hours.

5.3.2. Individual drawers containing documents are locked before leaving the desk at end of the day.

5.4. Backup and storage

5.4.1. A formal Procedure for backup of data is established to ensure a secure backup and storage of information for on-premises environment. Backups of critical data must be vaulted and stored offline or in a secure environment.

5.4.2. All Information assets, data, databases, configurations, applications, services, and software essential for the continuous operations of AE are backed up and periodically tested as per the backup schedule for recovery and reliability.

5.4.3. Backups of all AE HQ data must be retained such that all information assets, information systems are fully recoverable. At a minimum, backup AE HQ data will be retained for 30 days.

5.4.4. Backups are stored securely and in a physically separated location from the primary school network to ensure control against data loss or compromise.

5.4.5. The restored systems must be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

6. IDENTITY AND ACCESS CONTROL

6.1. Access to information and information processing facilities are controlled based on business and security requirements of individual applications.

6.2. Unauthorised system usage or abuse is subject to criminal prosecution.

6.3. Only approved external learning applications will be used in the school environment. Safeguards, such as single sign on mechanisms, must be implemented to ensure secure access and protect critical data.

6.4. System usage will be monitored and logged.

6.5. User Access Management

6.5.1. Activation of User accounts for contractors, consultants, temporary workers, or vendor personnel will only be in effect for the period that such individuals are actively performing duties or services for AE.

6.5.2. Access for third parties to business information assets will be provided only based on a supporting contractual agreement and non-disclosure agreement.

6.5.3. Generic ID's must not be used on any system.

6.6. Privilege Management

6.6.1. Users must not install any code, software or technique that circumvent the authorised access control mechanisms found in operating systems, application systems or infrastructure system access control mechanisms.

6.7. User responsibilities: End Users must co-operate in ensuring the effectiveness of the security measures adopted by AE. Users must exercise due diligence in respect of User accounts and passwords granted to access AE's information systems.

6.8. Network Control

6.8.1. Access to AE's network is controlled and protected to ensure the confidentiality, integrity, and availability of the information systems assets of AE.

6.8.2. Access to networks and network services are specifically authorised and controlled based on business and security requirements as well as access control rules defined for each network.

6.8.3. Users must only access organisation's information systems and resources through the pre-defined VPN 'enforced path'. Personal Computers (PCs) are not permitted to access AE information systems through the VPN (i.e., Webmail).

6.8.4. AE obtains detailed descriptions of the security attributes of all external services used (if any) from external network services providers to establish the confidentiality, integrity and availability of business applications and the level of controls (if any) required by AE. The description of the security controls must be included in the agreement of the service.

6.9. Remote Access Software

6.9.1. The software will have built-in controls to ensure the protection and privacy of Users' workstations.

6.10. DevSecOps

6.10.1. Developers must be required to follow secure coding practices when developing software. These practices must include using secure coding standards, avoiding known security vulnerabilities, and testing code for security vulnerabilities.

6.10.2. Automated security testing must be used to scan code for vulnerabilities and test for compliance with security regulations.

6.10.3. Continuous Integration and Continuous Delivery (CI/CD) must be used to automate the software development and deployment process, including security checks in a DecSecOps environment.

7. THIRD PARTY SERVICE MANAGEMENT

7.1. Information Security for Supplier Relationships

7.1.1. AE has identified and implemented procedures to address security risk associated with the use of products and services provided by suppliers.

7.1.2. AE has identified and documented the types of suppliers which can affect the confidentiality, integrity, and availability of the AE's information.

7.1.3. For outsourcing arrangements, AE ensures that security is maintained throughout the service operation.

7.1.4. AE assesses and manages the information security risks associated with:

- use of the AE's information and other associated assets.
- vulnerabilities of the products or services provided by the suppliers.

7.1.5. AE monitors the compliance with established information security requirements for each type of supplier.

7.2. Address Security within Supplier Agreements

7.2.1. Formal agreements with third parties for provision of access to AE's information systems must be consistent in all respects with AE's Information Security Policy, Procedures, standards, guidelines, and codes of practice. In addition, compliance with AE's Information Security Policy, Procedures and guidelines will be the basis for granting and revoking third-party access to AE's information systems infrastructure.

7.2.2. All relevant security and audit requirements are ensured in agreements with third parties.

7.2.3. The following terms are considered for inclusion in the agreements to satisfy the identified information security requirements:

- Legal, statutory, regulatory, and contractual requirements, including data protection, handling of Personally Identifiable Information (PII), intellectual property rights and copyright.
- Obligation of each contractual party to implement an agreed set of controls.
- Rules of acceptable use of information and other associated assets.
- Indemnities and remediation for failure of contractor to meet requirements.
- Incident management requirements and Procedures.
- Relevant provisions for sub-contracting.
- Right to audit the supplier processes and controls related to the agreement.
- Supplier's obligation to periodically deliver a report on the effectiveness of controls and agreement.
- Timely correction of relevant issues raised in the report.
- Availability of the service.

7.2.4. Responsibilities and legal actions for breach of information security must be addressed in the terms and conditions of all agreements with third parties.

7.2.5. AE ensures copyright and software license compliance during information exchange with outside entities.

7.2.6. Signed agreements such as non-disclosure agreement must precede the disclosure of sensitive information to external parties.

7.2.7. Security controls, service definitions and delivery levels included in the third-party service delivery agreements must be implemented and managed by AE and the third parties.

7.2.8. Wherever the business deems a need for high availability, agreements with external parties must address type and level of service to be provided to ensure business continuity.

7.2.9. Terms and Condition

- The agreements with contractors and other third parties must clearly state their responsibilities towards information security.
- Confidentiality or non-disclosure agreements reflecting AE's needs for the protection of information must be identified, documented, regularly reviewed, and signed by all Employees and other relevant interested parties.

7.3. Information and Communication Technology Supply Chain

7.3.1. To manage and mitigate supply chain risks, AE ensures the following:

- DTS products and services acquired for the business operations meet the defined security requirements at all stages of the supply chain, including the purchasing organization, suppliers, and any subcontractors involved.
- Validation is done to ensure that DTS products and services continue to meet the defined security requirements without any unexpected or unwanted features.
- Critical components must be traceable to their source of origin within the supply chain. Clear procedures must be established for information sharing between AE and its suppliers regarding risks, compromises, or issues affecting the integrity of the DTS supply chain.

7.4. Third Party Accesses

7.4.1. Third-party access to AE's information systems infrastructure must be formally authorized and governed by a formal agreement between AE and the concerned third party. However, AE will assess risks that are associated with sharing of systems, information, and assets via a formal risk assessment considering the following criteria:

- The type and level of access to be provided to the third-party.
- The risk classification (value and sensitivity) of the information asset(s) to which access is provided.
- The purpose of access.
- Background information concerning the third-party.
- The relationship of the third-party to AE.
- The effectiveness of the controls that need to be implemented to regulate and monitor the third-party access.

7.4.2. Prior to granting access to any information, AE will brief all third-party Users on information security roles and responsibilities by signing the responsible computing agreement.

7.4.3. Ad-hoc and 24/7 unmonitored connections by third parties to production systems will not be permitted.

7.4.4. AE ensures that sensitive data sent to third parties over communication channels such as the internet, WAN links, extranet links are adequately protected from interception and tampering.

7.4.5. Where large volumes of data, in the form of entire system backups or database dumps, are required to be exchanged with third parties; additional approvals will be required. Third parties must employ enough security controls to protect such data.

7.5. Monitoring, Review and Change Management of Supplier Services

7.5.1. The following parameters may be considered to monitor and review the services, reports and records provided by external parties:

- performance against service levels and reporting following major events.
- noncompliance and issues, e.g., against the SLA or security breaches.
- indications of service improvement opportunities.

7.5.2. Wherever necessary, AE will conduct audits/reviews of third-party services.

7.5.3. AE will monitor changes in supplier services including:

- Changes and enhancement to networks.
- Use of new technologies.
- Adoption of new products or newer versions or releases.
- New development tools and environments.
- Changes to physical location of service facilities.
- Sub-contracting to another supplier.

7.5.4. Changes will be done through addendums in the existing agreements, which obliges suppliers to comply with the Information Security Policy and controls.

8. INFORMATION SECURITY INCIDENT & THREAT MANAGEMENT

8.1. Incident response plan will be documented and regularly updated to guide the response to cybersecurity incidents.

8.2. Schools must follow the Incident Management Process established by AE to guide the actions of school Employees during an incident, including internal reporting to school leadership, AE, Aldar Group Information Security & Risk Management team and notification to ADEK.

8.2.1. Communication regarding cybersecurity incidents must be restricted to relevant internal stakeholders, ADEK, and the directly involved service providers. Schools must not communicate such incidents to any other external parties.

8.2.2. All actions taken in response to a cybersecurity incident must comply with applicable UAE laws and policies, including those set by the Abu Dhabi Digital Authority and the Federal Decree Law No. (34) of 2021 on Combatting Rumors and Cybercrimes.

8.3. Parents must monitor students' usage of digital devices outside of school premises and school hours to ensure safe and appropriate digital behavior.

8.4. Threat Management

8.4.1. AE has implemented threat detection capabilities across HQ and school network to identify compromised or infected devices in real-time. Any incidents identified for suspicious or malicious behavior will trigger an appropriate response as per the Incident Management Procedure.

8.4.2. Threat Management Procedure includes:

- Use of internal sources, such as access control, application and infrastructure logs, IDS, IPS, security tools, Security Information and Event Monitoring (SIEM).
- Use of reliable and relevant external sources, such as security forums, vendors, security organizations and specialist notification services.
- Defined methodology to analyse the threat information periodically.

- Relevant details on identified or collected threats, such as modus operandi, actors, motivation, and type of threats.
- Relevance of the derived intelligence and the action-ability for follow-up (for e.g., SOC, risk management).

8.4.3. Information about existing or emerging threats are collected and analysed to:

- facilitate informed actions to prevent the threats from causing harm to AE.
- reduce the impact of such threats.

8.4.4. It is ensured that threat intelligence is:

- relevant (i.e., related to the protection of the AE).
- insightful (i.e., providing the Company with an accurate and detailed understanding of the threat landscape).
- actionable (i.e., AE can act on information quickly and effectively).

8.4.5. Proactive information on threats:

- Users must subscribe with the providers of threat intelligence to remain updated on incidents and threats related to information security.
- Proactive information about threats must be kept and arranged in a flexible database suitable for formulating business notes and descriptive data for indicators such as the knowledge base.
- Intrusion prevention and detection systems must be updated with proactive threat information and the ability of these systems to detect threats and deal with them effectively must be ascertained.

9. DISASTER RECOVERY MANAGEMENT

9.1. AE has developed a Disaster Recovery Plan for disaster recovery management.

10. HUMAN RESOURCE SECURITY

10.1. Information security awareness trainings will be provided to all third-party Users to ensure that Users are:

10.1.1. Adequately briefed on their security roles and responsibilities.

10.1.2. Provided with guidelines defining these security expectations.

10.1.3. Motivated to fulfil the security Policies of the organisation.

10.1.4. Supported in and educated to exercise a level of security awareness.

10.1.5. Conforming to the terms and conditions of employment and security Policies.

10.2. Information Security Awareness, Education and Training

10.2.1. Each Employee and student will be educated about information security and security awareness through regular awareness material, email flyer, Intranet publications, etc.

10.2.2. The training will cover:

- Stating management’s commitment to information security throughout the Company.
- Best practices towards securing or protecting information belonging to AE and external parties.
- Information Security Policy and Procedures.

- Training records / attendance sheets signed by the trainees.
- Feedback of the training must be taken, and effectiveness of the training must be continuously improved based on the feedback.

10.3. Disciplinary Management

10.3.1. Disciplinary action will be initiated against any breach of AE's Information Security Policy and practices.

10.3.2. The intensity of the disciplinary action taken will be directly proportional to the severity of the offense committed.

10.3.3. Action will be undertaken fairly and appropriately justified. Disciplinary process is intended to act as a deterrent to the Users of the information systems of AE.

10.3.4. Breach of Information Security Policy by a third party e.g., vendor, will be dealt via mechanisms that are agreed with both parties and specifically mentioned in the contract.

11. REMOTE WORKING

11.1. Aldar has established a secure communication channel for remote connection.

11.2. All computers connected to AE internal networks via VPN, or any other technology must use the most up-to-date antivirus software of corporate standard, including PCs.

11.3. Only AE approved VPN clients may be used.

11.4. Respective school Principals must seek parents' consent for all live virtual interactions with invited visitors, inside or outside of class. All such interactions must be formally approved by ADEK, in line with the ADEK Extracurricular Activities and Student Protection Policies.

12. PHYSICAL AND ENVIRONMENTAL SECURITY

12.1. Physical and environmental controls are an integral part of the overall security posture adopted by AE. Each User must ensure that the physical security safeguards implemented by AE are consistently applied and assets are safeguarded from damage or misuse.

12.2. Secure Areas

12.2.1. Information system assets that are critical to the business of AE are housed in designated secure areas and protected with appropriate security barriers and physical entry controls.

12.2.2. The assets are protected from unauthorised physical access and damage. Protective measures are commensurate with the risks and criticality identified for such assets.

12.3. Physical Entry Control to DTS Facilities

12.3.1. Users accessing areas designated with restricted or limited access may only do so if they have been issued special access cards for restricted areas.

12.3.2. Only authorised Employees of vendors or contractors will be allowed to access AE's information systems facilities (limited access zones) and must sign either the main building reception log or the AE Data Center logs, as part of the security control.

12.4. Securing DTS Offices, Rooms, and Facilities

12.4.1. All data centre(s), equipment rooms and telecommunications closets have a documented evacuation plan integrated in the Disaster Recovery Plan.

13. ENDPOINT DEVICE SECURITY

13.1. Mobile Computing Security

13.1.1. Aldar data must not be transported and stored on personal computing devices such as home desktop computers or laptops.

13.1.2. Users must ensure that extra precaution is taken while working on information on laptops and iPads in public areas and ensure the following:

- Devices must not be left switched on, unlocked and unattended.
- Users must be wary of shoulder surfers.
- Devices must not be left unattended while travelling or transported in checked in luggage.

13.1.3. Users must ensure that all laptop devices, iPads, and other mobile computing devices are physically secure.

13.1.4. Any lost or stolen devices must be immediately reported to Aldar Education at sd@aldareducation.com.

13.1.5. Secure communication and collaboration platforms are in place to protect sensitive educational information shared among students and staff.

13.2. BYOD and Personal Device Usage

13.2.1. Personal devices used to access AE systems must comply with minimum security requirements, including up-to-date antivirus software, secure configurations, and approved device specifications.

14. PASSWORD MANAGEMENT

14.1. Passwords are an integral aspect of computer security. They are the front line of protection for User accounts. A poorly chosen password may result in the compromise of AE's entire corporate network, systems, and applications. As such, all Users of AE’s information systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

14.2. Minimum Standard for Password Protection

14.2.1. Users must always keep AE system access passwords confidential.

14.2.2. Passwords must not be shared under any circumstances. Each User must hold an individual account to ensure accountability and non-repudiation of transactions.

14.2.3. Users must ensure that passwords are not guessable i.e., using only simple dictionary words, names, and simple sequences of numbers or letters on the keyboard. Passwords must not be based on personal information, names of family, friends, relations, colleagues, etc.

14.2.4. Users must ensure that they do not use passwords for AE systems that are the same as passwords used for personal internet accounts such as Hotmail, Yahoo mail, Gmail, and social networking sites.

14.2.5. All Users must ensure that passwords are not printed, written down or stored in visible or accessible areas.

14.3. Reset of Passwords

14.3.1. Password reset for students will be managed by the school in a secure manner, with details communicated directly to parents as appropriate.

15. ANTI-VIRUS MANAGEMENT

15.1. AE ensures that consolidated endpoint protection software is installed and active on every machine including school managed devices. Next-generation firewalls and intrusion detection / prevention systems are enabled at the network layer. Such a system must provide for protection against viruses, spyware, mobile code, and intrusion attempts.

15.2. All files or data obtained from external sources, regardless of the storage media, must be scanned for viruses before being used.

16. SYSTEM LOGGING

16.1. Log Retention and its Protection

16.1.1. All audit logs recording exceptions and other security-relevant events will be produced for critical systems and kept for an agreed period to assist in future investigations and monitoring.

16.1.2. All logs and records must be maintained on the system. In case of capacity restrictions, log must be archived and stored via retrievable methods. Logs must not be deleted without verifying the retention requirements from Business, Internal Audit, and Digital Security & Risk Management.

17. SOFTWARE USAGES

17.1. Users must not duplicate any licensed software or related documentation for use either on the AE network or elsewhere unless it is expressly authorised to do so by agreement with the licenser. Unauthorised duplication of software may subject Users and/or AE to both civil and criminal penalties.

17.2. Users must not give software to any third party, including clients, contractors, friends, relative, personal use of Employees etc. AE Users must use software on local area networks or on multiple machines only in accordance with applicable license agreements.

17.3. Only software’s that has been approved by DTS Department must be used.

17.4. AE computers are Company-owned assets and must be kept both software legal and virus free.

17.5. Users must not bring software from home and load it onto AE computers. Company-owned software’s must not be taken home and loaded on a User's home computer.

17.6. DTS Department reserves the right to conduct periodic audits on AE computers, including laptops, to ensure compliance with software licenses.

18. CRYPTOGRAPHY

18.1. Decision on requirements of information encryption must be made considering the following criteria:

18.1.1. Risks in transmitting information internally and externally.

18.1.2. Risk in storing the information and access control.

18.1.3. Protection of information held on mobile User endpoint devices or storage media and transmitted over networks to such devices or storage media.

18.2. Sensitive data must be encrypted at rest and in transits.

C. DEFINITIONS

Term or Abbreviation	Definition
ADEK	Abu Dhabi Department of Education and Knowledge.
AE or Company	Refers to Aldar Education including all Aldar Education Operated Schools, Managed Schools, and ATA.
ATA	Refers to Aldar Training Academy managed by Aldar Education.
/	It implies ‘or’ and is used to link the alternatives.
CD	Continuous Delivery.
CI	Continuous Integration.
CIA	Confidentiality, Integrity, and Availability.
COBIT	Control Objectives for Information and Related Technologies.
Department	An organisational unit of the Company, which forms part of a Division. A Department falls under the leadership of a head position or higher, who reports directly to the Executive Manager of the Division.
Division	A vertical organisational unit of the Company, which falls under the leadership of an Executive Manager who reports directly to the CEO, and which may have subordinate Departments.
DNS	Domain Name System.
DTS	Digital & Technology Services Department of Aldar Education.
Employee	Includes temporary, permanent, full-time and part-time employees.
Executive Manager / EM	An individual holding the title of Chief, Director, or other title, in a leadership position of a Division, reporting directly to the CEO.
Framework	A specialised type of Policy which contains a logical structure developed to organize other Instruments into a plan, hierarchy, or structure.
Governing Instrument	Any document that establishes the rules, principles, or guidelines that the Policy/Framework must be aligned with.
HQ	Refers to Aldar Education Head Quarter / head office.
IDS	Intrusion Detection System.
Instrument	A document to provide guidance, impose obligations, define responsibilities or delegate authorities, such as, Framework, Policy, SOPs, etc.

Term or Abbreviation	Definition
IPS	Intrusion Prevention System.
ISO	International Organization for Standardization.
Managed Schools	Refers to ADNOC or ADEK schools that are managed by Aldar Education. Specific areas of responsibilities will be governed by the respective legal agreements entered into with these entities.
Operated Schools	Refers to schools that are fully owned and directly operated by AE.
PC	Personal Computer.
PII	Personally Identifiable Information.
Policy / Policy Manual	An Instrument containing statements of principles, business rules, or internal controls articulated and aligned with legal, regulatory, or organizational requirements, and by which Aldar will be guided in the management of its affairs and the development of its Procedures.
Procedure / Standard Operating Procedure (SOP)	An Instrument which describes the activities necessary to implement a Policy, focused on the responsibilities and requirements to carry out tasks, activities and processes.
Process	A series of tasks to be undertaken to carry out operational task, eventually achieve the intended results or outputs, and contribute to the successful operation of the Group. The process also identifies specific responsibilities and supporting documents necessary for its full implementation and maintenance.
SIEM	Security Information and Event Monitoring.
SLA	Service Level Agreement.
Supporting Documents	Documents which support the implementation of Instruments. Supporting Documents include but are not limited to guidelines, forms, templates, SOPs or any ‘uncontrolled’ documents (E.g., system generated or external).
User / End User(s)	Ultimate final consumer or user of a product, system, or service. These are individuals who interact directly with the final software application, hardware device, or digital service, utilizing its features and functionalities to meet their specific needs or requirements.
VPN	Virtual Private Network.
WAN	Wide Area Network.

D. APPENDIX

1. RELATED ISO CERTIFICATIONS

1.1. Clause 5.3 Organizational Roles, Responsibilities, and authorities
1.2. A.5.2 Information Security Roles and Responsibilities
1.3. Clause 5.1 Leadership and Commitment
1.4. Clause 5.2 Policy
1.5. Clause 6.1.2 Information security risk assessment
1.6. Clause 6.1.3 Information Security Risk Treatment
1.7. Clause 9.1 Monitoring, measurement, analysis, and evaluation
1.8. A.5.1 Policies for information security
1.9. A.5.2 Information security roles and responsibilities
1.10. A.5.3 Segregation of duties
1.11. A.5.4 Management responsibilities
1.12. A.5.5 Contact with authorities
1.13. A.5.6 Contact with special interest groups
1.14. A.5.7 Threat intelligence
1.15. A.5.8 Information security in project management
1.16. A.5.12 Classification of information
1.17. A.5.13 Labelling of Information
1.18. A.5.14 Information transfer
1.19. A.5.15 Access control
1.20. A.5.16 Identity management
1.21. A.5.17 Authentication of information
1.22. A.5.18 Access rights
1.23. A.8.2 Privileged access rights
1.24. A.8.3 Information access restriction
1.25. A.8.4 Access to source code
1.26. A.8.5 Secure authentication
1.27. A.8.18 Use of privileged utility programs
1.28. A.5.19 Information security policy for supplier relationships
1.29. A.5.20 Address security within supplier agreements
1.30. A.5.21 Managing information security in the ICT supply chain
1.31. A.5.22 Monitoring, review, and change management of supplier services
1.32. A.5.23 Information security for use of cloud services
1.33. A.5.24 Information security incident management planning and preparation

1.34. A.5.25 Assessment and decision on information security events
1.35. A.5.26 Response to information security incidents
1.36. A.5.27 Learning from information security incidents
1.37. A.5.28 Collection of evidence
1.38. A.6.8 Information security event reporting
1.39. A.5.29 Information security during disruption
1.40. A.5.30 ICT readiness for business continuity
1.41. A.8.14 Redundancy of information processing facilities
1.42. A.5.31 Identification of applicable legislation and contractual requirements
1.43. A.5.32 Intellectual property rights
1.44. A.5.33 Protection of records
1.45. A.5.34 Privacy and protection of PII
1.46. A.5.35 Independent review of information security
1.47. A.5.36 Compliance with security policies and standards
1.48. A.8.8 Management of technical vulnerabilities
1.49. A.8.34 Protection of information systems during audit testing
1.50. A.6.1 Screening
1.51. A.6.2 Terms and conditions of employment
1.52. A.6.3 Information security awareness, education, and training
1.53. A.6.4 Disciplinary process
1.54. A.6.5 Responsibilities after termination or change of employment
1.55. A.6.6 Confidentiality or nondisclosure agreements
1.56. A.6.7 Remote Working
1.57. A.7.1 Physical security perimeter
1.58. A.7.2 Physical entry controls
1.59. A.7.3 Securing offices, rooms and facilities
1.60. A.7.4 Physical security monitoring
1.61. A.7.5 Protecting against physical and environmental threats
1.62. A.7.6 Working in secure areas
1.63. A.7.7 Clear desk and clear screen
1.64. A.7.8 Equipment siting and protection
1.65. A.7.9 Security of assets off-premises
1.66. A.7.10 Storage media
1.67. A.7.11 Supporting utilities
1.68. A.7.12 Cabling security
1.69. A.7.13 Equipment maintenance

1.70. A.7.14 Secure disposal or reuse of equipment
1.71. A.8.1 User endpoint devices
1.72. A.8.6 Capacity management
1.73. A.8.7 Protection against malware
1.74. A.8.8 Management of technical vulnerabilities
1.75. A.8.9 Configuration management
1.76. A.8.10 Information deletion
1.77. A.8.11 Data masking
1.78. A.8.12 Data leakage prevention
1.79. A.8.13 Information backup
1.80. A.8.15 Logging
1.81. A.8.16 Monitoring activities
1.82. A.8.17 Clock synchronization
1.83. A.8.19 Installation of software on operational systems
1.84. A.8.20 Network controls
1.85. A.8.21 Security of network services
1.86. A.8.22 Segregation in networks
1.87. A.8.23 Web filtering
1.88. A.8.24 Use of cryptography
1.89. A.8.25 Secure development lifecycle
1.90. A.8.26 Application security requirements
1.91. A.8.27 Secure system architecture and engineering principles
1.92. A.8.28 Secure coding
1.93. A.8.29 Security testing in development and acceptance
1.94. A.8.30 Outsourced development
1.95. A.8.31 Separation of development, test, and production environments
1.96. A.8.32 Change management
1.97. A.8.33 Test information