George Mason University	*ITU Standard* **Remote Access Device**
Version 1.0	*Date of last revision: 09/16/2011*

The George Mason University's Information Technology Unit (ITU) maintains one or more Virtual Private Network (VPN) systems that support off-campus access to internal university networks and hosts. University departments desiring to install a "non-standard remote access system" (defined here as any VPN or gateway not managed by the ITU, which enables off-campus access to internal computing resources) must submit a request (http://tsd.gmu.edu/net/Forms/F0056_A.html) that will be first reviewed by the IT Security Office. Approval will be based on the completion of a documented system policy, as defined below, and the results of an initial risk assessment from the IT Security Office. Annual audits are required for continued service.

An approved non-standard remote access system will have the following components:

System Policy

1. The system owner must complete a system policy document defining: A. the business need; B. authorized users; and C. network access requirements.
2. Any changes to the system policy require the system owner to initiate a new risk assessment.

Account Management

1. Each user must have a unique login name; exceptions can be made for vendor companies and business partners as long as the vendor account's access is restricted to specific systems and/or applications. Vendor accounts must be re-authorized on, as a minimum, an annual basis.
2. The system owner is responsible for verifying a requestor's identity and documenting the Account Activation process.
3. Accounts must be deactivated within 24 hours of the account owner separating the university or changing role.

Password Policies

1. Passwords must meet the same requirements as Patriot Pass. The requirements are detailed on the following web site. http://strongpassword.gmu.edu/password_strength.html
2. User accounts should be temporarily locked out for a minimum of 15 minutes after no more than three failed login attempts.

System Management and Logging

1. The remote access system must have designated primary and backup system administrators. Both should be fulltime employees of the university.
2. System logs are to be reviewed by a system administrator on a regular basis.
3. The system owner must maintain auditable records of remote access attempts and sessions; these logs should be protected from compromise and must be retained for a minimum of 90 days.