Access Control Policy

Document Number: ITS-0022 **Date Published(sys):** 4/27/2022

General Description

Purpose:

The purpose of the Access Control Policy is to establish a framework for properly controlling access to Trinity University Information Technology assets in accordance with Trinity University business requirements, and applicable laws and regulations.

This document sets forth the policy for access control within Trinity University. Within this Policy, the terms “Trinity University”, “Trinity” or “TU” may be used interchangeably.

Scope:

This access control policy applies to all Trinity University (TU) staff, executives, faculty, students, and third parties with access to TU’s information technology assets and called from hereinafter TU Community Members.
This policy also applies to all Trinity University Information Technology assets and services storing, processing, or transmitting TU’s information classified as non-public[1] (see “Information Security Policy” for definition of what is a non-public information).

[1] Non-public information: Information that is not made available for public distribution or is not meant for public. Restrictions needs to be applied to the access, use or disclosure of this information. Non-Public Information includes both Protected and Restricted Information.

Exceptions:

Systems owned or managed by a business partner, vendor, or third-party must be handled according to this policy unless contractual obligations and/or third-party requirements come into conflict with this policy’s requirements. In that case, an exception must be submitted to the Chief Information Officer (CIO) office for further examination. The Office of the CIO will notify the requestor if an exemption can be given and any necessary compensating controls. Exceptions must be documented and reviewed on an annual basis.

Policy Content

Management Commitment

The content of this policy was written under the guidance of TU's Information Security Governance Committee and the IT Team Leadership. Trinity University Leadership is committed to protecting the confidentiality, integrity, and availability of Trinity University information assets.

Roles and Responsibilities

Trinity University uses different systems to help create, manage, and distribute organizational information. Several information systems are maintained by TU as part of the core business support program. Some of these, however, are third-party built and managed Software as a Service (SaaS) solutions. Consequently, there are various federated access control systems in use by the organization, each with their own user lists, systems of privileges, and enforcement tools.

To help coordinate a comprehensive access control program across these systems, TU has outlined a system of Data Stewardship within the Information Security Program. The following table outlines the most relevant roles for information management, each carrying its own responsibilities for data security and, correspondingly, access control management:

Role	Definition	Access Control Responsibilities
Chief Information Security Officer (CISO)	Executive designated with overall responsibilities for information security and security program management.	• The CISO or their designee must ensure that Trinity University systems and applications are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication, and implementing access control. • Verify that an inventory of information assets exists and are kept up to date, each asset with their respective Data Stewards. • Ensures that periodic reviews of domain's access control lists are conducted. • Overall ownership and

		management over TU information systems access control program.
Data Owner or Data Trustee	The data owner or trustee is the person/organization that 'owns' the data. It is the department that collected and/or generated the data. Data Trustees work with the CIO to ensure that the appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the entire university.	• Assigning and overseeing Data Stewards. • Overseeing the establishment of data policies in their areas. • Ensuring that data accessed and used by units reporting to them is done so in ways consistent with the mission of the office and the University • Determining legal and regulatory requirements for data in their areas. • Promoting appropriate data use and data quality.
Data Steward	Stewards are university officials, or their designees, who are assigned by the Data Owner or Trustee, having direct operational-level responsibility for the management of one or more types of institutional data. Data Stewards recommend policies to the Data Trustees and establish procedures and guidelines concerning the access to, completeness, accuracy, privacy, and integrity of the data for which they are responsible.	• Assisting in developing and maintaining data classification policies. • Assisting in developing, implementing, and managing data access policies. • Providing communications and education to Data Users on appropriate use and protection of institutional data. • Developing, implementing, and communicating record retention requirements to the university community in conjunction with University Archives. • Review and approve Restricted data usage and use requests. • Ensure that individuals with visibility to social security numbers have completed required training and have signed confidentiality statements. • Maintain a listing of data types stored and/or processed. • Perform periodic reviews to

		ensure continued compliance with the data protection and classification policies and all other university policies.
Data Custodians	Data Custodians are central or distributed university units or computer system administrators responsible for the operation and management of systems and servers which collect, manage, and provide access to institutional data. Data Custodians must be authorized by the appropriate Data Steward. Regular job titles for custodians are system or database administrator, or application access administrators. These are employees responsible to provision, modify and deprovision user access accounts to infrastructure and applications in general.	• Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody. • Complying with applicable university computer security standards. • Managing Data User access as prescribed and authorized by appropriate Data Stewards. • Following data handling and protection policies and procedures established by appropriate Data Stewards. • Administration of the provisioning, modification and deprovisioning of user access to systems and applications as authorized by the Data Steward. • Fulfills / grants / revokes access according to approved privileges. • Periodic review and certification of user access and privileges assigned to systems and applications.
Department Managers	Member of management that is responsible for defining employee responsibilities, managing day-to-day operations of their group, and requesting user access.	• Request data user access in writing, aligned to the Access Control Policy and procedures. • Notifies Human Resources of employee rights changes and/or terminations.
Data User	Person who is authorized to receive, process, or	• Adheres to TU's Acceptable Use Policies regarding the use

	otherwise handle information to fulfill business responsibilities.	of information technology and information. • Observes all relevant information security policies and standards.
Human Resources	Central point of contact for defining organizational roles and profiles, notification of termination of relationship and addressing non-compliant workforce members.	• Ensuring that the IT / Security department is promptly notified of employee or contractor terminations, department transfers, and pending terminations. • Establishing a sanctions policy for violations of the information security policy.

User Responsibilities

It is vital that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organization.
In order to maximize the security of our information every user must:

1. Use a strong password based on the Trinity University Password Policy.
2. Never tell anyone their password or allow anyone else to use their account.
3. Not record the password in writing or electronically where somebody else may have access to.
4. Avoid using the same password for other user accounts, either personal or business-related.
5. Ensure that any PC or device they leave unattended connected to the network is locked or logged out.
6. Inform the ITS Technical Support Services of any changes to their role and access requirements.

Failure to comply with these requirements may result in disciplinary action against the individual(s) concerned.

Policy Statements

General Principles of Identity and Access Management

The following general principles must be used when designing access controls for Trinity University's information systems, applications, and services:

1. Ownership: Each information asset (hardware, operating system, application, etc.) must have corresponding ownership responsibilities identified and documented.
2. Data Owners or their designated Data Stewards must determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the information security risks associated with the classification of the information being protected.
3. Business requirements for access control must be established as part of the requirements-gathering stage of new or significantly changed systems and services and must be incorporated in the resulting design and implementation.
4. Defence in Depth: Security must depend upon multiple layers of controls complementing each other.
5. Least Privilege: By default, the approach taken must assume that access is not required. All access granting systems employed by Trinity University will leverage the “deny all” principle. In other words, systems that enforce access controls will deny all rights, with specific user/role rights and privileges granted by the authority of a Data Steward. Systems that do not authenticate user identity will not be used to process sensitive information.
6. Need to Know: Trinity University must grant and provide access to the information required to perform a role, and no more.
7. Need to Use:
    a. Trinity University users will only be able to access logical systems and information required for their role to fulfill their job requirements.
    b. All access to information resources must be justified and authorized by the employee supervisor before being issued.
8. Segregation of Duty: Trinity must document and implement controls in information systems to enforce segregation of duties through assigned access authorizations, including but not limited to:
    a. The creation of the user account and the assignment of permissions are performed by different people.
    b. Audit functions will not be performed by security personnel responsible for administering information system access.
    c. Critical business ownership and information system management responsibilities will be divided.
    d. Information system testing and production functions between different individuals or groups will be divided; and
    e. An independent entity will conduct information security testing of information systems.
    f. Segregation of duties must be overseen by the Chief Information Security Officer.
9. On a yearly basis IT personnel will review users which are responsible for administration of information systems and ensure that they do not have critical business roles for those same systems.
10. Non-repudiation: User access credentials must be unique and exclusive for the use of each user. Two or more users must not share access accounts.

11. Logging: Access to confidential data must be logged and monitored.

As part of the selection of cloud service providers specifically, the following access-related considerations must always be taken:

a. User registration and deregistration functions must be provided.
b. Process for managing access rights to cloud services must exist.
c. Access to cloud services, cloud service functions and cloud service customer data must be controlled on an as-required basis.
d. Authentication for administrator accounts must support multi-factor authentication.
e. Procedures must exist for the allocation of secret information such as passwords.
f. Addressing these requirements as part of the selection process will ensure that the provisions of this policy can be met in the cloud as well as within on-premises systems.

12. **Training and Awareness:** Before granting access to the infrastructure, or to non-public information systems in Trinity University, the user, privileged or regular, must take mandatory information security training. Please refer to the Information Security Training and Awareness Policy.

User Access Management

1. Formal user access control procedures must be documented, implemented, and kept up to date by ITS for each application and information system, to limit access to information and information resources, ensuring only authorized users can access them. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access.
2. Data Stewards and Data Custodians must ensure that information system accounts are created, enabled, modified, disabled, and removed in accordance with Trinity University access control procedures.
3. Data Stewards and the Information Security team must work together to monitor the use of information system accounts to ensure compliance with this policy.
4. ITS must identify authorized account types to be used (e.g., individual, group, system & administrator, application, guest/anonymous, and temporary) and establish conditions for group membership:

Account Type	Conditions for access and/or membership
Individual: An account which is tied to a single individual and is not tied to any specific application. An example of this type of account is an Active Directory user	A person must be either an employee, a contractor, a faculty member or a student of Trinity or be providing services to Trinity via a third party in order to be

account or an application user account.	granted an individual account.
Group or Generic: An account which represents a group of employees usually belonging to a single department or project. Although this type of account is used by multiple employees, it is usually used only by a single employee at a given time. An example of this type of account is a social media account which is shared by members of the marketing department.	Generic user accounts (i.e. single accounts to be used by a group of people), must not be created as they provide insufficient allocation of responsibility.
System: An account which is not tied to a specific person, but rather a program, system service, application, or automated script.	An employee must be involved in the configuration, maintenance, or implementation of a system to be granted access to a system account. It is prohibited for any user to use a system account to access an information system or application, unless it is required and authorized for maintenance and support activities.
Application: An account which is tied to a specific user and specific application, program, or interface. Application accounts must be avoided, unless the application or system capabilities are limited and does not integrate with a centralized federated or single sign-on system.	An employee must have a business need to access data or make use of the specific application to be granted access.
Guest/Anonymous: An account which is used to grant access to an open system. An example of this type of account would be the guest account for an FTP server which is used to serve public documents such as newsletters.	Guest or anonymous access must be limited to publicly available data only. Guest or anonymous access to internal systems is prohibited.
Temporary: An account which has a limited duration and usually will be assigned to a non-permanent employee such as an intern, contractor, or outside party such as a government auditor.	An employee may be granted temporary access to a system or application when access will only be needed for the duration of a specific project/procedure, but not for the employee's day to day operations for the duration of their employment at Trinity.
System Administration:	System administration accounts must only

User account used for the exclusive purpose of implementing, maintaining, and supporting problem resolution of servers, systems, applications, and other information assets. Examples are Administrator accounts in Windows environments as well as the Root account on Unix/Linux based environments.	be provided to users that are required to perform system administration tasks.

5. Access must be granted based upon the principle of least privilege, access not explicitly permitted must be denied by default.
    a. IT staff must be responsible for implementing access according to least-privilege on system and network resources such file shares, email, remote and desktop access.
    b. Data Stewards must be responsible for implementing least-privilege within applications with assistance from IT.
6. An information security risk assessment must be completed by ITS when new business units or teams are assigned with privileged access to determine and apply any necessary mitigating controls.
7. ITS must regulate information system access and define security requirements for contractors, vendors, and other service providers.
    a. Contractors must be subject to a security questionnaire provided by IT personnel.
    b. Contractors must be subject to the same access control, remote access, and all other policies outlined in the information security policy.

User Registration and Deregistration

1. Access requests must follow the Trinity established approval process.
2. Access requests for users accounts must be documented in writing and stored at least for 12 months after an employee is terminated, transferred, promoted, or otherwise no longer with Trinity University, or for any student after they no longer hold the “student” status.
3. Access requests must include at least the following information:
    a. The name of the employee or student for whom access is being requested.
    b. The department and manager name of the employee, or the Admission Office responsible contact of students, for whom access is being requested.
    c. The system/application/data to which the employee needs access.
    d. The reason and business case/need for the employee to have access.
    e. The level of access requested (user, privileged, reporting, other).
    f. The date of the request.
4. An initial request for access to the organization’s network and computer systems for new employees must be submitted by a supervisor on behalf of the employee.

5. Trinity University Data Owner or Data Trustee or their appointed Data Steward must approve requests to create information system accounts based on a valid access authorization, intended system usage, and other attributes required by the function, before provisioning the user account. Data Stewards and Data Owner or Data Trustees must be identified in an appropriate systems and applications asset inventory.
6. Upon approval all access requests must be sent to the Data Custodians for provisioning. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorization is obtained prior to user account creation.
7. An initial strong password aligned with Trinity University Password Policy must be created on account setup and communicated to the user via secure means (e.g., direct voice call to the phone number provided, provided in person, via SMS to the provided phone number). The user must be required to change the password on first use of the account.
8. Managers, Supervisors, or Human Resources must notify Data Custodians when accounts are no longer required, when users are terminated and transferred, and when individual information system usage or need-to-know changes.
    a. When employees change departments, are promoted, transferred, or reassigned they will be stripped of all accounts and permissions with the only exception being their Active Directory account for email access. Their new manager will be responsible for submitting new access requests for all required systems and applications.
    b. Upon notification from HR and/or a Department Manager, IT staff must revoke all group membership within Active Directory for any user that is being transferred or promoted. The Active Directory account will remain active with minimal access (email and web browsing only). The Active Directory account must not be added to any new groups without a new access request form from the user's new manager.
    c. Human Resources (HR) and/or Department Managers must notify ITS of personnel terminations, transfers, promotions, or change of responsibilities which impact an employee's access rights.
    d. Upon notification from HR and/or Department Manager, the Access Administrator must revoke all group membership within Active Directory and applications for any user who separates from the organization (termination/resignation/leave of absence). The account password will be changed to a random value following the requirements established in the Trinity University Password Policy, and the account will be suspended/deactivated at the close of business on the employee's last working day, but not deleted. This will allow the organization to recover any relevant information from this user if needed. After 45 days, with the appropriate authorization of the Data Steward, that user account must be deleted.
        1. Suspended accounts from terminated/resigned employees may only be accessed with authorization from the department head.

2. Extensions may be configured as approved by Department Managers.

9. In cases where there is a perceived risk of harm to the organization that will be caused by an employee during or prior to termination, a request to remove access may be approved and actioned in advance of notice of termination being given. This precaution will especially apply in the case where the individual concerned has privileged access rights e.g., domain admin.
10. Trinity University must enforce a standard naming convention for user accounts.
11. User account names must not be reused as this may cause confusion in the event of a later investigation. The User Access Administrator must ensure that the user account name is different from any other user account that has been used in the past in the organization.
12. Trinity must ensure proper authorization and monitoring is being used for temporary accounts and notify relevant personnel (e.g., Data Custodians) when the account is no longer required.
    a. Access requests for temporary accounts must be submitted by Department Managers on behalf of employees and contractors. Each request must be addressed to the appropriate business Data Steward or Data Custodian as noted in the current inventory asset list.
    b. Trinity University will monitor these accounts and each temporary account will be disabled on its pre-defined expiration date. Managers will then have the option to extend the expiration of the account or allow it to be deactivated and removed.
13. Trinity must remove or disable default user accounts. If default accounts cannot be removed or disabled, they must be renamed.
    a. Upon deployment of a new system, program, service, or application IT staff must examine the system as part of the system hardening procedures and review the default user accounts on the system. Depending on the capabilities of the system, default accounts must be either disabled, removed, or renamed. The ideal option is to rename and disable the account and ultimately remove it after it has been determined to not be needed by other services. If the system will not allow an account to be removed then it will be renamed and disabled, if possible, and its password will be changed.

User Access Provisioning

1. Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform (role-based).
2. Group roles must be maintained in line with business requirements and any changes to them must be formally authorized and controlled via the change management process.
3. Ad-hoc additional permissions must not be granted to user accounts outside of the group role; if such permissions are required this must be addressed as a change and formally requested.

Removal or Adjustment of Access Rights

1. Where an adjustment of access rights or permissions is required, this must be carried out as part of the role change.
2. It must be ensured that access rights no longer required as part of the new role are removed from the user account.
3. If a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role must be requested via change management. Due consideration of any issues of segregation of duties must be given.
4. Under no circumstances will administrators be permitted to change their own user accounts or permissions.

Management of Privileged Access Rights

1. Privileged access rights must be identified for each system or network and tightly controlled.
2. Any account that has elevated privileges over any system or process (e.g., system / network administrators having root level access, database administrators, etc.), must only be allowed after approval by the IT Data Owner or Data Trustee. The approval must be granted to a limited number of individuals with the requisite skill, experience, business need, and documented reason based on role requirements.
    a. Access requests for a privileged account on any system will require approval by the ITS executive and the Data Steward.
    b. IT personnel are responsible for provisioning the account.
3. Technical users (such as IT support staff) will not make day to day use of user accounts with privileged access, rather a separate “administrative” user account must be created and used only when the additional privileges are required.
4. These accounts must be specific and unique to an individual. Generic admin accounts must not be used as they provide insufficient identification of the user.
5. Access to administrative level permissions must only be allocated to individuals whose roles require them and who have received enough training to understand the implications of their use.
6. The use of user accounts with privileged access in automated routines such as batch or interface jobs must be avoided where possible. Where this is unavoidable the password used must be protected and changed on a regular basis.
7. All privileged accounts must require multi-factor authentication to be enforced, when feasible.
8. Trinity must ensure that privileged accounts are controlled, monitored, and that access records are maintained to facilitate security reporting when required.

a. Privileged account activity must be logged and always monitored.
b. Monitoring will be focused on detecting unauthorized access or unauthorized use of or tampering with Nonpublic Information (NPI).

Review of Access Rights

1. Data Stewards (or their assigned delegates) and Data Custodians at Trinity are responsible to implement processes to enforce periodic review of user accounts and user access rights. User accounts reviews must be performed at least quarterly, and user access rights reviews must be done at least every year. The main goal of these reviews are to ensure the following:
    a. Access levels remain appropriate, based upon approvals, and only authorized users have access.
    b. User accounts only have authorized roles allocated.
    c. Terminated employees do not have active accounts.
    d. There are no group accounts, unless approved.
    e. User account provides adequate identification.
    f. There are no duplicate user identifiers.
2. During each access review, Data Stewards and Data Owners or Data Trustees must be provided with a list of all users with access to their system/data and the configured access privileges. Data Stewards must be responsible for determining if current access levels are appropriate based on job roles and responsibilities for everyone and report any discrepancies for remediation. Information security must review the discrepancies and the Access Administrator will re-provision accounts as necessary.
3. This review will be performed according to a formal procedure and any corrective actions identified and carried out.
4. A review of user accounts with privileged access will be carried out by the Data Owner or Data Trustee on a quarterly basis to ensure that this policy is being complied with.

User Authentication and Password Policy

1. Trinity University must create a password policy covering all the construction requirements for a secure password. Such policy is deemed an integral part of this Access Control Policy.
2. ITS must implement additional authentication methods based on a risk assessment which considers:
    a. The value of the assets protected
    b. The degree of threat that exists
    c. The cost of the additional authentication method(s)
    d. The ease of use and practicality of the proposed method(s)
    e. Any other relevant controls in place
3. Use of multi-factor authentication methods must be justified based on the above factors and securely implemented and maintained where appropriate.
4. Single Sign-On (SSO) will be used within the internal network where supported by relevant systems unless the security requirements are deemed to be such that a further logon is required.
5. Trinity systems must be configured to enforce a limit of unsuccessful login attempts during a Trinity-defined period. The number of login attempts must be commensurate with the classification of data hosted, processed, or transferred by the

information system. If not otherwise specified for any particular system, the standard to enforce in Trinity must be:
    a. A maximum of 5 failed attempts before locking the account.
    b. The account will remain locked out for a duration of 15 minutes.
    c. Unlocking the account prior to the expiration of the 15 minutes period will require manual intervention by ITS Technical Support Services.
6. Trinity systems must time-out sessions or require a re-authentication process after thirty (30) minutes of inactivity. Users must re-enter their passwords to resume their session.
7. The minimum password age before allowing users to change it again must not be less than 24 hours.
8. Trinity University must put controls in place to ensure that any PC or device with access to its network or systems, locks the screen after 10 minutes of inactivity.

Identity Management

1. Trinity must establish processes to enforce the use of unique system identifiers (User IDs) assigned to each user, including technical support personnel, system operators, network administrators, system programmers, and database administrators.
    a. Systems must be configured to not allow duplicate user identifiers.
    b. Username reviews must be performed on systems at a minimum of every 12 months to ensure that no duplicate user accounts have been configured.
    c. If employees share identical names, then additional characters must be added to their usernames in order to distinguish them (i.e., two employees with the name John Doe will have usernames similar to:
        1. JDoe
        2. JDoe1
2. Trinity must prevent reuse of user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier.
    a. Must the need for a retired identifier arise Trinity information security staff must perform an audit and ensure that all permissions are reset, and the date of reissue is noted.
3. Trinity must deny the use of group IDs. Only limited exemptions must be allowed, where these are necessary for business or operational reasons. Group IDs must be formally approved and documented.
    a. Group IDs require a formal request and business use case be presented to the Chief Information Security Officer (CISO) and Chief Information Officer (CIO).
    b. The CIO, with the consultation of the CISO, will decide if a group ID is the most appropriate option for meeting the business case needs.
    c. Requests for group IDs must be evaluated on a case-by-case basis.
    d. Group membership must be documented with an access request.
    e. Group ID and group membership will be evaluated every 12 months to ensure they are still required.

4. If Trinity requires group IDs, it must require individuals to be authenticated with a unique user account prior to using the group ID (e.g., network authentication prior to use of Group ID).
    a. Group IDs must be reserved for special use application systems only.
    b. Group IDs will only be usable after the user has established their identity on the network via another primary account such as Active Directory. This requirement serves to establish a system of record so that group ID usage may be tracked and monitored.
5. Trinity must minimize the use of system, application, or service accounts; and Trinity must document, formally approve, and designate a responsible party of this type of accounts.
    a. System, application, and service accounts must be limited to non-staff use. These accounts will only be used for automated tasks which require login credentials to systems in order to complete an automated task. These accounts must not be used by personnel for daily use.
    b. All system, application, and service accounts must be documented as part of system documentation. These accounts must be reviewed and accounted for during regular access control reviews.
    c. Information Security must be responsible for provisioning and maintenance of these accounts with minor input from third parties whose applications, services, or automated jobs/scripts depend on the accounts.
6. Trinity security system must be able to identify and verify the identification and, if deemed necessary by Trinity, the location of each authorized user.
    a. Authorized users of system, application, and service accounts must reside mostly within information security.
    b. Authorized users of system, application, and service accounts which do not reside within information security must be documented within a “special account user” spreadsheet.

Network Access

Remote Access

1. Specific approval must be obtained from the remote network access’ Data Steward (ITS) before connecting any equipment to the organization’s network (e.g., modems connected to non-organization owned PCs, or devices connected to the organization’s network).
2. The procedure for authorized individuals to access network or information systems from external systems, such as access allowed from an alternate work site (if required) are:

a. Access to internal resources from alternate work sites must be accomplished only via the use of approved encryption technologies like remote access VPN, site-to-site VPN access or Citrix.

b. Access to internal resources from external third-party services must be accomplished via VPN and/or encrypted web traffic such as HTTPS.
c. Connections will require vetting and approval by Information Security, the IT owner, and the business owner, as well as a valid business case.
d. Approved connections will be configured by the ITS infrastructure team.
e. Active connections will be always monitored by the ITS Core Infrastructure Team.

3. Approved VPN connections may only be established via the technology authorized by the IT Department.
4. Remote access must be requested in the same manner as regular access requests.
5. Establishing connections to Trinity information systems over clear text protocols such as Telnet, FTP, or HTTP, is strictly prohibited.
6. Trinity must utilize automated mechanisms to enable management to monitor and control remote connections into networks and information systems.

a. All VPN connections and Citrix interfaces will be logged, monitored, and reported on a regular basis.
b. All network activity traversing VPN and Citrix interfaces must be monitored (for example, using firewall monitoring, and SIEM systems).

7. For Restricted data and/or system administrators: Trinity employees and authorized third parties accessing Trinity information systems remotely must do so via an approved multi-factor authentication (MFA) technology.

a. Multi factor authentication will require the use of one of the following components as the secondary factor (in addition to the username and password):
    - Physical token
    - Mobile software authenticator
    - SMS (text message) based 1 time use passcode
    - Fingerprint scan
b. The secondary factor will be assigned by default to any user with access to an MFA-enrolled system and will vary based on available resources and the nature of the data and systems being accessed remotely.

8. Managers responsible for partner agencies or third-party suppliers must request access to the Trinity network on behalf of the partner. All requests must be sent to the ITS Technical Support Services department for approvals and provisioning. Any changes to supplier's connections (e.g. on termination of a contract) must be immediately notified to the ITS Technical Support Services so that access can be updated or ceased. All permissions and access methods must be controlled by the ITS Technical Support Services.
9. All access to partner agencies and third parties must be temporary in nature, with a validity of less than a year. At the end of the authorized period, temporary access must be removed. If access is required beyond the originally authorized period, an extension of the access need to be requested again by the responsible manager.

10. Partners or third-party suppliers must contact the ITS Technical Support Services on each occasion to request permission to connect to the network and a log of activity must be maintained. Remote access software and user accounts must be disabled when not in use.

Wireless Access

1. Trinity establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
    a. Trinity University Acceptable Use Policy has been established for use of the wireless networks.
    b. Two segregated wireless networks must exist at most Trinity work sites to include:
        1. Trinity-Guest
        2. Trinity-Air
    c. If more wireless networks are required, these must be risk-assessed, and must be authorized by the organization.
    d. Wireless networks will have the following implementation requirements:
        1. Trinity-Guest
            1. Network will be logically segmented from the production network.
            2. Network will (where possible) use a separate external connection for internet access.
            3. Network will make use of WPA2-PSK for authentication and encryption.
            4. One pre-shared key will be used for the network at each location.
            5. Unique pre-shared keys can be deployed per location as approved by the information security manager.
            6. Pre-shared keys will be changed on a periodic basis to prevent unauthorized access.
        2. Trinity-Air
            1. Network will be configured to have access to the internal Trinity network infrastructure.
            2. Network authentication will be enforced using Active Directory.
            3. Network will make use of WPA2 Enterprise for authentication and encryption.
            4. One pre-shared key will be used for the network at each location.
            5. Unique pre-shared keys can be deployed per location as approved by the information security manager.
            6. Pre-shared keys will be changed on a periodic basis to prevent unauthorized access.
2. Trinity must only use wireless networking technology that enforces user authentication.

   a. All wireless networks will require at a minimum a unique pre-shared key or passphrase to gain connectivity.
   b. Trinity will not run wireless networks which are open or require no form of authentication to access.
3. Trinity must authorize wireless access to information systems prior to allowing use of wireless networks.
   a. Access to the Trinity internal Wi-Fi network will require Mobile Device Management (MDM) software to be installed on employee devices prior to being granted access to the network.
   b. A request to ITS Technical Support Services must be submitted to have the software installed and configured.
   c. Access to the Trinity's Students and Faculty Wi-Fi network will require authentication control, and this network needs to be separated from the internal core infrastructure.
4. Trinity does not allow wireless access points to be installed independently by users.
   a. Trinity wireless infrastructure is capable of detecting unauthorized wireless networks. Wireless networks which are not operated by Trinity in or around Trinity facilities must be identified and removed if found to be connected to Trinity network infrastructure.
   b. Employee owned/operated wireless access points may not connect to or interfere with Trinity wireless networks.
   c. Special requests may be submitted to have a temporary wireless network deployed for training or other purposes.

Cloud Services

Trinity University makes use of cloud computing services in the delivery of its core business systems. The nature of these services is such that data is stored outside of Trinity's internal network and is subject to access and management by a third party.

1. Access control policies described in this document also apply to cloud services, and these become even more important when data is stored outside of Trinity University internal network.
2. Where available, multi factor authentication must be used to access all cloud services.
3. Audit logging must be enabled, sufficient to allow Trinity University to understand the ways in which its data is being accessed and to identify whether any unauthorized access has occurred.

Exemptions

Systems owned or managed by a business partner, vendor, or third-party must be handled according to this policy unless contractual obligations and/or third-party requirements come into conflict with this policy's requirements. In that case, an exception must be submitted to the Chief Information Officer (CIO) office for further examination. The Office of the CIO will

notify the requestor if an exemption can be given and any necessary compensating controls. Exceptions must be documented and reviewed on an annual basis.

Performance Evaluation

Consequences of Policy Violation:

All Users must comply with this policy. The Chief Information Officer, the Chief Information Security Officer, and each member of Information Technology management are responsible for ensuring User adherence to this policy.

Trinity University reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts normal operation of Trinity University information systems or violates state or federal law.
Users who violate this policy may be subject to disciplinary action, up to and including termination of employment or contract with Trinity University.
Trinity University cooperates with appropriate law enforcement entities if any User may have violated federal or state law. Instances of failure to adhere to this policy will be brought to the attention of the Chief Information Officer. The Chief Information Officer may seek consultation/advice from Human Resources.

Related Documents

Related Content:

Trinity University. (2021). Information Security Training and Awareness Policy.
Trinity University. (2021). Trinity University Acceptable Use Policy.
Trinity University. (2021). Trinity University Password Policy.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v2.0	4/27/2022 11:29 AM	Ben Lim
v1.0	1/27/2022 3:03 PM	Dan Carson

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer