Appropriate Use of ~~Computing~~University Technology Resources

Authority:

The Vice-President (Administration, Finance and Advancement) through the Chief Information Officer

Purpose

To outline the appropriate use of the University's ~~Computing~~Technology Resources by setting out rights and responsibilities and to establish a framework for consistency in campus practices and processes.

The University's ~~Computing~~Technology Resources are made available to faculty, staff, students, retirees, alumni, and Guests for the purpose of advancing the academic goals of: learning, teaching, research, and community outreach, for assisting in administrative operations which support these goals, and for assisting with alumni outreach.

Scope

All users of University ~~Computing~~Technology Resources, including, but not limited to, faculty, staff, students, retirees, alumni, and Guests. This policy also applies to Separately Incorporated Entities of Memorial University. It covers all uses of University ~~Computing~~Technology Resources, regardless of where they are located or where they are accessed (on campus or off campus).

Definitions

Account ~~——~~ — A ~~method~~set of ~~establishing~~credentials, such as a ~~User's identity~~username and ~~providing the authorization for a user~~password, used to ~~utilize~~access University ~~Computing~~Technology Resources. Accounts are provisioned with Least Privilege by default. Some accounts will have Elevated Privileges which are only to be used for approved purposes.

Authorized User — An individual permitted by a responsible Unit or University employee to make use of University ~~Computing~~Technology Resources. Authorized Users include faculty, staff, students, contractors, sub-contractors, consultants, retirees, alumni, and Guests who have an association with the University that grants them access to University ~~Computing~~Technology Resources.

~~**Electronic Communications** — Any electronic method used to communicate or transfer text, images, sounds, signals, or data, including electronic mail, instant messaging, websites, video recordings, voicemail, facsimiles, pagers, and telephones.~~

Elevated Privileges - Elevated privileges are special permissions granted to an Account.

Cloud — Internet-based computing provided by a third party for computer processing resources and/or data storage.

Computing Resource(s) — All devices (including, but not limited to, desktops, laptops, tablets, phones, USB keys, hard drives) which are used to access, process, or store University Electronic Data. Computing resources are those used for University business and may be: single- or multi-user; individually assigned or shared; stand-alone or networked; stationary or mobile.

Guest — An individual that is neither faculty, staff, nor student, who has permission from a responsible Unit or employee to access a University ~~Computing~~Technology Resource.

~~**Malicious Software** — Software programs that damage or perform other unwanted actions on a computer system. Includes viruses, worms, trojan horses, and spyware.~~

Least Privilege — The principle that each Unit and Authorized User be granted the minimum level of access consistent with the performance of authorized duties to protect University data.

Sensitive Electronic Data — Electronic data that has been designated as private or confidential by law or by the University. Sensitive Electronic Data includes, but is not limited to, data protected by the *Privacy* policy and the *Access to Information and Protection of Privacy Act*, 2015, SNL 2015, CA-1.2 (ATIPPA), including employment, health, academic and financial records, unpublished research data, third-party business data and all internal or business use only data. To the extent there is any uncertainty as to whether any data constitutes Sensitive Electronic Data, the data in question shall be treated as such until a determination is made by the University or proper legal authority.

~~**Shared Service** — A University Computing Resource available to all Authorized Users.~~

~~**Titled Account** — An account which is created to identify a particular role within the University's operation. A titled account does not identify an individual, nor is it owned by an individual.~~

Shared Mailbox — A shared mailbox is a mailbox that multiple users can access to send and receive email messages. A shared mailbox is used when you want to collaborate with others using a common email address (e.g. help@mun.ca) and/or when the user(s) accessing a mailbox changes periodically (e.g. dean@mun.ca).

Unit Head — For the purposes of this policy, unit head is the term used to mean Deans, Department Heads, Division Heads, Heads of Schools, Directors, Executive Directors,

University Librarian, University Registrar and other senior administrators at a comparable level; Associate Vice-Presidents and Vice-Presidents, as applicable.

University Electronic Data — Includes all data that belongs to or is used by the ~~circumstances~~University that is processed, stored, transmitted and/or copied to or from University Technology Resources. University Electronic Data may be considered Sensitive Electronic Data depending upon the data type.

University — Memorial University of Newfoundland.

University Funds — Funds administered by the University including but not limited to operating funds, research grant funds, PDTER funds and trust funds.

University Owned — All University Technology Resources and Computing Resources that are either owned or funded (in whole or in part) by the University or by funds administered by the University.

University Privacy Officer — The position with overall management responsibility for privacy policy and procedures at the University. *This is a functional description, not a position title*. The University Privacy Officer is appointed by the President of the University. Unless otherwise indicated, the University Privacy Officer is the Information Access and Privacy Advisor.

University Technology Resources — Computing Resources, networks, data storage, software applications, Cloud solutions, e-mail addresses, websites, domain names and identities that are either owned or funded (in whole or in part) by the University or by funds administered by the University.

Policy

1.0 General

Authorized Users of any University ~~Computing~~Technology Resources have a responsibility to use them in a way that is lawful, is in compliance with University policy, and is consistent with the purposes for which they were intended.

Unit Heads or delegates are responsible for ensuring compliance with this policy and its related standards and procedures. The University reserves the right to establish technical and security standards (hardware and software) as appropriate. All Authorized Users will be required to follow these standards.

The University cannot undertake to shelter users from offensive material or ~~behaviour~~behavior which they may encounter as a result of use of University Technology Resources.

2.0 Access

~~No person shall~~Authorized Users will be granted access to University ~~Computing~~Technology Resources with the principle of Least Privilege applied.

Logging in to a computer with Elevated Account Privileges poses an increased level of security risk. Elevated Account Privileges are only to be used to elevate access to do the action that requires such access (e.g. install approved software) and then immediately return to the Authorized User's individual Account.

An Authorized User assumes all risk and responsibility for potential security issues that may arise through improper use of Elevated Account Privileges.

Elevated Account Privileges assigned to an individual are not to be used to:

- create other ~~than those which they are properly authorized to access.~~

  ~~2.1~~local accounts with elevated privileges, elevate privileges for other existing accounts, or elevate an individual's own Account.
- modify group policy, system registry, or any core system configuration files/settings.
- wipe/remove/change or disable any accounts configured on University Technology Resources that OCIO has added.
- format or reinstall operating systems on University Technology Resources.

Elevated Account Privileges granted will be reviewed regularly to determine whether they are still required and continue to be used appropriately.

If Elevated Account Privileges are used for any action outside of the intended purpose, the Elevated Account Privileges will be removed, and the system will be restored to its original configuration.

The Authorized User's individual Account is to be used, where required, which is an account of least privilege by default.

2.2 Accounts and Identities

The University reserves the right to determine the structure and type of usernames, passwords and other identifying authorization mechanisms used to access University ~~Computing~~Technology Resources.

2.3 Personal Account Responsibility

-Accounts which allow users to access the University's ~~Computing~~Technology Resources are provided to individuals (Authorized Users) for their exclusive use. Authorized Users are prohibited from sharing such Accounts with others. The Authorized User is at all times responsible for the use of their Account.

2.~~3 Titled Accounts~~4 Shared Mailbox

All information communicated to a ~~Titled Account~~Shared Mailbox will be owned by the

University. Use and sharing of information in a ~~Titled Account~~Shared Mailbox will be managed by the Unit Head or delegate.

2.5 Access by non-account holder

Internal - Under certain circumstances, the failure to permit inspection and/or disclosure of an account could significantly impede the legitimate operations of the University, and it may be either inappropriate, not possible (e.g., In instances where an Authorized User has died), or not feasible to obtain prior approval of the Account holder. The University may access and use information contained in the Authorized User's Account where the Unit Head determines that it is necessary, in accordance with the Procedure for Requesting Access by Non-Account Holder.

External - When an Authorized User is deceased or is unable to access their account, the University may release information contained in the Authorized User's account upon application by their trustee, executor or administrator to the Unit Head of the unit in which the Authorized User last worked, in accordance with Procedure for Requesting Access by Non-Account Holder.

Requests will be compliant with all federal and provincial legislation and subject to the relevant provisions of any University Collective Agreement. The privacy of all personal information not pertinent to the issue giving rise to the request for access will be protected to such an extent as reasonably possible.

3.0 Usage

The University provides University ~~Computing~~Technology Resources ~~as a shared service to all~~to faculty, staff, students, retirees, alumni and Guests where appropriate.

3.1 Impact on Other Users or the University

The University reserves the right to limit the level of an Authorized User's resource usage where such use, in the opinion of the University, negatively impacts other users or the University ~~Computing~~Technology Resources.

3.2 ~~Personal~~ Use

~~Personal use~~ **of University** ~~Computing~~**Technology Resources** ~~and services~~

Use of University Technology Resources are provided to achieve the University's mission. Unless explicitly stated, personal use is only permitted ~~provided such use~~within reason, and where it does not ~~compromise~~impact the performance of an employee's duties, compromise the security and/or operation of the University, cause the University to incur costs, or damage the University's reputation ~~or involve activities that are inconsistent with the University's mission, except where otherwise authorized under applicable collective agreements~~.

3.3 Commercial Use

University ~~Computing~~Technology Resources shall not be used for commercial purposes or for the benefit of non-University organizations unless these purposes are consistent with University policies and procedures or authorized under applicable collective agreements or duly authorized contracts.

3.4 Campaigning and Lobbying
The University's ~~Computing~~Technology Resources shall not be used for political campaigning or similar purposes.

4.0 Legal Use
All use of University ~~Computing~~Technology Resources shall be in compliance with all federal, provincial, and privacy laws, and all applicable University policies. Illegal use includes but is not limited to violations of copyright, dissemination or storage of material which is in violation of law such as pornography, hate literature, harassment, defamation and discrimination, threats, criminal activities, and the knowing use of viruses or malicious software.

5.0 Memorial University's Identity
No employee may use University ~~Computing~~Technology Resources or identities to commit the University to financial or legal obligations unless existing formal policies or procedures have been properly followed.

~~A disclaimer, as found in the Electronic Communications Disclaimer in this Policy, will be automatically appended to outgoing e-mail.~~**6.0 Protective Measures**
The University has established ~~technical~~policies and standards for University ~~Computing~~Technology Resources which all users must follow. These ~~standards~~ include ~~protective software (e.g. antivirus, encryption) and will prevent~~ , but are not limited to, the Electronic Data Security Standards, Data Removal Policy, the ~~use of non-standard equipment in conjunction with University Computing Resources.~~
IT Investment and Governance Policy, the Privacy Policy and Protective Disclosure Policy.

6.1 Inspection, use and disclosure
The University may permit inspection, use and/or disclosure of data or information~~, including Electronic Communications,~~ under the following conditions, subject to relevant provisions of any University Collective Agreement:

1. The University is required by federal or provincial law, subpoena, or court order to divulge such data or information, or information pertaining to the account itself;
2. The University reasonably believes that a law or institutional policy has been violated;
3. Failure to permit inspection, use and/or disclosure would significantly impede the legitimate operations of the University, and it is either inappropriate or not feasible to obtain prior approval of the Account holder.

In such cases, approval of the Vice-President (Administration, Finance and Advancement) and~~,~~ the Vice-President (Grenfell Campus) or the Vice-President (Marine Institute) as appropriate, or delegate, in consultation with the University Privacy Officer must be obtained in advance, and the privacy of all personal information not pertinent to the issue giving rise to the access will be protected to such an extent as reasonably possible.

6.2 Enforcement, violations, and discipline

A violation of appropriate use of University ~~Computing~~Technology Resources refers to any matter in which University ~~Computing~~ Technology Resources are used for purposes that violate this or any University policy, federal or provincial legislation, or relevant provisions of Collective Agreements. Any person who becomes aware of a possible violation of appropriate use may report it, in accordance with the ~~Procedure for Reporting Suspected Violations of Appropriate Use of Computing Resources.~~Procedure for Reporting Suspected Violations of Appropriate Use of Technology Resources. If there is a possibility that Sensitive Electronic Data may have been disclosed, altered, or destroyed by an unauthorized individual, a security incident will be reported in accordance with the ~~Procedure for Reporting Suspected Security Incidents~~Procedure for Reporting Suspected Security Incidents.

Any breach of this policy may result in disciplinary action. Violators of this policy may be denied access to University ~~Computing~~Technology Resources and may also be subject to penalties under University policies, Collective Agreements, provincial and federal law. The University reserves the right to take the appropriate steps to temporarily suspend an Authorized User's account on the recommendation of the CIO, Vice-President (Administration, Finance and Advancement), the Vice-President (Grenfell campus) or the Vice-President (Marine Institute) as appropriate, or delegate, and in consultation with the General Counsel, where appropriate.

6.3 ~~Exemptions~~Deviations

Requests for ~~exemption~~deviation from this policy ~~should~~are to be addressed to the CIO, through the Vice-President (Administration, Finance and Advancement). - Requests should detail the section of the policy for which the exemption is being sought, and propose compensating controls if any. Requests for exemption must be endorsed by the Unit Head.

For inquiries related to this policy:

Office of the Chief Information Officer, (709) 864-4595

Sponsor: Vice-President (Administration, Finance and Advancement)

Category: Operations