# Password Policy

## Policy Contents

| I. | POLICY STATEMENT |
| II. | REASON FOR POLICY |
| III. | SCOPE |
| IV. | AUDIENCE |
| V. | POLICY TEXT |
| VI. | PROCEDURES |
| VII. | RELATED INFORMATION |
| VIII. | DEFINITIONS |
| IX. | FREQUENTLY ASKED QUESTIONS |
| X. | REVISION HISTORY |
| XI. | COMPLIANCE |
| XII. | POLICY EXCEPTION PROCESS |
| XIII. | APPENDICIES |

## Effective Date: 03-01-2015

## Last Updated: 02-26-2015

### Responsible University Officer:
Opinder Bawa  
Vice President, Chief Information Officer

### Policy Owner:
Director, Information Security Services

### Policy Contact:
ITS Help Desk
I. POLICY STATEMENT

A. The University of San Francisco relies significantly upon the use of university-provided credentials (e.g. USF username and password) to provide authentication for access to online IT resources. In particular, passwords constitute the first line of a layered defense program as the 'keys' users have to gain access to university information and information systems. The risk of compromise of these authentication credentials used by the university community leads to an increased impact on the confidentiality, integrity, and availability of IT systems and information. All users are bound by the Information Security Policy and Technology Resources Appropriate Use Policy to take appropriate measures, as described in these policies, to create and secure all USF associated passwords.

II. REASON FOR POLICY

A. The purpose of this policy is to establish minimum standards for protecting university password complexity (strength), in addition to mandate biannual password refresh. The application of individual accountability and the principle of least privilege are applied in this policy.

III. SCOPE

A. This policy applies to all IT systems managed and operated by USF faculty, students, staff, part-time staff, term staff (under contract employment), and affiliates. This policy may apply to certain non-ITS systems accounts that provide access to sensitive University information and information systems where the exposure to impact would have significant negative impact on University operations.

B. Wherever possible, 3rd party, externally hosted applications and services follow these same password guidelines.

IV. AUDIENCE

A. This policy applies to all university users who have, or are responsible for, user and system accounts in USF IT systems that store or process information.
V. POLICY TEXT

A. Individual Accountability
   1. All users of USF IT systems are each individually assigned a USF username and password for the purpose of unique identification for accessing online systems. In accordance with the USF Information Security Policy and Technology Resources Appropriate Use Policy, users are individually accountable for activities performed with their credentials.

B. Password Security
   1. All production system level passwords for data (e.g. Banner) must be part of the University's centrally administered account management system (e.g. integrated into LDAP or USF/ITS Active Directory). Passwords for USF systems should not be identical to those used for personal online accounts.

C. Password Strength Requirements
   1. User and system level passwords shall be constructed in a manner that minimizes the likelihood of password guessing or brute force attacks.
   2. The password length **must be 8 or greater**.
   3. The password length **must be 15 or less**.
   4. The password **must contain a letter**.
   5. The password **must contain a digit**.
   6. The password **must not be a previously used password**.

D. Password Refresh (Age)
   1. Passwords shall be refreshed biannually to reduce the impact of disclosure due to undetected theft of passwords or the sharing of passwords. In other words, passwords must be changed at least twice per year. Attempting to refresh your password with the same identical password is not permitted.
   2. Passwords may be changed on a more frequent basis depending upon departmental practices and risk to the information managed, processed, or stored. The recommended minimum password age is 1 day.
   3. Upon turnover of staff (change of personnel, rotation of job duties, etc.), system level passwords that are affected by such turnover will be changed within 30 days of the staff turnover. If extenuating circumstances exist, a risk-based
decision will be coordinated between the appropriate Department Manager/Business Officer and the Information Security Officer.

4. If the account credentials of a user or system are suspected to have been disclosed or otherwise compromised, the user shall immediately take steps to change and protect the password.

5. Technical measures may be implemented to ensure compliance with University Password Policy, Information Security Policy, and Appropriate Use Policy.

E. **General Password Protections for Network Logins**

1. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user (e.g. LAN account must be different than USF account).

2. Authentication mechanisms shall use encryption (e.g. SSL or TLS) to protect the login session.

3. Passwords must not be inserted into email messages or other forms of electronic communication without adequate protection (e.g. end-to-end encryption) of the credentials.

4. Applications that request a user ID and password shall not display the password in the data entry field.

F. **Operational Security Standards for Password Use**

1. Do not use the same password for USF accounts as for other non-USF access (e.g., personal ISP account, online stock trading, benefits, etc.). Where possible, don't use the same password for various USF access needs. The use of USF Single Sign On will reduce the number of accounts you need to track, but will make your USF account more valuable to protect.

2. Applications that request a user ID and password shall not display the password in the data entry field.

3. Do not share USF passwords with anyone, including administrative assistants or students (i.e. student workers, etc.).

4. All passwords are to be treated as confidential information.

5. Here is a list of don’ts:
- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to your supervisor or manager
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't share a password with family members: you are individually responsible for what is done with your account
- Don't reveal a password to co-workers while on vacation

6. If someone demands a password, refer them to this policy or refer them to the USF ITS Help Desk (itshelp@usfca.edu). The ITS Security Services department may also be contacted (infosecurity@usfca.edu).

7. Do not use the 'Remember Password' feature of web browsers.

8. Notifications of Changes: USF ITS staff will notify potentially affected end-users of IT systems approximately 10-30 days prior to the implementation of a system level password change.

9. Auditing: An audit cycle will be initiated within 30 days of the close of the password change cycle on selected events to identify the level of compliance and potential risk mitigation.

VI. PROCEDURES

A. (None)

VII. RELATED INFORMATION

A. (None)

VIII. DEFINITIONS

A. compromise

1. When anyone other than the assigned user knows the user's credentials, or the loss of positive control over secured assets and information.
B. **credentials**
   1. The combination of username and a password, and optionally, a third factor such as a security token.

IX. **FREQUENTLY ASKED QUESTIONS**
   
   A. 'Could you please provide me an example, I am a little confused.'
      1. Create a password you alone can easily remember. Use the basis of something you know well, such as a song title, affirmation, common misspelling, or other phrase (etc.). For example, the phrase might be: ‘Only the good die young’ and the password could be: ‘0tg00dDyg’ or ‘OTGd!3Y!’ or some other variation. As you can see in the above examples, numbers and/or symbols may take the place of letters. Further, using a mixture of capital and lower case letters will also assist in password security.
   
   B. 'Can my password contain special characters?'
      1. Yes. As mentioned above there are no special character restrictions for the majority of users; however, if you have authorized INB access - see details below:
         - **WARNING to INB (Internet Native Banner) users only:** use of special characters within your USF password may result in INB access and functionality issues.

X. **REVISION HISTORY**
   
   A. 08-19-2010 – First publication
   B. 02-26-2015 - Last update; new format
   C. 03-01-2015 – Effective date

XI. **COMPLIANCE**
   
   A. Failure to follow this policy can result in disciplinary action in accordance with [Human Resources Employment Handbook](#) and [Office of General Counsel](#) employee and labor relations. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.
XII. POLICY EXCEPTION PROCESS

A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES

A. (None)