HISPOL 002.1

The United States House of Representatives General Information Security Guidelines to Protect Member and Committee Office Systems from Unauthorized Use

CATEGORY: **General Information Security**

ISSUE DATE: **September 16, 1997**
Revised Date: **January 23, 2002**

The United States House of Representatives
Committee on House Administration

Title: United States House of Representatives – General Information Security Guidelines to Protect Member and Committee Office Systems from Unauthorized Use

Number: HISPOL 002.1

Category: General Information Security

Date: September 16, 1997
Revision: January 23, 2002

Status: Approved – Committee on House Administration

Purpose:

The purpose of the United States House of Representatives – General Information Security Guidelines is to provide all Members, Leadership Offices, and Committees with a policy governing general information security requirements and recommendations for using House computing and network resources during the current Congress.

Audience:

This document has relevance to all Members, Leadership Offices, and Committees.

References:

US House of Representatives Information Systems Security Program

HISFORM 008.0 – House Affirmation of Non-Disclosure

External References:

House Code of Official Conduct

Committee on House Administration Resolution – World Wide Web Sites, July 31, 1996

Table of Contents

1.0 INTRODUCTION

The purpose of this policy is to provide a comprehensive set of general guidelines for the responsible and secure use of U.S. House of Representatives (House) information systems and network resources. The secure use of these resources requires individual responsibility, knowledgeable users, and an effective information systems security program to ensure a safe and secure computing environment. In addition to the human aspect of the security program, technical solutions 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 systems against internal and external threats via the effective implementation of technical solutions and personnel policies. At the core of the House Information Systems Security Program are the system user responsibilities as follows.

1.1 General Information Security Guidelines

General Information Security Guidelines are part of a comprehensive program to provide information security at the House. They represent an approach whereby each employee is accountable for his/her actions and is subsequently responsible for information systems security. Because the procedures and technical controls necessary to address all security concerns cannot always be implemented in a cost-effective manner, General Information Security Guidelines establish ethical and practical guidelines predicated on the concept that knowledgeable employees are the foundation of a successful information systems security program.

General Information Security Guidelines identify to the user community their roles and responsibilities with regard to protecting information. The guidelines imply that a proactive approach be taken to ensure that employees are: (1) alert to threats and vulnerabilities, (2) knowledgeable in security policies and procedures, and (3) aware of their responsibility to report incidents to the proper authorities. Employees are also called upon to take initiative and accept responsibility for safeguarding information resources.

The primary threats to information security have typically been from insiders who access information and systems on a routine basis. With the proliferation of distributed networks, public access systems including the Internet, and dial-in capability, threats now include those from external sources. Within all computing environments, technical controls such as firewalls are not enough to ensure an adequate and comprehensive information systems security program. Management controls such as password management and physical security must be used to augment technical controls.

1.2 Overall Strategy for General Information Security Guidelines

The implementation of information systems security at the House focuses not only the protection of information and network systems, but the protections necessary for safeguarding the information itself. Therefore, the General Information Security Guidelines address all forms of computer generated information including hardcopy and electronic formats. NOTE: This policy does not address or pertain to records retention issues.

General Information Security Guidelines:

- must be included in security planning for both general support systems and major application systems,
- establish personnel, technical and physical controls,
- set guidelines and expectations,
- establish work procedures, automated control mechanisms, and capabilities for system backup and recovery,
- implement an enforcement mechanism.

1.3 Intent of This Document

This document has been developed to:

- be used as part of daily operations to ensure an adequate level of security exists for information systems used throughout the House,
- explain the general requirements for information systems security that can be used to develop security for general support systems and major applications. As such, this policy can be augmented as required by specific guidance in the form of an in-office policy additional House policies (HISPOLs) and procedures (HISPUBs) which will be developed, approved, and disseminated as needed.

2.0 REQUIREMENTS FOR GENERAL INFORMATION SECURITY GUIDELINES

As stated in the previous section, the General Information Security Guidelines are designed to address both general support systems and major applications. The definitions are as follows:

A *general support system* is defined as…

…an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

An in-office local area network (LAN), House-wide backbone, communications (voice and data) network, data processing center, and shared information processing service organization are all examples of general support systems.

A *major application* is defined as…

…an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application.

Examples of major applications in use at the House are the Federal Financial System (FFS) and the House Messaging System.

General Information Security Guideline issues must be included in the security planning, policy, and procedural rules for all general support systems and major applications.

The level of system risk must be used as a basis for defining General Information Security Guidelines.

Guidelines must only be as stringent as necessary to provide an adequate level of security. Guidelines must delineate the responsibilities and expected behavior of all individuals with access to an information system.

2.1 Risk Analysis

Prior to authorization for connection to networks or operation of major applications, each system should be analyzed to ascertain the level of risk associated with operating the system. This risk approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of the current or proposed safeguards. The goal of the risk analysis is to assist management in finding an economic balance between the impact of the risks and the cost of protective measures. The system risk should be analyzed using a quantitative or qualitative methodology and a comprehensive analysis report prepared.

2.2 Existing System Guidelines

For existing systems, the guidelines created for the system must correspond to and support technical controls (e.g., if the rules dictate that a eight character password comprised of numbers and characters is required, the rules must state this requirement).

2.3 Policy and Procedural Rules

Policy and procedural rules must address the following environments:

- work at home,
- authorized telecommuting personnel,
- dial-in access,
- connections to the Internet,
- use of copyrighted works,
- proper use of House equipment,
- assignment and limitation of system privileges,
- separation of duties,
- individual accountability,
- information dissemination,
- access control to and from other systems, including limitations on external access.

2.4 System Security Plan

Prior to authorization for connection to networks or operation of major applications, each system's security policy and procedural rules should be developed and documented. The security policy and procedural rules should be implemented, and processes defined to monitor security to ensure reasonable and effective management of the system and compliance with the system security plan.

2.5 Limitations

Policy and procedural rules must include limitations on:

- ♦ modifying data,
- ♦ searching databases,
- ♦ divulging information.

2.6 Security Training

The rules developed for each system must be addressed as part of the security training provided for each general support system and major application.

2.7 Consequences

Consequences must be written into various rules so that House employees, contractor personnel, or any other authorized persons using House systems are adequately advised.

3.0 GENERAL PRINCIPLES

The following principles apply to House employees using or providing support for various House information systems. Section 3.1 applies to general users of House systems. Section 3.2 applies to certain unique users and provides specific principles over and above Section 3.1. Guidance on specific procedures unique to specialized systems will be provided as needed. Written guidance cannot be generated for every system contingency; therefore, personnel may sometimes have to go beyond stated principles and use their best judgment to guide their actions. Personnel must understand that 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 4.4 for consequences for non-compliance.

Guidance in this and other documents may be categorized under the headings of either *"must"* or *"recommendation."* Items designated as *"must"* are considered requirements because their absence can adversely affect the security posture of the entire House. Items designated as "must" will be enforced. Items under the designation of *"recommended"* are considered prudent security practices but will not be enforced by the House. Employing authorities may require adherence to recommended items to better protect their individual information systems.

3.1 Principles of Behavior

Principles of Behavior for General Use of House Information Systems

Official Business	House information systems may not be used contrary to public law, House Rules, and Committee on House Administration regulations.

Accountability	Be accountable for their own actions and responsibilities related to information and information systems entrusted to them.
Access	Access and use only information for which they have official authorization.
Confidentiality	Protect information from unauthorized disclosure.
Integrity	Protect information from unauthorized, unanticipated, or unintentional modification, including the detection of such activity.
Availability	Protect information so that it is available on a timely basis to meet mission requirements or to avoid substantial losses.
Password and User ID	Protect information security through effective use of user IDs and passwords.
Hardware	Protect computer equipment from damage, abuse, theft, sabotage, and unauthorized use.
Software	Use appropriate software in a safe manner so that software is protected from damage, abuse, theft, sabotage, and unauthorized replication or use (copyright infringement).
Awareness	Stay alert to security policies, requirements, procedures, and issues.
Reporting	Report security violations, incidents, and vulnerabilities to proper authorities.

3.1.1 Official Business

House information systems may not be used contrary to public law, House Rules, and Committee on House Administration regulations.

Employees are expected to use House equipment, systems, and information to carry out their official duties. Employees must remember that public service is public trust; information gained through employment at the House must be used in accordance with applicable laws and rules of the House. House Offices are responsible for following and enforcing guidelines set forth in the House information security policies.

Employees must:

- 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,

- not use central House systems for profit or campaign use,

- 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,

- not conduct system risk assessments, vulnerability scans, or penetration tests without notification to the CAO HIR Information Sysems Security Office, and prior written authorization from their Employing Authority, including a description of the requested action, which shall be filed with the Information Systems Security Office,

- not initiate or propagate harassing e-mail, chain letters, or other inappropriate use of electronic communication systems.

3.1.2 Accountability

Employees must be accountable for their actions and responsibilities related to information resources entrusted to them.

Each employing authority is responsible to develop policies and procedures relative to employee accountability issues.

3.1.3 Access

Employees 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. Only need to know individuals will have access to 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.

Employees must:

- follow established procedures for accessing central House systems and in-office procedures for accessing office systems and information (User Identification (ID) and passwords),
- follow established channels for requesting and disseminating information (for Members, this policy applies to information located outside their offices),
- not attempt to perform actions or processing on a computer for which they do not have authority, or which exceeds their authority, including system risk assessments, vulnerability scans, or penetration tests,
- not give information to individuals who do not have authorization.

It is recommended that employees:

- not store sensitive files on a fixed hard drive if access to that particular computer cannot be limited to authorized users,
- set PCs to lockup (i.e., screensaver passwords) after a specified amount of idle time,
- take measures to limit who can access personal computer files and printed information – only people who need the information should be able to get it.

3.1.4 Confidentiality

Employees must protect the confidentiality of sensitive information from disclosure to unauthorized individuals or groups.

Access to sensitive information must be restricted to authorized individuals who need it to conduct their jobs. This entails not only refraining from intentional disclosure but also using measures to guard against accidental disclosure. When an employee changes positions or terminates employment with the House, he/she is still obligated to protect the confidentiality of information.

The principles here do not address National Security Information (NSI). NSI is information relative to the national defense or foreign relations of the United States and requires special protection provisions. Members, Leadership Offices, and Committees that have a need to process NSI should contact the appropriate security organization for guidance.

Individual Members have a reasonable expectation of privacy with respect to all of their electronic communications in the performance of official duties (including but not limited to use of telephones, voice mail, facsimile transmissions and electronic mail), and may determine whether such communications are to be made available to third parties or to the public. Absent such a determination, unauthorized interception, use, or disclosure of electronic communications in the performance of official duties is a violation of Federal law and may lead to criminal prosecution, suit for invasion of privacy, or in the case of a Member, Officer or employee of the House of Representatives, discipline by the House.

Employees must:

- ♦ determine the sensitivity of information and categorize the information as being NSI, confidentially sensitive information, or information available for public release,

- ♦ be aware of the sensitivity levels of information being accessed and protect it accordingly,

- ♦ protect the following kinds of confidentially sensitive information:

    - Confidential Business Information (CBI): procurement, commercial, information technology, etc. (e.g., network infrastructure information, telephone credit card numbers, contract proposals, etc.),
    - Confidential House or Employing Authority Information (CHI): personal information about individuals contained in "systems of record" (e.g., medical history, work performance, etc.).

- ♦ not allow unauthorized personnel access to facilities and resources that store or process sensitive information,

- ♦ dispose of diskettes and disk drives using approved procedures,

- ♦ not leave paper copies of sensitive information unattended,

- ♦ not store or transmit sensitive information on any public access system such as e-mail or via the Internet without protective measures (e.g., using encryption). Encryption is software or hardware that give users the capability to convert/recover data that has been put into an unreadable format while it is in transit or in storage. Contact the HIR Information Systems Security Office or TSR for details.

It is recommended that employees:

- ♦ not allow sensitive data to remain on their screen or be visible by someone who is not authorized to view the data,

- protect all computer generated print outs and media (e.g., disks, tapes, etc.) containing confidentially sensitive data,

- mark CBI and CHI sensitive media accordingly.

3.1.5 Integrity

Employees must protect the integrity and quality of information.

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. Information quality is dependent on its source – it must be correct when created and maintained in that same quality.

Employees must:

- protect information against viruses and similar malicious code by using a current virus detection and correction (anti-virus) software. Anti-virus software can be configured to stay resident on your system and scan for the presence of computer viruses.

It is recommended that employees:

- 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 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 HIR Information Systems Security Office.

3.1.6 Availability

Employees should protect the availability of information and systems.

Computer systems and media (e.g., 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.

It is recommended that employees:

- 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 Uninterruptable Power Supplies (UPS) on file servers to ensure no loss of data in the event of power outage,
    - protect media, including disks, tapes, and printed reports,
    - maintain an inventory of files and programs.
- store backups in a metal cabinet where they will be safe from fire and water damage,
- 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.

3.1.7 Passwords

Protect information through the effective use of User IDs and passwords.

User IDs and passwords are the most widely used security controls for automated information systems. If used properly, they are quite effective in preventing accidental or negligent damage and access. (Protection from hackers usually requires more sophisticated techniques.) For user IDs and passwords to be effective, all House employees, privileged users, and vendors/contractors must follow guidelines for constructing and using them.

Employees must:

- protect information through effective use of user IDs and passwords,
- if they are privileged users, construct passwords that are a minimum of eight characters in length,
- construct complex passwords that are a minimum of eight characters in length and:
    - do use a combination of alpha and numeric characters,
    - avoid obvious ones like variations of your name, address, Social Security Number, hobby, or personal attributes,
    - do not use a readable word (i.e., from a dictionary) in any language,
    - do not use words associated with offices, committees, Capitol Hill, etc.
- follow login procedures without automating steps that insert passwords (i.e., ensure that you manually enter your ID and password),
- never share your user ID or password without good reason since system audit logs identify users based on user IDs,
- not attempt to guess someone else's ID or password (Guessing on the part of a legitimate user would falsely indicate suspicious activity to the system's audit function.),
- report unauthorized attempts to access your system to your staff contact or the HIR security staff,
- change passwords frequently – at least every 90 days or immediately when they may have been disclosed.

It is recommended that employees:

- use a password on your PC power up and screensaver options if applicable,
- enter a password only when no one else is present or at least watching your entry on the keyboard,
- not use the same user ID and/or logon on multiple systems,
- safeguard your password – commit it to memory, do not write it down or post it, do not store it on a computer,
- when changing your password, use one that you have not used in the past.

3.1.8 Hardware

Protect computer equipment from damage, abuse, theft, sabotage, and unauthorized use.

Each employee has a duty to protect and conserve House property either owned or under evaluation, including information processing equipment. 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 maintenance regularly. Backup and recovery plans and mechanisms for general support systems and major applications will be addressed by separate documentation.

Employees must:

- protect computer equipment from damage, abuse, theft, sabotage, and unauthorized use,
- follow established procedures for removing equipment from House campus.

It is recommended that employees:

- protect computer equipment from hazards, such as:
    - extreme temperatures,
    - water and fire,
    - electrical storms,

- static electricity,
- spills from food and drink,
- dropped objects,
- dust and dirt,
- combustible materials.

♦ keep an inventory of all equipment assigned to them,

♦ when equipment requires repair by service personnel, ask to see the service person's identification and keep records of the work performed,

♦ if possible, use modems only when necessary. Leaving them on after normal business hours creates a security risk.

3.1.9 Software

Use appropriate software in a safe manner so that it is protected from damage, abuse, theft, and unauthorized replication or use (copyright infringement).

Computer users must use only appropriate software on their systems and are responsible for preventing damage to both software and data from viruses, unauthorized use, and theft.

Employees must:

♦ use a House-provided or equivalent, current anti-virus program to scan software prior to installing on any office computers,

♦ not use, install, or download software, other than Employing Authority-approved network operating systems and diagnostic programs, that allows an individual workstation to act as a server permitting other users to connect to that workstation and share files,

♦ not use, download, or install hacker or cracker software or scanning tools on House computer systems without notification to the CAO HIR Information Systems Security Office, and prior written authorization from their Employing Authority, which shall be filed with the Information Systems Security Office.

It is recommended that employees:

♦ use software in a safe manner that protects the system from damage and abuse,

- use only authorized software. Install shareware or public domain software only in accordance with office policies,

- not alter software, or allow another person to do so, except as authorized,

- consider maintaining up-to-date, safeguarded back-ups. Store back-ups in a different location from the primary copy, preferably under lock and key.

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.

3.1.10 Awareness

Stay alert to security policies, requirements, procedures, and issues.

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

HIR will develop various forms of security training and awareness methods that will be 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.

It is recommended that employees:

- 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,
    - low morale,
    - poor relationships between management and staff.

- be alert to clues of abuse, including:

- unauthorized computer products in the office (e.g., games, 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 provided,

♦ use security training programs and materials,

♦ read security information available to employees through Web pages, e-mail, newsletters, memos, and other sources,

♦ attend in-house workshops and exhibitions,

♦ talk with security officials.

3.1.11 Reporting

Report security violations, incidents, and vulnerabilities to proper authorities.

It is each employee's responsibility to report any form of security violations in accordance with in-office policy. It is important that the HIR Information Systems Security Office be contacted in cases of computer-related emergencies and violations so that action can be taken immediately to contain the exposure and minimize the impact on the rest of 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 authorities.

Employees must:

♦ report security vulnerabilities and violations as quickly as possible to proper authorities so that corrective action can be taken,

♦ report emergency incidents to the HIR Information Systems Security Office,

- ♦ 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 willingly with official action plans for dealing with security.

3.2 Principles of Behavior for Special Circumstances

The principles below apply to users in special circumstances. They are meant to provide extra guidance focused on specific situations where users have especially high responsibility for information security. Users addressed below include:

- *privileged users,* which includes those with special access privileges for system development, delivery, and administration,
- *authorized telecommuting personnel*,
- *work from home* and other *remote users,*
- *users of public access systems,* particularly the Internet.

Requirements for privileged users other than Office staff are covered in more detail in HISPOL 002.0. A summary chart listing the principles of behavior for these special users and circumstances follows.

Principles of Behavior for Special Circumstances – User Responsibilities

Privileged Users	Privileged users must perform their duties meticulously and reliably in order to preserve information security.
Authorized Telecommuting Personnel, Users working from Home, And Other Remote Users	Telecommuting and remote personnel must comply with all House policies and procedures to ensure continued protection of House information.
Administrators of Public Access Systems	Users must conduct only Official Business through public access systems according to authorized procedures.

The following section discusses each special principle and lists practical means of implementing each principle.

3.2.1 Privileged Users

Privileged users include:

- system administrators (This function can be performed by Office staff, HIR Technical Service Representatives, or contractors and can perform such functions as: control and change passwords, add users to systems, and maintain the equipment.)

Privileged users of information systems must assume a high level of responsibility and initiative for security. With special skills and access rights, privileged users could, through negligence or malicious behavior, wreak havoc on a system. It is critical that they adhere to high ethical standards. Each office should maintain approved methods for each employing authority to gain access to supervisor/privileged passwords for contingency purposes. In these cases, written supervisor/privileged passwords should be protected from unauthorized access.

Privileged users are expected to take initiative in protecting against errors, abuse, theft, and sabotage.

Privileged users must make an effort to notice the threats to and vulnerabilities of information systems, calling these to the attention of management and working to develop effective countermeasures.

System developers must adhere to sound development practices in the development process. That is, software must be designed and programmed to perform accurately according to user requirements.

Privileged user responsibilities:

- perform their duties meticulously and reliably in order to preserve information security, integrity, availability, and confidentiality,

- use special access privileges only when they are needed to carry out a specific system function (whenever possible, use a non-privileged account),

- restrict access to all shared drives, directories, and other accessible resources to authorized users only,

- construct complex passwords that are a minimum of eight characters in length,

- use utility programs or operating system settings that will force users to construct strong passwords,
- implement a logon Warning Banner, as described in House guidance, notifying individuals that House systems are to be used for official business only, unauthorized system usage may violate House rules or United States Code, and disciplinary sanctions could result from unauthorized actions,
- protect the supervisor or administrator password at the highest level possible,
- help train users on appropriate use and security of the system,
- be aware of and monitor users who have responsibility for several functions (data entry, analysis, backups, output, etc.) that could potentially lead to abuse,
- report all security incidents to the appropriate authority,
- ensure virus protection is in place, functional, and current,
- never use information resources for personal business or gain,
- never gain access to data for the purpose of unauthorized copying, modification, deletion, and general viewing,
- use precautionary procedures and technical measures to protect privileged accounts from fraudulent use,
- watch for signs of hacker activity or other attempts at unauthorized access, such as multiple failed login attempts,
- review audit logs on a routine basis, at least weekly,
- watch for unauthorized use of information resources, including the presence of unauthorized software and data,
- take appropriate action to reduce damage from security violations, such as disconnecting a PC with a virus from the network or disabling a suspicious user account,
- alert the appropriate personnel when a system goes down or experiences problems,
- assist with recovery activities,

- be aware of the security requirements of their specific system and install software patches, etc. as appropriate.

3.2.2 Telecommuting Personnel, Users Working from Home, and Other Remote Users

---

The House has committed to providing a secure means for accomplishing work from a remote location. House employees utilize computers when they travel, work at home, or participate in the House-approved telecommuting program. A higher level of responsibility for information security lies with these remote users because the employees work unobserved, and the work environment falls outside the physical protection of a House facility. Remote users must take initiative to understand issues related to their work environments. This means staying up-to-date on House security policies concerning remote access.

Virtual Private Network (VPN) Users:

The House provides a Virtual Private Network (VPN) service for single-person District Offices, telecommuters, and House staff to access the House Network via House-owned PCs and laptops using their high-speed connections, SecurID cards and the Internet. Secure use of this service requires the following three security measures:

- Current antivirus software must be installed on the system and operational at all times,
- A secure authentication device (SecurID card) must be used to access the House network,
- A personal firewall supported by the House VPN solution must be installed on the system and operational at the time of each connection to the House network.

R*emote users must:*

- utilize a House-approved authentication mechanism,
- ensure the confidentiality of House information,
- disconnect or deactivate modems when they are not in use,
- use special measures to protect information and access capabilities across dial-up lines, such as changing passwords often and using approved remote access authentication devices.

It is recommended that remote users:

- ensure that adequate security provisions are implemented in the remote work environment to protect hardware, software, information, and infrastructure,
- be alert for anomalies and vulnerabilities and report security incidents to authorities,
- accept only access to House systems which are necessary to perform the job,
- avoid uploading and downloading confidentially sensitive information,
- encrypt information when it is reasonable and worthwhile.

3.2.3 Administrators of Public Access Systems

Information security for public access systems (e.g., Internet) is problematic and requires diligent monitoring. Hackers can get passwords and steal Internet Protocol (IP) addresses. Caution should be used when surfing the Internet to ensure House information is protected at all times.

While each Member and Leadership Office has control over the use of their systems, users must remember that publicly available information portrays the House image to the public. Much of the information placed on House public access systems represents House policy and positions, and such information must reflect high standards of integrity. Users must be careful to avoid the appearance of favoritism to or endorsement of any commercial entity.

Users must:

- adhere to all applicable HISPOLs and HISPUBs,
- conduct only official business through public access systems according to established office procedures,
- place only appropriate authorized information on a public access system, (Do not place prohibited, personal, or unofficial information on a World Wide Web (web) page on the Internet, send it via E-mail, nor enter it in a news group,
- not distribute or receive information in violation of copyright laws.

It is recommended that users:

- not allow sensitive information to be sent, received, or accessed through public access systems without proper precautions (e.g., encryption). Be careful to not place

segments of information on public access systems that could be pieced together to infer confidentially sensitive information,

- ♦ when maintaining e-mail and FAX distribution lists:

    - include only those who need and want the information,
    - update distribution lists as frequently as needed, but review at least annually.

4.0 IMPLEMENTING GENERAL INFORMATION SECURITY GUIDELINES

4.1 Integrating General Information Security Guidelines into Security Planning

Good business practice mandates that General Information Security Guidelines become part of the security plan for general support systems and major applications. Guidelines should address:

- ♦ responsibilities and expectations of all users with access to the system,

- ♦ consequences for non-compliance.

4.2 Integrating Guidelines into Training

Employees should familiarize themselves on General Information Security Guidelines before they access a House system. General Information Security Guidelines will be included as part of initial system training in order to reduce security violations. Users trained in ethical standards and technical procedures are the strongest part of the information security program. Most people want to do the right thing. As long as they understand why they are asked to do things, they will usually strive to do them. On the other hand, users not aware of the implications of negligence, for example, may very well circumvent rules in an effort to get their jobs done efficiently. Trained users know what is required and why, and will be much more likely to act responsibly and expect others to act responsibly.

It is recommended that offices keep appropriate records and institute a process of security training that users must complete before being granted access to systems, and periodically thereafter. House Information Resources will continue to provide guidance to offices through various Information Security Awareness Training.

4.3 Addressing Individual System Requirements

Each office may have its own unique General Information Security Guidelines. It is recommended that each office use the applicable principles set forth in this document as guidelines in developing their policy.

For an existing system, the rules must correspond with existing technical security controls. For example, a system is set with certain account types; a corresponding rule would state that users must access only the account type(s) granted them, without attempting to gain higher access through illicit actions such as hacking the network or using someone else's account. Those who write the General Information Security Guidelines must consider the intent behind each technical control, and write the corresponding rule to state that intent.

4.4 Consequences of Non-Compliance

Non-compliance with the any element of this House Information Security Policy 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.

The listed disciplinary actions are merely suggestions that can be used depending on the severity of the violation. This 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 under 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 on non-compliance should be fully disclosed to all users and each user should sign an acknowledgement that the user has received, understands and agrees to abide by the guidelines (policies).