**IT Password Group Setup Form**

Use this form to initially establish a group of HSU Users whose HSU Username Passwords need to be held to an aging standard due to audit requirements, state or federal law, or HSU Departmental Policy. **See following HSU IT Procedure HSU-004 for more information.**

HSU Username Passwords are a minimum of eight characters and must include at least one numb er, one letter, and one special character.

Enhanced Password Settings for this Group

| | |
|---|---|
| Maximum Age of Password | Days |

Initial Group Membership for

| Full Name | HSU Username | Full Name | HSU Username |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

The following group administrator and backup group administrators are authorized to maintain the group membership through the HSU Registry Group Administration web form

| Group Administrator | Backup Group Administrator |
|---|---|
| | |

The following Administrator (MPP or Department Chair) has authorized that the above HSU Users be held to this enhanced password policy

| Name | Title | Signature/Date |
|---|---|---|
| | | |

# HSU-IT-Procedure:
# Group Based Password Aging
# Status: Procedure
# Classification: Required
# Procedure Number: HSU-004

## 1.0 Purpose

The purpose of this document is to provide a process by which Humboldt State University business units can define a password aging policy for a defined group of users.

## 2.0 Scope

This procedure establishes how groups for which password aging policies are to be applied are defined, authorized, and maintained by the relevant business unit's management and technical support staff. Once a group has been defined, the HSU Username Passwords of that group's members will be aged according to the requested password policy. A user who is a member of more than one group will have the most restrictive password aging and depth settings from the groups that they are a member of.

## 2.1 Intended audience

Changes made through this process will be initiated by the ITC community and ITS staff, but could affect all campus users.

## 3. Procedure

## 3.1 Compliance

3.1.1 Prior to requesting that a group be defined for password aging, the unit must define:

a. Password Group Designation, a meaningful description of the group.

b. Initial Group Membership, a list of users or a definition based on data in a campus source of authority (CMS or Banner) which can be used to accurately populate the group programmatically.

c. Maximum Age, the maximum amount of time that members of the group can keep a password.

Password Depth, the number of historical passwords the system should maintain and deny repeat use of for each group member.

e. Group Administrators, the requesting business unit needs to designate a primary and backup employee who will have the responsibility of modifying the group membership over time.

## 3.2 Authorization

3.2.1 Requests for new Password Groups need to be authorized by an MPP with the authority to impose password policy changes on the group in question.

3.2.2 Requests will be reviewed by the ISO before approval is granted.

## 3.3 Notification

3.3.1 Group members will receive a warning e-mail that their password is nearing expiration at least one week before expiry, with follow-up e-mails sent three, two, and one days before expiration.

3.3.2 Wherever possible systems which use the HSU Username and Password will be configured to notify users if their passwords are within one week of expiring.

## 3.4 Change Lifespan/ Review process

3.4.1 Password Aging Groups should be reviewed every other year

## 4.0 Compliance

The ISO is responsible for compliance.

## 5.0 Enforcement

The ISO is responsible for enforcement.

## 6.0 Revision History

| Action | By | Date |
|---|---|---|
| Created | Josh Callahan | 3/28/2007 |
| Draft Procedure | HSU Security Group | 4/05/2007 |
| RFC Draft Procedure Posted for IT Council | ITC: Working Group | 4/10/2007 |
| Recommended Procedure Approved by IT Council | IT Council | 5/08/2007 |
| Procedure Approval | CIO/ISO: Kircher | 6/14/2007 |
| Posted | | date |
| Reviewed | | date |
| Obsoleted | | date |