

Policy Title: Password Policy and Standards	Approval Date: 12/18/2008
Policy ID: 5101	Effective Date: 12/18/2008
Oversight Executive: VP for Information Technology & CIO	Review Date: 7/1/2009

1. Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The purpose of this policy is to establish a policy for creation of strong passwords standards to protect University systems and data.

2. Policy

General Password Guidelines

- Users must maintain exclusive control of passwords and never share passwords with other users.
- Users must maintain unique passwords for each system they have access to.
- Users must maintain separate passwords for University and non University personal accounts (e.g., Google Mail, eBay, Facebook, online banking, ...).
- Passwords must not be sent via email or other forms of electronic communication without the use of an approved encryption method.
- Passwords should not be written down. If it is required to write down a password, it must be documented and stored securely.
- Systems must be configured allowing users to change their password at will.
- The display of passwords must be suppressed on the screen when logging in.
- Passwords must never be stored in documentation, system files, program files or scripts in clear text.
- Passwords must be changed at first login or when the account is activated.
- All passwords should be based on the following password complexity rules:
 - At least eight characters in length
 - Passwords should not be based on a single dictionary word or username
 - Passwords should use at least three of the following
 - Special characters
 - Alphabetical characters
 - Numerical characters
 - Combination of upper case and lower case letters
- Users must notify the RU Information Security Officer (ISO) and change their password immediately if they suspect their password has been compromised.
- The RU Information Security Officer (ISO) or his/her delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

University Owned Mobile Devices

- Users of University owned handheld devices including PDAs, Blackberries, iPhones and smart phones must use a password or 4 to 5 digit PIN.

Minimum Standards for Passwords on Non-Sensitive Systems

- All user-level passwords for Active Directory (portal, email, WebCT, library, home directory, etc.) must be changed at least every 12 months.

Minimum Standards for Passwords on Sensitive Systems (*IFAS/IRIS, Banner, System Level Accounts*)

- Account access to sensitive IT systems and information should require a password.
- Group accounts and shared passwords are prohibited on accounts that have access to sensitive IT systems.
- All passwords on sensitive IT systems must be changed every 90 days.
- Systems should be configured to maintain a history file to prevent the reuse of the same password.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

SNMP Passwords Standards

- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

3. Procedures

4. Definitions

ISO – Information Security Officer

SNMP – Simple Network Management Protocol

5. Related Information

6. Policy Background

7. Approvals and Revisions

Approved: December 18, 2008 by Radford University Cabinet