USAID
FROM THE AMERICAN PEOPLE

Password Creation Standards

A Mandatory Reference for ADS Chapter 545

Full Revision Date: 09/14/2017
Responsible Office: M/CIO/IA
File Name: 545mau _091417

Table of Contents

1. Overview

This document, a mandatory reference for **ADS 545, Information Systems Security**, provides guidelines for creating passwords.

2. Introduction

2.1 Purpose

This document helps you understand a password, create a password, protect a password, and work with password exceptions.

2.2 Scope

This reference describes mandatory standards for USAID passwords on USAID-managed network space, service accounts, and GFE laptops and servers.

2.3 Background

The Office of Management and Budget (OMB) mandates that agencies use a list of security settings known as the United States Government Configuration Baseline (USGCB). Recommended by the National Institute of Standards and Technology (NIST) for general-purpose microcomputers connected directly to a network of a United States government agency, the entire USGCB has been adapted by USAID, including standards for creating passwords.

3. Understanding Passwords

3.1 Defining a Password

A password is a unique string of characters that a user must type to gain access to a computer system.

3.2 Defining Password Purpose

The purpose of a password is to authenticate a user before the user is granted access to a USAID IT resource. A password allows a user to access an IT resource, admits the user with a password that meets established criteria, and rejects a user with a password that does not meet criteria. A password defends against unauthorized access of USAID IT resources that could result in a compromise of personal or institutional data.

4. Creating a Password

4.1 Meeting Standards for a USAID Password

When a USAID user creates a password, it must meet USGCB password standards.

A USAID password must:

- Be at least 12 characters in length;
- Contain at least three of the four following character types:
    1. Uppercase (ABCDEFGHIJKLMNOPQRSTUVWYXZ),
    2. Lowercase (abcdefghijklmnopqrstuvwyxz),
    3. Symbols (,./`~<?;':"[]{}\|!@#$%^&*()-=_+),
       Note: Usable symbols vary by Operating System (OS) and application. Some symbols may designate meta-characters, instructions, or delimiters which may be reserved by the OS or application and may not be used with passwords.
    4. Numbers (0123456789);
- Not be similar to or contain any portion of your name;
- Not be similar to or contain any portion of your login name;
- Not contain words (English) that are longer than four letters;
- Not begin or end with a number;
- Not be the same as any of the previous 24 passwords in the password history;
- Be changed at least once every 60 days; and
- When password is changed, at least four characters must be changed.

4.2 Meeting Standard for Administrative and Service Accounts

When a USAID user creates a password for an administrative or service account, the password must meet USGCB standards.

A USAID password for administrative and service accounts must:

- Be at least 20 characters in length;

- Contain at least three of the four following character types:

    1. Uppercase (ABCDEFGHIJKLMNOPQRSTUVWYXZ),

    2. Lowercase (abcdefghijklmnopqrstuvwyxz),

    3. Symbols (,./`~<?;':"[]{}\|!@#$%^&*()-=_+),
    Note: Usable symbols vary by OS and application. Some symbols may designate meta-characters, instructions, or delimiters which may be reserved by the OS or application and may not be used with passwords.

    4. Numbers (0123456789);

- Not be similar to or contain any portion of your name;
- Not be similar to or contain any portion of your login name;
- Not contain words (English) that are longer than four letters;
- Not begin or end with a number;
- Not be the same as any of the previous 24 passwords in the password history;
- Be changed at least once every 30 days; and
- When password is changed, at least four characters must be changed.

4.3 Guidelines for Creating a New USAID Password

The following are guidelines for creating a strong password:

- Use substitute vowels:

    1. 'a' can be replaced with '@',

    2. 'e' can be replaced with '3',

    3. 'i' can be replaced with '1',

    4. 'o' can be replaced with '0',

    5. 's' can be replaced with '$',

    6. 't' can be replaced with '+',

7. ‘v’ can be replaced with ‘^’, etc.

- Turn a passphrase into a password:

    a. Think of a passphrase, for example: “Now is the time for all good men to come to the aid of their country.”,

    b. Identify the initial letter of each word in the passphrase: nittfagmtcttaotc,

    c. Use vowels to substitute for the initial letters to create a password: N1++f@GM+ctt@0+c;

- Do not use a sequence of keys on the keyboard, such as ‘qwerty’ or ‘12345’, etc.);

- Do not use information about yourself, family members, friends, or pets. This includes (in whole or part) names, birthdates, nicknames, addresses, or phone numbers;

- Do not use words associated with your occupation or hobbies;

- Do not use words associated with popular culture (e.g., names of television shows, characters, bands, band members, song titles, athletes, or teams, etc.); and

- Do not reuse passwords used for other accounts.

5. Protecting a Password

Passwords protect your USAID account from unauthorized use. You are responsible for all activities associated with your USAID account. To show due diligence, USAID employees must protect their passwords from unauthorized access, use, modification, or disclosure. USAID employees must never share, write down, or insecurely store their passwords.

There is a qualification for the use of group passwords. According to **ADS Chapter 545**, group passwords may be used when necessary under this guidance: “Use of group passwords is limited to situations dictated by operational necessity or mission accomplishment. The Approval Official (AO) and Chief Information Security Officer (CISO) must approve use of a group user ID and password.”

If you suspect that your USAID password has been compromised, change it immediately, and then notify your System Administrator, your local Information System Security Officer (ISSO), the Bureau for Management, Chief Information Office (M/CIO) Service Desk (**CIO-Helpdesk@usaid.gov**), or the CISO, as appropriate. USAID

reserves the right to change your password or to force you to change your password in order to protect the integrity of its information systems.

6. Requesting a Password Exception

If an OS, application, network appliance, or other device cannot meet the USGCB standard, the System Owner (SO) should contact the CISO for guidance by opening a ticket with the M/CIO Service Desk (**CIO-Helpdesk@usaid.gov**). The SO should include details of the standard which cannot be met, why the standard cannot be met, the compensating control from the standard, and justification for the compensating control. The CISO will evaluate the details and the compensating controls and may issue a written waiver, to be signed by the SO, the CISO, and the CIO, acknowledging and accepting the risk to the Agency.

545mau _091417