Information Security Policies

Name: Tania Diaz
Course/Module: CIST-2881-D1/Module 1

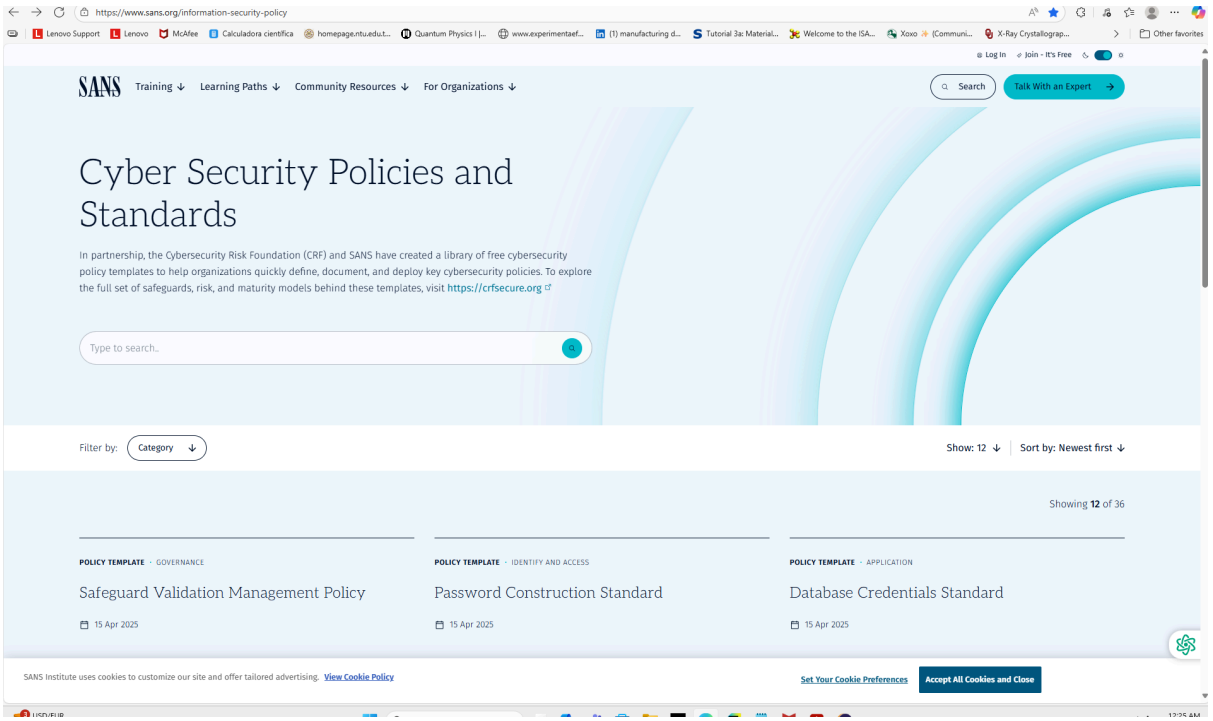
Date: 08/23/2025

Introduction

In this assignment, I researched Information Security Policies, compared them with templates from SANS, and reviewed my institution's policy to identify similarities and differences.

1. Open your web browser and go to http://www.sans.org/security-resources/policies/.

Figure 0: Cyber Security Policies and Standards web



2. Browse through the templates offered and identify key components of the templates.

SANS Policy Templates

Description:
I reviewed the following SANS policy templates:

- SANS Password Construction Standard

Key Components of the SANS Password Construction Standard Template

Purpose. This part explains why the password policy exists. The main goal is to make sure everyone creates strong passwords that are hard for hackers to guess. It gives guidance on how to keep accounts and sensitive information safe.

Scope. This section tells who the rules apply to. It includes employees, contractors, consultants, temporary workers, and anyone connected to the company. It also applies to all types of passwords, like email accounts, system accounts, voicemail, routers, and screen savers. Basically, if you use a password for work, this policy applies to you.

Safeguards / Rules. Here, the policy explains the actual rules for making strong passwords. Passwords should be long, at least 16 characters. It suggests using passphrases, which are multiple words strung together, because they are easier to remember and still very strong. For example, “block-curious-sunny-leaves” is a good passphrase. The policy also says that the company’s security team may test passwords to see if they are weak, and if a password fails the test, the user has to change it.

Policy Sanctions / Enforcement .This part explains what happens if someone does not follow the rules. Consequences can range from refresher training and written warnings to losing access to company systems or even losing your job. In serious cases, there could also be legal consequences. The policy emphasizes that following these rules is important for protecting the company’s data and systems, and everyone will be treated fairly and consistently.

- SANS Cloud Service Provider Management Policy

Key Components of the SANS Cloud Service Provider Management Policy

Purpose.This section explains why the policy exists. Its main goal is to make sure the organization carefully selects and monitors cloud service providers to protect data, maintain security, and follow compliance rules. It focuses on reducing risks like data breaches, downtime, or service problems.

Scope. This part explains who the policy applies to. It includes employees, part-time staff, consultants, and external partners who use cloud services. It covers all types of cloud services like SaaS, PaaS, and IaaS, and ensures that security, access, and data protection standards are followed.

Safeguards / Rules. This section lists the specific steps the organization must take to keep cloud services secure. It includes keeping an inventory of cloud providers and accounts, setting cybersecurity benchmarks, scanning for vulnerabilities, using data loss prevention systems, and collecting logs from cloud services. These rules make sure cloud systems are safe and properly managed.

Policy Sanctions / Enforcement. This part explains what happens if someone does not follow the policy. Consequences can include training, warnings, temporary loss of access, or even termination. Legal action is possible if laws are broken. Enforcement is fair and depends on how serious the violation is.

- SANS Database Credentials Standard

Key Components of the SANS Database Credentials Standard

Purpose. The policy is meant to make sure database usernames and passwords are stored and used safely so that unauthorized people cannot access the database.

Scope. It applies to software engineers and anyone writing programs that access company databases. It covers all programs, libraries, and APIs that connect to production databases.

Rules. The policy says credentials should not be in the main code, must be stored securely, use strong encryption, read only when needed, and cleared from memory after use. Each program should have its own credentials, and only people who need them can know them.

Consequences. If someone breaks the rules, they may face training, warnings, suspension, or termination. Legal actions may also happen if laws are broken.

Screenshots:

Figure 1: SANS Password Construction Standard

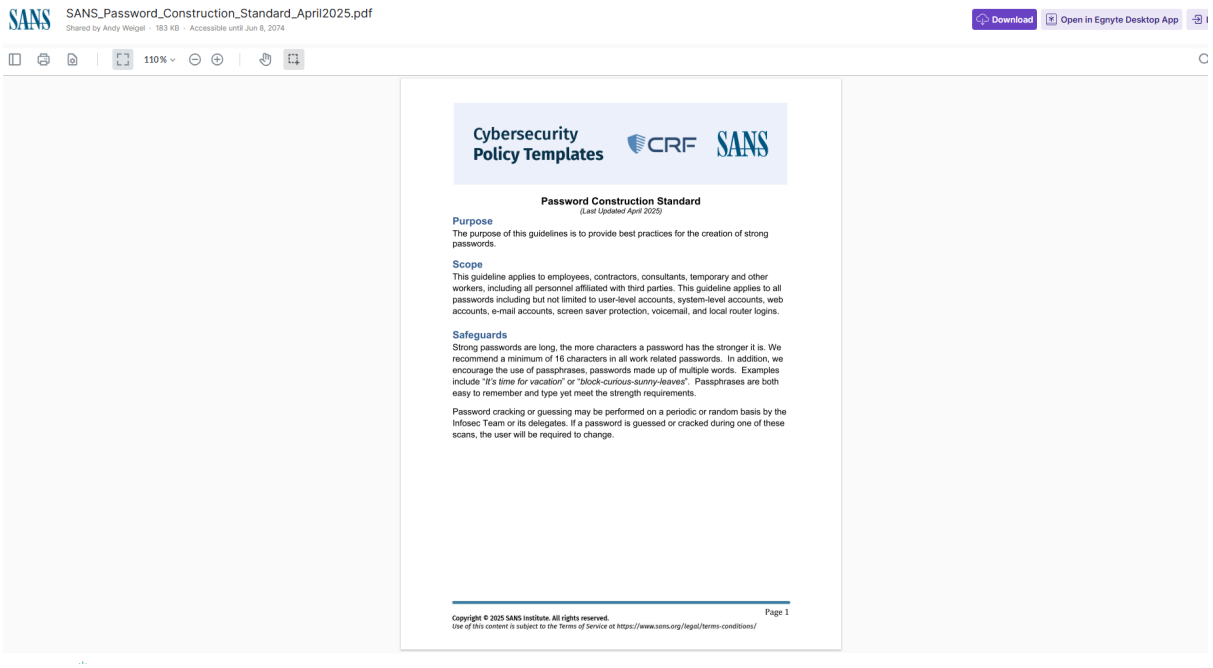
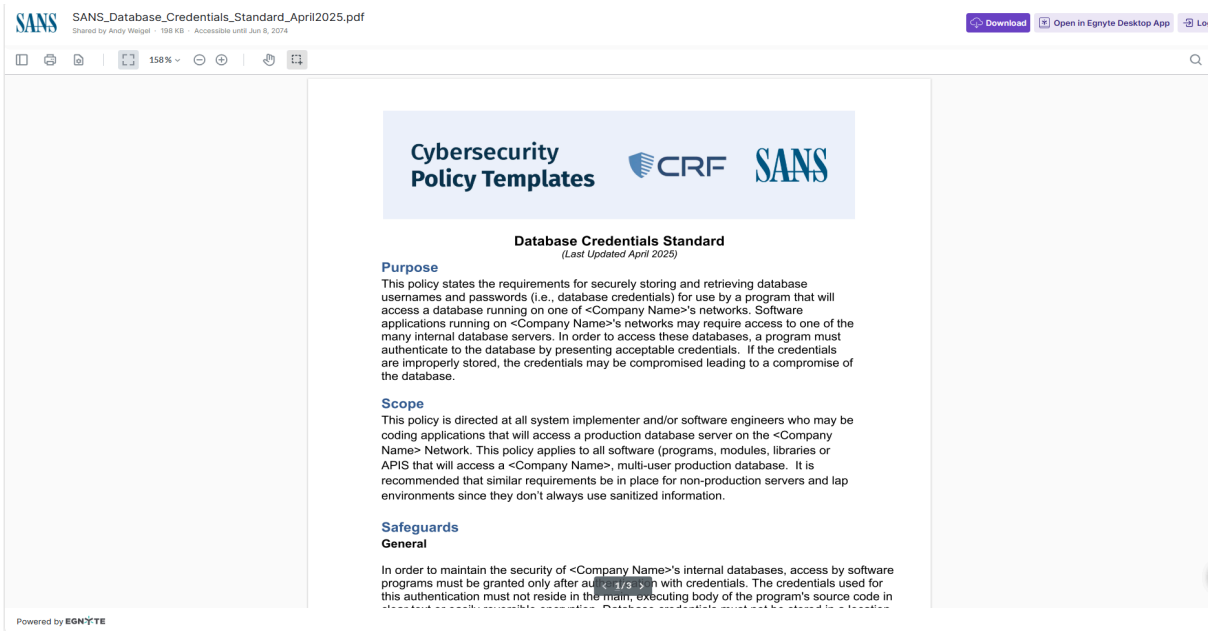


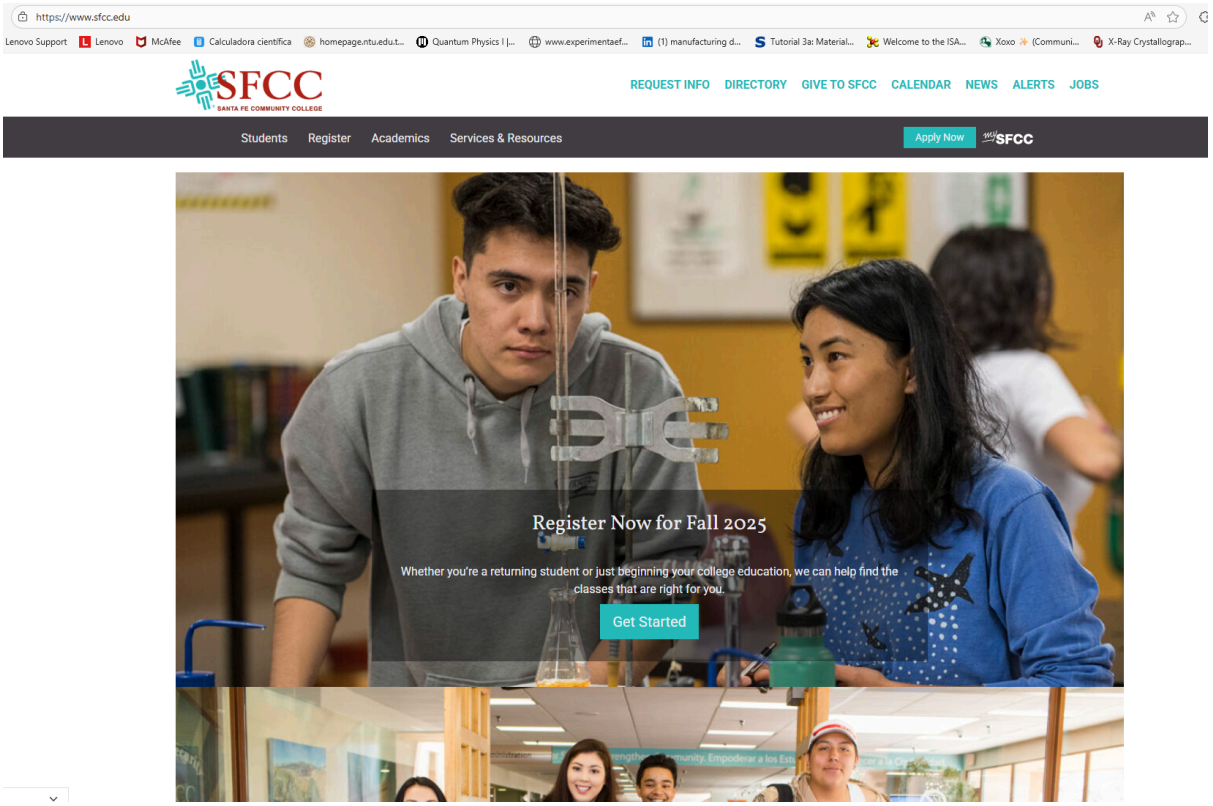
Figure 2: SANS Cloud Service Provider Management Policy

Figure 3: SANS Database Credentials Standard



3. Open a new web browser window and go to your institution's URL.

Figure 3: Institution's Information



4. Search your institution for its Information Security Policy (ISP); it may also be called a Computer Security Policy. Do not mistake this for an Acceptable Use Policy or a Computer Use Policy. You want the document that handles all information security.

Institution's Policy

Description:
I found the following policy on my institution's website: 7-1: Information Technology Resources, Usage and Security – Procedures

Key sections include:

Network Drives

Accounts, Authentication, and Password Management (Includes Preferred Name)

Banner Workday Access Permissions and Requests

Microsoft 365 and Azure

Connecting Personal Equipment to SFCC Networks

Security Breaches or Personally Identifiable Information Exposure

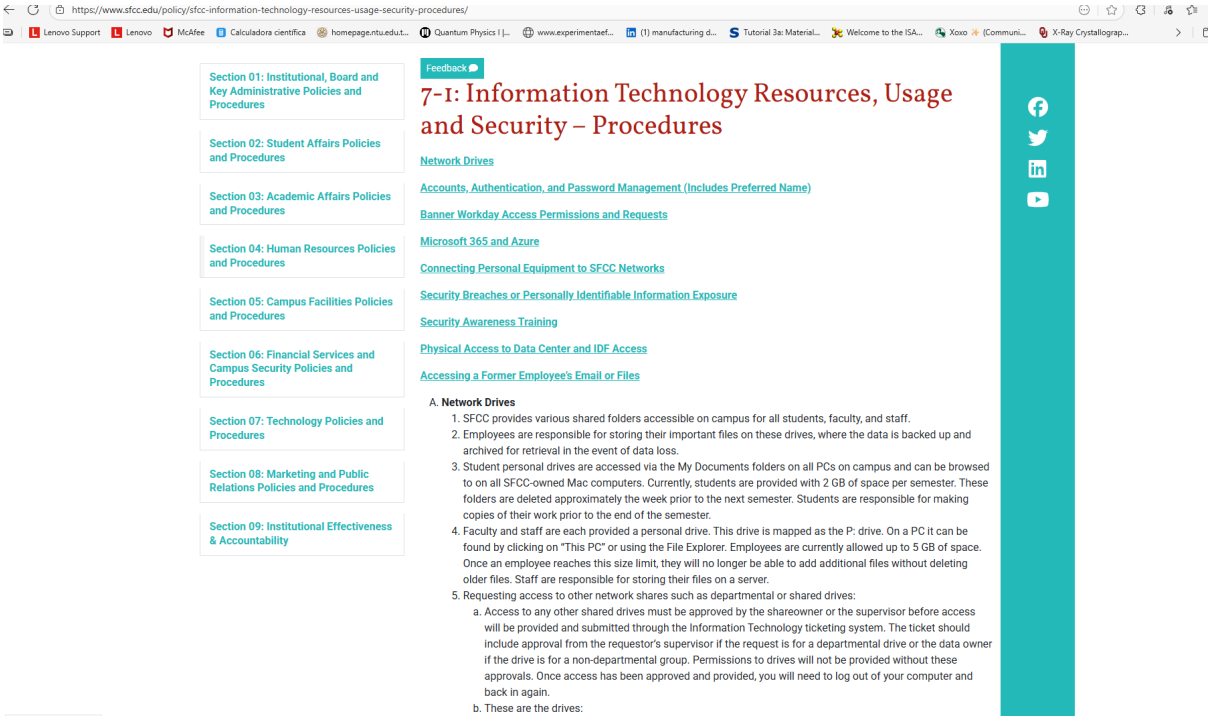
Security Awareness Training

Physical Access to Data Center and IDF Access

Accessing a Former Employee's Email or Files

Screenshots:

Figure 4: Institution's Information Security Policy



5. If you find an ISP, review the document's structure. Compare the policy with the templates you found on the SANS website. Does the ISP contain sections that are included in other policies? Do these policies match the templates found on the SANS website?

The SFCC ISP contains sections that match SANS templates. The "Accounts, Authentication, and Password Management" section is similar to the SANS Password Construction Standard, and the "Security Breaches & Personally Identifiable Information Exposure" section aligns with the SANS Data Inventory Management Policy. SFCC follows SANS guidelines but adds college-specific rules and details. The rest of the comparison is described below.

Comparison

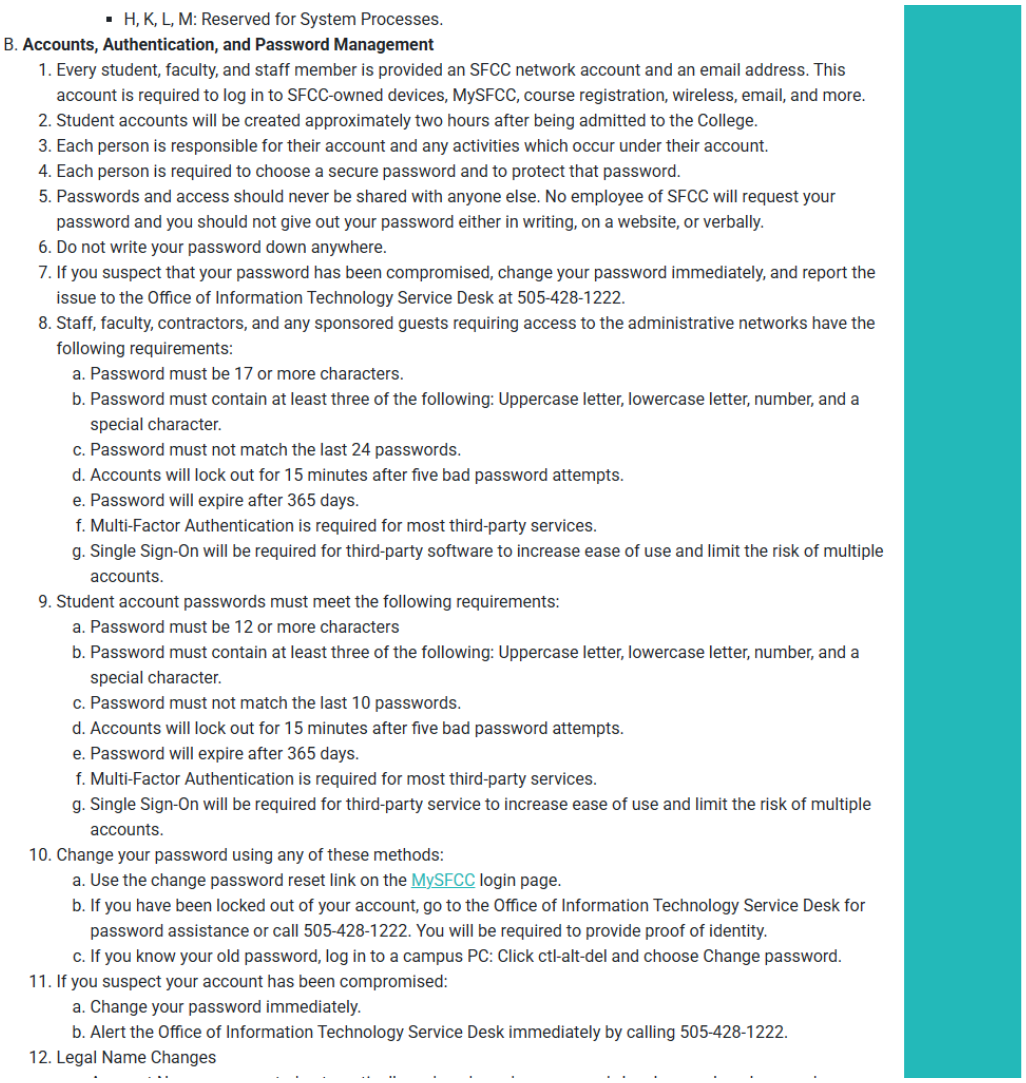
SANS Template: Password Construction Standard
SFCC Section: Accounts, Authentication, and Password Management

Both tell you who needs to follow the rules. SANS focuses on employees and contractors, while SFCC includes students, faculty, and staff.

SANS says to make strong passwords with at least 16 characters. SFCC gives exact rules: students need 12+ characters, staff and faculty 17+, with uppercase, lowercase, numbers, and special characters, plus multi-factor authentication.

Both say users are responsible for following the rules. SFCC also explains how to protect accounts, report problems, and other college-specific rules like network drives and email.

Figure 5: **SFCC Section:** Accounts, Authentication, and Password Management



- H, K, L, M: Reserved for System Processes.

B. **Accounts, Authentication, and Password Management**

1. Every student, faculty, and staff member is provided an SFCC network account and an email address. This account is required to log in to SFCC-owned devices, MySFCC, course registration, wireless, email, and more.
2. Student accounts will be created approximately two hours after being admitted to the College.
3. Each person is responsible for their account and any activities which occur under their account.
4. Each person is required to choose a secure password and to protect that password.
5. Passwords and access should never be shared with anyone else. No employee of SFCC will request your password and you should not give out your password either in writing, on a website, or verbally.
6. Do not write your password down anywhere.
7. If you suspect that your password has been compromised, change your password immediately, and report the issue to the Office of Information Technology Service Desk at 505-428-1222.
8. Staff, faculty, contractors, and any sponsored guests requiring access to the administrative networks have the following requirements:
   a. Password must be 17 or more characters.
   b. Password must contain at least three of the following: Uppercase letter, lowercase letter, number, and a special character.
   c. Password must not match the last 24 passwords.
   d. Accounts will lock out for 15 minutes after five bad password attempts.
   e. Password will expire after 365 days.
   f. Multi-Factor Authentication is required for most third-party services.
   g. Single Sign-On will be required for third-party software to increase ease of use and limit the risk of multiple accounts.
9. Student account passwords must meet the following requirements:
   a. Password must be 12 or more characters
   b. Password must contain at least three of the following: Uppercase letter, lowercase letter, number, and a special character.
   c. Password must not match the last 10 passwords.
   d. Accounts will lock out for 15 minutes after five bad password attempts.
   e. Password will expire after 365 days.
   f. Multi-Factor Authentication is required for most third-party services.
   g. Single Sign-On will be required for third-party service to increase ease of use and limit the risk of multiple accounts.
10. Change your password using any of these methods:
    a. Use the change password reset link on the MySFCC login page.
    b. If you have been locked out of your account, go to the Office of Information Technology Service Desk for password assistance or call 505-428-1222. You will be required to provide proof of identity.
    c. If you know your old password, log in to a campus PC: Click ctl-alt-del and choose Change password.
11. If you suspect your account has been compromised:
    a. Change your password immediately.
    b. Alert the Office of Information Technology Service Desk immediately by calling 505-428-1222.
12. Legal Name Changes

Figure 6. SANS Template: Password Construction Standard

Cybersecurity Policy Templates

CRF SANS

Password Construction Standard

(Last Updated April 2025)

Purpose

The purpose of this guidelines is to provide best practices for the creation of strong passwords.

Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Safeguards

Strong passwords are long, the more characters a password has the stronger it is. We recommend a minimum of 16 characters in all work related passwords. In addition, we encourage the use of passphrases, passwords made up of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type yet meet the strength requirements.

Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change.

SANS Template: Data Inventory Management Policy
SFCC Section: Security Breaches & Personally Identifiable Information Exposure

The SFCC policy talks about how employees have to protect data on campus. It says they need to report lost computers, stolen USB drives, or any problem with accounts, and they have to protect personal information like Social Security numbers, bank accounts, and medical records. It also gives steps for keeping data safe, like locking offices, using strong passwords, shredding documents, and encrypting emails.

The SANS Data Inventory Policy is similar because it also focuses on protecting data. It explains how organizations should track all the data they have, know who owns it, classify it by sensitivity, and make sure it is secure. It also says employees must follow rules and there are consequences if they don't.

Both policies are about keeping information safe, making sure people know their responsibilities, and reporting problems if something goes wrong. The main difference is that

SFCC talks more about personal data for students, staff, and faculty, while the SANS policy is more general for all types of data in an organization.

Figure 7.SANS Template: Data Inventory Management Policy

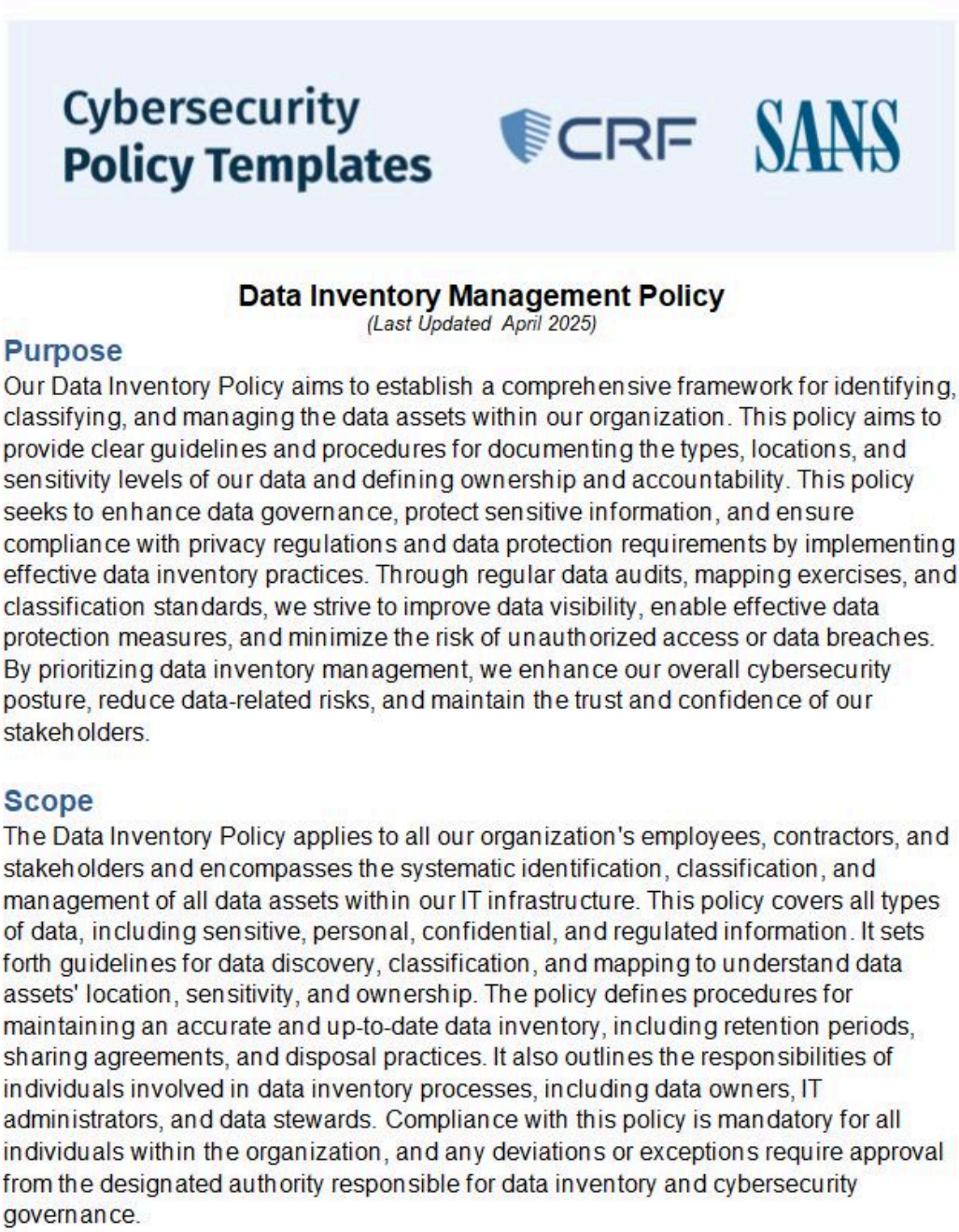


Figure 8.SFCC Section: Security Breaches & Personally Identifiable Information Exposure

F. **Security Breaches & Personally Identifiable Information Exposure**

1. ALL SFCC employees are responsible for protecting campus data.
2. Security breaches can involve stolen or lost computers, stolen or lost USB drives, theft of electronic media, theft or loss of hard copy documents, or unauthorized use of an SFCC account.
3. Even if an employee is not sure that there is a breach, it is best to report the incident to the Office of Information Technology.
4. Employees who handle personal information, which includes Social Security numbers, bank account numbers, driver's license numbers, student identification numbers, birthdates, medical information, or any other identifying information must take steps to protect this information by doing the following:
    a. Alert the supervisor of any actual or suspected security breaches involving personal information. This may include lost or stolen computers, exposed paperwork, or unauthorized access to an employee account. If employees are unsure, it is better to err on the side of caution and report the incident.
    b. Take security steps to maintain confidentiality and integrity of personal information:
        i. Lock offices, rooms, and file cabinets.
        ii. Do not leave paperwork with personal information on desks or in open areas.
        iii. Lock computer access automatically.
        iv. Use unique passwords.
        v. Change passwords often.
        vi. Do not share or document passwords in unencrypted formats.
        vii. Encrypt personal information when sending via email.
        viii. Shred documents containing personal information.
        ix. Ensure screens are not accessible to other people.
        x. Avoid leaving laptops, tablets, and other devices in autos or unlocked areas.
    c. If a data breach has occurred or is suspected, the employee or supervisor must report the incident to the Chief Information Officer or designee. The employee and supervisor should include as much information as possible:
        i. Nature of the breach,
        ii. The information that was exposed,
        iii. To whom it was exposed, and
        iv. For how long it was exposed.
    d. Based on the type of breach, these additional steps should be taken:
        i. If the breach is believed to have occurred on a particular device or system:
            1. Employee(s) should stop using the device or system.
            2. Employee(s) should immediately contact the Chief Information Officer and the Office of Information Technology.
        ii. The Office of Information Technology will determine the best method to evaluate the potential breach.
    e. If the data may have been exposed as a result of a stolen or lost computer:
        i. Report the theft or loss immediately to Campus Security, Safety and Security Office, Main Hallway, Room 101, 505-428-1222.
        ii. Provide details of the data that may have been exposed.