

EXHIBIT "G"
AUTHORITY PASSWORD POLICY

STANDARD PROCEDURE

Hillsborough County
Aviation Authority

Number: S270.07

Effective: 02/04/05

Revised: 09/20/07

Page: 1 of 5

SUBJECT: PASSWORD SECURITY

PURPOSE: To establish a standard for creating, protecting, and changing passwords used to access Authority information systems.

GENERAL: Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all Authority employees and contractors utilizing Authority information systems are required to take appropriate steps to ensure they create strong, secure passwords and keep them safeguarded at all times.

All passwords must be changed at least every 90 days. Passwords must not be inserted into e-mail messages or other forms of electronic communication. All passwords must conform to the Authority password standards.

The scope of this procedure includes all personnel and third party contractors who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Authority facility, has access to the Authority information systems, or stores any Authority information.

PROCEDURES:

A. General Password Construction Guidelines:

Passwords are used for various purposes including: user level accounts, web accounts, e-mail accounts, screen saver protection, voicemail password, and system administration. Strong passwords must be created for use with Authority information systems.

1. Passwords must have the following characteristics:
 - a. Contain both upper and lower case characters (e.g., a-z, A-Z);
 - b. Have digits and punctuation characters as well as letters (e.g., 0-9, !@#%&^&*()_+|~=-\`{}[]:;';<>?,./);

EXHIBIT "G"
AUTHORITY PASSWORD POLICY

STANDARD PROCEDURE

Hillsborough County
Aviation Authority

SUBJECT: PASSWORD SECURITY

Number: S270.07

Effective: 02/04/05

Revised: 09/20/07

Page: 2 of 5

-
- c. Have at least eight alphanumeric characters; may be a passphrase (Ohmy1sturbedmyt0e).
2. Passwords must not have the following characteristics:
 - a. Contain less than eight characters
 - b. Be a word found in a dictionary (English or foreign)
 - c. Be a common usage word, such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.;
 - Computer terms and names, commands, sites, companies, hardware, software;
 - The words "The Authority", "HCAA" or any derivation;
 - Birthdays and other personal information, such as addresses and phone numbers;
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321,etc.;
 - Any of the above spelled backwards;
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
 - d. Not a word in any language, slang, dialect, jargon, etc.
 - e. Not based on personal information, names of family, etc.
 - f. The password cannot be the same as the past four passwords.
- B. Password Protection Standards:
1. Do not use passwords from personal account logons (e.g., personal Internet account, electronic banking, benefits, etc.) for Authority logon. Where possible, do not use the same password for various access needs. For example, create separate passwords for network access account and Oracle accounts.

EXHIBIT "G"
AUTHORITY PASSWORD POLICY

STANDARD PROCEDURE

Hillsborough County
Aviation Authority

Number: S270.07

Effective: 02/04/05

Revised: 09/20/07

Page: 3 of 5

SUBJECT: PASSWORD SECURITY

2. Do not share Authority passwords with anyone, including administrative assistants or ITS staff. All passwords are to be treated as sensitive, confidential Authority information.
3. Do not reveal a password over the phone to anyone.
4. Do not reveal a password in an e-mail message.
5. Do not reveal a password to your supervisor.
6. Do not talk about a password in front of others.
7. Do not hint at the format of a password (e.g., "my family name").
8. Do not reveal a password on questionnaires or security forms.
9. Do not share a password with family members.
10. Do not reveal a password to co-workers while on vacation.
11. If a password is requested from you by an individual, refer them to this document or send an e-mail to HelpDesk.
12. Do not use the "Remember Password" feature of applications (on the Internet).
13. Do not write passwords down. Do not store passwords in a file on any computer system (including Palm Pilots or similar devices) without encryption.
14. Passwords must be changed at least every 90 days.
15. If an account or password is believed to have been compromised, report the incident via an e-mail to the HelpDesk and change all passwords.

EXHIBIT "G"
AUTHORITY PASSWORD POLICY

STANDARD PROCEDURE

Hillsborough County
Aviation Authority

Number: S270.07

Effective: 02/04/05

Revised: 09/20/07

Page: 4 of 5

SUBJECT: PASSWORD SECURITY

16. Password cracking or guessing may be performed on a periodic or random basis by ITS or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards:

Applications developed by the Authority, new applications developed by third parties and purchased by the Authority, and existing legacy and third party applications (to the extent possible) must contain the following security precautions:

1. Must support authentication of individual users, not groups;
2. Must not store passwords in clear text or in any easily reversible form;
3. Where possible, must provide for role management, such that one user can take over the functions of another without having to know the other's password;
4. Require forced password changes whenever system capability is available.

D. Enforcement:

Violation of this procedure may result in suspension or termination of an individual's or firm's right of access to Authority information systems, disciplinary action by appropriate Authority employees, referral to law enforcement authorities for criminal prosecution, or other legal action, including action to recover civil damages and penalties.

Non-enforcement of any policy or procedure herein does not constitute consent or waiver, and the Authority reserves the right to enforce such policy or procedure at its sole discretion.

EXHIBIT "G"
AUTHORITY PASSWORD POLICY

STANDARD PROCEDURE

Hillsborough County
Aviation Authority

SUBJECT: PASSWORD SECURITY

Number: S270.07

Effective: 02/04/05

Revised: 09/20/07

Page: 5 of 5

APPROVED: /s/ John Wheat

DATE: 09/20/07