HISPOL 010.0

The United States House of Representatives Information Security Policy for the Protection of Sensitive Information

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

Table of Contents

1 Introduction

This policy addresses security concerns relating to information considered sensitive to the United States House of Representatives (House). All users of House sensitive information must protect the confidentiality of sensitive information from disclosure to unauthorized individuals or groups. Observance of this policy ensures that House sensitive information remains protected at all times in all forms.

1.1 Scope

This policy applies to all House Offices, employees, contractors, and vendors that use House sensitive information in all forms, printed and electronic.

2 Policy Guidelines

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, they are still obligated to protect the confidentiality of information.

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 an House Office, employee, contractor, or vendor of the House of Representatives, discipline by the House.

2.1 Determining Information Sensitivity

Data owners are responsible for determining the sensitivity of their information, in accordance with House Information Security Policy and Publications. All users of House sensitive information must protect it accordingly. In general, the following types of House information are considered sensitive:

- Procurement;
- Proprietary and privacy-related;
- Financial; or
- Information technology-related data, such as network configuration information.

This also includes non-sensitive data that, when combined with other non-sensitive data, can be assembled together to provide a sensitive result. For example, a roster

of Security personnel combined with a list of training courses may reveal the specific security technology being used at the House.

2.2 Physical Protection of Sensitive Information

- All documents and removable magnetic media containing House sensitive information should remain on House property. If such documents and media must be removed from House property, it must remain in the possession of a House employee.
- Printed documents and media containing House sensitive information must be stored out of sight, preferably in a locked container. While in transit, they must be carried in a folder or envelope.
- Sensitive data should not remain on a computer screen or be visible by someone who is not authorized to view the data.
- House sensitive information should be marked accordingly. All printed documents and removable media containing sensitive information should be clearly marked "Confidential to the U.S. House of Representatives". Their distribution must be limited to only those House Office staff, employees, contractors, and vendors with a clearly defined need to access the information.

2.3 Electronic Protection of Sensitive Information

- Users of House sensitive information must 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 gives 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 ISSO, (202) 226-4988, or the Call Center, (202) 225-6002 / (800) 447-8737, for details.

2.4 Personnel Precautions

- Unauthorized personnel must not be allowed access to facilities and resources that store or process sensitive information.
- Contractors and vendors must sign a Non-Disclosure Agreement prior to receiving House sensitive information.

2.5 Disposal of Sensitive Information

- Diskettes, compact disks (CDs), and disk drives must be disposed of using approved procedures. Printed documents containing House sensitive information must be shredded when no longer needed. Electronic media may be provided to the Information Systems Security Office (ISSO) who will degauss and destroy the media.