HISPOL 009.0

The United States House of Representatives Information Security Policy for Password Protection

Version:	**1.0**
Approved:	**August 2006**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

1 Introduction

User Identifications (UserIDs) and passwords are the most widely used security controls for automated information systems. Passwords are the first line of defense for user accounts. When used properly, they are quite effective in preventing accidental or negligent damage and access. A poorly chosen password may result in the compromise of the United States House of Representative's (House) entire network. For UserIDs and passwords to be effective, all House staff, contractors, and vendors must follow these guidelines.

1.1 Scope

The purpose of this policy is to provide all users of the House network with guidance in establishing strong passwords. The scope of this policy includes all House Offices and employees, contractors, and vendors that connect to the House network.

2 Policy Guidelines

- Information must be protected through the effective use of UserIDs and passwords.
- Passwords must contain a minimum of eight characters in length <u>and</u> the following:
    - A combination of upper and lower case characters (e.g., a-z, A-Z);
    - A combination of numbers and special characters (e.g., 9, !*&%$, etc.);
    - <u>Avoid</u> obvious passwords like variations of name, address, Social Security Number, hobby, or personal information; and
    - <u>Do not</u> use words associated with offices, committees, Capitol Hill, etc.
- All passwords must be changed at least every 90 days or immediately when compromised.
- Login procedures must be followed without automating steps that insert passwords (e.g., the "Remember Password" feature of applications).
- Do not share UserIDs and passwords with anyone. System audit logs identify users based on UserIDs.
- Do not attempt to guess another person's UserID or password. Guessing on the part of a legitimate user would falsely indicate suspicious activity to the system's audit function.
- When setting up new systems, system administrators must ensure that all accounts are password protected and default account (e.g., administrator, supervisor, etc.) passwords are changed.
- PC power up and screensaver passwords must be used.

- Passwords should be entered only when no one else is present or is watching entry on the keyboard.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords should be safeguarded and memorized. Passwords should not be written down, posted, or stored on a computer without encryption.
- Passwords should be unique and not one that has been used in the past.
- Users should not use the same password on multiple systems; it is permissible to use the same UserID on multiple systems.
- Unauthorized attempts to access House systems must be reported to the office manager or the Information Systems Security Office.