# TSH Password Standards

## Policy and Practices for a Baseline Password Standard for TSH

*3/06/2012*

**Policy Rationale**

The purpose of this policy is to provide guidance to customers, employees and other authorized users regarding passwords in order to protect individual and TSH information and resources. Adherence to this policy will help ensure that the TSH network and information systems are secure and available to all.

**Policy Statement**

Devices and systems connected to the TSH network must require passwords meeting the minimum standards set by the TSH and, if possible, technically enforce them. Customers and employees must adhere to the Minimum Passwords Standards for all systems and applications that come into contact with TSH resources.

**Remedies**

TSH reserves the right to:

- suspend access to preserve the confidentiality, integrity and availability of the network, systems or information;
- periodically audit passwords for compliance;

**Minimum Password Standards**

The following standards have been developed based upon current security standards. Absent a more secure password selection, the baseline password standard for users and owners of these systems is as follows:

- Passwords chosen *must*
  - be a minimum of eight (8) characters in length
  - be memorized; if a password is written down it must be secured
  - contain at least one (1) character from three (3) of the following categories:
    - Uppercase letter (A-Z)
    - Lowercase letter (a-z)
    - Digit (0-9)
    - Special character (~`!@#$%^&*()+=_-{}[]\|:;”’?/<>,.)
  - be private

- Passwords chosen should *not:*
  - contain a common proper name, login ID, email address, initials, first, middle or last name

- It is strongly recommended that:

  - passwords are changed twice per year (e.g., when clocks are adjusted in the spring and fall)

  - each password chosen is new and different