# HUCK-IT-P004: Remote Access

**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 remote access to resources that are provided by the Huck Institutes of the Life Sciences. The policy also outlines requirements for the configuration of services that are made available for remote access as well as requirements for the clients that access those services.

## 3.0 Scope

This policy applies to any person who manages or accesses resources that are provided by the Huck Institutes of the Life Sciences. This 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 General

It is the responsibility of everyone who manages or accesses a remotely accessible service on Huck Institutes of the Life Sciences networks to ensure that the connection is given at least the same consideration as on-site connections. Access and control will be enforced via Penn State University and/or Huck Institutes of the Life Sciences gateway and firewall services. Additionally, Penn State University Minimum Security Baseline protections apply to data no matter where it resides. The owner of the account under which remote access actions take place is responsible for the consequences should the access be misused.

4.2 Requirements

HUCK-IT-P007 Firewall Policy identifies the various segments (Virtual LANs or VLANs) that the Huck Institutes internal network is separated into. Remote access connections are configured such that end users have access to the minimal number of VLANs that they need to accomplish their job functions remotely. It is preferred that remote access users utilize a restricted connection into a specific service or system, but considerations are made for remote access users that require broader access.

- Special VLANs will be available for publicly accessible services hosted on the Huck Institutes network. Access to services on these VLANs will be firewall-controlled under the philosophy of “deny all and only allow the minimum necessary connectivity”.
- Services hosted outside of the publicly accessible VLANs will only be accessible by first connecting to the Huck Institutes LAN(s) via a VPN service managed by Huck IT staff.
- The HUCK VPN service will only provide application-level connectivity unless a network-level connectivity exception is requested and granted.
- No direct connectivity to local login services, such as SSH, hosted on trusted VLANs will be allowed except through an established VPN connection.

  - Clients connecting remotely must ensure that their endpoint devices are clean of malware, are implementing sufficient endpoint protection mechanisms and are only being used by approved Penn State personnel. Effectively, Penn State University policies still apply.
  - VPN connections should be terminated as soon as they are no longer needed. If you walk away from a system that has an established VPN connection, you must disconnect before leaving the system.
  - Client endpoint devices that connect to internal resources on Huck Institutes networks should be password protected. Password protection includes:
    - A strong password is required to log into the system.
    - The system lock screen should be password protected.
    - No application-level password saving features should be used.

## 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
- HUCK-IT-P003: Authentication and Access Control

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