Password Security Standard

Version 2.0

Reference: 6.100 – Information Technology and Security Policy
6.101 – Use of County Information Technology Resources

Developed by: Host Strengthening & Isolation SET Team

Table of Contents

1.0 Purpose

This standard document establishes the minimum practices for management of passwords to support authentication of system users when accessing County Information Technology (IT) resources. Although the focus is based on industry best practices for minimum security, Departments are encouraged to go beyond the minimum requirements as suited to the business need.

2.0 RELEASE NOTES AND HISTORY LOG

The content in this document will be periodically updated to reflect the changes in the County environment. In addition, this document will be constantly maintained to capture industry best practices as the technology and standards continues to evolve.

DATE	NEW VERSION NUMBER	MODIFIED BY:	DESCRIPTION of CHANGE
07/18/08	1.0	D. Diamond (DCFS)	1) Created first draft of standard
8/28/08	1.0	D. Diamond (DCFS)	1) Removed End User Practice items from Checklist 2) Created section “Password Rules for Users”
01/16/09	1.0	D. Diamond (DCFS)	1) Finalized standard per SET input on 01/15/09 2) Changed Password Rules for Users to Password Guidelines for Users
05/19/09	1.0	D. Diamond	1) Updated document per Policy SET 2) Removed User Guidelines and made separate document.
07/18/13	1.0	HSI SET	1) Updated password complexity requirements
08/15/13	2.0	HSI SET	1) Separated password requirements for desktops, laptops, servers, tablets versus smartphones and cellphones. Added password requirements for smartphones and cellphones
06/05/14	2.0	N/A	1) Approved by ISSC

3.0 Overview

Passwords are an important aspect of computer security. They are the primary means used to authenticate a user's access to IT resources. Passwords are the first technical line of defense against unauthorized access to those resources.

All County systems and associated equipment that rely on passwords as the means to authenticate users must implement effective password management in accordance with this standard. This applies to "Service" and "Maintenance" accounts. Systems may also use biometrics or public-key infrastructure certificates as additional means to control access. The access controls used must provide security commensurate with the level of sensitivity of the system or of specific resources (i.e. information or special devices).

Service accounts are assigned to functions, utilities or applications and not individuals. Examples include but are not limited to Exchange, BlackBerry, or Fax accounts.

Maintenance accounts are used by vendors to remotely access County IT resources to perform contracted service or maintenance activities. Maintenance account rules are also applied to workstation local administrator accounts used for workstation maintenance.

All staff who have administrative/console access to servers must use an individual User ID and Password, not a group or shared access account (i.e., Administrator accounts).

The following checklist must be completed by the System Administrator at the time a device or system is configured for installation or implementation. The checklist must be reviewed whenever the device or system is reconfigured to accept significant additional functionality or to store or access data of greater sensitivity, and updated as required. All completed checklists with deviations from the Standard are to be reviewed and approved by the appropriate Manager. Signing and dating the completed checklist indicates approval.

The settings in this Standard are grouped into two categories, "Mandatory" and "Recommended." These categories are defined as follows:

> **Mandatory** – All Mandatory settings must be applied with no exception.
>
> **Recommended** – All Recommended settings must be applied unless the business operation is severely impacted. Exceptions to settings in this category must have documented justification for the exception from the Departmental Information Security Officer (DISO).

4.0 PASSWORD SECURITY CHECKLIST

This checklist notes the password requirements which are to be applied to systems and applications.

4.1.0	PASSWORD REQUIREMENTS	Mandatory	Recommended
4.1.1	Eliminate the use of common or shared passwords	X	
4.1.2	Encrypt passwords for all information systems when stored electronically	X	
4.1.3	Secure legacy systems that do not have the technical capability to encrypt passwords	X	
4.1.4	Secure legacy systems that do not have the technical capability to meet the password configuration requirements of this Standard	X	
4.1.5	Do not display passwords (Password Masking) as they are entered into information systems	X	
4.1.6	Do not transmit passwords through non-encrypted means	X	
4.1.7	Use two-factor authentication using secure tokens for local access to servers for administration purposes	X	
4.1.8	Use two-factor authentication using secure tokens to remotely access all IT resources	X	
4.1.9	Centrally manage access (User IDs and Passwords) to network devices through TACACS, Radius or equivalent	X	
4.2.0	**PASSWORD CONFIGURATION FOR DESKTOPS/LAPTOPS/SERVERS/TABLETS**		
4.2.1	Each user must have unique Username and Password	X	
4.2.2	Require complex passwords (Must contain at least three of the following four characteristics)	X	
4.2.2a	• Contain at least 1 alpha and 1 numeric character		X
4.2.2b	• Contain at least one upper case character		X
4.2.2c	• Contain at least one lower case character		X
4.2.2d	• Contain one special character		X
4.2.3	Minimum password length – 8 characters	X	
4.2.4	Minimum password age – 2 days	X	
4.2.5	Maximum password age – 90 days	X	
4.2.6	Password expire warning – 14 days		X
4.2.7	Remember last 6 passwords	X	
4.2.8	Prevent the reuse of at least three characters from the previous password		X
4.2.9	Lock out after a minimum of 3 to a maximum of 5 failed logon attempts within 30 minutes	X	
4.2.10	Password account lockout must be completed by designated system administrator or automated process	X	
4.2.11	Reset account after 5 minutes after last failed logon attempt, if available	X	
4.2.12	Encrypt Password in transit, if capable	X	
4.2.13	Encrypt password at rest, if capable	X	
4.2.14	System must lock or log off after 30 minutes of inactivity	X	
4.2.15	Disable accounts after 90 days of inactivity	X	

4.3.0	**PASSWORD CONFIGURATION FOR SMARTPHONES/CELLPHONES**		
4.3.1	Each user must have unique Username and Password	**X**	
4.3.2	Require complex passwords (Must contain at least one of the following four characteristics)	**X**	
4.3.2a	• Contain at least 1 alpha and 1 numeric character		**X**
4.3.2b	• Contain at least one upper case character		**X**
4.3.2c	• Contain at least one lower case character		**X**
4.3.2d	• Contain one special character		**X**
4.3.3	Minimum password length – 4 characters	**X**	
4.3.4	Minimum password age – 2 days	**X**	
4.3.5	Maximum password age – 90 days	**X**	
4.3.6	Password expire warning – 14 days		**X**
4.3.7	Remember last 6 passwords	**X**	
4.3.8	Prevent the reuse of at least three characters from the previous password		**X**
4.3.9	Lock out after a minimum of 3 to a maximum of 5 failed logon attempts within 30 minutes	**X**	
4.4.0	**PASSWORD MANAGEMENT**		
4.4.1	Disable the ability of auto-login resources (auto fill/remember password)	**X**	
4.4.2	Access to password files or databases must be restricted	**X**	
4.4.3	System Administrator Passwords must be changed when associated users leave service or are reassigned a new job function	**X**	
4.4.4	Enable logging of password changes, if available	**X**	
4.4.5	Password masking: Enforce the use of wildcard masks to cover the typing of passwords.	**X**	
4.5.0	**SERVICE ACCOUNTS (UNEXPIRED) REQUIREMENTS**		
4.5.1	Limit access to Service Accounts to a minimal number of administrators	**X**	
4.5.2	Limit service account access rights to their assigned function	**X**	
4.5.3	Service Accounts Passwords must be changed when associated users leave service or are reassigned a new job function	**X**	
4.6.0	**MAINTENANCE ACCOUNTS REQUIREMENTS**		
4.6.1	Only enable maintenance accounts when needed, if applicable	**X**	
4.6.2	Limit maintenance account access rights to their assigned function	**X**	
4.6.3	Maintenance Accounts Passwords are to be changed when associated employees leave service or are reassigned a new job function	**X**	

4.7.0	**APPLICATION DEVELOPMENT FOR WINDOWS**		
4.7.1	Applications must support authentication of individual users and not groups, where applicable	**X**	
4.7.2	Applications must not store passwords in clear text or in any easily reversible form, if capable	**X**	
4.7.3	Applications must provide for appropriate access based upon job function	**X**	
4.7.4	Applications must be developed to support strong authentication mechanisms such as Kerberos, LDAP or equivalent security retrieval wherever possible	**X**	
4.8.0	**ADDITIONAL AND/OR CUSTOM SETTINGS**		
Ref.	**JUSTIFICATION FOR DEVIATIONS**		