HUCK-IT-P006: Administrative Privileges

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 usage and expectations of elevated privileges while operating within the Huck domain. We have evaluated how other groups similar to ours at Penn State and other academic institutions, as well as government and commercial entities, provide services similar to ours at the staffing levels that we have available.

3.0 Scope

This policy encompasses any and all users requesting elevated privileges as well as any and all machines or devices that the user can access with elevated privileges. This policy will cover the use of elevated privileges on mobile devices, both foreign and domestic, so long as it was procured through Huck funds and/or budgets.

This policy augments the following Penn State University policies and may augment additional Penn State University policies where applicable.

- **AD95 Information Assurance and IT Security (Formerly AD20)**
- **AD96 Acceptable Use of University Information Resources**
- **AD11 – University Policy on Confidentiality of Student Records**

4.0 Policy

- The user agrees to operate under the Principal of Least Privilege (PoLP). PoLP means ONLY using an administrative account when needed, such as when an update needs to be applied or a program installed.
- The user agrees to take every measure to secure and protect their administrative account credentials. Pursuant to AD95 Information Assurance and IT Security (Formerly AD20), you may not share these credentials with anyone else for any reason.
- If a user is on the system where administrative privileges enable them to create accounts, they may never elevate any of them to administrative level. This includes granting sudo. Administrator level account must be created only by Huck IT for auditing purposes. Any SSH keys must be placed systems only by Huck IT staff.
- If there are existing accounts (including administrative level accounts) on a system on which a user has administrative privileges, they may not tamper with them in any way. They may not change their passwords, disable them, alter their privileges or login as them (this includes su)
- Users with elevated privileges may not install any software not approved by Huck IT, Penn State IT or the Office of Information Security
- Users with elevated privileges may not disable or alter any pre-installed applications or system services, including the host-based firewall and device encryption without the approval of Huck IT
- Users with elevated privileges may not disable or alter any security restrictions, auditing tools or logging processes or the resultant log files for any reason.
- Users with elevated privileges may not alter any SELINUX configuration without consultation and approval of Huck IT.
- The user agrees to notify HUCK IT immediately if device is lost, left at travel destination, or stolen.

- The user acknowledges that even though they have been granted elevated privileges, HUCK IT is not personally responsible for any data contained on the device. The user must be responsible for backing any and all data up securely and reliably.
- Use of elevated privileges shall be limited to designated computer(s) or systems.
- An administrator on any system shall not access any data for which he/she is not authorized. Any data accessed for any reason, including troubleshooting must be treated with the utmost confidentiality regardless of its classification and may not be divulged to any third party for any reason.
- Administrators may not use their elevated privileges to access data on any device for any third parties.
- The use of elevated privileges will be granted for one calendar year. After that year, the user must then re-apply for the elevated privileges. Users may submit a renewal request no more than 30 calendar days before their account expires. It will be left up to the user to manage and keep track of their eligibility for elevated privileges as well as expiration dates.
- Huck IT support on devices with administrators outside of IT will be on a "best effort" basis only.
- Administrative privileges may be revoked at any time without notice or explanation.

5.0 Exceptions

Exceptions to this policy can only be granted by completing form **HUCK-AD-F001: Request for Policy Exception or Exemption.** This form must be fully completed and signed by either the Director of the Huck Institutes or the Director of Administration for the Huck Institutes or their designees.

6.0 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.

7.0 Supporting Documents

- Principle of Least Privilege: https://en.wikipedia.org/wiki/Principle_of_least_privilege
- HUCK-IT-P001: Acceptable Use
- HUCK-IT-P002: Data Protection
- HUCK-IT-P003: Authentication and Access Control
- 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.