## Duke University's Protected Network for Sensitive data

Duke's Office of Information Technology (OIT) and the University's IT Security Office (ITSO) established the Protected Network as a resource for storage and analysis of Sensitive research data. The network is separated virtually from the general Duke network and has more extensive security protections. It comprises dedicated storage and virtual machines (VMs), and requires specific authorization from the Campus ITSO for access.

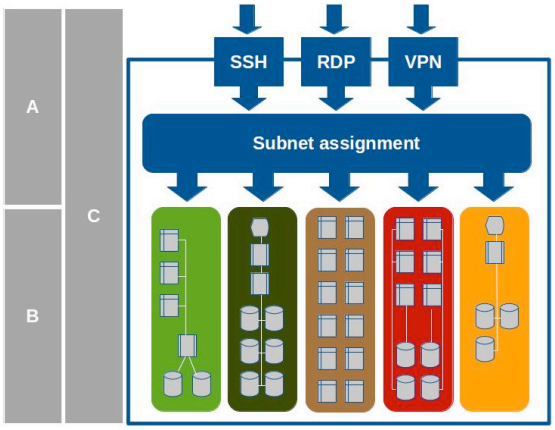
## Protected Network Components

The Protected Network has a dedicated VM and storage infrastructure designed to accommodate Sensitive data. A firewall and network rules separate the Protected Network from the Duke Network and Internet, preventing unauthorized inbound and outbound connections. Systems in the Protected Network comply with the University ITSO's Server Security Standards including: regular patching; removal of unneeded services; logging to a central logging infrastructure; active host-based firewall; running an antivirus program; and regular backups. Systems in the Protected Network also require multi-factor authentication.

The infrastructure is located in a Duke University secured datacenter with physical access limited to authorized Duke IT staff. All backups of the research project data are encrypted and located in the same secured data center.

Researchers accessing resources in the Protected Network are required by policy to enact the following protections on their computers accessing the Protected Network: regular patching; running an antivirus program; laptop encryption; and active host-based firewall.

**Figure 1: Schematic depicting the environment**




The Duke Protected Network uses (A) two-factor authentication to accept users into SSH, RDP, or VPN connections. Using Access Control Lists managed by Grouper, users are then directed to specific subnets (B) that are tailored to computational requirements of research projects. Within the subnets, individual machines can further restrict access to data or computational resources. The entire infrastructure (C) uses Grouper for authorization, from initial access to the environment (A) to individual devices within the various subnets (B). Initial authentication via SSH, RDP or VPN is multi-factor, using Duke's NetID (Kerberos & AD) and Duo.

## Protected Network Access

Access to the Protected Network requires an encrypted connection through Secure Shell (SSH), Remote Desktop Protocol (RDP) or Virtual Private Network (VPN). Access requires a valid Duke NetID (user account) combined with multi-factor authentication (e.g., using Duo). The group management tool Grouper is used to control access to the Protected Network and systems within the network. Principal Investigators, or their delegates, are responsible for approving user access to their Protected Network project's groups.

## Responsibilities

Users of the Duke Protected Network accept the policies and terms of use established for that network. For each research activity, a person responsible for maintaining contractual and/or legal obligations for data protection is identified (the "data steward"). An "administrator" is also designated by the data steward to manage Grouper groups, and therefore, provision access to their project, directly. The "data steward" and the "administrator" may be the same person.