AL ZUHOUR PRIVATE SCHOOL

IT Security and Privacy Policy

JUNE 24, 2025

ICT & IT DEPARTMENT

Backup Policy

Overview

The AL ZUHOUR PVT. SCHOOL IT Systems Department maintains systems to hold and retain all essential data for each individual department. This storage area, or group drive as it is referred to, is used to securely store all data for any given department. Because of this centralized storage arrangement, the AL ZUHOUR PVT. SCHOOL IT Department can offer secure backup capability ensuring all data will be accessible in the event of a disaster or other event in which the data would be destroyed.

This policy establishes regular backup schedules for our group drive storage devices and pertains to all this data. With that said, this does not pertain to individual, departmental, or computer lab devices, mobile devices, or other portable storage medium where the data resides locally on the device or medium. The AL ZUHOUR PVT. SCHOOL IT Department does not guarantee backup for these types devices or storage medium.

Policy

Every effort shall be made by the individual departments and employees at AL ZUHOUR PVT. SCHOOL to store sensitive, important, confidential data on their respective group drive. As mentioned above, the AL ZUHOUR PVT. SCHOOL IT Department cannot be held liable for issues with data stored elsewhere.

Regular backup schedules are in place within the group drive storage device to ensure that backups occur at regular intervals and over a time span to provide ample opportunity for the AL ZUHOUR PVT. SCHOOL IT Department to recover a file, folder, or group of such. It should be noted that the AL ZUHOUR PVT. SCHOOL IT Department does require immediate notification in the event a file, folder, or collection of either is found to be missing, corrupt, or otherwise damaged. Waiting to inform the AL ZUHOUR PVT. SCHOOL IT Department decreases the probability of successful recovery.

Specific information regarding backup restoration on an institution scale can be found in the AL ZUHOUR PVT. SCHOOL IT Department's Disaster Recovery Plan (DRP) or the associated Backup Priority List (BPL). These deal with catastrophic recovery needs that affect multiple departments or the institution.

The hardware that the AL ZUHOUR PVT. SCHOOL IT Department uses consists of the NAS storage system which is scheduled for daily auto backup at 08:00pm. These devices is placed in the server area of the IT department. The primary storage will be the File server and the secondary will be the NAS storage device. Backup retention period will be 90 days after which it will be overwritten with new data.

The primary device at the premises holds all data and backups and serves as the primary device for file access and immediate backup. The secondary in-site device NAS device replicates all data from the primary device to create a stable in-site copy of the data and backups present on the File server device.

For this document, considering the type of hardware described above, normal backups do not necessarily retain the same meaning as when used in conjunction with other hardware devices. Because of this, the following descriptions are provided, based on the current hardware being used, to better understand the overall backup process.

Data Retention Policy

Overview

This policy will determine how long data shall be retained under the guidelines of institutional policies as dictated herein.

Policy

All data shall be retained, at minimum, the time frame as specified in any current, standing institutional policy. No data residing within any AL ZUHOUR PVT. SCHOOL facility or technology equipment will knowingly be destroyed prior to this timeframe unless modified policies are in place which reflect a new time frame. If such changes do occur, the new timeframe will be susceptible to the new policy and all data will be retained within the new specifications.

Under no circumstances is data to be removed, discarded, disposed of, or otherwise destroyed that will compromise legal compliance, data integrity, or institutional needs. The AL ZUHOUR PVT. SCHOOL IT Department shall make every effort to extend the data retention timeframes of all data if sthe institution requires access without compromising any legal statues set forth regarding storage or destruction of such data. No data will be destroyed prior to or retained longer than any legal requirement dictates.

The AL ZUHOUR PVT. SCHOOL IT Department will continually utilize backup equipment, and regular backup schedules to ensure that critical data is retained and kept from corruption or other types of data loss. Every effort shall be made to ensure the institutional data needs are given top priority in the event of a loss of data, corruption of data, or if data recovery is necessary.

This policy shall never decrease the retention time, but may only increase the retention timeframe required by the institution. This increase may only be applicable as long as it does not compromise the integrity, storage capability, or otherwise degrade the overall storage capability of the system being used.

Electronic Communications Policy

Overview

Electronic communication is necessary to fulfill multiple roles and activities here at AL ZUHOUR PVT. SCHOOL. Because of the varied types of electronic communication, we will focus on those used primarily here at AL ZUHOUR PVT. SCHOOL:

- Email
- Videoconferencing
- Digital Signage
- SMS

Email is the official method of communication at AL ZUHOUR PVT. SCHOOL, both for students and employees. Business is conducted every day via email. Since email has both positive and negative connotations, it is imperative that we recognize that the positive aspects greatly outweigh the negative aspects. However, we must also realize that the negative aspects exist and ensure that this method of communication is used effectively, efficiently, and for its intended purpose.

Videoconferencing equipment is used to facilitate conferences and meetings with other institutions, state agencies, or other third-party entities. Since this type of communication conveys not only audio, but video as well, it is particularly important for it to be used for its intended purposes.

Digital signage is used on campus to convey student activities, important academic dates, campus events, and other information to students, employees, and visitors. Since this is also a visual and auditory communication mechanism, it is also important to ensure it is used for its intended purpose as well.

Policy

Regardless of the type of technology being used, electronic communication is meant to serve the needs of the School by sharing information with students, employees, vendors, other state agencies, campus visitors, and other individuals. Because of the unique capabilities of each system it is important to realize that each type of communication method contains unique issues that must be addressed on a case-by- case basis; however, general rules can be set forth to ensure that any communication method is used wisely and according to its intended purpose.

In general, AL ZUHOUR PVT. SCHOOL's electronic communication mechanisms are to be used to share information with students, employees, vendors, other state agencies, campus visitors, and other individuals.

It is also important to note that the true definition of information sharing at AL ZUHOUR PVT. SCHOOL is to adequately convey the appropriate knowledge so that the school mission is not hindered but enhanced. This information is always to be distributed under the following assumptions:

Electronic communication from a AL ZUHOUR PVT. SCHOOL resource…

- …is always understood to represent an official statement from the institution.
- …shall never be used for the creation or distribution of any information that meets the following criteria:
  - Disruptive
  - Offensive
  - Derogatory
  - Specific comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
  - Any information that could be used to sabotage institutional progress
  - Any personally identifiable information
- …shall not be used for personal gain
- …shall not be used extensively for personal use
- …shall not be used to distribute malicious or harmful software or information.

Illegal File Sharing

Overview

Legal compliance is a primary focus at AL ZUHOUR PVT. SCHOOL. Because of this, we have set forth this policy which addresses illegal file sharing, legal alternatives to illegal file sharing, and disciplinary actions on violation.

This policy applies to all AL ZUHOUR PVT. SCHOOL employees, students, vendors, or visitors utilizing AL ZUHOUR PVT. SCHOOL-owned computers, equipment, or the AL ZUHOUR PVT. SCHOOL network.

Policy

File sharing (peer-to-peer) software programs have led to significant increases in anti-piracy efforts and legislation. Peer-to-peer software allows the sharing of files often consisting of copyrighted content such as music, movies, and software which usually occurs without the consent of the owner.

It is the policy of AL ZUHOUR PVT. SCHOOL to respect copyright ownership and protections given to authors, owners, publishers, and creators of copyrighted work. It is against AL ZUHOUR PVT. SCHOOL policy for any employee, student, affiliate, or visitor to copy, reproduce, or distribute any copyrighted materials on AL ZUHOUR PVT. SCHOOL-owned equipment or the AL ZUHOUR PVT. SCHOOL-managed network unless expressly permitted by the owner of such work.

AL ZUHOUR PVT. SCHOOL also discourages the use of any file-sharing program as these types of programs may allow copyrighted material to be downloaded to a AL ZUHOUR PVT. SCHOOL-owned computer or device. Many of these programs automatically place downloaded files in a shared folder on your computer, which means you could be sharing files without your knowledge. This also means that you may be held responsible for illegal file sharing, whether you are aware that copyrighted files are being shared or not.

AL ZUHOUR PVT. SCHOOL also employs the use of network appliances, equipment, and rules to limit the amount of file- sharing traffic on the AL ZUHOUR PVT. SCHOOL network. Active blocking of peer-to-peer traffic is used to protect the AL ZUHOUR PVT. SCHOOL network from unwanted traffic and the presence of potentially malicious files introduced through file- sharing programs.

Information Sensitivity Policy

Overview

Information sensitivity is a primary focus at AL ZUHOUR PVT. SCHOOL. Since we are an educational entity, we deal with many different types of information, some for public use, some not. To make these distinctions, this document will address both types of information.

This policy is intended to help employees determine what information can be disclosed to non- employees, as well as the relative sensitivity of information that should not be disclosed outside of AL ZUHOUR PVT. SCHOOL without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as via phone and videoconferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect confidential information (e.g. confidential information should not be left unattended in conference rooms.).

NOTE: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your supervisor or the AL ZUHOUR PVT. SCHOOL IT Department. Questions about these guidelines should be addressed to the AL ZUHOUR PVT. SCHOOL IT Department.

Policy

By grouping information into two different categories, we can adequately address the needs of each type of information. The first type, public Information, is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the institution. The second type, confidential information contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information and should be protected in a more secure manner. Included is information that should be protected very closely, such as specific personnel information, student data, billing information, etc. Also included in confidential information is information that is less critical, such as telephone directories, personnel information, etc., which does not require as stringent a degree of protection.

A subset of the latter is third-party confidential information. This is confidential information belonging to or pertaining to another corporation which has been entrusted to AL ZUHOUR PVT. SCHOOL by that company under non- disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into AL ZUHOUR PVT. SCHOOL's network to support our operations

AL ZUHOUR PVT. SCHOOL personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor and/or the AL ZUHOUR PVT. SCHOOL IT Department for more information and instructions on how this information should be handled.

The sensitivity guidelines below provide details on how to protect information at various sensitivity levels. Use these guidelines as a reference only, like AL ZUHOUR PVT. SCHOOL Confidential Information at each level may necessitate stringent measures of protection depending upon the circumstances and the nature of the AL ZUHOUR PVT. SCHOOL Confidential Information in question.

- Minimal Sensitivity
    - Description: General information, some personnel, and technical information.
    - Access: AL ZUHOUR PVT. SCHOOL employees, associates, or third parties with a business need to know.
    - Distribution internal to AL ZUHOUR PVT. SCHOOL: Approved electronic mail and approved electronic file transmission methods.
    - Distribution external to AL ZUHOUR PVT. SCHOOL: Approved electronic mail and approved electronic file transmission methods.
    - Storage: When viewing data, do not allow viewing by unauthorized individuals. Do not leave data open and/or unattended in any format. Protect data from loss, theft, or misplacement. Electronic information should have individual access controls where possible and appropriate.
    - Disposal/Destruction: Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy should be observed for original copies.
- More Sensitive
    - Description: Business, financial, technical, and most personnel information.
    - Access: AL ZUHOUR PVT. SCHOOL employees, associates, or third parties with signed non-disclosure agreements with a business need to know.
    - Distribution internal to AL ZUHOUR PVT. SCHOOL: Approved electronic file transmission methods.
    - Distribution external to AL ZUHOUR PVT. SCHOOL: Approved electronic file transmission methods via a private link to approved recipients external to AL ZUHOUR PVT. SCHOOL locations.
    - Storage: Individual access controls are highly recommended for more sensitive electronic information.

- Disposal/Destruction: Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy should be observed for original copies.

- Most Sensitive

  - Description: Operational, personnel, financial, source code, & technical information integral to the security of the institution.

  - Access: Only those individuals (AL ZUHOUR PVT. SCHOOL employees and associates) designated with approved access and signed non-disclosure agreements.

  - Distribution internal to AL ZUHOUR PVT. SCHOOL: Approved electronic file transmission methods.

  - Distribution external to AL ZUHOUR PVT. SCHOOL: Approved electronic file transmission methods to recipients within AL ZUHOUR PVT. SCHOOL. Strong encryption is highly recommended.

  - Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored on a physically secured computer.

  - Disposal/Destruction: A necessity. Electronic data should be permanently expunged or cleared. Reliably erase or physically destroy media. Data retention policy and federal and state retention guidelines should be observed for original copies.

Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of AL ZUHOUR PVT. SCHOOL's entire network. As such, all AL ZUHOUR PVT. SCHOOL employees (including contractors and vendors with access to AL ZUHOUR PVT. SCHOOL systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that belongs to AL ZUHOUR PVT. SCHOOL, resides at any AL ZUHOUR PVT. SCHOOL location, has access to the AL ZUHOUR PVT. SCHOOL network, or stores any AL ZUHOUR PVT. SCHOOL information.

Policy

All passwords will meet the following criteria:

- All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days.
- Passwords must NOT be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

Passwords are used for various purposes at AL ZUHOUR PVT. SCHOOL. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every AL ZUHOUR PVT. SCHOOL employee should know how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password or a subset of the password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software
    - The words "AL ZUHOUR PVT. SCHOOL", "Connors", "state", “School” or any derivation
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret) Strong passwords

have the following characteristics:

- Contain between 8 and 32 characters
- Contain both upper- and lower-case characters (e.g., a-z, A-Z)

- Contain at least one number (e.g., 0-9)
- Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
- Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
- Does not contain personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Please do not use either of these examples as passwords!
Do not use the same password for AL ZUHOUR PVT. SCHOOL accounts as for other non-AL ZUHOUR PVT. SCHOOL access. Do not share AL ZUHOUR PVT. SCHOOL passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential AL ZUHOUR PVT. SCHOOL information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to a supervisor.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers.
- Don’t reveal a password to vendors.
- In short, don’t reveal a password to ANYONE.
- Do not use the "Remember Password" feature of applications.
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer.

Other items to remember:

- If someone demands a password, refer them to this document or have them call the AL ZUHOUR PVT. SCHOOL IT Department to determine the validity of their request.
- If an account or password is suspected to have been compromised, report the incident to the AL ZUHOUR PVT. SCHOOL IT Department immediately and change all passwords as soon as possible.

Password cracking or guessing may be performed on a periodic or random basis by the AL ZUHOUR PVT. SCHOOL IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.
Never give your password out to anyone. This may or may not include your supervisor, a friend or relative, a student or part-time worker, or even a co-worker.

Physical Security Policy

Overview

This policy will establish physical security guidelines that apply to all computing and networking equipment locations. It is important to note that incremental degrees of security will be needed for each area depending on the actual equipment configuration and critical need to the institution.

Policy

All areas will be classified into two categories:

- Office
- Restricted

Office areas are simply that, office locations for AL ZUHOUR PVT. SCHOOL IT Department employees. These areas contain computing equipment and other data that should be always protected.

Restricted areas are those areas that belong to the AL ZUHOUR PVT. SCHOOL IT Department and contain equipment owned and/or operated by the AL ZUHOUR PVT. SCHOOL IT Department or a third-party vendor (i.e. Etisalat) such as:

- Switch closets
- Server rooms
- IT Department storage areas

At the time of this policy, our current physical security offerings are somewhat limited so more advanced options cannot currently be used. As upgrades occur, recommended options will be changed to required options to increase and enhance security.

At minimum, all office and restricted locations require the following security mechanisms:

- Solid wood or steel door
- Either keyed handle or deadbolt lock

All AL ZUHOUR PVT. SCHOOL IT Department restricted, and office locations should contain the following recommended security mechanisms:

- Reinforced steel doors and frames
- Keyed deadbolt locks
- ID card access
- Steel bars over windows.

Wireless Communication Policy

Overview

Wireless implementations are a benefit to AL ZUHOUR PVT. SCHOOL as well as its faculty, staff, and students. Maintaining this equipment can be a tedious process but is a necessity.

At present, this policy allows access to the AL ZUHOUR PVT. SCHOOL wireless network via any data communication device containing the hardware required to connect. Connecting to the AL ZUHOUR PVT. SCHOOL wireless network does not grant a user access to the internal networking infrastructure or any internal information of AL ZUHOUR PVT. SCHOOL, only external access to the internet. Utilizing AL ZUHOUR PVT. SCHOOL's wireless network for access to the internal network and/or information requires credentials that must be obtained through the AL ZUHOUR PVT. SCHOOL IT Department.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of AL ZUHOUR PVT. SCHOOL's wireless networking access points. This includes any form of wireless data communication device capable of transmitting packet data.

Policy

All wireless data communication devices connected with AL ZUHOUR PVT. SCHOOL's wireless network will be required to have current virus-scanning software installed with the most recent updates and perform a full scan a minimum of once per week.

All wireless data communication devices connected with AL ZUHOUR PVT. SCHOOL's wireless network that require access to AL ZUHOUR PVT. SCHOOL's internal network and/or information will be required to utilize specific software and/or access credentials obtained through the AL ZUHOUR PVT. SCHOOL IT Department to do so.

At no time shall any device connected to the AL ZUHOUR PVT. SCHOOL wireless network operate outside the parameters defined in the Acceptable Use Policy provided herein. All wirelessly connected devices may be monitored and their information such as IP address, MAC address, general hardware profile, etc. be archived for future use. Random scans may also be performed to ensure the security of the wireless networks and connected devices and to obtain a general device survey to further enhance the accessibility and usability of AL ZUHOUR PVT. SCHOOL's wireless networks.