Information Technology Security Standards and Protocols

Rio Hondo Community College District

Contents

ITS 01 - Information Security Program Overview

1.0 Purpose, Scope, and Maintenance

1.1 Purpose

This Information Technology Security Standards (ITSS) document provides an overview of the Rio Hondo Community College District (RHCCD) information security program and the specific details for each aspect of the program. The central and critical role of information systems at RHCCD requires ensuring the protection of these systems.

The ITSS outlines the responsibilities and expectations for security of information assets managed by RHCCD. The controls described in this ITSS are collectively known as **RHCCD's Security Program**, which is designed to:

- Reflect RHCCD business objectives,
- Prevent the unauthorized use of or access to RHCCD information systems, and
  Maintain the confidentiality, integrity, and availability of information.

This ITSS is guided by security requirements specific to RHCCD operating environment, laws and regulations that are relevant to RHCCD and information security best practices. These control requirements are documented and aligned with an internationally recognized industry standard for security, ISO 27002, *Code of Practice for Information Security Management* and designed to meet the requirements of the *Payment Card Industry Data Security Standard*.

1.2 Scope

This ITSS applies to all computer and network systems, software, and paper files owned by and/or administered by RHCCD.

Computer and network systems include, but are not limited to, the following items owned or leased by RHCCD and used by RHCCD personnel for information access: servers, storage systems, personal or laptop computers, network equipment, telecommunications systems and mobile devices.

The ITSS also applies to IT related hardware (e.g. laptop computers, desktop computers, portable computers, printers, copy machines, networking equipment, etc.) purchased by grant funding or donated to the college and will be using college resources such as Network, IT Support, or licensed software.

Software includes operating systems, databases, and applications, whether developed by RHCCD or purchased from application software vendors, or shareware / freeware in use within production systems.

1.2.1 Applicability to Staff

This ITSS applies to all RHCCD employees, consultants, and contractors and students using RHCCD-owned or leased equipment or systems

1.2.2 Applicability to External Parties

This ITSS applies to all computer and network systems, software, and paper files administered or managed by third parties for RHCCD. This includes consultants, contractors, temporary workers,

interns, students and business partners who are acting on behalf of RHCCD and/or access RHCCD's information software, software, and networks.

Targeted guidance for specific audiences may be created to communicate elements of the Security Program to parties external to RHCCD.

1.3 References and Related Documents

Throughout this document, references are made to additional RHCCD Information Technology Security Standards, procedures, guidelines, and standards that support or further clarify this Information Security ITSS. Please refer to the following Information Technology Security Standards included in this document for additional information and references including definitions:

- ITS 01: Information Technology Security Program Overview
- ITS 02: Acceptable Use
- ITS 03: Access Control
- ITS 04: Change Control
- ITS 05: Data Classification
- ITS 06: Secure Operations
- ITS 07: Network Security
- ITS 08: Physical Security
- ITS 09: Logging & Monitoring
- ITS 10: Remote Access
- ITS 11: Security Incident Response

1.4 Maintenance and Support

This ITSS is maintained by the office of the Vice President of Finance and Business and the Director of Information Technology Services, who serves as the Information Security Officer. It will be reviewed at least annually and modified when applicable as a response to any major changes in RHCCD's information security or regulatory requirements. Questions related to this ITSS should be directed to itssecurity@riohondo.edu.

2.0 Security Organization

RHCCD's security organization is designed with central oversight and governance and consists of both information security and physical security elements. This organization meets periodically to address specific security issues and develop initiatives to continuously improve RHCCD information security policies, standards, guidelines, and procedures.

2.1 Security Responsibilities

While information security is ultimately the responsibility of the Board of Trustees and the Superintendent/President, the office of the Vice President of Finance and Business, and the Director of Information Technology Services and his/her designates administer the College's security program. All employees who uses RHCCD's systems and networks and have access to RHCCD information, share in the responsibility for its protection.

2.1.1 Information Security

The Information Security Officer coordinates the information security program for RHCCD. Those with primary responsibility for information security within Information Technology Services (ITS) are supported by individuals within business areas that include core administrative functions such as Human Resources (HR), Student Services, and Finance and Business. Together, the IT organization and these additional stakeholders have responsibility for different aspects of the Security Program.

2.1.2 Physical Security

Campus and District Office Safety provides a safe and secure environment for students, faculty, and staff, and work with ITS to ensure that facilities and secure areas are controlled.

2.1.3 Data Owners

Data Owners are responsible for data quality and determining the appropriate classification level for the information contained within the respective applications under their purview. All applications have one or more designated Data Owner(s). The Data Owner may delegate responsibilities regarding classification and handling but is ultimately responsible for determining that the responsibility has been correctly discharged.

2.2 Security Program Governance

The office of the Vice President of Finance and Business and the Director of Information Technology Services are responsible for establishing Information Technology Security Standards that provide operational oversight and direction to the RHCCD information security program.

3.0 Data Classification

Classifying information is at the core of an information security program because it specifies how information will be secured and handled, based on its sensitivity and value.

3.1 Data Classification Objectives

RHCCD's strategy is to classify information regardless of medium (paper or electronic) according to its sensitivity and the potential impact of disclosure. In general, information is disclosed to employees or others only when there is a business need-to-know.

Information must be consistently handled according to its requirements for confidentiality and disclosure. Data Owners are responsible for determining the appropriate classification level for the information contained within the respective applications they own.

Information on paper documents or other media has the same classification level as in an electronic format.

ITS will provide appropriate security technology solutions (such as encryption) for electronically stored information should this level of protection be required.

3.2 Data Classification Categories

RHCCD data are classified into three categories. The definitions below are supplemented by the information and definitions in the *ITS 05: Data Classification*. The correct classification level is established by the Data Owner.

- **Public** information applies to information made available for public distribution through authorized District or college channels. Examples include press releases, marketing materials, public web pages, and other data routinely available to the public.
- **Internal** information is available that must be protected due to proprietary or business considerations, but which is not personally identifiable or sensitive, such as internal policies, telephone listings, or data on the Intranet that has not been approved for external communication. *Internal* information is generally available to all employees and other authorized users.

- **Restricted** information is sensitive in nature, proprietary, and specific to RHCCD's business. Unauthorized compromise or disclosure would likely have serious financial, legal, or regulatory impacts. Examples include personally identifiable data, credit card data, health care data, human resources data, or computer system details. *Restricted* information is only available on a need-to-know basis. It may be appropriate to mark this type of information as "Confidential" or "Restricted Information".

For purposes of this ITSS, the term "personally identifiable information" means an individual's first name and last name or first initial and last name in combination with any one or more items of personal information, such as social security number or other identity verification number, driver's license number or state-issued identification card number, financial account number, credit or debit card number, date or place of birth, and gender; provided, however, that "personally identifiable information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Both RHCCD and any computer service providers are required to comply with regulations designed to protect sensitive and personally identifiable information from unauthorized disclosure and identity theft. Encryption is mandated by many laws and standards for some information transmission or storage. Refer to the handling standards described in *ITS 05: Data Classification* for guidance.

4.0 Human Resources

4.1 Acknowledgement

In addition to the other agreements that may be required, acknowledgement of this Information Technology Security Standard and the *ITS 02: Acceptable Use* are part of the terms and conditions of employment with RHCCD. Acknowledgement is required at the time of initial employment.

Where applicable, the sponsoring RHCCD manager must ensure that temporary workers, interns, students, consultants, or contractors working for RHCCD have been provided with a copy of this ITSS and *ITS 02: Acceptable Use*. Additionally, it is the responsibility of the sponsoring manager to ensure compliance with this and all RHCCD Information Technology Security Standards.

All district employees will be required to participate in annual security awareness training.

4.2 Employee Administration

The Human Resources department initiates the addition of new access by providing notification to ITS and other business areas who administer application security. HR updates the Human Resources System with new hires, transfer, and termination information.

Managers are responsible for notifying HR and ITS when an employee, contractor, consultant, temporary worker or intern is no longer associated with RHCCD for any reason so that access can be disabled or removed.

Pre-employment background checks are conducted on all employees whose job responsibilities require them to access credit card information and other data classified as restricted (see *ITS 05: Data Classification*).

4.3 Contractors and Temporary Workers

Temporary workers are processed through HR. Contractors must complete an agreement and be approved by the Board. Once a contractor has been approved, managers must work with HR and ITS to submit the appropriate forms so that appropriate access can be granted, and a deadline to revoke access can be established.

4.4 Acceptable Use

RHCCD's information and technology resources must be used in an approved, ethical, and lawful manner. Employees and contractors must always be alert to actions and activities they may perform that could breach the *ITS 02: Acceptable Use*, which details specific restrictions regarding the Internet, electronic mail, social networking, and use of RHCCD's computing resources.

All computer systems belong to RHCCD and may only be used for business purposes. RHCCD personnel should not have an expectation of privacy in anything they create, store, send, or receive via the RHCCD computing environment.

If users have any uncertainty on the appropriateness of their actions, they should clarify their understanding with their manager or contact itssecurity@riohondo.edu for guidance.

5.0 Physical Security

5.1 Physical Security Controls

Information protection is dependent on adequate physical security. All RHCCD information technology facilities employ access control measures to ensure that all facilities remain secure.

Campus Security and ITS have responsibility for physical security and work together to investigate incidents that could involve information compromise. Campus Security provides continuous surveillance of the facilities.

5.2 Equipment and Media Security

Lost or stolen electronic devices must be reported to the ITS Help Desk located on the main campus immediately. This includes laptops, smart phones, or removable storage devices that contain RHCCD data.

Strict control must be maintained over the internal or external distribution of any media that contains restricted information. RHCCD information that is classified as *Restricted* is limited to authorized users on a need-to-know basis and must not be copied to unencrypted devices, e-mailed without encryption or printed without adequate physical controls.

Users must shred or securely dispose of classified information in accordance with established retention policies. If secure disposal methods are required, contact the IT Help Desk.

Contractors or consultants using personal equipment to conduct RHCCD business are responsible for physically securing equipment in their possession that contains RHCCD-related information. Loss of equipment containing *Restricted* information, even if personally owned, must be reported immediately to the IT Help Desk.

6.0 IT Security Controls

ITS manages the infrastructure and controls for centralized networks, servers, databases and desktop computers. Users must not disable, uninstall, or modify the security software, settings or encryption installed on laptops or mobile devices.

6.1 Security Logging and Monitoring

Logs of key system events and access to sensitive information are in place and administered by ITS personnel. Systems that provide initial entry / authentication into the RHCCD network and any application system that processes RHCCD *Restricted* information must be configured to capture security audit log data.

System or application administrators must routinely monitor system or application logs for anomalies regarding access to information. Exceptions must be investigated, and appropriate action taken.

6.2 Third-Party Access

Third-party (non-employee) access to RHCCD's systems must be governed by formal written agreements or contracts. Network connections between the RHCCD environment and third parties must follow agreed upon security procedures. These agreements may require signed Confidentiality and Non-Disclosure statements restricting the subsequent usage and dissemination of RHCCD information.

Vendors or other third parties with access to RHCCD-owned or leased equipment or systems housed in a RHCCD data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

7.0 Access Controls

7.1 Access Control

Access to RHCCD systems and applications is role-based and will be granted to authorized users based on job classification. Users are limited to the system capabilities they need based on job function or role and as authorized by management.

RHCCD computers are equipped with screen saver locks that will activate after 15 minutes of inactivity as required by PCI-DSS 2.0 section 8.5.15. Users must manually logoff or lock workstations if they will be unattended prior to activation of the screen saver lock.

7.2 System and User Accounts

Accounts are assigned to an individual and may not be shared. Guest accounts must be disabled if a system or application is provided with one. Vendor-supplied default accounts and passwords must be disabled or changed.

System accounts, such as background accounts that are used for internal processing, are exempt from time-based password change requirements

7.3 Passwords

Passwords are confidential and must not be shared. Passwords must be changed on first use or if they have been reset for the user by the IT Help Desk or an administrator.

The IT Help Desk and other administrators resetting passwords must verify the identity of all users requesting a password reset prior to performing the reset.

End user passwords should be more than 8 characters long. Increased password length is the best method of increasing password security. End user password should include uppercase letters, lowercase letter, numbers, and symbols. End users should not reuse passwords across systems.

Multi-factor authentication should be used by end-users on all systems whenever possible. Multi-factor authentication drastically decreases the chances that an account will be compromised.

Administrative users shall use highly complex and long passwords. Administrative password should be kept in a secure location such as an encrypted password manager or printed and kept in a physical vault.

Multi-factor authentication shall be used by administrative users on all system where it is available.

Refer to *ITS 03: Access Control* for further information.

7.4 Account Review

IT senior management and Data Owners or their designees must review the user accounts for the systems and applications they administer and verify the appropriateness of continued access. This review must be performed at least every twelve months.

Access should be disabled immediately upon notification from Human Resources that an employee (or appropriate department in the case of a contractor) is no longer with RHCCD and its entities.

7.5 Network Connectivity

ITS manages RHCCD's network, and all new wired connections must be requested through them. Wired devices, such as servers, that will be connected to the network must be approved and implemented by ITS teams for their respective networks.

Employees and other authorized users must request remote access and use established connectivity methods to connect to RHCCD networks from a remote location. Use of other remote connectivity methods is prohibited. Refer to the *ITS 07: Network Security* and *ITS 10: Remote Access* for additional information.

8.0 Application Development

8.1 Changes to Applications

Change Management is a security issue because unauthorized or accidental changes to applications may impact the integrity and availability of the data. The ability to change applications in production is limited to authorized users.

Change Management processes are required to mitigate risk associated with changing business applications, minimize the impact of change, and provide a stronger linkage between production problems and the events that caused them. Applications managed by IT must be controlled as described in *ITS 04: Change Control*.

8.2 Application Security Standards

Application managers must consider secure coding practices that will prevent or minimize security vulnerabilities, especially for any Internet-facing application. If a third party is hosting an application, data protection controls provided by the third party must be adequate to meet regulatory and contractual requirements for security.

9.0 Security Incident Response

9.1 Security Incident Response

All users must report suspicious activities or actual occurrence of any unauthorized activities to the IT Help Desk. Notification should be made immediately or as soon as reasonably possible. This includes unauthorized use of accounts, logon IDs, passwords, loss of laptops or other devices, or potential breaches of RHCCD computer systems and networks. Help desk personnel shall notify the Information Security Officer who will complete an Incident Report and conduct any investigation that may be required. Helpdesk staff may assist in the investigation as required by the Information Security Officer.

Incidents that involve information compromise, such as a data breach or other loss of information, will be handled according to the *ITS 11: Security Incident Response*. ITS will work with Campus Security and business areas as required to resolve the incident and ensure that correct notification procedures are followed.

Users detecting potential information security events should immediately report them to the IT Help Desk.

9.2 Backups

RHCCD's data is regularly backed up using defined business requirements for information recovery.

Critical information shall be stored on network file servers or production servers to ensure regular and automatic backup and recovery. Critical information should not be stored on personal computers or laptops alone, or on unencrypted personally-owned devices. If additional storage space is needed, contact the IT Help Desk for options.

Backup operations shall be conducted in such a way as to protect district data from the possible infection of malware that encrypts data for ransom or other malicious network and/or file attacks. Protected backup data cannot be modified by such malware.

10.0 Compliance and Audit

10.1 Compliance with Legal Requirements

The Information Security Program supports compliance with state and federal laws and applicable international laws and standards, including HIPAA, GLBA, PCI, and FERPA.

10.2 Third Party Service Providers

Additional security requirements may be required for any third-party service provider that receives, stores, maintains, processes, or otherwise is permitted access to personally identifiable information provided to them by RHCCD.

Whenever selecting and retaining any third-party service provider, ITS will (1) take reasonable steps to confirm that the service provider can maintain appropriate security measures to protect personally identifiable information consistent with all applicable laws and regulations, and (2) require the service provider to contractually agree in writing with RHCCD to implement and maintain such appropriate security measures.

10.3 Audit

Audit reviews are conducted by an external auditor and/or by IT consultants on a regular basis. Selected application security reviews may be performed as part of internal audit plans or general controls audits.

11.0 Enforcement and Compliance

11.1 Enforcement

Those detecting violations of this ITSS must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to the Director of Information Technology, and the Vice President of Finance and Business who will determine the extent of risk that any non-compliance condition presents and remediation activities that are required.

Users who deliberately violate information security standards as outlined in this document will be subject to disciplinary action up to and including termination from employment or association with RHCCD.

11.2 Exceptions

Business needs may occasionally require variance from established Information Technology Security Standards. A business function may not be able to be performed effectively, reasonably, or may present an unreasonable financial cost, if the ITSS is followed. In these instances, the Vice President of Finance and Business must be notified through email to itssecurity@riohondo.edu, briefly stating the underlying business problem and recommended approach or proposed compensating controls. Alternatives and any potential risks or problems the alternatives may cause will be considered. If a variance is granted, the affected Information Technology Security Standards will be updated and communicated.

ITS 02 - Acceptable Use

1.0 Purpose and Scope

The objective of this ITSS is to outline the acceptable use of electronic assets at Rio Hondo Community College District (RHCCD). Inappropriate use exposes RHCCD to risks including compromise of network systems and services, human resources, and legal issues.

This is one of a series of information security Information Technology Security Standards maintained by the Information Technology Services (ITS) department designed to protect RHCCD information systems.

2.0 Acceptable Use

2.1 Acknowledgement of User Responsibilities

All users must review and acknowledge their understanding of RHCCD Acceptable Use ITSS and other job appropriate information security Information Technology Security Standards. Human Resources (HR) will provide the ITSS and acknowledgement links to new staff and contractors upon hire or contract establishment. These documents are BP3720 and AP 3720.

2.2 Personal Use

Computers and computer accounts given to users are provided to assist district employees and volunteers in the performance of their jobs. All computer systems belong to RHCCD and are intended for business and instructional use. Users are expected to exercise good judgment regarding the reasonableness of personal use of RHCCD information systems and assets. Personal use should not conflict in any way with business objectives or interests, organizational values, or standards of business conduct. RHCCD prohibits the use of any software not licensed or approved by ITS. If unlicensed software is found to reside on a RHCCD computer, it must be removed.

RHCCD considers all information transmitted through or stored in its systems, including e-mail, instant messaging (IM) or chat data, and voice mail messages, as RHCCD information. All files and other information stored on RHCCD systems, even if considered “personal” by an employee, are and remain the property of RHCCD. RHCCD may review or use such information as it deems appropriate.

Where allowed by law, RHCCD’s ITS reserves the right to monitor activities that occur on its systems to troubleshoot system problems, disruptions, or outages. For this reason, users should not have an expectation of privacy for anything they store, create, send, or receive on a District or college system. Suspected inappropriate use of systems by individuals may also be investigated to protect the organization.

2.3 Confidentiality

RHCCD has/shall adopt a Data Classification (see ITS 05) ITSS which categorizes different types of information and how it will be protected based on its value and sensitivity. Sensitive, personally identifiable, and customer information are classified as *Restricted*, and must always be kept confidential. This information is accessible only to those RHCCD staff who need such access to perform their jobs, or to others who have been expressly authorized by RHCCD for specific limited purposes. Unauthorized disclosure of information that has been classified as *Restricted* could cause great harm to RHCCD and may be prosecuted by law.

Restricted information must be protected from disclosure to third parties (non-employees) by default. Third parties may be given access to RHCCD information only when a demonstrable need-to-know exists. Such disclosure may be authorized by RHCCD management or by contract, such as with a temporary worker, consultant, or service provider. A non-disclosure agreement may be required as directed by the relationship and RHCCD legal requirements.

Restricted information may be stored in designated locations only and must be securely deleted when it is no longer required. If stored online, on portable devices or on tape, *Restricted* information requires encryption so that it cannot be read by unauthorized persons. *Restricted* information that is on paper or other media must also be stored securely. Refer to the *Data Classification Handling Procedures* for additional information on this topic.

Specific information about RHCCD's computer network, information system security, security controls, or potential vulnerabilities may not be distributed to persons who do not have a demonstrable need-to-know, and without prior approval from the Director of Information Technology Services. All information systems assets provided by RHCCD remain the sole property of RHCCD. Any data or intellectual property created by the user, including voicemail and electronic messages, remain the property of RHCCD and should not be removed, copied or shared with any person or entity except as part of the user's normal job responsibilities.

2.4 Electronic Messaging

RHCCD has an electronic mail (e-mail) network and provides instant messaging (IM) services. Users are responsible for using these technologies responsibly and within the following procedures:

- RHCCD's e-mail system is not to be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.
- Sending unsolicited e-mail messages is prohibited, including the sending of junk mail or other advertising material to individuals who did not specifically request such material.
- Creating or forwarding chain letters or pyramid schemes of any type is prohibited.
- Users must not create any messages that may be considered offensive or disruptive. Examples of messages deemed to be offensive are any which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
- RHCCD business communications transmitted by e-mail must use the appropriate District e-mail address (<userid>@riohondo.edu and employ the standard e-mail signature for external communications. Falsifying e-mail headers or routing information to obscure the origins of the e-mail or identity of the sender is a violation of this Information Security Standard.
- Because e-mail records and computer files may be subject to discovery in litigation, users must avoid making statements in e-mail that would not reflect favorably on RHCCD if disclosed in litigation or otherwise. Delete unnecessary e-mail promptly.
- Unauthorized access to others' e-mail accounts is prohibited.
- Information classified as *Restricted* (sensitive, personally identifiable, or student information) must not be e-mailed over public networks or stored on portable devices without encryption.
- Caution must be used when opening e-mail attachments or following hypertext links received from unknown senders, which may contain malware or viral code.

2.5 Social Networking Technologies

Social networking tools (blogs, online social networks, Facebook, Twitter, etc.) provide an open exchange of information and a means to establish relationships with colleagues and members of the public. These tools represent a communication model where a fine line exists between business and personal statements.

RHCCD's or another person or company's confidential or proprietary information is not to be shared. Users must ask permission to publish or report on conversations that may have intended to be private or internal to RHCCD. Check with the PIO if you have any questions about what is appropriate to publish or say online.

2.6 Use of RHCCD Assets

Using RHCCD electronic assets for abusive, unethical, or inappropriate purposes will not be tolerated and may be considered grounds for disciplinary action, including termination of employment. Unacceptable use of electronic assets includes, but is not limited to:

- Illegal activities
- Revealing or publicizing RHCCD intellectual property or proprietary information for unapproved or non-business-related reasons
- Use or distribution of unlicensed software
- Unauthorized use of copyrighted materials
- Sharing of user names and/or passwords
- Leaving *Restricted* or any confidential or sensitive materials in plain sight without taking protective measures
- Transferring or storing information on untrusted third-party servers. Contact ITS for approved locations / services
- Presenting your own viewpoints or positions as those of RHCCD, or attributing them to RHCCD
- Effecting security breaches or disruptions of network communications
- Circumventing user authentication or security of any computer, network or account
- Facilitation of the compromise of RHCCD information security controls
- Disabling software designed to prevent viruses or malware, or disabling screen savers or encryption methods
- Providing information about or lists or organizational charts of RHCCD employees to external parties.

3.0 Enforcement

Those detecting violations of this ITSS must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to ITS and/or Human Resources as appropriate. RHCCD Management will determine the extent of risk that any non-compliance condition presents and remediation activities that are required.

Users who deliberately violate Information Technology Security Standards will be subject to disciplinary action up to and including termination from employment or association with RHCCD.

ITS 03 – Access Control

1.0 Purpose and Scope

The objective of this ITSS is to provide internal controls for access to the Rio Hondo Community College District (RHCCD) sites, information and applications. This ITSS is part of a series of IT Security Standards governing the secure use and access of Information Technology Systems and Services.

Access controls may be physical (such as locks and badges), administrative (such as the ITSS to safeguard passwords) or technical (protections enforced by software settings or privileges). These controls are designed to either allow or restrict the ability to view, update, or delete information within the RHCCD networks and systems, or paper documents.

2.0 Access Control

2.1 Access Control Principles

There are three basic access control principles at the RHCCD:

- All information is made available only to those with a legitimate "need-to-know". Access is provided on this basis, guided by job requirements and data classification.
- Access controls for RHCCD systems will be provided in a manner that promotes individual accountability. Audit trails and monitoring of access establishes accountability and allows for follow-up of access violations and security breaches.
- Users with the highest levels of privilege on a computer system will be restricted to the least privileges necessary to perform the job.

2.2 Authentication to RHCCD Systems

Authentication is the verification of a user's claimed identity. Identification is required by all individuals prior to gaining access to secured RHCCD facilities or systems such as server rooms, cash handling rooms, and other areas where security is in the interest of the District.

Internal (RHCCD personnel) and external (non-personnel) users must provide a valid and unique user ID to authenticate to the network. In addition to a unique ID, the authentication method must include at least one of the following:

- A password or passphrase
- Token device or phone app
- Biometric

If the new user is a contractor or non-employee, the user ID will be identifiable as such by its naming convention.

Group, shared, or generic accounts do not provide accountability, and are not to be used for network or application authentication. Some exceptions may apply to this requirement, such as a system account that is required for server or network processing.

Physical access to secured facilities requires that RHCCD users possess appropriate credentials to enter all sites. Some areas, such as computer rooms, may require additional levels of access, cards or keys. Refer to the *ITS 08: Physical Security* for specific information.

2.3 Authorization to Applications

Addition, modification and deletion of user IDs and other credentials must be controlled. Data Owners (or their designate) have responsibility for making security decisions about applications which process data for which they are responsible. Assuming the role of Owner may require:

- Approving and re-certifying access by users to systems or data they control.
- Classifying data belonging to the application system they manage (determining the level of confidentiality or classification that should be assigned to an application's data, which will dictate its level of protection).

Access to certain functions may be provisioned automatically based on job position. Otherwise, the appropriate IT department, as authorized by Data Owners, must approve all new accounts except for those provisioned automatically. Each request for access must contain written and/or electronic evidence of approval by the Owner or ITS. Extension authorizations for contractor accounts must be applied by ITS to provide an audit trail.

Access requests must specify access either explicitly or via a "role" that has been mapped to the required access. Outside of initial standard network access provided based on the job position of the users, access to additional applications or capabilities is discretionary and must be both requested and approved by the Data Owner. For additional access, users should submit an access request.

Remote access is not automatically provided to all users and must be requested and approved. Refer to the *ITS 10: Remote Access* for additional information.

2.4 Security Administrators

The ITS Department is responsible for administering overall system access within RHCCD and so may request information from appropriate managers or administrators, such as who has access to their applications, and the procedures that they have put in place to provision them.

Some users (in ITS or business departments) may have a higher level of access privilege to administer systems or applications. They may have the ability to add, modify, or delete other users for the applications they control.

Systems administrators, under management supervision, have a responsibility to maintain appropriate access controls for the applications they maintain to protect information from unauthorized access. The number of administrators should be tightly controlled and limited to as few as necessary.

Security administrators should only use their privileged accounts to carry out administrative tasks that require privileged access. A non-privileged account should be used to perform routine tasks.

2.5 Passwords

Users of the RHCCD computer systems will be provided with one or more unique accounts and associated passwords.

Users are held accountable for work performed with the account(s) issued to them and are responsible for the confidentiality of their passwords. Passwords must be difficult to guess and kept private. Users must not disclose their password to anyone.

The following rules apply to password composition:

1. Must not be left blank when a new account is created. New passwords must not be the same for all users.
2. Must have a minimum length of 8 characters 3. Must contain both numeric and alphabetic characters
4. Must contain at least 1 capital letter.
5. New passwords must be changed immediately upon first use
6. New passwords must not be the same as the four previously used passwords

If a user requests a password reset via phone, email, web, or other non-face-to-face method, administrators authorized to reset passwords must verify the user's identity, such as by providing an element of personal information, prior to changing the password.

2.6 Account Lockout

Accounts will also be locked after three (3) invalid login attempts. Once an account is locked, a System Administrator or authorized student services representative is required to reset the account after the user's identity has been verified. The lockout duration will be set to a minimum of 30 minutes or until an administrator enables the account.

Except for some system accounts, user accounts have a session idle time of 15 minutes after which the session will be locked.

2.7 Emergency Accounts

An Emergency Account / User ID will be established when access is needed to diagnose or correct a problem. The request to create the Emergency ID must be made through the appropriate ITS manager or administrator. The ID will be enabled only for a 24-hour period unless a specific time period is requested.

The Requestor must inform the ITS Director upon completion of the work so that the ID can be disabled.

2.8 Termination of Access Privileges

Supervisors are responsible for notifying Human Resources if personnel will be leaving RHCCD. HR will contact ITS security administrators as required so that access is removed. Access must be disabled immediately upon notification.

2.9 Review of Access

An annual audit of computer resource authorizations to confirm that access privileges remain appropriate will be conducted by appropriate IT staff. After an additional sixty (60) days, inactive accounts will be purged. These requirements may not apply to certain specialized accounts (e.g., Windows Administrator, root).

ITS working with HR, may periodically validate employment and may immediately suspend users who are on leave-of-absence or extended disability. At least annually, IT will request that Data Owners verify continued access by users who have access to their applications.

ITS and/or external auditors will periodically review security administration procedures for specific applications and may employ monitoring tools to audit and verify access controls.

2.10 Payment Card Industry Requirements

RHCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). The following additional requirements are mandatory for systems that store, process, or transmit cardholder data. References to the relevant PCI section numbers are in parentheses after each requirement:

- Implementation of an automated access control system (7.1.4)
- The access control system must cover all (PCI) system components (7.2.1)
- The access control system must assign privileges based on job classification and function (7.2.2)
- The access control system must be set to a default "deny all" setting (7.2.3)
- Render all passwords unreadable during transmission and storage on all system components using strong cryptography (8.4)
- Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID (8.5.14)
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users (8.5.16)

ITS 04 – Change Control

1. Purpose and Scope

The objective of this ITSS is to ensure a standardized method for handling changes to Rio Hondo Community College District (RHCCD) infrastructure and associated software. Change control promotes the stability of the environment, which is essential to its security and integrity.

This is one of a series of information security Information Technology Security Standards maintained by the Information Technology Services (ITS) department designed to protect RHCCD information systems.

2.0 Change Control

A change is any modification or enhancement to an existing production system. Modifications can be in the form of updates to existing data, functionality, or system process.

2.1 Change Roles

The following roles have been established to guide the Change Management process.

- **Customer**: the individual or entity initiating a change, which may be either an internal RHCCD employee or contractor, or an external organization.
- **Product Owner**: the role that qualifies and prioritizes Change Requests from the Customer. The Product Owner may represent interests within a specific organizational entity.
- **Change Management Committee (CMC)**: one or more organizational bodies that review and prioritize Change Requests submitted by Product Owners. We currently do not have such a committee.
- **Development Team**: the internal RHCCD group responsible for implementing and/or delivering the Change Requests.

2.2 Process Tools

The primary tools used to manage Change Requests are the District-wide Help Desk system (Spiceworks).

2.3 Change Requirements for Vendor Maintained Software

Software provided by vendors or other organizations must follow these basic requirements for Change Management:

- ITS is notified by the vendor or customer of an available update or patch to a software package.
- The update must be requested through the service desk system.
- The update must be authorized by the appropriate user management.
- The update must be thoroughly tested in a test environment and approved by the customer prior to installation.
- Production data must not be used for testing data unless it has been scrubbed.
- The update must be accompanied by back-out procedures to be used in the event of unexpected error conditions.

2.4 Change Requirements for infrastructure related technology

Purpose built hardware containing updateable operating systems including but not limited to network switching hardware and general-purpose computing hardware such as servers and desktops must follow these basic requirements for Change Management where the device provides services to end users: ITS is made aware of an update or patch to a device.

- The update's criticality is assessed to determine appropriate implementation scheduling.
- Where possible, the update is tested in a non-production environment to evaluate the service impact.
- ITS discuss the impact and scheduling of the update.
- The rollout of the update is scheduled and announced at the weekly ITS Infrastructure stand up meeting.
- Backups of the existing configuration settings are verified up to date and complete.
- The rollout is completed, and functional testing is performed to ensure there is no user impact to services.
- Completion of the update is announced, and the update is documented in the infrastructure change control logs.

2.5 Application Security Knowledge Transfer

Changes related to new or significant implementation efforts should include a knowledge transfer of relevant security information from the Development team to the Network and Security staff and other interested parties.

ITS 05 – Data Classification

1.0 Purpose and Scope

The purpose of this ITSS is to provide information security requirements for ownership, classification, and protection of Rio Hondo Community College District (RHCCD) information assets.

An information asset is a definable piece of information, regardless of format, that is recognized as valuable to the organization. Classifying information is at the core of an information security program because it specifies how information, based on its sensitivity and value, will be protected from unauthorized disclosure, use, modification, or deletion.

This is one of a series of information security Information Technology Security Standards maintained by the Information Technology Services (ITS) department designed to protect RHCCD information systems.

2.0 Data Classification

Users of RHCCD systems need to understand the importance of securely handling the information they access and the standards that have been created to ensure data protection. For the purposes of this ITSS, data includes both electronic and paper.

Specific protection requirements are mandated for certain types of data, such as credit card information, personally identifiable information, or financial data. Where information is entrusted to us by our students, employees, or business partners, their expectations for secure handling must be met. Consistent use of this Data Classification ITSS will help to ensure that we maintain adequate data protection.

2.1 Classification of Data Assets

RHCCD classifies information regardless of medium (electronic or paper) according to its sensitivity and the potential impact of disclosure.

In general, information is disclosed to employees or others when there is a business need-to-know. Information must be consistently handled according to its requirements for confidentiality and disclosure.

Data Owners, defined below, are responsible for determining the appropriate classification level for data for which they are responsible or for the same information maintained on paper documents.

If the classification level is set too high, the cost of protection will be excessive in relation to the value or sensitivity of the data. If it is set too low, the risk of compromise could be increased. Downgrading to a lower classification at a future date is appropriate should conditions warrant.

2.2 Data Ownership

Every business application must have one or more designated Data Owners. The Data Owner is the person responsible for (or dependent upon) the business process associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, or otherwise processed, and is therefore best suited to make decisions about the information on behalf of the organization.

The Data Owner is ultimately responsible for security decisions regarding the data. The Data Owner will work with the appropriate campus or ITS department to ensure that minimum security standards are met.

The Information Technology Services (ITS) department will provide appropriate security technology solutions (such as system or application security controls or encryption methods) based on classification level.

If the Data Owner has chosen to outsource processing or storage of information at a location outside of RHCCD's control, such as on a cloud-based service, the Data Owner retains full accountability for security of the information. Security controls that are required to be performed by the third-party service provider must be detailed in the contract with that provider and monitored by the Data Owner.

The Data Owner's responsibilities include:

- Classifying data for which they are responsible. This includes determining the level of confidentiality that should be assigned to information, which will dictate its level of protection.
- Working with ITS to select security controls that are appropriate to the level of sensitivity, value, or confidentiality of the application or data it processes.
- Ensuring that third parties to whom data has been entrusted meet RHCCD security requirements.
- Establishing and maintaining response plans which identify actions to be taken for their area of control, such as Security Incident Response processes and defined Business Continuity Plans.
- Depending on location, provide ITS management with administrative access maintain continuity of access to systems and services.

2.3 Data Classification Categories

Information that is owned, used, created, or maintained by RHCCD must be classified into one of three categories:

- Public
- Internal
- Restricted

2.3.1 Public

Data classified as *Public* is suitable for routine public disclosure and use. Security at this level is the minimum required by RHCCD to protect the integrity and availability of this data. Examples of this type of data include, but are not limited to, data routinely distributed to the public such as publicly accessible web pages, marketing materials, and press statements.

2.3.2 Internal

Internal data is information about RHCCD or internal processes that must be guarded due to proprietary or business considerations, but which is not personally identifiable or otherwise considered confidential. This classification may apply even if there are no regulatory or contractual requirements for its protection.

Data in this category is generally available to employees, contractors, students, or business associates, but is not routinely distributed outside RHCCD. Some *Internal* data may be limited to individuals who have a legitimate business purpose for accessing the data, and not be available to everyone. Examples of *Internal* data may include:

- RHCCD procedures and manuals
- Organization charts
- Data which is on the internal Intranet (SharePoint), but has not been approved for external communication
- Software application lists or project reports
- Building or facility floor plans or equipment locations

2.3.3 Restricted

Restricted data is information that is sensitive in nature, and may be proprietary, personally identifiable, or otherwise be sensitive. Unauthorized compromise or disclosure of the information would be likely to cause serious financial, legal, or reputation damage to RHCCD, or result in embarrassment or difficulty for RHCCD, its employees, or students. *Restricted* data may be protected by statutes, regulations, or contractual requirements. Disclosure is limited to those within RHCCD on a "need-to-know" basis only. Disclosure to parties outside of RHCCD must be authorized by appropriate management and covered by a binding confidentiality or non-disclosure agreement.

Examples include:

- Personally identifiable (as defined below) information of our employees, contractors, or students
- HR, employee or payroll records
- Student data
- Audit reports or results
- System and network configuration details, including diagrams, passwords, programs or other IT-specific documentation
- Intellectual property
- Health records
- Legal documents

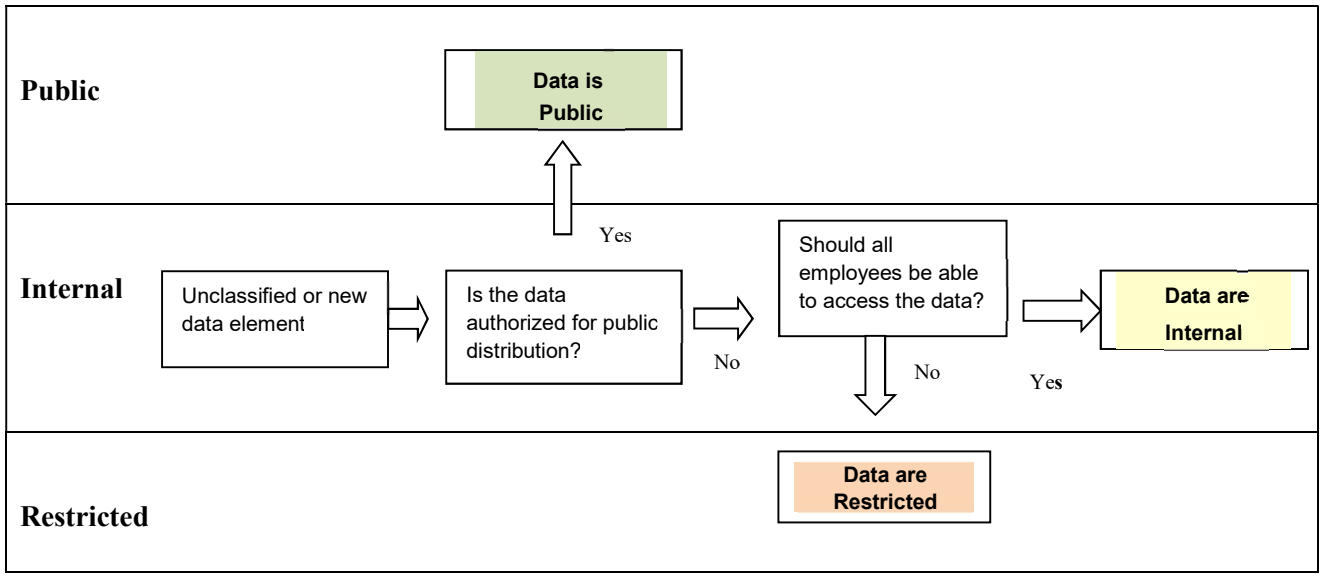
For purposes of this ITSS, the term "personally identifiable information" means an individual's first name and last name or first initial and last name in combination with any one or more items of personal information, such as social security number or other identity verification number, driver's license number or state-issued identification card number, student and/or employee ID numbers, financial account number, credit or debit card number, date or place of birth, and gender; provided, however, that "personally identifiable information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

2.4 Minimum Classification

All information should be assumed *Internal* unless classified otherwise.

2.5 Classification Flow Chart

The Classification Flow Chart on the following page is intended to assist a Data Owner, document creator or user to assist in quickly determining the classification of a data element or document.



2.6 Information Access

The Data Owner makes access decisions regarding information they are responsible for and must be consulted when access decisions are to be made, extended, or modified. Please refer to ITS 12 - Information Security – Access Control for additional information.

2.7 Periodic Review

Information asset classifications must be reviewed by the Data Owner at least every two years, or when necessary based on business need.

ITS 06 – Secure Operations

1.0 Purpose and Scope

The objective of this ITSS is to describe policies for secure operations of Rio Hondo Community College District (RHCCD) information and systems. The following topics are covered:

- Operations Processing
- Virus Management
- Patches and Updates
- Backup AR
- Third Party Management

2.0 Secure Operations

2.1 Virus Management

All applicable systems must be configured with ITS-approved anti-virus software. The software must be configured to scan for viruses in real-time. Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software.

All systems with anti-virus software must be configured to update virus signatures automatically.

End users must not be able to configure or disable the software.

All anti-virus mechanisms must generate audit logs to aid ITS in detecting and responding to virus outbreaks.

All RHCCD employees may obtain approved anti-virus software to install on RHCCD assets from ITS.

2.2 Patches and Updates

RHCCD must ensure that all system components and software are protected from known vulnerabilities by installing the latest vendor-supplied firmware, security patches, hot fixes, and service packs found to be applicable to RHCCD computing resources.

ITS system administrators must keep up with vendor changes and enhancements. New or modified non-urgent patches must be scheduled and installed within one month of release. Urgent patches that address security vulnerabilities must be installed as soon as is feasible without introducing instability or impacting service availability.

Where feasible, patches must be tested in a test environment prior to production deployment. Testing must ensure that systems function correctly.

Changes to servers and networks should be tested prior to implementation and follow normal change control management procedures.

ITS must identify new security vulnerabilities by monitoring available vendor or industry security sources. Hardening and configuration standards must be updated as soon as practical after new vulnerabilities are found.

2.3 Software and Asset Management

The Electronic Communications and the Acceptable Use ITS 01 set forth usage procedures for critical technologies that include e-mail usage and Internet usage and defines proper use of these technologies. ITS may also issue mobile devices (such as laptops or removable storage devices) and will maintain a list of issued devices and personnel with access to assist in determining owner, contact information, and purpose.

ITS will maintain a list of company-approved products and software.

2.4 Backup and Media

Users must store all critical files on the local area network so they can be properly backed up.

Any backup media that must be transferred that contains *Restricted* information must be sent by secured courier or other delivery method that can be accurately tracked. Management must approve all media that are moved from a secured area.

Strict control must be maintained over the storage and accessibility of backup media. Inventory logs of all media must be maintained and reviewed at least annually.

Media must be destroyed when it is no longer needed for business or legal reasons. Data retention requirements must be documented.

2.5 Third Party Management

A third-party user is a non-RHCCD employee or entity that is authorized to access RHCCD systems and networks. Examples of third-party users include consultants, contractors, temporary employees, interns, vendors, business partners, service providers, and suppliers of products, services, or information.

A process for engaging service providers must include proper due diligence prior to beginning the engagement. A list of all third-party providers must be maintained.

Network connections between the RHCCD environment and third parties must follow agreed-upon security procedures and/or confidentiality requirements. Such connections and other third-party access to RHCCD's systems must be governed by formal written agreements or contracts.

These agreements may require signed Confidentiality and Non-Disclosure statements restricting the subsequent usage and dissemination of RHCCD information.

Vendors or other third parties with access to RHCCD-owned or leased equipment or systems housed in RHCCD data center are restricted to only the specific equipment and systems they are authorized to maintain or monitor.

2.5.1 HIPAA Third Party Agreements

HIPAA regulations specify that formal written agreements must be established with each party (often considered a "business associate") who will access protected health information (PHI). The parties must agree to protect the integrity and confidentiality of the information being exchanged, and the agreement would clearly define responsibilities of both parties.

- RHCCD security policies and security mandates, including any fines and penalties that may be incurred for HIPPA or PCI non-compliance for lack of compliance with the regulations
- Ownership and acceptable uses of PHI and other classified information
- Requirements for business continuity by the third party, in the event of a major disruption, disaster or failure
- Audit provisions for RHCCD or RHCCD-approved entities in the event of a data compromise. Provisions to ensure that RHCCD, or a RHCCD-approved auditor, will be provided with full cooperation and access to conduct a thorough security review after a security intrusion. The review will validate compliance with RHCCD standards and HIPAA regulators for protecting PHI and other RHCCD information.
- Security of PHI and RHCCD information during third party contract terminations or data transfers.

2.5.2 PCI Third Party Requirements

RHCCD maintains a program to monitor its PCI DSS service providers' compliance status at least annually.

Payment Card Industry Data Security Standard (PCI DSS) requires that shared hosting providers protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A of the PCI DSS.

A written agreement that includes an acknowledgement from any PCI service providers must be maintained to ensure that the third party accepts responsibility for the security of cardholder data the service providers possess.

All service providers providing PCI services must be monitored at least annually to ensure their continued compliance with PCI DSS.

ITS 07 – Network Security

1.0 Purpose and Scope

The objective of this ITSS is to describe controls required to protect Rio Hondo Community College District (RHCCD) information and systems. Network infrastructure must be configured securely to protect RHCCD systems and maintain network integrity and availability. Effective network security will reduce potential vulnerabilities and help to enforce secure access to RHCCD information and technology.

2.0 Network Security

The ITS manages, administers, and maintains RHCCD infrastructure, network components, and firewalls.

2.1 General Network Controls

System configuration standards are in place for critical network and server components that are managed by ITS. Standards must address known security vulnerabilities and industry best practices and provide specifications for "hardening" the native operating system or platform from known security weaknesses.

ITS maintains appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connections. This must include wireless network components and show connections to all networks, any cardholder data (PCI) locations, and wireless networks.

Network diagrams and configuration details must not be disclosed to unauthorized parties unless identifying IP addresses and names have been removed. The data classification level for sanitized (IP addresses, server names, and other identifying elements removed) diagrams is *Internal*. Unsanitized network diagrams have a data classification of *Restricted*. Refer to the *Data Classification: ITS 05* for classification requirements.

Only necessary and secure services, protocols, daemons, etc., should be enabled as required for the function of the system. For any required services, protocols or daemons that are considered insecure, appropriate security features must be enabled. For example, secure technologies such as SSH, S-FTP, SSL, or IPsec VPN should be used to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be unsecure must be maintained by ITS.

Vendor-supplied defaults must be changed before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

System security parameters must be configured to prevent misuse. All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed.

Publicly accessible network jacks should be restricted to authorized systems.

2.2 External Connections and Firewalls

ITS management must approve all new external connections, inbound or outbound, to the RHCCD internal network. All connections into and out of the internal network must be documented and managed.

Firewalls must be deployed to restrict inbound and outbound connections to the RHCCD network.

New network connections requested to be allowed through RHCCD firewalls must be approved by IT Management and require a business case justification.

Ad-hoc modification of firewall rules can jeopardize the security of RHCCD network. Established change control procedures must be followed for all firewall changes.

Where technically possible, firewall rules should be tested prior to implementation.

A review of all firewall and routers must be reviewed annually. This activity must include a review of the specific ports/services/protocols allowed into the environment and proper documentation of the review.

2.3 Wireless Security

Wireless connectivity is provided as a convenience for staff, students, and authorized users utilizing College campus wireless implementation. Staff must be pre-configured by ITS to use the "secure" network. Students and visitors to the College have access to the Guest network, which provides limited access to the Internet and internal resources.

Any other wireless network implementations must be approved by ITS. Ad-hoc wireless networks are not permitted.

Wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings, must be changed prior to implementation.

2.3.1 Wireless Environments and PCI

Wireless networks are not presently used applications that may store, process or transmit cardholder data. If wireless is used for any part of this environment, perimeter firewalls must be installed between any wireless networks and the cardholder data environment and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

For wireless environments connected to the cardholder data environment or transmitting cardholder data, vendor defaults must be changed. This includes but is not limited to default wireless encryption keys, passwords, and SNMP community strings.

2.4 Encryption

Encryption scrambles sensitive information that is stored or transmitted electronically. Cryptographic solutions must adhere to Federal Information Processing Standards (FIPS). Encryption must be used at RHCCD in the following situations.

2.4.1 Passwords

All passwords must be encrypted and unreadable. This includes password files for users, firewalls, routers, operating systems, applications, databases, and web servers.

Password or credential files stored on third party platforms must also be encrypted.

2.4.2 Restricted Data

The Data Classification Policy describes how data is categorized based on its sensitivity, need for confidentiality, or value to RHCCD. Data classified as *Restricted* is the most sensitive category. Its unauthorized disclosure may violate regulations or standards, such as PCI, or contractual agreements with third parties or service providers.

Restricted data may exist in applications, databases or files. Various access controls protect data when in its original location, but when copied, reproduced or transmitted, the original protections are lost. However, the classification and level of protection for a data element must travel with it regardless of its location or format.

Storing *Restricted* data on unencrypted removable devices, personal drives, or various types of USB storage may expose sensitive or confidential data to unauthorized disclosure and is against RHCCD Information Technology Security Standards. If transporting or storing restricted data must be on a removable device, users must work with ITS to ensure the data is secure.

If *Restricted* data is copied from its original location (e.g., to other files, removable devices, or on backup media) it must be encrypted. If sent via e-mail or other transmission means on public networks, it must be encrypted.

2.4.3 Remote Administrator Access

Remote access by security, system, or firewall administrators to perform maintenance or troubleshoot problems presents a greater security risk due to the elevated privileges these individuals possess. System Administrators must connect securely using the VPN to ensure that communications with RHCCD networks from a remote location are over an encrypted channel. This includes any non-console administrative access. Two-factor authentication is required for all network accounts.

2.4.4 Key Management

Key management procedures must be documented for all processes and procedures involving encryption keys, especially if used for cardholder data. PCI DSS requirements mandate strong keys, secure key distribution and storage, periodic key changes, and other requirements.

2.5 Scanning and Vulnerability Management

ITS management must be informed of information security issues and vulnerabilities applicable to RHCCD computing systems. When security issues are identified, ITS is responsible for notifying appropriate personnel, including system and network administrators and IT management.

The primary method for identifying new threats as they arise will be through vendor and security Internet mailing lists. RHCCD will identify and assign a risk ranking to newly discovered security vulnerabilities. As appropriate, platform hardening standards must be updated to reflect measures required for protection from any newly discovered vulnerability.

RHCCD performs internal vulnerability scans on a weekly and monthly basis or after any significant network changes.

The results of these tests are available to ITS management.

2.6 Network Time Protocol (NTP)

All critical system clocks and times must be configured to acquire, distribute, and store a consistent time. All RHCCD production systems must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment.

Internal NTP servers will be configured to request time updates from the Internet site http://time.nist.gov. Client systems able to retrieve time settings from the NTP server will be limited through Access Control Lists (ACL).

The NTP system will always be running the latest available version of the software.

2.7 Payment Card Industry (PCI) Requirements

The following additional network controls are specific to network locations in-scope for PCI:

- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
- Firewall and router configurations must restrict connections between untrusted networks and any system components in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.
- Prohibit direct public access between the Internet and any system component in the cardholder data environment. Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment
- Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Limit inbound Internet traffic to IP addresses within the DMZ.
- Install a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. Do not allow internal addresses to pass from the Internet into the DMZ. Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
- Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)
- Place system components that store cardholder data (such as a database) in an internal network zone.
- Where feasible, implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)
- Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment and alert personnel to suspected compromises.
- Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

ITS 08 – Physical Security

1.0 Purpose and Scope

All Rio Hondo Community College District (RHCCD) information systems must be properly protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within. This ITSS describes physical access methods, visitors, data center security and media disposal.

This is one of a series of information security Information Technology Security Standards maintained by the Information Technology Services (ITS) department designed to protect RHCCD information systems.

2.0 Physical Security

All RHCCD technology locations will employ security control measures to prevent unauthorized physical access, damage, or interference to the premises and information.

2.1 Physical Security Responsibilities

The Campus Security Department manages perimeter security for the college's office and campuses. This group has physical keys to buildings allowing access to all facilities.

ITS is responsible for all data centers in the District: Rio Hondo College in Whittier, El Monte Education Center in El Monte, South Whittier Education Center in Santa Fe Springs, Pico Rivera Education Center in Pico Rivera, and the Fire and Wild Land Academy in Santa Fe Springs.

2.2 Data Center Access

The ITS and College data centers are critical processing facilities that must be protected by defined security perimeters with appropriate security access controls.

An authorized ITS employee is responsible for making sure that visitors entering a RHCCD data center are properly supervised. It is mandatory that all visitors check in with ITS reception or College Technology Departments.

2.3 Equipment Maintenance and Environmental

ITS and College IT must ensure that all utilities (e.g. UPS, generator) and other equipment is monitored in accordance with manufacturer specifications and correctly maintained to ensure the availability, integrity, and confidentiality of information contained within it.

The data center has HVAC units, environmental protection, redundant UPS systems, and exterior backup diesel generator.

Only authorized maintenance personnel can perform repairs. All repairs or service work must be documented. Documentation records must be maintained by Facilities.

Computer room personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers, and in the proper response to smoke and fire alarms.

Smoking, drinking, and eating in computer processing rooms is prohibited.

2.4 Media Disposal and Destruction

ITS must ensure that electronic information storage devices (e.g., hard drives, tapes, USB sticks, removable hard disks, floppy disks, CD's and DVD's) are disposed of in a manner commensurate with their information classification.

All electronic storage devices must be electronically wiped by a process such that data on the storage device cannot be recovered by individuals and/or technology.

External firms responsible for disposing of any type of RHCCD information must be held to any standards specified by contract. This includes confidentiality agreements and adequate security controls.

All Data Owners must ensure that media containing *Restricted* data is destroyed when it is no longer needed for business or legal reasons.

Employees must use proper destruction methods when disposing of RHCCD information. Paper copies of sensitive information must be shredded or incinerated. Users of the information are responsible for disposing of it in secure disposal containers or using another proper destruction method.

2.5 Payment Card Industry (PCI) Requirements

The following additional physical security controls are specific to areas that may contain systems or media that are in-scope for credit card data processing or storage:

- Physical access to publicly accessible network jacks must be restricted. Network ports for visitors should not be enabled unless network access is explicitly authorized by appropriate IT department.
- Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines must be restricted to those authorized to work with cardholder data.

ITS 09 – Network Logging & Monitoring

1.0 Purpose and Scope

The objective of this ITSS is to document the requirements for logging and monitoring at Rio Hondo Community College District (RHCCD). RHCCD monitors its IT infrastructure so that potential security incidents can be detected early and dealt with effectively.

This is one of a series of information security Information Technology Security Standards maintained by the Information Technology Services (ITS) department designed to protect RHCCD information systems.

2. 0 Logging and Monitoring

Monitoring helps speed resolution of system problems and aids in the identification of access control policy violations. The monitoring program also verifies correct operation and the overall success or failure of network, server, and application security controls.

2.1 Logging Responsibilities and Tools

ITS serves as the primary focal point for network logging and monitoring. The RHCCD sites have tools and systems for monitoring network and desktop systems which can also be used by ITS as requested.

Centralized log analysis and event correlation of operating system event logs is performed continuously.

2.2 Basic Logging Requirements

Automated audit trails should reconstruct the following events for all firewalls, routers, database servers, and critical servers, including:

- Alarms generated by network management devices or access control systems
- Changes to the configuration of major operating system network services / utilities / security software
- Anti-virus software alerts

These events should be tracked by:

- User identification (User ID / account name)
- Type of event
- Date and time stamp
- Success or failure indication
- Name of affected data, system component, or resource

2.3 Log Access and Retention

Access to audit files must be limited to authorized administrators and IT management. Only individuals with a job-related need should be able to view, initialize, or create audit files.

Audit files must be kept secure so that they cannot be altered in any way, through file permissions or other means. Precautions must also be taken to prevent files or media containing logs from being overwritten and that sufficient storage capacity is present for logs.

Logs must be kept for the minimum period specified by any business or legal requirements.

2.4 Log Review Schedule

The following table lists logging checks to be performed on a daily, weekly, or ongoing/as needed basis.

IT Security Event	Frequency	Responsibility
Alarms generated by network management devices or access control systems	Daily	ITS Management
Anti-virus software alerts	Daily	ITS Management
Changes to the configuration of major operating system network services / utilities / security software	Weekly or as required	ITS Management
Application logs (e.g., SIS)	As required	ITS Management

2.5 Payment Card Industry (PCI) Requirements

The following additional network controls are specific to network locations in-scope for PCI:

- Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting servers.

ITS 10 – Remote Access

1.0 Purpose and Scope

The objective of this ITSS is to control access to Rio Hondo Community College District (RHCCD) information and systems when connections are made to those systems from a remote location.

This is one of a series of information security Information Technology Security Standards maintained by the Information Technology Services (ITS) department designed to protect RHCCD information systems.

2.0 Remote Access

All connections into and out of the internal network must be documented and managed by ITS. Remote access is not automatically provided to all personnel and must be requested and approved as described below. The exception to this is access to the Student Information System (SIS) through the AccessRio Portal using an Internet browser. Access to the Portal is authorized for both staff and students, based on their job function and role, using assigned credentials and passwords.

Users must use established remote access mechanisms or gateways to District systems. Aside from the web-based AccessRio Portal, three primary approved connection methods are used to gain access to RHCCD systems: an SSL VPN client (supplied by ITS) or the "Remote PC" or "Splashtop" software.

Remote access is prohibited from any public or shared computer or Internet kiosk.

Users may not establish new remote access systems or methods unless approval has been granted as noted below.

All remote access will be audited annually by ITS management.

2.1 Requests for Remote Access

Users create service desk tickets to request remote access. Refer to the *ITS 03 - Access Control* for further information.

2.2 Approvals for Remote Access

New remote access methods: ITS must approve any new remote access method or system.

2.3 Access Controls for Remote Connections

Remote access sessions will be automatically disconnected after 15 minutes of inactivity.

Personal firewall software must be installed on all RHCCD or employee-owned computers with direct connectivity to the Internet that are used to access a District network. Anti-virus software must also be installed and must include the most recent software updates and virus profiles.

Any remote access connection that has been established for a vendor, business partner, or other third party for purposes of support must be immediately deactivated once it is no longer in use.

2.4 Transmission Over Networks

If RHCCD *Restricted* data is to be transmitted over any communications network, it must be sent only in encrypted form. Networks include RHCCD email mail systems, connections using the Internet, and

supplied RHCCD remote access systems. All such transmissions must use software encryption approved by the ITS department. Refer to the *ITS 05: Data Classification* for further information.

2.5 Payment Card Industry Considerations

RHCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). Where cardholder data is present, remote access to those systems must incorporate two-factor authentication. This refers to network-level access originating from outside the RHCCD network to the RHCCD network by employees and third parties.

For personnel accessing cardholder data via remote-access technologies, copy, move, and storage of cardholder data onto local hard drives and removable electronic media is prohibited unless explicitly authorized by the Superintendent/President or the Vice President of Finance and Business.

ITS 11 – Security Incident Response

1.0 Purpose and Scope

The purpose of the Security Incident Response ITSS is to provide requirements and procedural steps that will enable a quick and effective recovery from unplanned Rio Hondo Community College District (RHCCD) security incidents.

This is one of a series of Information Technology Security Standards maintained by the Information Technology Services (ITS) department designed to protect RHCCD information systems.

This Procedure contains:

- Requirements for responding to information security incidents or breaches
- Roles and responsibilities
- Basic procedures needed to respond in a systematic manner

ITS Departmental Procedures exist which contain:

- Security Incident Report template
- Contact information
- Preservation of Evidence
- Breaches of Confidential or Personal Information
- Additional Resources

The primary audience for this ITSS is the Computer Incident Response Team (CIRT), system and network administrators, and those in District and campus or business areas who have been designated to participate in incident response teams.

Depending on the of the incident, steps noted here may be supplemented by additional RHCCD procedures, such as those that exist in other documentation, business continuity plans, operational procedures, technical standards, or in other processes and procedures fitting the circumstances of the incident.

2.0 Security Incident Response

Incident response is an expedited reaction to an issue or occurrence either electronic or physical. Those responding must react quickly, minimize damage, minimize service interruptions, and restore resources, all the while attempting to guarantee data integrity, and preserve evidence.

2.1 Incident Response Information Technology Security Standard

Unplanned security events must be reported to the appropriate operational manager and the District-wide IT Help Desk as quickly as possible. A consistent approach to security incident response can minimize the extent and severity of security exposures.

All security incidents must be documented. Where appropriate, security incidents will be reviewed with ITS management. The Security Incident Report template is used for this purpose.

The process for handling security incidents has the following phases:

- Immediate actions
- Investigation
- Resolution
- Recovery and Reporting

The recommended actions for each phase are described in Section 3.

Any directives issued by a member of the CIRT during a response may supersede this document.

2.2. Maintenance

This Security Incident Response ITSS will be reviewed and updated on an annual basis at a minimum, or as relevant personnel, locations, threats or regulatory/contractual requirements change.

The Incident Response plan and procedures should be tested at least annually.

2.3 Roles and Responsibilities

This section defines roles and teams involved in Incident Response process. Procedures and processes these teams may follow are in Section 3 of this document.

2.3.1 Incident Response Coordinator

All security incidents must be reported to ITS through the IT Help Desk. Where appropriate, Campus Management will determine who will be the overall Incident Response Coordinator (IRC). The IRC will maintain this Security Incident Response ITSS and Incident Reports and coordinate tests and any required training.

2.3.2 Computer Incident Response Team (CIRT)

The Computer Incident Response Team (CIRT) will be responsible for handling the overall RHCCD response effort. CIRT members represent the IT, Legal, HR, and campus organizations. CIRT members who are RHCCD managers may assign others to work on specific tasks of the incident response process.

Not all members of the CIRT will be involved in any given incident. All CIRT members must be willing to accept the responsibility that is required of them and to be able to respond to an emergency at any hour.

2.3.3 Business Response Teams

Business Response Teams may be involved in the incident response process when an incident occurs in a RHCCD business area. Both primary and secondary contacts have been designated for each business area.

2.3.4 Users

Despite the existence of system and audit logs, computer and network users may be the first to discover a security event or possible breach. As noted in the *ITS 07 Network Security*, end users need to be vigilant for signs of unusual system or application behavior which may indicate a security incident in progress.

All RHCCD users are responsible for reporting incidents they detect, which may include virus or malware infections, a system compromise, or other suspected security incidents. Incidents must be reported to the ITS Help Desk.

2.3.5 Managers

RHCCD managers must ensure that employees are aware of their monitoring and reporting responsibilities. They are also responsible for reporting all suspected information security incidents to the District-wide IT Help Desk as soon as possible.

2.4 Contact Information

Refer to ITS departmental procedures for designated personnel and contact information for the IRC, CIRT, and Business Response Teams.

3.0 Incident Response Process

The following section describes the procedures that are common to all types of security incidents and the recommended steps for each phase of a security incident. Please refer to Section 3.3 for specific security incident types.

3.1 Documentation and Preservation of Evidence

Evidence of a computer security incident may be required for civil or criminal prosecution or to document the event for insurance reasons. To preserve evidence**,** all relevant information collected during the incident must be protected. To maintain the usefulness of possible evidence, RHCCD staff must be able to identify each note or piece of evidence and be prepared to explain its meaning and content.

The chain of custody for all evidence must be preserved. Documentation will be required that indicates the date, time, storage location, and sequence of individuals who handled the evidence. There must not be any lapses in time or date. The hand-off of evidence to authorities must also be documented.

3.2 Control of Information

The control of information during a security incident or investigation of a suspected security incident or breach is critical. If people are given incorrect information, or unauthorized persons are given access to information, there can be undesirable side effects, for example, if the news media are involved.

No RHCCD staff member, except the Superintendent/President or the Vice President of Finance and Business or his/her designate(s) has the authority to discuss any security incident with any person outside of the District. If there is evidence of criminal activity, he/she or his/her designates will notify law enforcement and request their assistance in the matter.

The IRC is the main point of contact for all communications (internal or external) to reduce the spread of misinformation, rumors, and compromise of the response. All CIRT members should refer requests for information to the IRC, who will work with the Superintendent/President or the Vice President of Finance and Business and the Public Information Officer (PIO) regarding any communications.

If a hacking incident were to occur, a secure communications mechanism may need to be implemented since the attacker may be monitoring network traffic. All parties must agree on what technology to use to exchange messages. Even the act of two people communicating could indicate to an intruder that they

have been detected. Greater care needs to be exercised when an internal person is suspected or could be an accomplice to the compromise.

Incident-specific information is not to be provided to any callers claiming to be involved. This includes but not limited to systems or accounts involved, programs, or system names. All requests for information should be documented and forwarded to the Incident Response Coordinator (IRC). Members of the CIRT, working with the IRC, will handle any questions regarding the release of any information pertaining to a security incident. Communication may be from the IRC, a member of the CIRT, or through voicemail or IT bulletins.

If a breach involving personally identifiable or cardholder / credit card information has potentially occurred. The relevant Business Response teams must work with the IT and Legal to determine the specific procedures that should be followed and the nature of notification processes.

The Superintendent/President and the Vice President of Finance and Business or his/her designates will be the only persons who may authorize contacting external law enforcement agencies should this be necessary.

3.3 Security Incident Categories

Security incidents at RHCCD fall into one of the following four categories:

Incident Category	Description	Examples
Internal	Any user (authorized or unauthorized) misusing resources, violating the acceptable use ITSS, or attempting to gain unauthorized access	• Unauthorized use of another's account • Authorized user misusing privileges • Intentionally modifying production data • Inappropriate use of College and District computing resources.
External	Unauthorized person attempting to gain access to systems or cause a disruption of service	• Denial of service attacks • Mail spamming • Malicious code • Hacking/Cracking attempts
Technical Vulnerabilities	A weakness in information system hardware, operating systems, applications or security controls	• Compromised password data that should be protected appears to be available • Data integrity issues
Loss or theft	Loss or theft of RHCCD-owned hardware, software; loss or theft of *Restricted* information.	• Lost laptop • Lost smart phone • Lost device or documents containing confidential RHCCD data • Airport authority confiscation of RHCCD hardware or software

		• Theft of RHCCD hardware or other materials • Breach of student data

3.4 Security Incident Severity Levels

An incident could be any one of the items noted in the "Description" column, and be classified as having a severity level, with corresponding actions to be taken to begin investigation of the incident.

Incident Severity Level	Description	Action required
SEVERE / URGENT	• Successful hacking or denial of service attack • Confirmed breach of Personally Identifiable Information (PII) • Significant operations impact • Significant risk of negative financial or public relations impact	**1. Activate CIRT team and notify the IRC.** **2. Notify all necessary management team members** **3. If a breach of PII or regulated information is suspected**
HIGH	• Hacking or denial of service attack attempted with limited impact on operations • Widespread instances of a new computer virus not handled by anti-virus software • Possible breach of student information or PII	**1. Notify Incident Response** **2. Coordinator, who will notify CIRT team members as necessary.** **3. If a breach of Confidential information is suspected**
MEDIUM	• Hacking or denial of service attacks attempted with no impact on operations • Widespread computer viruses easily handled by anti-virus software • Lost laptop / smart phone, but no data compromised	**1. Notify Incident Response Coordinator, who will notify CIRT team members if necessary.**
LOW	• Password compromises – single user • Unauthorized access attempts Account sharing • Account lockouts	**1. Notify Incident Response Coordinator.**

3.5 Security Incident Phases

The process for handling all RHCCD security incidents has four general phases:

1. Immediate actions
2. Investigation
3. Resolution
4. Recovery and Reporting

3.5.1 Immediate Actions

The first actions to be taken are to make an initial identification of the category of incident occurring (Internal, External, Technical Vulnerabilities, Loss or Theft) as described in the table above and notify the IT Help Desk.

The RHCCD *ITS 02: Acceptable Use* directs users to notify the IT Help Desk immediately upon identifying a security incident of any type. As a rule, users should also notify their immediate manager to inform them of the incident. The IT Help Desk will then notify the appropriate response teams to begin investigation and resolution phases.

Response to an incident must be decisive and be executed quickly. Reacting quickly will minimize the impact of resource unavailability and the potential damage caused by system compromise or a data breach.

3.5.2 Investigation

Once reported to the IT Help Desk, a determination will be made as to the Severity Level (Severe / Urgent, High, Medium, or Low) of the incident based on initial reports. The Superintendent/President or the Vice President of Finance and Business or their designate (designate may include college management) has the authority to declare a *Severity* level incident and activate the CIRT. Upon declaration of a security incident, the following actions may also occur depending on the severity and nature of the incident:

- Notification of executive management team members / campus Security
- Notification of ITS Management / Notification of Arctic Wolf
- Notification of any outside service providers
- Notification of Business Response Teams impacted by the security event
- Initiation of a public relations response plan or development of emergency communications
- Notification of business partners and others who may be impacted by the security event
- Implementation of incident response actions for the containment and resolution of the situation needed to return to normal operations

3.5.3 Resolution

RHCCD's immediate objective after an incident has been reported and preliminary investigation has occurred is to limit its scope and magnitude as quickly as possible.

3.5.4 Recovery and Reporting

After containing the damage and performing initial resolution steps, the next priority is to begin recovery steps and make necessary changes to remove the cause of the incident. Reports and evidence must also be organized and retained.

A process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments will be managed by ITS.

3.6 Incident Response Contact Matrix

The following table describes common incidents and the primary reporting contact for each. The Primary contact will be responsible for assigning an IRC.

Category	User Group	Primary Contact
Internal, External, Loss or Theft	Students	Vice President of Student Services
Technical Vulnerability	Students	Vice President Student Services, Director ITS
Internal, External, Loss or Theft	Faculty	Vice President of Academic Affairs
Technical Vulnerability	Faculty	Vice President of Academic Affairs, Director ITS
Internal, External, Loss or Theft	Staff	Executive Director of Human Resources
Technical Vulnerability	Staff	Executive Director of Human Resources, Director ITS

4.0 Glossary / Definitions

Term	Definition
Business Response Teams	Business Response Teams can be activated to enhance RHCCD's response to incidents that affect specific business areas. These teams have established designated contacts for handling incidents or security breaches and enhance collaboration between diverse groups.
Computer Incident Response Team (CIRT)	The CIRT will act as the core incident coordination team for severe security incidents or breaches and is represented by individuals from ITS and business areas.
Incident Response Coordinator (IRC)	The IRC serves as the primary point of contact for response activities and maintains records of all incidents. This individual has overall responsibility and ownership of the Incident Response process.
Security Breach	Unauthorized release or exposure of information that is confidential, sensitive, or personally identifiable. The definition of a breach and the actions that must be taken can vary based on regulatory or contractual requirements.
Security Incident	A security incident is any adverse event that compromises the confidentiality, availability, or integrity of information. An incident may be noticed or recorded on any system and or network controlled by RHCCD or by a service provider acting on behalf of RHCCD.
Security Violation	An act that bypasses or contravenes RHCCD Information Technology Security Standards, practices, or procedures. A security violation may result in a security incident or breach.