HISPOL 016.0

The United States House of Representatives Information Security Policy for Privileged Account Management and Security

Version:	**1.0**
Approved:	**September 2015**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

Introduction

Privileged user accounts (Privileged Accounts) are accounts that extend access to the U.S. House of Representatives' (House's) information systems beyond what is granted to normal users. Misuse or mismanagement of Privileged Accounts significantly increases the risk to the House's information systems and information. As such, it is imperative that Privileged Accounts are rigorously managed and monitored, that the capabilities of Privileged Accounts are limited wherever possible to the functions necessary to accomplish assigned tasks, and that the rigor of security and access controls to Privileged Accounts are commensurate with the risk to which their existence exposes House information and the House's information system.

1 Scope

This policy applies to any and all individuals that use Privileged Accounts associated with any information systems attached to any part of the House network, including House systems owned and operated by House Officers, House Committees, House Member Offices, other House entities, and vendors and contractors that provide services to the House community.

2 Definitions

Authorization: The act of granting access privileges to a user, program, or process.

Authorizing Official (AO): An official with the authority to formally assume responsibility for providing access to an information system at an acceptable level of risk to House operations (including mission, functions, image, or reputation), House assets, or individuals.

Hiring Authority: The head of an employing office and the person with final authority to appoint, hire, discharge, and set the terms, conditions, or privileges of the employment of an employee of that employing office.

House Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of House information.

House Office: The personal office of a Member of the House of Representatives; a committee or joint committee of the House of Representatives, including any subcommittees; or any other office headed by a person with the final authority to appoint, hire, discharge, and set the terms, conditions, or privileges of the employment of an employee of the House of Representatives.

Least Privileges: The security objective of granting users only those accesses they need to perform their official duties.

Personally Identifiable Information (PII): For the purposes of this document only, Personally Identifiable Information (PII) is information that may be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or

identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Privileged Account: An information system account with approved authorizations of a user who is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

3 Policy

To reduce the risk associated with Privileged Accounts, all House Offices using Privileged Accounts associated with information systems attached to the House network shall, in accordance with all House policies, procedures, standards, and guidelines:

1. Have rigorous Privileged Account management requirements capable of accounting for the inherent risk of Privileged Accounts;
2. Incorporate separation of duties and principles of Least Privilege for Privileged Accounts;
3. Implement account security measures capable of mitigating the inherent risk of Privileged Accounts as outlined in privileged access security standards and procedures;
4. Implement a minimum of two-factor authentication for access to Privileged Accounts (no later than 180 days following promulgation of standards and procedures to secure Privileged Accounts);
5. Monitor all usage for potential misuse;
6. Ensure that Privileged Accounts are only used for the purposes for which they are created (i.e., administration); and
7. Ensure non-privileged user accounts are used in all cases except when Privileged Accounts are required.

3.1 Minimization of Privileged Accounts

No House Offices shall create a Privileged Account unless there is a specific business need necessitating the creation of a Privileged Account. All House Offices shall immediately disable and remove any unnecessary Privileged Accounts for which they are responsible, including local administrative accounts.

3.1.1 Minimization of Administrative Accounts

Member Offices and Committee Offices may not have more than four Privileged Accounts within the Organizational Unit Administrative Group (OU Admin Group) that consists of vendors or shared staff. This limitation does not apply to permanent staff in Member Offices and Committee Offices.

All HIR personnel with access to the OU Admin Group for Member and Committee Offices shall have a documented business need and written authorization in order to gain or maintain access to the OU Admin Group in accordance with this policy and

associated standards and procedures. Any HIR personnel within an OU Admin Group do not count against the four OU Admin account limit.

Member Offices and Committee Offices may exceed four accounts with administrative privileges that do not belong to the OU Admin Group. Member and Committee Offices shall ensure that all administrative accounts are necessary and that unnecessary or inactive accounts are immediately disabled or removed.

3.2 Least Privileges

In accordance with principle of Least Privileges, House Offices shall assign all Privileged Accounts the least amount of privileges necessary to perform the functions for which the account exists. In cases where House Offices cannot tailor Privileged Accounts, the House Office shall grant the Privileged Account the least amount of functions offered by the information system with which the Privileged Account is associated.

At a minimum, Privileged Accounts shall:

1. Not have access to email or electronic messaging services that have direct communication outside the House network;
2. Not have access to the Internet; and
3. Only have networked access to information systems and devices to which the responsibility of the Privileged Account applies.

3.3 Privileged Account Management

Users may only receive access to an information system to perform actions beyond those associated with typical users through an authorized Privileged Account.

3.3.1 Privileged Account Authorization

House Offices shall only create Privileged Accounts on an as-needed basis. House Offices shall scrutinize users requiring Privileged Accounts to a greater degree than normal system users. House Offices should create Privileged Accounts only by authorization from their particular office's Authorizing Official or Hiring Official.

3.3.2 Designating an Authorizing Official

The Hiring Authority of a House Office shall designate an Authorizing Official to create and use the House Office's Privileged Accounts. The Authorizing Official is responsible for taking all appropriate measures to ensure that the risk associated with the existence of a Privileged Account does not exceed the risk tolerances of the House and the House Office.

An Authorizing Official designated by a Hiring Authority should:

1. Have sufficient responsibility to ensure that all appropriate measures are taking to reduce risk associated with Privileged Accounts for his/her House Office;

2. Be a House employee (not a contractor or vendor);
3. Be employed by the office for which they serve as an Authorizing Official; and
4. Not have the ability to authorize himself/herself as a user of a Privileged Account.

House Offices may designate more than one Authorizing Official provided he/she meets the requirements enumerated above and throughout this policy.

Authorizing Officials will serve as a point of contact between their House Office- and the Office of the Chief Information Security Officer (CISO) for matters related to its Privileged Accounts.

3.3.3 Authorizing Privileged Accounts

When making a decision to authorize a Privileged Account, an Authorizing Official shall:

1. Examine the documented business need for the creation of a new Privileged Account to ensure that the new Privileged Account is necessary;
2. Examine user qualifications and abilities to determine that the user has been trained appropriately and does not present a risk to the system;
3. Ensure that the user of the Privileged Account has reviewed, accepted, and signed all applicable rules of behavior forms in accordance with applicable House policies and procedures (see, for example, Appendix A: *U.S. House of Representatives Rules of Behavior for Privileged Account Users*);
4. As authorized to do so by the Hiring Officer or his or her designee, examine user background for elements that may make trustworthiness of a user questionable.
5. Review the intended privileges associated with the Privileged Account to ensure that the account has only necessary privileges; and
6. Notify the Office of the CISO when authorizing elevated privileges within active directory or local administrator groups.

In accordance with House policies, standards, and procedures, the Office of the CISO shall:

1. Maintain a copy of the authorization form of Privileged Accounts for House Offices for purposes of administration; and
2. Ensure that only authorized Privileged Accounts exist on the House network.

3.3.4 Temporary Privileged Accounts

House Offices may create and use temporary Privileged Accounts in accordance with House policy, standards, and procedures. House Offices may have temporary Privileged Accounts for no longer than 14 days. House Offices may create temporary accounts for a number of reasons, including, but not limited to:

1. Administrative redundancy during vacations or emergencies;
2. Limited application installation; and

3. To satisfy a critical business need prior to authorization of a Privileged Account.

The House Office's Authorizing Officials must approve any temporary accounts prior to creation. House Offices shall set temporary Privileged Accounts to expire within 14 days. House Offices shall remove or disable temporary accounts when they are no longer needed, or after 14 days.

3.3.5 Sharing Accounts

Multiple users shall not share access to an individual Privileged Account.

3.3.6 Disabling, Removing, and Restricting Privileged Accounts

If a Privileged Account is unneeded or inactive, the House Office shall remove or disable the Privileged Account in accordance with House standards and procedures.

3.3.7 Administrative Account Use

House Offices shall provide Privileged Users with two accounts, one that provides Privileged Access, and one that provides normal system user functionality. Privileged Users may not use Privileged Accounts for functions associated with general user accounts. Privileged Account use is limited to laptop or desktop computers issued by the House.

3.3.8 Shared Service Accounts

Wherever possible, users shall only use one Privileged Account to administer systems across all House Offices for which the user is an authorized administrator. Privileged Accounts used to administer systems across multiple House Offices may not extend to any House Office that have not authorized the Privileged Account.

3.3.9 Enterprise Administration and HIR Privileged Accounts

All Privileged Accounts affiliated with duties that extend across the entire House, and Privileged Accounts associated with HIR personnel, shall operate only with the written authorization of the CISO.

3.3.10 Vendor Call Centers

Vendors operating call centers that provide services to multiple House Offices shall only use Privileged Accounts with the written authorization of the associated Contracting Officer's Representative.

3.3.11 Training Requirements

No user shall have access to a Privileged Account without having a current HIR Security and Privacy Awareness Training certificate granted by the Office of the CISO. Users shall also receive and pass HIR-provided role-based trainings for Privileged Account users upon receiving access to a Privileged Account. Privileged Users shall retake the HIR-provided role-based trainings for Privileged Account users every twelve

months thereafter. All Privileged Accounts shall expire twelve months after the date of the last completion of the HIR-provided role-based trainings for Privileged Accounts.

3.3.12 Background Checks

The Hiring Officer or his or her designee must assess the trustworthiness of each Privileged User prior to that person receiving authorization to use a Privileged Account. The Office of the CISO suggests that Hiring Officers and their designees use the rigorous criminal history records search services provided by the United States Capitol Police before authorizing an individual to be a Privileged User. Individuals under consideration for a Privileged User role should be notified in advance that placement in such a role is contingent on the Hiring Officer's determination that the individual is suitable for a Privilege User role.

3.3.13 Retention of Authorization Records

House Offices shall retain in its records the authorization form for a Privileged Account, as well as all associated documentation (i.e., Rules of Behavior forms, background check documents, etc.) for no less than one year after an employee who used the assigned Privileged Account separates from the House Office.

Any documentation associated with the authorization of a Privileged Account that contains Personally Identifiable Information (PII) should be destroyed by shredding it once it is no longer required for record-keeping purposes.

3.4 Privileged Account Authentication

No later than 180 days following promulgation of standards and procedures to secure Privileged Accounts, House Offices—with the support of HIR—shall restrict access to Privileged Accounts using multifactor authentication. House Offices shall establish authentication for Privileged Accounts, consisting of a minimum of two discrete authentication measures that are commensurate with the risk that the Privileged Account poses to the information system.

3.5 Privileged Account Record Review and Monitoring

House Offices and the Office of the CISO shall collaborate to monitor and regularly review Privileged Accounts in a manner consistent with this House policy.

3.5.1 Privileged Account Records Review

To promote the accuracy of the Office of the CISO's and a House Office's Privileged Account records, the Office of the CISO and the House Office shall collaborate to review Privileged Accounts at least quarterly as defined in this House policy and its associated standards and procedures. Unless otherwise set forth in this House policy, the Office of the CISO may not access the content of the Privilege Account without the authorization of the Hiring Official or Authorizing Official.

3.5.2 Privileged Account Monitoring

The Office of the CISO shall implement automated tools to monitor the use of Privileged Accounts where possible, consistent with the requirements of this House policy and its associated standards and procedures. Unless otherwise set forth in this House policy, the Office of the CISO may not access the content of the Privilege Account without the authorization of the Hiring Official or Authorizing Official.

4 Exceptions

The CISO, in consultation with a House Office's Hiring Authority, may grant exceptions to this policy that do not exceed 180 days in length. The CISO may also provide a termination date for the exception that is shorter than 180 days.

5 Roles and Responsibilities

House Offices, Authorizing Officials, Hiring Authority, the Office of the CISO, and Privileged Account users all have significant roles and responsibilities in mitigating the risks to House information systems inherent to Privileged Accounts.

5.1 House Offices

House Offices shall:

1. Maintain an internal, written authorization process for the creation and use of Privileged Accounts;
2. Ensure that all user information associated with Privileged Accounts within the House Office has been submitted to the Office of the CISO;
3. Conduct a quarterly review of Privileged Accounts within the House Office to ensure that all Privileged Accounts within the House Office have current authorization from the organization's Authorizing Official for the information system to which they belong;
4. Conduct a quarterly review of Privileged Accounts within the House Office to ensure Privileged Users only have access rights/privileges required to do their assigned work;
5. Conduct a quarterly review of Privileged Accounts within the House Office to ensure they are active and still needed;
6. Ensure that Privileged Accounts within the House Office comply with the security requirements enumerated in House policy, standards, and procedures;
7. Disable or remove all Privileged Accounts within the House Office that are used in a risky or atypical manner, or that have been compromised;
8. Immediately report to the Hiring Official all Privileged Accounts that are used in a risky or atypical manner and all Privileged Accounts that are potentially compromised. The Hiring Official, or his or her designee, must promptly report such instances to the Office of the CISO;

9. Ensure background checks, as defined in this policy, have been conducted on all Privileged Users within the House Office; and
10. Create, enable, modify, disable, and remove Privileged Accounts only in accordance with applicable House policies.

5.2 Authorizing Officials

Authorizing Officials shall:

1. Authorize Privileged Users within the House Office;
2. Authorize the creation and activation of Privileged Accounts within the House Office;
3. Maintain records of written authorization of Privileged Users and Privilege Accounts within the House Office;
4. Ensure that Privileged Users within the House Office have appropriate role-based training for the system with which the Privileged Account is associated, and ensure that Privileged Users have obtained current HIR Security and Privacy Awareness Training certificates;
5. If designated to do so by the Hiring Authority, review Privileged Users' backgrounds and, to the best of their ability, attest to the trustworthiness of Privileged Users;
6. Ensure that Privileged Accounts within the House Office comply with requirements of separation of duties enumerated in this policy;
7. Ensure that Privileged Accounts within the House Office comply with requirements of Least Privileges enumerated in this policy; and
8. Ensure that the House Office immediately reports to the Hiring Official all Privileged Accounts used in a risky or atypical manner and all Privileged Accounts that may be potentially compromised. The Hiring Official, or his or her designee, must promptly report such instances to the Office of the CISO.

5.3 Hiring Authority

Hiring Authorities shall:

1. Designate an Authorizing Official for their House Office;
2. Monitor proper creation and management of privileged accounts; and
3. Promptly report all Privileged Accounts used in a risky or atypical manner, or Privileged Accounts that are potentially compromised, to the Office of the CISO.

5.4 Office of the CISO

The Office of the CISO shall:

1. Assist House Offices in establishing oversight of Privileged Accounts in accordance with the requirements enumerated in House policies and procedures;

2. Assist House Offices in limiting the access of Privileged Accounts to only the devices to which the responsibility of the Privileged Account applies;
3. Maintain records of Privileged Users authorized to exist within the House IT environment;
4. Conduct quarterly reviews of Privileged Accounts in accordance with House standards and procedures;
5. Monitor the House network for unauthorized Privileged Accounts;
6. Monitor the network for accounts associated with Privileged Users who do not have current HIR Security and Privacy Awareness Training and appropriate role based training;
7. Develop and maintain standards, guidelines, procedures, and templates associated with the Privileged Account authorization process;
8. Develop and maintain standards, guidelines, procedures, and templates to secure Privileged Accounts;
9. Access and review risks, and grant exceptions to policy when required;
10. Oversee the remediation of risks caused by misuse or compromise of Privileged Accounts when detected; and
11. Authorize enterprise-wide Privileged Accounts and Privileged Accounts that support call centers.

5.5 Privileged Users

Privileged Users shall:

1. Use or access Privileged Accounts only to perform the intended functions for which the Privileged Account was created;
2. Use only a House issued laptop or desktop to access Privileged Accounts;
3. Use only their user account to perform general user functions;
4. Protect access to Privileged Accounts, including any physical devices associated with identification and authentication;
5. Report to the Hiring Authority compromising or atypical behaviors associated with Privileged Accounts. The Hiring Authority must promptly report such instances to the Office of the CISO;
6. Review, accept, and sign the *U.S. House of Representatives Rules of Behavior for Privileged Users* (Rules of Behavior); and
7. Complete HIR role-based training for Privileged Account users upon receiving access to a Privileged Account and at least every twelve months thereafter.

6 Related Documents

6.1 House of Representatives Policies, Publications, & Standards

1. HISPOL 001.0 - The United States House of Representatives Information Security Policy Structure and Organization

2. HISPOL 002.0 - The United States House of Representatives Information Security Policy for Protecting Systems from Unauthorized Use
3. HISPUB 0XX.X - The United States House of Representatives - Privileged Account Management Procedures
4. HISPUB 07.1.58 - OU Account Management
5. House IT Policy 004.0 - The United States House of Representatives Information Technology Policy for Active Directory Naming Conventions
6. House IT Policy 005.0 - The United States House of Representatives Information Technology Policy for Organizational Unit Admin Security Group Membership
7. HIR Publication - User and Email Administration Recommended Practices (Active Directory/Exchange): Version 3.0, January 28, 2013

6.2 National Laws, Best Practices, & Standards

1. NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations: Security Controls (Access Controls, Security Assessment and Authorization; Risk Assessment, and Systems and Service Acquisition)
2. NIST Interagency Report 7298 - Glossary of Key Information Security Terms: All technical terminology taken from Glossary

7 Consequences of Non-Compliance

The Office of the CISO may disable Privileged Accounts that fail to meet House policies, standards, and procedures. In cases where a Privileged Account poses a risk to House information or House information systems, the Office of the CISO may disable the Privileged Account without notice, except as required herein and by House policies, standards, and procedures. The Office of the CISO must provide notice to the House Office's Hiring Authority when disabling a Privileged Account.

In non-emergencies, the Office of the CISO shall provide the House Office reasonable notice prior to disabling the Privileged Account. The House Office shall have five business days from receipt of the notice to concur or contest the removal of the Privileged Account.

All entities and/or personnel covered by this House policy that do not to comply with any part of this policy, or fail to take prompt action to remediate vulnerabilities, risks, or negative actions associated with Privileged Accounts, as directed by the Office of the CISO, may have some or all of their information systems and/or access to information systems blocked from the rest of the House network until compliance is once again achieved.

The Office of the CISO shall report to the Committee on House Administration (CHA) any House Office intentionally violating House security policy as well as any House Office that fails to remediate known vulnerabilities or non-compliance within five business days of receiving notice from the Office of the CISO. Additionally, any House

Office that fails to remediate known vulnerabilities or non-compliance within seven days of notification. Additionally, a House Office that has not taken actions to remediate known vulnerabilities or non-compliance within five business days of receiving notice from the Office of the CISO may have its access to the House network suspended, consistent with this policy. If exigent circumstances due to imminent danger exist, House Offices may immediately have their network access suspended, with parallel notification to their Hiring Authority and CHA.

All Privileged Users covered by this House policy who fail to comply with any part of this policy or the Rules of Behavior referenced herein, or who fail to reasonably take prompt action to remediate vulnerabilities, risks, or negative actions associated with Privileged Accounts as directed by their House Office pursuant to this policy, may be subject to (i) the administrative suspension or cancellation of their Privileged Account and/or (ii) disciplinary action by their Hiring Authority, up to and including termination of employment.

HISFORM 016.02
U.S. House of Representatives Rules of Behavior for Privileged Account Users and Remote Access

Individual: Enter Individual's Name

Date: Click here to enter a date

U.S. House of Representatives Rules of Behavior for Privileged Account Users

In accordance with the security policies of the U.S. House of Representatives ("House") and to protect the confidentiality, integrity, and availability of data processed and owned by the House, Privileged Users of House information systems must accept and follow the *U.S. House of Representatives Rules of Behavior for Privileged Account Users*.

This document provides common rules on the appropriate use of House information technology resources for Privileged Users, including House employees and contractors. Privileged User account roles have elevated privileges above those in place for general user accounts regardless of account scope (e.g., including both local and domain administrator accounts).

Potential compromise of Privileged Accounts carries a risk of substantial damage and therefore Privileged Accounts require additional safeguards.

All users of Privileged Accounts must read these rules, initial beside each rule, and sign the accompanying acknowledgement form before accessing House information, systems, and/or networks in a privileged role.

_____ I understand and acknowledge that, as a Privileged User, I shall:

1. Use my Privileged Account(s) for official administrative actions only;
2. Protect all Privileged Account credentials (passwords, tokens, etc.) at a security level commensurate with the highest level of data that the Privileged Account can access on the associated information system;
3. Protect the administrative or root-level authentication information at the highest level demanded by the sensitivity of the system;
4. Comply with all system/network administrator responsibilities in accordance with House policies;
5. Use special access privileges only when they are needed to carry out a specific system function that requires elevated privileges on assigned systems;
6. Use a non-privileged (i.e., general user) account whenever administrative privileges are not required (e.g., e-mail, web browsing);
7. Log on to my non-privileged account and then subsequently login to my Privileged Account to perform actions requiring privileges (to the maximum extent possible). For example, I understand that on a UNIX operating system, the user must login to a non-privileged account before logging in as "root," and on a Microsoft Windows computer, the user must login to a non-privileged account before performing a privileged function that requires authentication as a Privileged User;

8. Notify the respective Hiring Official and/or Authorizing Official immediately when privileged access is no longer required;
9. Use precautionary procedures to protect a Privileged Account from fraudulent use;
10. Watch for signs of inappropriate or illegal (e.g., hacker) activities or other attempts at unauthorized access and immediately report them to my Hiring Official and/or Authorizing Official upon discovery. My Hiring Official, or his or her designee, must promptly report such instances to the Office of the Chief Information Security Officer ("CISO"); and
11. Complete any specialized role-based security training as required before receiving privileged system access.

_____ I understand and acknowledge that, as a Privileged User, I shall **not**:

1. Share Privileged User account(s) or password(s);
2. Create or logon to a group or shared user account that is not authorized by policy;
3. Remove or destroy a system audit, security, event, or other type of log;
4. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls;
5. Introduce unauthorized or malicious code into House information systems or networks;
6. Knowingly write, code, compile, store, transmit, or transfer malicious software code, including, but not limited to, viruses, logic bombs, worms, and macro viruses;
7. Use Privileged Account(s) for day-to-day communications (to include accessing the Internet);
8. Use Privileged Account(s) to access data or other information unless I am explicitly authorized to do so as part of my official duties;
9. Elevate the privileges of any user without prior approval from the Authorizing Official;
10. Use special privileges for personal business, gain, or entertainment;
11. Use privileged access to circumvent House policies or security controls; or
12. Use a Privileged User account for Web access.

_____ As a user of a Privileged Account, I understand and acknowledge that **I HAVE NO REASONABLE EXPECTATION OF PRIVACY,** while using any Privileged Account on an information system that processes, transmits, or stores House data.

_____ I understand and acknowledge that all Privileged Account activity on information systems in support of the House *may be monitored, intercepted, recorded, read, copied, or captured* by my Hiring Authority or by authorized House personnel, only as enumerated in HISPOL 016.0, or by my Hiring Authority. My Hiring Authority may give law enforcement officials any potential evidence of crime, fraud, or misconduct found on House information systems.

_____ I understand and acknowledge that such Privileged Account monitoring by House personnel may consist of:

a. review of audit logs of any Privileged Accounts on IT devices used to support the House;

b. review of access and use of the Internet by Privileged Account users while on the House network;

_____ I understand and acknowledge that I shall successfully complete HIR Information Security and Privacy Awareness training on an initial and annual basis as required or risk having my access to House information systems suspended.

_____ I understand and acknowledge that I may have access to sensitive information depending on my job duties. I shall protect the confidentiality, integrity, and availability of House information in a manner consistent with its sensitivity.

_____ I understand and acknowledge that, if I access Personally Identifiable Information ("PII") or sensitive information as a requirement of my duties, I will encrypt PII or sensitive information as required by House policy. This includes, but is not limited to, encrypting PII or sensitive information that is

a. downloaded from House or House organization information systems onto a House authorized portable storage device; or

b. e-mailed to any entity external to the House organization (to a non-"HOUSE.GOV" email address).

Approved encryption levels are AES 256 or greater. Any questions concerning encryption should be directed to the Office of the CISO.

_____ I understand and acknowledge that I will delete PII and sensitive data downloaded from House information systems immediately when its official use is no longer required.

_____ I understand and acknowledge that I will immediately report a security breach, password compromise, or anomaly in system performance to my Hiring Official and that my Hiring Official or his or her authorized representative must promptly report such instances to the Office of the CISO.

_____ I understand and acknowledge that I will protect my passwords and/or authentication tokens from disclosure and loss at all times. I will take all efforts to avoid disclosing my passwords. I will not construct my password from obvious personal data (i.e., social security number, telephone numbers, relatives' names, or pet's name, etc.).

_____ I understand and acknowledge that I am accountable for all actions taken under my User ID. I will not allow others to use my Privileged Account's User ID and I will not access other users' accounts, unless required to as part of my official duties. I will not attempt to access accounts or data that I am not expressly authorized to use.

_____ I understand and acknowledge that when logged on, I will lock my workstation prior to leaving my workstation.

_____ I understand and acknowledge that I may not install, use, or reproduce unauthorized or illegally obtained software on House information systems. Privately owned software is strictly prohibited on House information systems.

_____ I understand and acknowledge that I shall not connect unauthorized devices to House information systems under any circumstance.

_____ I understand and acknowledge that changes in my employment status or changes in my job responsibilities may require modification or termination of my access to House information systems.

_____ I understand and acknowledge that I am using an unclassified information system. This system is not designed and secured for the handling of classified information. I am NEVER authorized to originate or knowingly process, and/or store classified information on an unclassified system.

_____ I understand and acknowledge that this agreement shall not nullify or limit in any manner any other confidentiality, nondisclosure, or computer use agreement that I have executed or may execute with the Office of the CISO and my Hiring Authority.

_____ I understand and acknowledge that I shall never attempt to tamper with, circumvent, or otherwise impede the security of any House system. I understand and acknowledge that I shall never install or utilize any tools designed to assist in doing the same.

_____ I understand and acknowledge that if I do not comply with these rules, I am subject to (i) the administrative suspension or cancellation of my access privileges by the Office of the CISO or my Hiring Authority, and/or (ii) disciplinary action by my Hiring Authority, up to and including the termination of my employment.

_____ I understand and acknowledge that this agreement shall not serve to create an actual or implied contract of employment between myself and the Office of the CISO or my Hiring Authority, or to confer any right to remain an employee of my Hiring Authority, or otherwise to change in any respect the employment-at-will relationship between myself and my Hiring Authority.

My signature below is my acknowledgement that I understand and acknowledge my responsibilities under the *U.S. House of Representatives Rules of Behavior for Privileged Account Users* and that I will comply with these rules of behavior and will reaffirm this acknowledgement annually in writing.

_____	_____	_____
Printed Name, Title	Signature	Date

U.S. House of Representatives Rules of Behavior for Remote Access

In accordance with House policies, and to protect the confidentiality, integrity and availability of data processed and owned by the House, users must accept and follow the *House Rules of Behavior for Remote Access* in order to be permitted to perform House duties from a remote location.

House Rules of Behavior for Remote Access apply to all users of House information systems (which includes House employees, contractors, vendors, and agents with a House-owned computer or workstation used to connect to the House network.) *House Rules of Behavior for Remote Access* apply to remote access connections used to do work on behalf of the House, including reading or sending email and viewing Intranet web resources.

1. Users (which includes House employees, contractors, vendors, and agents) with remote access privileges to the House's network are responsible for ensuring that their remote access connection is given the same security considerations as the user's on-site connection when connecting to the House. For example, if an individual is processing sensitive personnel information via remote access, he/she must not process that information from a public facility such as a coffee shop or bookstore.
2. The user is responsible for ensuring, to the best of his/her ability, unauthorized users do not access the House network, do not perform illegal activities, and do not use the access for outside business interests. The user may bear responsibility for the consequences if the user's access is misused. Misuse of the user's access by an unauthorized user may result in (i) revocation of the user's network access by the user's Hiring Authority or the Office of the Chief Information Security Officer (CISO) and/or (ii) disciplinary action against the user by his or her Hiring Authority.
3. Users are prohibited from sharing any House network passwords (email, administrative account, etc.) with any other person or entity other than the user's Hiring Authority.
4. Users with remote access privileges must ensure that their House-owned or personal computer is not connected to any other network at the same time they are logged into the House's network.
5. Users with remote access privileges to the House's network should not use non-House email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct House business, thereby ensuring that official documents and correspondence are appropriately protected and are maintained separately from non-official documents and correspondence.
6. By way of example, users should avoid being logged into the House network via a local Ethernet connection and then dialing into AOL or another Internet

Service Provider; or being on a House-provided VPN tunnel and then connecting into another person's remote access tunnel provided to them by a non-House employer or service.

7. All hosts (which may include but are not limited to laptops, desktops, workstations, etc.) that are connected to the House's internal networks via remote access technologies must use the most up-to-date anti-virus software and definitions, as approved by the Office of the CISO.

I have read the *U.S. House of Representatives Rules of Behavior for Remote Access.* My signature below is my acknowledgement that I understand and acknowledge my responsibilities and that I will comply with these Rules of Behavior.

_____	_____	_____
Printed Name, Title	Signature	Date