HUCK-IT-P003: Authentication and Access Control

On this page:

1.0 Overview

The purpose of this document is not to impose restrictions that are contrary to the Pennsylvania State University's established culture of openness, trust and integrity. The Huck Institutes of the Life Sciences is committed to protecting our employees, partners and the University from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 Purpose

The purpose of this policy is to outline the requirements for authenticating people, services and devices so that they may access resources that are provided by the Huck Institutes of the Life Sciences. The policy also outlines the requirements for control of said access to resources once authentication has occurred.

3.0 Scope

This policy applies to any person who utilizes resources that are managed by the Huck Institutes of the Life Sciences or to any person who handles data that is the property of the Huck Institutes of the Life Sciences. We encourage you to read "HUCK-IT-P000 Introduction to IT Services at the Huck Institutes of the Life Sciences" for a primer on the philosophy adopted as part of the management of information at the Huck Institutes of the Life Sciences. The policy augments the following Penn State University policies as well as additional applicable policies:

- **AD95 Information Assurance and IT Security (Formerly AD20)**
- **AD96 Acceptable Use of University Information Resources**

4.0 Policy

4.1 Authentication

Whenever possible, the Huck Institutes systems and services will utilize Penn State Access accounts for authentication. In the event that a system or service cannot use a Penn State Access account, said system or service shall implement a user account and password to meet or exceed minimum requirements as described in this document.

4.1.1 Requirements for Credentials

Accounts managed by the Huck Institutes will, at a minimum, follow password creation and maintenance requirements as outlined in the Choosing Your Penn State Account Password document. The Huck Institutes reserves the right to implement more stringent password requirements on devices owned and managed by the Huck Institutes.

- Special user accounts created for privilege escalation purposes must have a different username and password from all other accounts held by that user.
- SNMP community strings must be defined as something other than the standard defaults of "public", "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available and SNMPv2 or higher must be implemented wherever possible.

- Strive to use strong passwords meeting the characteristics outlined in the following list - even if the system does not require that all of these characteristics are satisfied:
    - Contains at least three of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - “Special” characters (e.g., @#$%^&*()_+|~=\`{}[]:”;`<>/ etc)
      Contains at least fifteen characters

4.1.2 Protection of Credentials

- It is the responsibility of account holders to safeguard passwords and/or other sensitive access control information. Such information must not be transmitted to, shared with, or divulged to others.
- The user agrees not to share any account passwords, nor allow another user to access a device under his or her credentials.
- The user understands that he or she is responsible for any actions taken on a computer logged in under his or her credentials and the user is solely responsible for those actions.
- For each account, the user agrees to adhere to secure password criteria and comply with the requirement for periodic changes.
- Passwords should never be written down unless they are disassociated from other identifying information. Passwords stored online must be encrypted.
- Never reveal a password in any electronic communications.
- If someone demands that a password be disclosed, refer them to relevant Penn State and Huck Institutes policies.
- Refrain from using application-level “Remember Password” features.

4.1.3 Limited vs. Escalated Privileges

- Users are required to log into systems using non-administrator or non-root accounts. The following exceptions are granted:
    - Initial system configuration so that a non-administrator or non-root account can be created for future logins.
    - Periodic administration by Huck Institutes IT staff. All changes made by Huck Institutes IT staff during these administration sessions shall be logged in the Huck Institutes Service Desk system.
- Huck Institutes staff who demonstrate a specific business need to administer their local devices may request an exemption, but there is no guarantee that these requests will be granted. All others must request local administrator access through the system managers of their device(s).
- Accounts used for privilege escalation will be separate from existing limited user accounts.
- Users should only execute tasks requiring privilege escalation if they have signed a privileged user agreement that is on file with the system managers of their device(s).
- At their discretion, the Huck Institutes IT staff will have an administrator-level account on every system that they manage. ***CHANGES TO THIS ACCOUNT CAN ONLY BE MADE BY HUCK IT STAFF***.
- All system-level passwords must be changed at least once per year.

4.2 Access Control

- Access to shared resources must be constrained according to the security and data classification requirements of the resource.
- The default policy for any access control list must be “Deny all and only allow based upon need to know”. This is effectively the principle of “least privilege”.
- It is the responsibility of the end user to understand and manage access to any shared resources under their control.
- Access Control Lists (ACLs) for shared resources must be reviewed regularly (at least annually) to ensure that the principle of “least privilege” is maintained.
- Any device that is left unattended must be secured at a level that is commensurate with the data that it holds. This is true regardless if the device can be accessed actively or passively.
- To the fullest extent possible, access to shared resources must be logged. Logging should include access connection and disconnection time stamps, user initiating access and the resource being accessed. Additional logging details may be required depending upon the classification of the data being accessed via the shared resource.

5.0 Enforcement

Any employee, student or visitor found to have violated this policy may be subject to revocation of privileges as well as disciplinary action by their Administrative unit, the College, or the University.

6.0 Supporting Documents

- HUCK-IT-P000: Introduction to IT Services at the Huck Institutes of the Life Sciences
- HUCK-IT-P001: Acceptable Use
- HUCK-IT-P002: Data Protection and Retention
- HUCK-IT-P004: Remote Access

Visit the Huck Institutes of the Life Sciences on the web at http://www.huck.psu.edu.

This publication is available in alternative media on request.