Assistant Secretary for Administration
U.S. Department of Health and Human Services

Best Practices on HHS System Security

Securing user access and protecting sensitive information in HHS systems is vital, given the prevalence of cyber threats orchestrated by advanced malicious entities in the digital realm. Recognizing the seriousness of these threats is key to developing proactive defense strategies. To strengthen system security and counter the risks posed by these sophisticated methods used by bad actors, consider the following best practices:

Set Role-Based Access Controls

To manage user access, accounts, and permissions, first identify each user's roles and needs. Roles can be categorized based on functions and responsibilities, and user needs can be specific requirements and expectations of each role. Setting user role-based access controls will help define the appropriate user access and permissions.

Adopt a Zero-Trust Policy

A zero-trust policy means that individuals and devices are regarded as potential threats and should be treated accordingly. When working under the zero-trust policy, staff should be able to identify and verify the identity of all users and devices, detect and respond to potential security risks, and consistently authenticate and authorize access to resources. It is also essential to identify any abnormal behaviors while tracking activities and risk levels.

Follow the Principle of Least Privilege

The Principle of Least Privilege is a security best practice. It ensures users have the minimum access and permissions to perform their tasks. Practicing this principle helps reduce the risk of unauthorized access, data breaches, and vulnerabilities. To implement this, review and audit each user's current access and permissions regularly and deactivate or restrict any unnecessary privileges that are not consistent with set role-based access controls.

Inventory, Update, and Audit User Accounts

Regularly inventory, update, and audit accounts. Establish a schedule and a process for evaluating and modifying user access and permissions based on your network's feedback, reports, audits, and role-based access controls. It ensures user access is current and allows HHS to identify accounts that should be deactivated quickly. Additionally, it can help identify and resolve issues or errors affecting your funds' availability.

Educate and Train Users

Educate and train users to be aware and understand the policies, procedures, and best practices for accessing and using HHS systems. It can help reduce human errors, negligence, or misconduct that can compromise the security of your account. Be sure users take and pass required organization cybersecurity awareness, phishing, scamming, and other training courses. Also, ensure guidelines and instructions are current and make resources on securely accessing and using HHS systems readily available for users.

People using assistive technology may not be able to access information in this file fully. For assistance, email psccommunications@hhs.gov.