Idaho Technology Authority (ITA)

Enterprise Guidelines G500 – Security Procedures

Category: G560 – Passwords

CONTENTS:

I. Definition
II. Rationale
III. Guideline
IV. Procedure Reference
V. Contact Information
VI. Password Overview
VII. Composing Passwords
VIII. Protecting Passwords
IX. Integrating Passwords with Network Rules
X. The Importance of User Education
Revision History

I. DEFINITION

Password - for the purposes of this policy, includes those combinations of letters, numbers and special keyboard characters that authenticates a user's identification to a state network via their desktop personal computer, laptop, mobile device, etc.; that authenticates remote access to a state network; or that authenticates access to network servers and infrastructure.

II. RATIONALE

This guideline is intended to assist agencies with developing password policies that apply a level of security appropriate to their needs. While there are senior executives in prominent technology companies who are pushing for replacement of passwords as inadequate to today's security needs, most technology executives recognize that there must be and will continue to be a place for passwords in networks for some time to come.

III. GUIDELINE

There is no guideline for this guideline.

IV. PROCEDURE REFERENCE

Policies for passwords are detailed in ITA Information Technology Enterprise Policies *P4110 – Agency IT Security Coordinator.*

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

VI. PASSWORD OVERVIEW

Passwords are obviously intended to protect access to information and systems. While there are a number of two factor authentication systems available today that are designed to provide increased security over the traditional password, this guideline is focused on the conventional passwords we've been using for years.

Malevolent hackers may try a number of things to circumvent protections provided by passwords. They may make thousands of attempts to 'guess' a single user's password through an automated attack. This type of attack will certainly include a lengthy list of common passwords. They may also try a shorter list of commonly used passwords against numerous users, all in the hopes of finding a weakness. The method they use depends on what information they already have and what they're trying to accomplish. Apart from those 'brute force' approaches, they may try some social engineering scam to trick a password out of unsuspecting users.

Agencies need policies that minimize the chance an unauthorized person will obtain passwords no matter what method they use. One important aspect of this effort is helping users choose strong passwords in the first place.

VII. COMPOSING PASSWORDS

With just lower case letters and 8 positions, there are over 200 billion possible password combinations. That's a lot of potential passwords to guess, so why would an agency need a special policy? One reason is that "many users choose very easily guessed passwords, where the system will allow them to do so". It's common sense that people might do that, but we can verify the truth of it in National Institute of Standards and Technology (NIST) Special Publication 800-63-2, Electronic Authentication Guideline.

Here are some things agencies and users can do to create **strong** passwords:

1. Use a least 8 characters. The longer the better.

2. Use upper and lower case letters (A-Z, a-z).

3. Use at least one number and one special character (0-9, ! @ # $ % ^ & * ( ) [{] } etc.).

4. Be creative and unique.

5. If a PC's operating system is Windows 2000 or newer, don't be afraid to use a passphrase of 20 characters or more! Complex passphrases (e.g. '1 Must reMember 2 Do Thi$') offer powerful protection, are easy to remember, allow creativity, and can be surprisingly quick to type.

Here are some things users should avoid, because they make for **weak** passwords:

1. Including part of your full name or user identification.

2. Including personal information such as birthdays or anniversaries.

3. Using a word, whether it's foreign, slang, jargon or dialect.

4. Using names of family, friends, heroes, pets, etc.

5. Using a password or phrase you've seen as an 'example'.

6. Using 1. - 5. above backwards.

7. Adding a number or special character to the beginning or end of 1. – 6. above.

VIII. PROTECTING PASSWORDS

Creating a super password that's easy to remember, difficult to guess, and quick to type is not that tricky. But, the effort is wasted if we don't make the extra effort to protect the password.
Conventional wisdom indicates that we should not write passwords down, but that may be becoming an impractical rule. As the number of passwords one must know increases, so does the likelihood that they will be written down, regardless of policy, simply to help manage them.

The issue is really where the written password is too often left … on a sticky note on the computer, taped under the keyboard, or in a memo pad in the desk drawer. That's no more secure than hiding a door key under your welcome mat. Safe combinations protecting classified defense information are routinely written down, but then are protected as classified information in their own right. Why not record passwords where appropriate?

Rather than make a rule that employees may not be able to practically follow, some argue it would actually be more secure to allow passwords to be written down but to require that they be locked away, encrypted in a data file or otherwise secured when not in use.

There are prominent security experts who advocate allowing users to record passwords. That may not be suitable for every agency or every system in an

agency, but if it is right for your agency, make sure to set and enforce rules on when, where and how to store passwords … taped behind the family portrait on a desk is not the right place.

Some rules users should follow to protect their passwords:

1. Never reveal a password over the phone, in an email, or to a co-worker.

2. Don't give hints about your password's composition.

3. Don't reveal your password for surveys, questionnaires, or any other such purpose.

4. Don't use the "Remember Password" feature.

5. Don't use the same password for multiple systems.

IX. INTEGRATING PASSWORDS WITH NETWORK RULES

Passwords and network rules work hand in hand. Once rules for password composition are established, set up network rules that reject passwords that don't meet those requirements.

Network rules can also help defend against brute force attacks by locking out user accounts after some number of missed attempts at a password. Even if the account is only locked for a few minutes after two or three failed attempts, that severely limits how many passwords an intruder can attempt in a given amount of time.

For example, with just a 10 minute lockout after three attempts, a brute force attack will be able to make about 150,000 attempts in a year. But, with an 8-character, complex password, there are over 6 quadrillion possible combinations. Combine strong passwords with a reasonable change interval, and there's not likely to be enough time to break a password before it changes.

It's generally true that a shorter password lifecycle offers better protection, but agencies need some balance between the threat and user convenience. Depending on the needs of the agency and the sensitivity of the information or system protected changing passwords every 3 months only. Highly sensitive systems or information may require stricter rules, but with proper rules in place and educated users, that balance can be achieved.

Having network rules on password composition will also help defend against brute force attacks aimed at multiple users, as it prevents some all too common but truly weak passwords (like 'password', '1password', etc.) from being used.

Whatever rules are set, don't make exceptions to the password policy. Those individuals important enough to warrant special treatment are typically also those who are more visible to the public and, therefore, often more attractive targets for attack.

X. THE IMPORTANCE OF USER EDUCATION

Yes, there are over 6 quadrillion possible combinations in an 8-character, complex password, but many users will choose the weakest password the system allows. Sorry, but '@Password1' will not last long against an attack. That's why education is important.

Protecting access to state information and systems is everyone's responsibility. That some individuals have specific responsibilities does not detract from the basic responsibilities everyone shares, such as adhering to policies established by their agency or the state.

Let users know why they should follow, rather than circumvent or ignore, security policies and give them some accountability for this.

Make clear what's at stake, whether it's a compromise of a state or agency system, of information on that system or perhaps even the user's own information, because the reality is that a weak or unprotected password from a single user may result in far greater compromise than that single user's own information or system.

Get the idea across that passwords and protecting state information are important. Whether dealing with education, health and human services, public safety, natural resources, economic development, or general government there is a threat out there.

Help users understand that a hacker may be motivated by anything from simple 'bragging rights' among peers to personal financial gain or forwarding some ideological agenda, so no system is sufficiently obscure to avoid attention. An internet search on 'cracking passwords how to' returned 2.5 million hits in about half a second.

And, here's another plug for passphrases. Let users know about them, and how they and the state can benefit from them. The sheer number of possible passphrases is staggering, increasing exponentially with every added character. Passphrases belong in the security toolkit.

REVISION HISTORY

07/01/13 – Changed "ITRMC" to "ITA".

6/16/09 – Added Guideline, Procedure Reference, Contact Information and Revision History to this guideline; changed the layout and deleted Timeline.

Effective Date: October 24, 2005