DTM and GL Computing Policy

This section details the usage policies and procedures for computing resources at the Department of Terrestrial Magnetism and Geophysical Laboratory located on the BBR campus

DTM and GL are responsible for assuring the integrity of its computer systems. Ultimately, however, the integrity of shared computing resources depends on responsible behavior on the part of the users of these systems. The purpose of this policy is to ensure that all computing and network users understand their responsibilities to safeguard the access privileges granted to them.

Every user of the BBR campus's computer/information systems is expected to know this policy and follow it in conjunction with other applicable Department policies.

General Use

DTM and GL computer systems are provided to assist the researchers and staff in the pursuit of education and research. Computing resources are intended to be used to carry out the legitimate business of the departments, although some incidental personal use is permitted. The use of the facilities for commercial purposes is prohibited.

Employees are responsible for using these facilities in an effective, ethical and lawful manner.

Access Policy

Anyone given access to the system is accountable for its use. It is the user's responsibility to protect the integrity of accessible systems and preserve the confidentiality of accessible information as appropriate. In particular users shall not share with others account passwords, access codes or other authorization that have been assigned to them. Passwords should be protected and not kept in plain sight or written to unprotected files or login scripts.

Unauthorized electronic access is prohibited.

User Accounts

DTM and GL provide individual computer accounts for all employees. Such accounts provide email access and access to the Internet.

For support staff, email and account access ends upon termination. Autoreply providing new contact information can be provided for a limited time.

Accounts for postdoctoral researchers will be removed two months after termination to allow time to transfer files and data to a new institution. Extensions beyond two months can be arranged.

Research staff leaving before retirement may keep their account for one year following their departure.

Retired Research staff may keep their account indefinitely. However, if there is no usage for a period of one year their account will be removed.

Accounts are provided to non-employees in certain circumstances. Visiting investigators from other institutions can be provided with user accounts. The Department employee who requests access for Visiting Investigators is responsible for requesting termination of their account when the collaboration ends.

Network Use

Each computer connected to the network requires an IP address. IP addresses must be allocated by the Computer Manager and while allocated cannot be used for other computer systems. Computers and mobil devices needing access to internal network resources must be registered by the Computer Systems Manager before they can be connected to the network.

Some computer systems connected to the BBR network may be in the administrative control of individual users. All network services provided by these and other computers on the network must be authorized by the Department's IT Manager. A network service is any software that accepts communication with another computer on the BBR network or the Internet. Examples of such services include, but are not limited to, telnet servers, ssh servers, ftp servers, http servers, database servers, email servers and file sharing services. The network is routinely scanned to detect unauthorized servers.

Email Use

Email access is provided for legitimate work purposes. Some incidental personal use is allowed. Other than when specifically arranged, email accounts are provided for access by a single individual and may not be shared.

Users shall not use email for inappropriate or unauthorized uses. Some examples of inappropriate use are sending threatening, discriminating, libelous or harassing emails to individuals or organizations; sending chain mail or spam messages; sending email that attempts to hide the sender or represents the sender as someone else; engaging in other illegal conduct or conduct prohibited by DTM policies.

To protect the integrity of the computer system, all users must have functioning up to date anti-virus protection and should use care when opening email attachments.

Internet Use

Internet access is provided for all users. Internet access is provided for legitimate work purposes. Some incidental personal use is allowed.

DTM and GL limit use of the Internet to specific Internet protocols by use of a firewall and by policy.

Users are allowed to publish personal web pages. Such personal pages must not contain any content that is threatening, discriminating, political, libelous, harassing, commercial or pornographic, or prohibited by law or by Department policy. DTM and GL retain the right to remove personal web pages at its discretion and without notice.

The intended use of Internet access is research and the transfer of scientific data. Any use of the Internet which interferes with legitimate use or the integrity of any other computer system, or is prohibited by law or any Department policy is prohibited. Examples of prohibited activity include downloading, providing or storing material in violation of copyright, software license agreements, patent protections and authorizations; disruption or monitoring of electronic transmissions; attempting unauthorized access to computer systems; port scanning; commercial activity.

Privacy Policy

Users have a right to a reasonable expectation of privacy. However system failures or design faults may compromise this privacy.

Authorized Department personnel, such as the IT Manager, have access to all data, files, messages and software stored on BBR systems. Privileged access is only made for legitimate work reasons.

Department IT Managers may routinely examine network transmission patterns, such as source/destination, packet type and size and employ pattern matching algorithms to detect security

intrusions, virus activity, software misconfiguration and policy violations. To verify the integrity of the computer system some routine logging of access data does occur, such as the origin of remote account logins, web server access logs, ftp server access logs and the sender and recipient (but not subject or content) of email messages.

While DTM and GL will not, as a routine matter, review the substantive content of electronic transmissions or stored data, it retains the right to do so when required for legitimate reasons. Such legitimate reasons include, but are not limited to, responding to lawful subpoenas or court orders, investigating misconduct and compliance with Department polices and locating electronic messages, data or other records.

Policy Enforcement

DTM and GL regard any violation of this policy as a serious offense. Violators of this policy are subject to disciplinary action up to and including termination as well as prosecution under the terms of applicable laws.