Acceptable Use Policy Sample

Policy Brief and Purpose

This policy is meant to set the expectations on the acceptable use of any devices used to access organization data.

Scope

All organizational members, including employees, contractors and guests are expected and required to use all organizational information and communication technologies (ICT) including devices and network in a legal, ethical, secure, responsible and respectful manner.

Policy Elements

1) To use ICT legally and ethically, users must:
Limit any download, copy or distribution of materials such as publications, software, music or movies to the terms of the applicable license agreement copyright law.

Maintain confidentiality and privacy of the information to which they have access and view, collect or use only authorized information

2) To use ICT securely users must:
Protect identities and information in accounts by selecting secure passwords, preventing others from viewing or obtaining passwords, logging out when accounts are not in use and ensuring important information is backed up. Organizational members are encouraged to use multi-factor authentication (MFA) whenever and wherever possible for organizational and personal accounts.

Secure ICT infrastructure and data by ensuring the latest software security patches are installed, and protecting equipment from malicious software.

Safeguard information confidentiality by using secure access methods such as the organization's virtual private network (VPN) tool. When communicating confidential information electronically choose appropriate communications methods depending on information value, use and sensitivity. Many electronic methods, such as email, are inherently insecure and may be inappropriate for transmitting confidential data.

Ensure sensitive data is encrypted at rest and in transit. Ensure devices have encryption turned on.

3) To use ICT responsibly , users must:

Be accountable for all activity in personal or sponsored accounts, using the accounts and information available through the accounts only for the purposes for which they were intended. Personal activities such as, but not limited to viewing pornographic material is strictly prohibited and must not take place on organizational-owned technology.

This policy recognizes that certain activities which might otherwise be prohibited may be authorized for research or other legitimate purposes. However, it is the responsibility of the individual user to obtain pre-authorization prior to and during such periods of required use, limited to such authorized purposes and that proper controls and safeguards are in place to mitigate risk.

Exercise good ICT stewardship and care by not endangering ICT infrastructure and by using resources efficiently and effectively. Install only authorized software from trusted sources to prevent malware infections. Store data in accordance with data management standards of the organization and delete outdated information in accordance with retention schedules.

4) To use ICT respectfully users must:

Be professional and courteous in all organizational electronic communication such as voicemail, email, texting, and tweeting.

The organization may monitor its information and communication technologies at any time in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

Consequences

Violation of this policy could result in removal of some or all IT access and could result in disciplinary actions up to termination of employment.