HISPOL 002.0

The United States House of Representatives Information Security Policy for Protecting Systems from Unauthorized Use

Version:	**2.0**
Approved:	**August 2006**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

1 Introduction

The purpose of this policy is to provide a comprehensive set of guidelines for the responsible and secure use of United States House of Representatives (House) information systems. The secure use of these systems requires individual responsibility, knowledgeable users, and an effective security program to ensure a safe and secure computing environment. In addition to the human aspect of the security program, technical solutions will continue to be implemented for both the perimeter (i.e., firewall) and internal host protections. The overall strategy of the House Information Systems Security Program is to protect all House information systems against internal and external threats via the effective implementation of technical solutions and personnel policies.

1.1 Scope

The purpose of this document is to provide all users of House information systems with guidance governing general information security requirements recommendations. All House Offices and employees that connect to the House network must follow this policy since improper use can potentially put the entire House network at risk.

The implementation of information systems security at the House focuses not only on the protection of information and network systems but also on the protections necessary for safeguarding information in general. This document addresses all forms of computer-generated information, including hardcopy and electronic formats.

2 Principles of Behavior for Use of House Information Systems

The following principles apply to all users of House information systems. Because written guidance cannot be generated for every system contingency, the user community is encouraged to contact the Information Systems Security Office (ISSO) when unusual circumstances occur. Many of the principles are based on Federal law and the House Code of Official Conduct. As such, there are consequences for non-compliance with the "Principles of Behavior"; refer to *Section 3, Consequences of Non-Compliance*.

2.1 Official Business

House information systems may not be used contrary to public law, House Rules, and Committee on House Administration regulations. Users are expected to use House equipment, systems, and information to carry out their official duties. At the same time, users must remember that public service is a public trust – information gained through employment at the House must be used in accordance with applicable laws, rules of the House, and regulations of the Committee on House Administration. House

Offices are responsible for following and enforcing guidelines set forth in the House information security policies.

House information systems are assets owned by the House and its Members. House Offices are responsible for determining their own policies for in-office equipment, including equipment used to access or process electronic information. All such in-office policies must comply with House information systems security policies and must not change the intent of these policies. House Offices are responsible for following and enforcing guidelines set forth in the House information security policies.

- Follow House guidelines regarding the use of information systems, recognizing that incidental personal use is permitted only when such use is negligible in nature, frequency, time consumed, and expense.
- Do not use government information for private gain (e.g., an employee of a procurement organization must not use knowledge of a pending contract award as a basis for purchasing stock in the vendor's company).
- Avoid the appearance of impropriety.
- Do not initiate or forward harassing e-mail, chain letters, or other inappropriate use of electronic communication systems.
- Do not send electronic mail that causes any House user to be flooded with unwanted, irrelevant, or inappropriate electronic messages, which could be construed as spam.
- Ensure all House-sponsored automated mailing list servers ("listservs") are protected with a confirmation mechanism to verify that each user has submitted a subscription request.
- Implement a logon Warning Banner on all systems, notifying individuals that House systems are to be used for official business only and unauthorized use may violate House rules.
- Do not conduct vulnerability scans or penetration tests without notification to the ISSO.
- Do not use information in a way that would adversely affect public confidence in the integrity of the House as a body.

2.2 Access

Users shall access and use only information for which they have official authorization. The concepts of *need-to-know* and *least privilege* are important tenets of information access security. *Need-to-know* means only authorized individuals who have a demonstrated need to access information will have access to such House information. *Least privilege* means each information user is only provided rights necessary to access

information or services needed to carry out job responsibilities (e.g., multiple logins for system administration, access to financial systems, etc.). These concepts apply to non-public information (e.g., procurement, data, employee records, etc.) and systems.

- Follow established procedures for accessing information, including use of User Identification (UserID), user authentication, passwords, and other physical and logical control measures.
- Follow established channels for requesting and disseminating information (e.g., Do not ask another employee with different or higher access privileges to get information.).
- Do not give information to anyone who does not have authorization to it.
- Do not attempt to perform actions or processing on a computer for which authority has not been granted, including system risk assessments, vulnerability scans, or penetration tests.
- Do not store sensitive files on a fixed hard drive if access to that particular computer cannot be limited to authorized users.
- Screensaver passwords should be set to lock after ten minutes of inactivity.
- Users must take measures to limit who can access files and printed information – only those who need the information should be able to get it.
- Watch for unauthorized use of information systems, including signs of hacker activity and the presence of unauthorized software and data. Notify the ISSO if such activity occurs.

2.3 Accountability

House Offices and their employees are accountable for their actions and responsibilities related to information systems entrusted to them. Organizations can only build partial accountability through structure and procedural controls. Largely, the benefits of accountability depend on the trustworthiness of each employee. It is each employee's responsibility to behave ethically, develop technical proficiency, and stay informed about issues and systems related to his or her job. Employees must approach information security with a spirit of cooperation and responsibility.

- Agree to and participate in accountability controls, such as automated transaction logging and manual logs.
- Acknowledge actions and accept responsibility for correcting errors and rectifying problems.
- Do not attempt to override internal controls.
- Be alert to threats and vulnerabilities to information security from both internal and external sources.

- Sign and adhere to the *HISFORM 010.1 - Affirmation of Non-Disclosure* if required by the job function.
- Employees should ensure that no single person has sole access or control over sensitive information.
- It is recommended that employees prevent others from using his/her accounts by using procedures such as:
    - Logging off when leaving the vicinity of the terminal or PC.
    - Setting a password on automatic screen savers.
    - Password-protecting or encrypting (using two or more public keys) sensitive files and software.
- Employees should help remedy security breaches.

2.4 Integrity

Employees must protect both the integrity and quality of information. Information integrity can be corrupted by intentional alteration or accidental damage. Information is of high quality if it is accurate, complete, and up-to-date. Quality of information is dependent on its source; it must be correct when created and maintained in that same manner.

- Protect information against viruses and malicious code by using virus detection and correction software. (Anti-virus software can be configured to stay resident on the system and scan for the presence of computer viruses. The House provides anti-virus software, contact the Call Center, (202) 225-6002 / (800) 447-8737, for details.)
- Review information as it is collected, generated, and used to make sure it is accurate, complete, and up-to-date.
- Prevent unauthorized alteration, damage, destruction, or tampering of information (e.g., use effective passwords, write protect files and programs on disks, keep area clear of food and drinks, etc.).
- Use protective measures to ensure against accidental loss of information integrity (e.g., backups, etc.).
- Avoid using unofficial software such as shareware and public domain software.
- Take appropriate training before using a system to learn how to correctly enter and change the data.
- Discontinue use of a system at the first sign of a virus infection and seek technical assistance from the Call Center, (202) 225-6002 / (800) 447-8737.

2.5 Availability

Employees should protect the availability of information and systems. Computer systems and media (e.g., CDs, DVDs, diskettes, hard drives, tapes, etc.) should be protected from environmental factors such as fire, water, heat, and food spills. They should also be protected from theft, unauthorized alteration, and careless handling.

With preparation, employees can minimize the impact of contingencies such as natural disasters, loss of information, and disclosure of information. It is each employee's responsibility to be rehearsed in recovery activities associated with their systems.

- Use physical and logical protective measures to prevent loss of availability of information and systems, such as:
    - perform and protect good backups, never storing backups in the same location as primary copies,
    - use Uninterruptible Power Supplies (UPS) on fileservers to ensure no loss of data in the event of power outage,
    - protect media that store information, and
    - maintain an inventory of files and programs.
- Store backups in a metal cabinet where they will be safe from fire and water damage, and keep hardware away from direct sunlight or extreme temperatures.
- Take appropriate action to restore availability when information or systems become unavailable due to disaster, damage, or unplanned shutdown.

2.6 Contractors

Contractors are expected to follow the same standards and rules of conduct with regard to the support of House information systems as House employees. Contractor personnel may perform in the same capacity as House system support personnel and as such must adhere to the guidelines contained herein. Additionally, all contracts will explicitly state that Contractor personnel:

- Must be eligible for a Federal government security clearance if access to sensitive information is required.* Individual House Offices or CAO Business Units may require an Office of Personnel (OPM) Extended Background Investigation or other security clearance, as deemed necessary,
- Must not remove sensitive information from the Capitol campus, and
- Must sign an *Affirmation of Non-Disclosure* prior to conducting House business.

*Upon written request, the ISSO can grant exceptions to this requirement when access to House information is limited in scope and contract duration, and when

the Employing Office proposes sufficient compensating controls to protect House information. Written requests should address the specific circumstances, the rational for the exception, compensating controls, and the resulting risk to House information.

2.7 Hardware

Each employee has a duty to protect and conserve House property either owned or under evaluation. Employees have access to many kinds of office and computing equipment and must handle such equipment carefully to protect against hazards. Further, employees must prevent problems by performing regular maintenance. Backup and recovery plans and mechanisms for general support systems and major applications will be addressed by separate documentation.

- Protect computer equipment from damage, abuse, theft, sabotage, and unauthorized use (i.e., by locking office doors, permitting only authorized personnel access, etc.).
- Disconnect or deactivate modems, unless attached to a fax machine, as directed in United States House of Representatives Information Security Policy.
- Follow established procedures by using a property pass when removing equipment from House premises, if appropriate.
- Protect computer equipment from hazards, including extreme temperatures, water and fire, static electricity, and spills from food and drink.
- Keep an inventory of all equipment assigned.
- When equipment requires repair by service personnel, employees should ask to see the service person's identification and keep records of the work performed.

2.8 Software

Computer users must utilize only appropriate software on House-provided computer systems and must protect those systems from viruses. Software downloaded from the Internet presents the greatest potential vulnerability associated with virus infections to House computing systems.

It is the policy of the House to comply fully with all copyright laws pertaining to computer software. Accordingly, the House prohibits the illegal duplication or use of any software or related documentation. If appropriate, sign and register software license agreements with the vendor within a few days of receipt.

- Use the House-provided or an equivalent current anti-virus program to scan software prior to installing on any office computers.

- Do not use, install, or download software that allows an individual workstation to act as a server permitting other users to connect to that workstation and share files.
- Do not use third-party applications that circumvent approved House remote access policy.
- Do not use, install, or download hacker or cracker software or scanning tools on House computer systems without notification to the ISSO.
- Do not alter or use software such that the network is vulnerable to damage or abuse.
- Use only authorized software that has current patches installed. Use shareware or public domain software only in accordance with office policies.
- Consider maintaining up-to-date, safeguarded back-ups. Store back-ups in a different location from the primary copy, preferably under lock and key.

2.9 Security Awareness

Employees should make a conscientious effort to avert security breaches by staying alert to potential vulnerabilities of House information and systems. Employees are in a position to see how security measures are truly used (or not used) and where potential problems exist. Certain human factors and activities may suggest that fraud or negligence may occur within the organization.

The ISSO has developed various forms of security training and awareness methods that are available to all users. Users are also called on to stay abreast of current security information. It is an undisputed fact that an organization's strongest security measure is knowledgeable users.

- Stay abreast of security policies, requirements, and issues.
- Be alert to human factors that may indicate a security risk including:
    - employees with gambling or substance abuse problems,
    - employees who do not take leave as they are possible candidates for increased levels of stress or potential involvement in external coercion,
    - low morale,
    - poor relationships between management and staff.
- Be alert to clues of abuse:
    - unauthorized computer products in the office (e.g., sports pools, personal business software),
    - possession of unauthorized equipment,
    - unscheduled programs running on a recurring basis.
- Challenge unauthorized personnel in the work area.

- Participate in security training as required.
- Use security training programs and materials.
- Read security information available through Web pages, e-mail, newsletters, memos, and other sources.
- Attend in-house workshops and exhibitions.

2.10 Reporting

It is each employee's responsibility to report any form of security violations in accordance with in-office policy. It is important that the ISSO be contacted in cases of computer-related emergencies and violations so that immediate action may be taken to contain the exposure and minimize the impact to the House. Violations include non-compliance with established in-office procedures as well as approved House policies. In cases where laws may have been broken, employing authorities should also take action to contact law enforcement.

- Report security vulnerabilities and violations as quickly as possible to proper authorities so that corrective action can be taken.
- Report emergency security incidents to the ISSO.
- Take reasonable action (e.g., isolate equipment involved and do not use it until it has been analyzed) immediately upon discovering a violation to prevent additional damage.
- Cooperate with official action plans for dealing with security violations.

3 Consequences of Non-Compliance

Non-compliance with any element of this document may subject the violator to appropriate disciplinary action including, but not limited to the following:

- suspension of access privileges,
- warning (verbal or written),
- reprimand,
- suspension from employment,
- demotion from job position,
- termination of employment,
- financial liability for actual, consequential and incidental damages,
- criminal and civil penalties, including prison terms and fines.

These disciplinary actions are merely suggestions that can be used depending on the severity of the violation. The list is not exhaustive and does not imply that disciplinary

actions are mandatory. It is within each employing authority's discretion to determine appropriate disciplinary measures for each circumstance. However, under the scope of House Rules and Committee on Standards of Official Conduct jurisdiction, certain violations may result in action by the House.

The consequences for non-compliance should be fully disclosed to all users and each user should sign an acknowledgement that they have received, understand, and agree to abide by the policies.