



Fermilab Remote Access Policy

Fermilab recognizes the need for secure remote access to login or similar services available on the Fermilab network. This policy seeks to minimize the risks of remote access while maintaining essential functions, and shall apply to all computers on the Fermilab network offering such services.

1 Categories of Remote Access Services

Remote access may be offered for any range of services appropriate to the functionality required. Fermilab recognizes three broad categories of remote access services, which entail different levels of risk, and which therefore require different levels of protection:

1. Those which provide interactive access to a system and allow execution of arbitrary commands or bidirectional transfer of arbitrary data. These services require centrally-managed authentication;
2. Services which do not fall in the first class, but have been identified as presenting a significant risk, for example, web servers. These services may require specific waivers or conformance to specific system and service configuration baselines;
3. All other services;

An inventory of services offered on the Fermilab network is maintained by the Fermilab Computer Security Team as part of the risk assessment process. In this process, system administrators identify those services offered by systems they are responsible for, and the risk is formally accepted by their management.

These classes of services are treated with specific policies in the environment security plans.

2 System Requirements

The Policy on Computing (<http://security.fnal.gov/Policies/cpolicy.html>) requires that all computer systems on the Fermilab network conform to the current version of the relevant Fermilab operating system configuration baseline, or document the reasons why the system cannot be brought up to date and how the system is patched and configured to provide the same level of security as provided in baseline configurations. In addition, certain services (such as web servers) cannot be offered on systems which do not meet baseline configurations.

Services may also be subject to baseline configuration requirements. When a baseline configuration exists for a service, computer systems on the Fermilab network which offer that service must conform to the current version, or document the reasons why the baseline cannot be met and how the service is configured to provide the same level of security as provided in baseline configurations.

Requests for waivers to baseline requirements are placed online [through](#) the Fermi Service Desk.

All computer systems on the Fermilab network must have a current risk assessment including any remote access services they offer. The risk assessment policy and process is described in the [Policy on Computer Security Life Cycle](#) (<https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=1508>).

Additional items include the use of host-based firewalls and other endpoint protection measures, and administrative restrictions and control of accounts as appropriate.

2.1 General Computing Environment

Remote access services offered by systems in the GCE must conform to the [Security Plan for the General Computing Environment](#) (<https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=1185>) and the [Fermilab Authentication Strategy for the GCE](#) (<https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=2436>).

2.2 Open Science Environment

Remote access services offered by systems in the OSE must conform to the [Security Plan for the Open Science Environment](#) (<https://cd-docdb.fnal.gov:440/cgi-bin/ShowDocument?docid=1191>).

3 Offsite Access Methods

In general, all methods of off-site network connection are *restricted* as defined in the [Policy on Computing](#) (<http://security.fnal.gov/Policies/cpolicy.html>) and may only be offered by the Computing Sector.

3.1 General Internet Access

Many remote access services may be directly accessible to the general Internet, subject to controls determined by policy and risk assessment.

3.2 VPN Access

Remote access services may use, as an additional control, either the central Fermilab VPN service (<http://ncs.fnal.gov/nvs/vpn.php>) or a VPN service

approved for use with a specific Major or Minor Application. VPN service is a restricted service under the Policy on Computing.

3.3 *Dial-in Modem Access*

Dial-in modem access to the Fermilab network is not supported.

4 Restricted Remote Access Authentication Methods

Use of authentication mechanisms that provide credentials to a third party vendor, or pass the session through a third party server (commonly used by many software support companies), are restricted. In most cases, these resources are viewable by all other registered users world-wide, and do not meet the Fermilab requirements of using a centrally managed account or safe transmission of the authentication credentials. Refer to the relevant service configuration baseline.

5 Policy Enforcement

Fermilab Computer Security continuously scans for remote access services offered on the Fermilab network. Systems which do not conform to this policy may be blocked from network access. Attempts to obfuscate services from scanning or to circumvent access controls without prior Fermilab Computer Security approval, may be viewed as a violation of policy and are subject to possible disciplinary action.