Department of Earth, Environmental, and Planetary Sciences
Computer Use Policy

January 2024

Introduction

This Computer Use Policy outlines the minimum security requirements and guidelines for computer use within the Department of Earth, Environment, and Planetary Sciences (EEPS). It is essential to maintain a secure computing environment to protect the confidentiality, integrity, and availability of the department's information systems and data.

Scope

This policy is applicable to all members of the faculty, staff, students, and any other individuals who are granted access to the department's computer resources. The scope of this policy primarily outlines the minimum security requirements set forth by the department. However, it is important to note that the university maintains other comprehensive policies (https://it.wustl.edu/policies).

Security Requirements

Antivirus Software

All users are required to install and regularly update antivirus software on their computer systems. Antivirus software must be capable of detecting, removing, and protecting against viruses, malware, and other malicious software. Users are responsible for ensuring that their antivirus software is active and up to date at all times.

Security Patching

Users must promptly apply security patches and updates to their operating systems, software applications, and other relevant components. Regularly updating software is critical to protect against known vulnerabilities. Users are expected to configure their systems to automatically download and install security patches whenever possible. In cases where automatic updates are not available, users must manually apply patches within a reasonable timeframe.

Operating System Security

Users must ensure that their operating systems are supported and receive security patches from the respective vendor. It is essential to use an operating system that is regularly patched to address security vulnerabilities. Unsupported or outdated operating systems pose a significant risk to the department's computing environment.

User Responsibilities

Usage and Maintenance

Users are responsible for proper usage and maintenance of their systems. In addition to security requirements outlined in this policy, users should ensure their system configuration and content are backed up and that they keep their system physically secure.

Security Awareness and Training

Users must stay informed about best practices for computer security and are encouraged to participate in any security awareness or training programs provided by the university or department. Users should familiarize themselves with common security threats, phishing techniques, and social engineering attacks to minimize the risk of compromise.

User Account and Password Management

Users are responsible for maintaining the confidentiality of their user accounts and passwords. Users must not share their credentials with others or use easily guessable passwords. Strong passwords, consisting of a combination of upper and lowercase letters, numbers, and special characters, are recommended. Users should promptly report any suspected or unauthorized use of their accounts to the appropriate IT support personnel.

Reporting Security Incidents

Users must promptly report any suspected security incidents, including malware infections, unauthorized access attempts, or other suspicious activities, to the IT support team. Prompt reporting helps in timely mitigation and investigation of potential security breaches.

Consequences of Non-Compliance

Failure to comply with this policy may result in the suspension or revocation of computer access privileges.

Policy Review

This Computer Use Policy will be reviewed annually and is available on the EEPS website. Any changes to the policy will be communicated to users within a reasonable timeframe.

By using the computer resources provided by the EEPS, users agree to abide by the terms and conditions outlined in this policy.

For additional information related to computing resources provided by the department, see https://sites.wustl.edu/epscomputing/.