



## **ASU Privileged Account Standard**

Version 0.2  
March 2009

## Table of Contents

1 PURPOSE .....	3
2 SCOPE .....	3
3 ENVIRONMENTS.....	3
4 STANDARD.....	3
5 ENFORCEMENT.....	3

## 1 PURPOSE

The purpose of this document is to meet security requirements for managing login access, e.g., SSH and RDP, to the UTO enterprise Dev, QA and Prod server environments.

## 2 SCOPE

The standard set in this document will apply to ASU faculty, staff, student workers, and other individuals who have been granted access to UTO servers. This procedure doesn't apply to UTO general public access servers, e.g., general.asu.edu and stats.asu.edu.

## 3 ENVIRONMENTS

- A. **Dev** environments are those servers used for the development and testing of applications.
- B. **QA** environments are servers used for pre-production quality assurance of applications.
- C. **Prod** environments are the final deployment areas for applications. Applications that run in the Prod servers are the outward facing public applications such as [my.asu.edu](http://my.asu.edu).

## 4 STANDARD

Access to UTO Enterprise Dev/QA/Prod server environments is granted on a need-basis, as defined by a user's role within the University. Access will be removed if a user changes positions or leaves the University. If a user has changed positions, continued access will be contingent upon whether or not access is required for the user's new role.

## 5 ENFORCEMENT

Maintaining access to UTO servers for users whose role has not changed is determined by usage. If an account has not logged into a server within the past 90 days, a suspension notification will be emailed to the user and access to the server will be removed.

Account access will be locked out if an account password has not been changed within the past 90 days.

## 6 STANDARD SAFEGUARDING

Modification and review of this standard will occur every six month and is to be approved and put in place exclusively by the Chief Information Security Officer. To offer suggestions and/or recommendations, please contact DL.WG.INFOSEC.