Chinle Unified School District # 24
Information technology Department
Computer Services Department

User Account Management Policy

DEFINITION

New user account policy and access to network resources (i.e., email, mainframe, Student database, Power School, Finance Systems, Active Directory, file shares, etc…) will be granted after proper paperwork has been submitted and approved. Each user will be issued his/her own account to access network resources. User accounts shall not be shared. Users will be responsible for maintaining a strong password on their account to prevent possible misuse of their account this password MUST meet the (Company Name) Password Policy.

ACCOUNT CREATION

All users requesting an account on the (Company Name) network MUST submit a new user account form prior to receiving their account. This includes, but is not limited to; Staff, Interns, and Part Time Employees. No account will be created until the new user account form has been approved and submitted to IT Department.

- The new user account form must be filled out completely and signed by the new user's manager.
- The new user account form may be faxed to IT Department after obtaining signatures, and an EIS but original must be submitted in person or by regular mail.
- The new user MUST read and signed the Acceptable Use Policy and Procedures.
- The new user MUST read and signed the Non-Disclosure Agreement.
- The new user MUST read and signed the Policy Statement on Insider Trading.
- The user can NOT outsource data using District Computers and Networks without permission from the IT department and Superintendent in duty; otherwise will be consider hacking, stealing, data from District Server banks.

ACCOUNT DELETION

IT Department will be notified by Human Resources (HR) immediately, with a list of user(s) that have left the company. If the IT Department has not received this list by the HR, a reminder email will be sent to HR requesting this information. After the completion of each month, the Payroll Department will provide a list of the most current employees on the payroll, including full and part time staff.

- User accounts, whose names are on the list provided by Human Resources, will be disabled for 30 days prior to deleting the user account, email and web accounts.
- User accounts, whose names are not on the most current payroll, will be disabled for 30 days prior to deleting the user account, email and web accounts.

ACCOUNT PERMISSION CHANGES

IT Department will be notified 7 days in advance when a user will be changing departments in order to get their new permission and move them into the current Organizational Unit (OU).

- The new user account form must be filled out completely and signed by the new user's manager.

The new user account form may be faxed to IT Department after obtaining signatures, but original must be submitted in person or by regular mail.

USER'S ACCESS IN CORE SERVER'S

All technical staff accessing Servers that is consider core servers, must create, sign and produce a log in hard copy the reason, activities, changes done while they were in Server, Server room, Server Farm and or Main MDF were Server is located. Document or report produce must include Location, Device IP and Model, Serial Number and activities done on devices.

- Every month the department Director will review documentation and evaluate the integrity of the security and amend if necessary to protect information saved at each Server, SAN, SQL, Oracle, VM Ware data banks and any new devices consider data storage.

PASSWORDS MANAGMENT

CUSD # 24 retains and supports the district school technology local and district level. Access to the network is required to be member of an OU, or user of CUSD to have access to resources in place.

Administrators Passwords or core Passwords is only assigned to 3 members of the District that includes Superintendent of Business, IT Director, and ADM for student access databanks.

PowerUsers and domain Passwords is assigned to the IT department Technical Staff to maintain support our school networks and devices.

Local OU Group Administrator is assigned to the local technical staff assigned at each School.

General Staff Users must have a username, member of a group and password to access their resource assigned to them.

- Every 6 months, all users in the Active Directory must change their password. The passwords must follow Microsoft recommendation and encryptions.
- All users must have an EIS signed before access is given to technology resources.

ACCOUNT MAINTENANCE

Routine account maintenance will be performed to remove disabled accounts and accounts that have not been used in the three month.

- Every 3 months, January, April, July and October, a list of Windows Active Directory user's accounts will be generated. Disabled accounts older that three months, will be deleted.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY:

Release No.	Date	Revision Description

REVIEW SCHEDULE

Email HR for an updated list of employee's – Monthly
Review and removal or disabled user accounts – Quarterly

OWNER

Chinle Unified School District # 24
IT/Computer Services.

DELEGATED OWNER

Network Manager/ IT Director
Victor Trejo