System Administrator and System Registration Revisited

University Policy 1301 – Responsible Use of Computing
University Policy 1304 - Public Internet Address Policy
And University Policy Number 1312 –Physical and Logical Access

S.A.L.T. Presentation, May 10th , 2012
Curtis McNay - Director, IT security

University Policy Number 1301

- Responsible Use of Computing

http://www.gmu.edu/facstaff/policy/newpolicy/1301gen.html

- **System Administrator (SA).** Anyone who has the responsibility to maintain, configure, operate, or repair Mason's computing resources. System Administrators have special privileges and special responsibilities under this policy.

- **System Administrator.** The **SAs** have extraordinary powers to override or alter access controls, configurations, and passwords. This power should be exercised with great care and integrity. SAs' actions are constrained **by this policy and by the policies of local administrative units.**

- **Data Stewards** of Mason units who employ **SAs** are responsible for ensuring that the SAs comply with and enforce the requirements of this policy in the systems for which they are responsible. **SAs who violate this policy or who misuse their powers are subject to disciplinary action.**

- If an **SA** observes someone engaging in activities that would seriously compromise the confidentiality, availability, or integrity of a Mason system, network, or electronic Mason data, the **SA may take immediate action to stop the threat or minimize the damage or contact the ITU Support Center to activate the Computer Security Incident Response Team (CSIRT).** **SAs** who observe suspected violations of law should immediately alert the Mason Police.

University Policy Number 1304 – Public Internet Address Policy

http://www.gmu.edu/facstaff/policy/newpolicy/1304gen.html

I. SCOPE

The Public Internet Address Policy applies to all users of George Mason University computing resources. This policy governs all computers directly connected to George Mason University networks, with the exception of student owned computers in the residence halls. Student owned computers in the residence halls are on a separate network that has similar policies.

II. POLICY STATEMENT

Allowing outside systems to initiate connections to a university computer increases the university's risk to threats from the Internet.

The applicant must register the computer with the Information Technology Unit (ITU). Registration information will include the name and contact information for the person who is responsible for administering the computer (the SA) as well as verification that security configurations are in place and that the person maintaining the computer will follow appropriate security procedures. **The applicant will need to describe any highly sensitive data, as defined in the Data Stewardship Policy, which is stored on the computer. Once the registration information has been received and verified as complete, the ITU will contact the SA to finalize the process.**

Public Internet Address Policy continued..

IV. RESPONSIBILITIES

ITU will send out, at a minimum, **an annual request** for update of information about registered computers.

The ITU will take measures to protect all university computers without a publicly addressable address from connections initiated by external systems**.**

Departments and administrative units are responsible for ensuring the security and safety of the computers in their department. They are to develop and administer their own local procedures for establishing security configurations as well as ensuring that university best practices for server management are followed in their departments. These procedures must include computers accessing and storing regulated and highly sensitive data.

System administrators (SA) will make a commitment to obtain and maintain their security knowledge and to maintain the security of the computers for which they are responsible.

The Office of Internal Audit will monitor compliance with this Policy.

Public Internet Address Policy continued..

V. OTHER INFORMATION

The Public Internet Address Request form can be found at: http://tsd.gmu.edu/net/forms.html. At a minimum, the following information will be required:

- **Make and model of the hardware platform**
- **Operating system version**
- **Domain Name Service (DNS) name**
- **Assigned or requested IP address**
- **Name of the person responsible for management of the computer (including phone number and email address)**
- **Physical location of the computer**
- **Internet services being offered**
- **Security Protection measures applied to the computer**
- **Computer's primary purpose**
- **Description of any regulated or highly sensitive data stored on the computer.**

VI. COMPLIANCE

All persons installing computers in University owned or leased spaces, except residence halls, shall comply with this policy.

Grievance matters with this policy should be directed to the Executive Director, ITU Technology Systems Division, for resolution. If the conflict is not able to be resolved at this level, the matter may be escalated to the Vice President for Information Technology for further review and action.

University Policy Number 1312

Physical and Logical Access Security Policy

I. SCOPE

Administrative Policy Number 1312 applies to all academic and operational departments and offices at all George Mason University locations, owned and leased. The policies and procedures provided herein apply to all University faculty, staff, students, visitors and contractors.

This policy governs the physical and logical access to all university systems and applications to protect the privacy, security, and confidentiality of university systems, especially highly sensitive systems, and the responsibilities of institutional units and individuals for such systems.

Policy 1312 continued.. Account Management

All systems and applications will have documented policies and procedures for:

a. approving and terminating access

b. obtaining and disabling temporary accounts

c. consistent periodic review and assessment of all accounts for continued needs with documentation as evidence of the review

d. locking accounts after a period of inactivity, with the period of time appropriate to the sensitivity of the system and associated risks

Policy 1312 continued.. Controls

It is the policy of the university to use all reasonable IT security control measures to:

a. Protect university information resources against unauthorized access and use

b. Maintain the integrity of university data

c. Ensure university data residing on any IT system is available when needed

d. Comply with the appropriate federal, state and other legislative, regulatory and industry requirements

Protecting information resources includes:

- **Physical protection of information processing facilities and equipment**
- **Assurance that application and data integrity are maintained**
- Assurance that information systems perform their critical functions correctly, in a timely manner, and under adequate controls
- **Protection against unauthorized access to protected data through logical access controls**
- **Protection against unauthorized disclosure of information**
- Assurance that systems continue to be available for reliable and critical information

Policy 1312 continued..
Provisioning, De-provisioning

The organization responsible for an information system is responsible for the prompt deactivation or disabling of accounts when necessary including but not limited to accounts subject to the following circumstances:

a. the accounts for terminated individuals shall be removed/disabled/ revoked from any computing system at the end of the individual's employment or when continued access is no longer required

b. the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location

c. the accounts for employees who are not working due to any sort of leave, disability or other authorized purpose, or when continued access is no longer required, shall be temporarily disabled for a period consistent with the employee's personal usage needs and duration of absence

d. the accounts for employees suspended for more than one day for disciplinary reasons shall be disabled

Policy 1312 continued.. Least Privileges

4. There will be no anonymous “guest” accounts on any system classified as sensitive.

5. Accounts on all systems will use non-shared, unique passwords. In the instances when systems classified as sensitive must use a shared account in order to do business, strong mitigating controls must be documented and practiced.

6. Physical and logical access to any system will be granted based on least privilege. When establishing accounts, standard security principles of “least privilege” to perform a function must always be used, where administratively feasible.

7. Access security designs for all systems will be group or role based and privileges assigned to groups or roles will be based on least privilege.

8.Access privileges granted to each individual user will adhere to the principles of separation of duties. Technical or administrative users, such as programmers, System Administrators, Data Base Administrators, security administrators of systems and applications must have an additional, separate end-user account to access the system as an end-user to conduct their personal business.

10. **No passwords for any system may be stored or transmitted in clear text.**

Policy 1312 continued.. IV. Responsibilities

Vice presidents, deans, department heads and their staffs are responsible for the security, confidentiality, availability and integrity of data and systems to the extent that they have access and or access control.

This policy also places responsibility on department heads and directors to encourage appropriate computer use as specified in Responsible Use of Computing Policy, ensure compliance with information technology policies and standards by people and services under their control, **and implement and monitor additional procedures as necessary to provide appropriate security of information resources within their area of responsibility.**

Departments and administrative offices **shall develop, manage and review local operating policies and procedures to create the proper security practices for the logical and physical security of information resources.**

Policy 1312 continued.. Compliance

System owners must have documented procedures for access control and must be able to produce the documented procedures when required for auditing purposes. Evidence of account approval, termination, and disabling must be available when required for auditing purposes.

Failure to honor the requirements set forth in this policy may result in disciplinary or administrative action.