OFFICE OF INFORMATION SECURITY

Tools

Request Support

Policies and Regulations

Hot Topics

- Phishing
- Identity Theft
- Protect Your Computer
- Protect Your Data
- Security Awareness
- Secret Question and Answer Pairs

Report an Incident

ArchPass

- Log In With ArchPass

Password Policy

1.0 Overview

Passwords are one of the primary mechanisms that protect University information systems and other resources from unauthorized use. Constructing secure passwords and ensuring proper password management are essential. Poor password management and construction can allow both the dissemination of information to undesirable parties and unauthorized access to University resources. Poorly chosen passwords are easily compromised. Standards for proper password creation and management greatly reduce these risks.

2.0 Objective / Purpose

This document establishes the need for minimum standards for password creation and management used by MyID and other University computing accounts. This document also outlines enforcement for password policy violations.

3.0 Scope

This policy applies to MyID and all other accounts on computing resources administered by the University.

4.0 Policy

Computing accounts shall be protected by strong passwords. Account holders and system administrators shall protect the security of those passwords by managing passwords in a responsible fashion. System developers shall develop systems that store or transmit password data responsibly and that use secure authentication and authorization methods to control access to accounts.

5.0 Enforcement and Implementation

5.1 Roles and Responsibilities

Each University department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this Policy.

The Office of Chief Information Officer is responsible for enforcing this policy and is authorized to set specific password creation and management standards for University systems and accounts.

5.2 Consequences and Sanctions

Violations of this policy may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

Systems and accounts that are found to be in violation of this policy may be removed from the UGA network, disabled, etc. as appropriate until the systems or accounts can comply with this policy.

6.0 References

- Password Standard
- Progressive Discipline Guide

- Student Code of Conduct

EITS 〉Access and Security 〉Office of Information Security 〉Policies and Regulations 〉Policies, Standards, and Guidelines 〉Password Policy

Service Categories:

Email & Calendar
Learning & Training
Network & Phones
Access & Security
Hardware & Software
Servers & Storage
Support
Web & Applications
About EITS

helpdesk@uga.edu
706-542-3106
101 Cedar Street
Athens, GA, 30602-1130

Media Contact