Polk State College Computer Network Guidelines

The Polk State College computer network includes an ERP system, file servers, printers, personal computers, network routers/switches, UPS systems, and network cabling. File servers and the ERP system provide employees with access to networked applications/records and access to specific network directories and files.

The College provides all of its employees with college network and internet access to facilitate work related functions and duties.

Inappropriate college network and software usage will result in the loss of network access and appropriate disciplinary action, including the possibility of termination.

I – Procedure Purpose

The purpose of the Network and Account Guidelines is to provide a secure computer network environment for the College's technology infrastructure.

II. Network Account Creation

- User IDs and passwords provide controlled access to all College Technology resources.

- For an employee to gain network access, Technology Services will assign a user ID upon receipt of a completed Network Security Request Form that is received via the Human Resources onboarding processes. To insure timely access to the Polk State network and ERP system(s), Human Resources will enter new employee information into the "RedCarpet" onboarding portal and the new employee access form will be sent to hiring manager once the employee is authorized for employment.

- An employee's job function and department requirements, identified by the supervisor, will determine the level of access to network directories and applications. Exceptions and additional access may be granted to employees upon supervisory request and data owner approval.

- All network accounts require both a user ID and a password.

II - Account Logins

- Each employee is assigned a user ID and password and is held responsible for all actions performed and all data which is modified or retrieved under their user ID and password.

- User IDs, accounts or passwords will not be shared with another person under **any** circumstances. When login information is shared with Technology Services staff for technical support purposes, a password change will be required upon completion of the work.

- Administrator passwords for local workstations attached to the Polk State College network will only be known by Technology Services staff and will not be shared with any other person under any circumstances.
- Administrator Domain passwords will only be known by the Chief Information Officer, Manager of Computing Systems, and the Network Engineer. The account(s) or passwords will not be shared with another person under any circumstances.

- Users are limited to three incorrect sign-on attempts. After the third attempt the account is automatically suspended. Employees must call the College Help Desk to have the account re-activated.

- User IDs or passwords may not be embedded in a procedure, program, function key, logon profile or script, or non-encrypted password file.

III - Account Passwords

- All accounts will require both a username and a password.

- Passwords must be 8 characters or more.

- Network passwords must be changed every 60 days.

- Passwords shall contain a combination of letters, numbers, and special characters.

- Passwords shall never be written down or emailed.*

- Passwords shall not be common words used at College, family member's names, sports teams, bank or personal identification numbers.

- Passwords will retain a history; this will not allow previous passwords to be used until the ninth password change.

- No program, procedure, hardcopy report, terminal, monitor, or computer screen may display or echo a password.

- If a password needs to be reset, the employee requesting the password reset must be present, or verify identity, in order to complete the request.

- There will be a mandatory password change the first time a customer logs onto the Polk State College network. After the initial password change the password will need to be changed every 60 days.

IV - Temporary or Contracted Personnel/Vendors

- Temporary or contracted personnel/vendors gain access by the same procedures referenced above for full-time employees.

- All temporary or contracted employees must be issued a College network account to gain access to the College network.
- Upon processing by Human Resources and/or Contract Services, Technology Services will provide a College user ID and password for network access and application use for temporary or contracted employees.

- Temporary or contracted employees will have a non-employee record created in the Human Resources system for tracking purposes.

- No generic logons will be allowed to be created for network logon access.

- Vendor/contractor accounts will automatically be disabled every 60 days, requiring communication between technology services to facilitate ongoing account management for external constituents.

- Upon expiration of contract, the Information Technology department will be notified to disable access for contracted personnel/vendors by the College's contract administrator.

V - Account Modification

- For employees to have changes approved in their level of network access, Technology Services must receive a completed Network Security Change Request Form. The employee's budget head and supervisor must sign the form and submit to Human Resources for processing. No forms submitted directly to Technology Services will be processed as accounts require appropriate HR approval to establish employee status.

- Job function and department requirements, identified by the supervisor, determine the level of access to network directories and applications.

VI - Account Removal

- Upon termination, employees College network access is permanently deleted.

- Technology Services staff is responsible for immediately deleting all network, email, and software access upon notification of voluntary separation or termination from the College by Human Resources. Other College departments that control software, user accounts, and access rights will also be notified through the Human Resources off boarding process.

- Faculty and adjuncts will have their network access removed after twelve months of non-activity on their Human Resource record.

- Monthly security reports will be created and reviewed to validate appropriate user system and network access that may result as employee internal job role/function changes. In this case, the employees will have system or network access immediately deleted and or modified and their supervisors will be notified of the change.

VI- Default and Industry Known User IDs

- Default and industry-known user IDs and passwords should be disabled and or deleted d by approved Polk State College user IDs and passwords performing identical functions.

- If a default user ID cannot be replaced, it should be closely monitored and the associated password or access control changed periodically.

VIII - Account Logoff

- To prevent account and system information from being viewed by anyone other than the user of that account, any information displayed on a terminal or monitor signed onto the ERP system will be locked after fifteen minutes of inactivity. This will require the user to login again to unlock the workstation environment.

- Users shall use the Windows screen saver feature on their workstation to blank out and lock their computer display screen after a period from one to fifteen minutes of inactivity.

IX - Network Usage

- Use of the College network shall be based on college or academic need.

- With the exception of academic reasons, the College prohibits employees from using the Internet to intentionally visit sites that are pornographic, sexually explicit, copyrighted material, known malware, spyware, virus/Trojan sites, racially or ethnically biased or harassing or offensive in any way, either in graphic or text form.

- The College reserves the right to monitor any and all network activities to and from any computer directly connected to the college network, including internet access. Such activities may be archived and monitored at a future date.

- Passwords transmitted or used online should be of different variation from those used within College.

X - Software Usage

- The College will provide licensed software for College-owned personal computers as part of a standard desktop configuration. Any additional software installed on a personal computer will be the responsibility of the department or individual. Software may only be installed in strict accordance with the license agreement accompanying the software.
- Only licensed software or evaluation software compatible with the College network will be installed on College computers.

- Computers and hardware devices that are designated as part of a curriculum may be modified as required by the curriculum. Coordination with Information Technology to ensure that the modifications are not having adverse effects on the College network is the responsibility of the department overseeing the curriculum.

- Computers that do not have active, approved virus detection shall not be connected to the College network.

- Technology Services will configure desktop computers to have active virus detection software.

- Technology Services will configure desktop computers to include virus detection software and update the virus definitions on a daily basis.
- Users must not cancel automatic virus scanning or updating of definitions. If such automatic activity interferes with the user's duties, the user should contact the College Help Desk for additional support.

- All software and files downloaded from non-College sources via the internet (or any other public network) must be screened with College approved virus detection software.

- Users shall not open email attachments with .exe, .vbs or .com extensions and should be aware of the procedure to scan their computer hard drive using College supplied virus detection software.

- The College reserves the right to remove any software that has not been properly approved or is detrimental to the stability of the College network or desktop environment.

XI – Network Performance and Security Port Scanning

- Polk State College will review, on each server, the network performance monitor and will also verify internal and external network bandwidth performance levels.

- Polk State College processes an entire port scan on the PCC network each month for critical servers and key infrastructure components i.e. firewall, switches, and routers. This port scan is incorporated into a scheduled monthly routine.

- The port scan reports and network performance monitor are reviewed by the Technology Services staff and will be brought to the CIO for his/her review as necessary. If any anomalies are recognized in the port scan reports they will be investigated and reviewed by the appropriate appointed individual.

XII - The following activities are **prohibited**:

- Attempts to adversely affect the availability or quality of service of the College network.

- Storing, posting or displaying obscene or offensive data, even temporarily, in areas where someone might view them passively or inadvertently, except in cases where academically necessary.

- Attempts to circumvent established security procedures or to obtain access privileges to which a user is not entitled.

- Attempts to modify computer systems or software in any unauthorized manner.

- Unauthorized access, alteration or destruction of another user’s data, programs or electronic mail.

- Attempts to obtain unauthorized access to either local or remote computer systems or networks.
- Manipulation of others to gain information for the purpose of gaining access to commit fraud or damage to the system.

- Using a program or procedure that looks like a normal logon process but instead records the user’s password and user name.

- Executing any form of network monitoring which will intercept data not intended for the user’s host.

- Attempting port scanning, network sniffing, packet spoofing, denial of service and forged routing information for malicious purposes.

- Using any program, script, command, or sending messages of any kind with the intent to interfere with or disable a user’s network session.

- Theft or destruction of computer hardware or software.

- Any criminal activity or any conduct that violates applicable laws.

*Please contact Technology Services for secure storage of passwords in an encrypted bit locker environment.

Reference: Information Security Guidelines

History: