Draft Policy for Consultation
Electronic Data Security Policy
Feedback can be sent to Policy@Mun.ca

Electronic Data Security

Authority:

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

Purpose

To outline the responsibilities of all Authorized Users in supporting and upholding the security of ~~Sensitive~~University Electronic Data, regardless of the Authorized Users' affiliation or relation with the University, and irrespective of where the data is accessed, utilized, or stored. This Policy is not exhaustive of all Authorized User responsibilities, but is intended to outline specific responsibilities that each Authorized User acknowledges and agrees to follow when using ~~Sensitive~~University Electronic Data ~~provided to and/or by the University~~. This Policy conforms with the University's *Privacy* Policy and the *Access to Information and Protection of Privacy Act (ATIPPA) of Newfoundland and Labrador*.

Scope

All ~~Sensitive~~University Electronic Data in the custody and/or control of the University; and all Units and Authorized Users of the data.

Definitions

Authorized User — An individual permitted by a responsible Unit or University employee to make use of University 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.

Computing Resource(s) — All devices (including, but not limited to, ~~personal computers~~desktops, laptops, tablets, phones, USB keys, ~~PDAs, and Smart phones~~hard drives) which are used to access, process, or store University ~~data~~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.

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

Custody and/or Control — Having direct possession of, or authority over another's direct possession of~~,~~ Sensitive Electronic Data.

~~**Electronic Data** — Includes all data that belongs to or is used by the University that is processed, stored, transmitted and/or copied to or from computing resources.~~

IT-Classified Staff — Employed by the various technology service providers for Memorial University campuses and select Units with Director/Head and Human Resources approval to provide local IT Support.

Encryption — The conversion of readily comprehended plaintext into encoded *ciphertext* such that unauthorized users cannot discern its original meaning.

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

~~**Peer-to-peer (P2P) file sharing** — Any of a number of programs or protocols used to distribute files anonymously. Examples include Ares, Bearshare, eMule, Kazaa, and Limewire.~~

Multi Factor Authentication (MFA) — Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA requires one or more additional verification factors beyond username/password, which decreases the likelihood of a successful cyberattack. MFA may include, for example, an authentication app on your phone to verify identity.

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.

Unit — Academic or administrative unit, as defined in the University Calendar, or any board or other body appointed or elected to carry out University business.

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 University that is processed, stored, transmitted and/or copied to or from ~~Technology~~ Computing 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 ~~Computing~~Technology Resources purchased by Memorial University through University Funds.

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.

Virtual Private Network (VPN) — A Virtual Private Network (VPN) is an encrypted private connection over the internet from a device to a network.

Policy

All Authorized Users have a responsibility to protect ~~Sensitive~~University Electronic Data and University Technology Resources from unauthorized disclosure, modification, and destruction. All Authorized Users and Units shall adhere to this Policy, the related standards and the related procedures in the interest of protecting ~~said data~~University Electronic Data.

Unit Heads are responsible for ensuring compliance with this policy and its related standards and procedures. IT-Classified staff are responsible for initial secure setup and ongoing management of University-Owned Computing Resources and following technical guidelines per the Tangible Asset Policy and Data Removal Policy.

Standards for approved security software and configurations shall be set by the Office of the Chief Information ~~Technology Services,~~Officer (OCIO) in consultation with the various campuses and periodically revised in response to best practices and emerging technologies.

Emerging security threats, vulnerabilities and incidents may require immediate response. ~~Emerging technologies may present unique and novel challenges.~~ When such circumstances arise, the ~~Vice-President (Administration and Finance), Vice-President (Grenfell Campus) or Vice-President (Marine Institute),~~OCIO, as appropriate, has the authority to revoke an existing standard and/or introduce a new one.

Provincial legislation and the *Privacy* policy define personal information broadly. It is assumed that, except in extraordinary circumstances, all ~~computing resources~~Computing Resources contain some degree of Sensitive Electronic Data (which includes personal information) requiring protection under this policy. Sensitive Electronic Data shall not be used nor disclosed except as provided by University policy, legislation, or court order or where access to the data is needed by officers of the University to conduct the business of the University.

Account Access

~~Sensitive data~~University Electronic Data access shall be limited in accordance with the principle of ~~least privilege~~Least Privilege. Authorized Users needing access to a subset of data shall not be granted access to all records for instance, nor shall they be provided write access if creating or modifying records is beyond the scope of their authorized duties. Application of the principle of ~~least privilege~~Least Privilege can greatly limit damage resulting from user error and unauthorized access. Principle of Least Privilege is to be employed ~~unless Authorized Users complete and granted approval using the Elevated Account Privileges for Desktop Administration Request~~wherever possible.

Change of Authorized User Status

When an Authorized User who has been granted access changes responsibilities or leaves employment, their access rights shall be re-evaluated by the Unit(s) involved and any access to data outside of the scope of the new position or status shall be revoked ~~as soon as possible but not later than five working days.~~ per the Procedure for Managing University Records of Exiting Employees and the Process for Exiting Employees.

Operating Systems

All Computing Resources purchased with University Funds shall run a currently supported operating system ~~for which security patches are actively released and applied~~outlined in the Electronic Data Security Standards.

Software Applications

All Computing Resources purchased with University Funds shall run currently supported software applications outlined in the Electronic Data Security Standards.

Cloud Solutions

As per the IT Investment and Governance policy, Cloud services and storage that meet any of the current criteria set by the IT Governance and Collaboration Council (available here) shall be assessed through the IT Governance and Collaboration Framework.

Anti-virus

All desktops and laptops purchased with University funds shall run approved anti-virus software~~.~~ per the Electronic Data Security Standards. *(Updated below)*

Encryption

All ~~laptops~~mobile or off-site Computing Resources purchased with University funds ~~and all laptops used to transport or store Sensitive Electronic Data~~ must have approved encryption software installed~~.~~ per the Electronic Data Security Standards. *(Updated below)* Other ~~devices (including, but not limited to, USB keys) that are used to transport or store Sensitive Electronic~~

~~Data must also employ~~ approved encryption ~~software.~~methods are also covered under the Electronic Data Security Standards. *(Updated below)*

Sensitive Electronic Data

~~**Peer-to-Peer File Sharing**~~

~~Peer-to-peer file sharing software shall not be installed on or operated from computers containing or accessing Sensitive~~Sensitive University Electronic Data is to be ~~communicated~~shared using ~~referencing~~ secure file sharing solutions ~~where possible. If transmitting Sensitive Electronic Data. Sensitive Electronic Data transmitted via email to off-campus recipients, or via or instant messaging to any recipient, shall therefore be encrypted using approved is required, encryption software.~~

~~For internal emailing of Sensitive Electronic Data, Authorized Users must assess~~is recommended ~~where possible.~~ See the ~~data~~Electronic Data Security Standards *(Updated below)* for ~~sensitivity and necessity for encryption. If the necessity of encryption is unclear, clarity should be sought from the associated unit head or from the University's Information Access and Privacy Protection office. When any doubt exists, approved encryption methods shall be used.~~more information.

~~When encryption methods are used, decryption passwords must be exchanged separate from the data itself, preferably via a different means (e.g., face-to-face or over the phone).~~

~~**Smartphones**~~

~~BlackBerry and other smartphone-like devices~~**Information and Training:**

The OCIO shall provide security awareness information and/or training to members of the university community as it pertains to this policy.

~~Email and messaging are among the many potential vectors for a cyberattack. Bad actors will impersonate colleagues or services, and attempt to entice action to install malware, obtain financial information or credentials. Authorized Users must be made aware of these risks and protect University Electronic Data.~~

Network Access

University-owned and managed Computing Resources are to connect to the Memorial wired or @Memorial wireless services where possible, requiring Memorial credentials. ~~and not to~~ Guest, Residence or other network services should not be used by University-owned and managed Computing Resources while on campus unless otherwise approved for a specific purpose. Eduroam is available for v~~While v~~isiting institutions which are members of the Canadian Access Federation (CAF)~~, such as Memorial University, Eduroam is also an available and appropriate service~~. The OCIO has the right, under this policy, to refuse to connect equipment that does not meet the Standards outlined in the Policy or which may negatively affect the campus network.

University-owned Computing Resources connecting to Memorial's network require the use of the approved VPN service for remote work arrangements or any off-site use of Computing Resources, per the Electronic Data Security Standards. *(Updated below)* Use of Multi-factor

Authentication (MFA) is required for some services and otherwise recommended where available.

Passwords

Computing Resources or University Technology Resources which store University Electronic Data must be password protected with a strong password meeting Memorial University standards. This is part of the normal setup process when IT-Classified Staff set up Computing Resources, per the Electronic Data Security Standards. *(Updated below)*

University-provided solutions

University Technology Resources are to be used to conduct university business. Please refer to the Electronic Data Security Standards *(Updated below)* for university-provided solutions. It is recommended to access your files remotely using University Technology Resources and not carry or transfer files to non-University owned systems. For tools outside the defined Standards, please consult with IT Classified Staff.

Mobile/cellular devices

Memorial issued or approved mobile/cellular devices must employ approved security configurations ~~and/or software.~~, per the Electronic Data Security Standards. *(Updated below)* Encryption, ~~versus~~in addition to PIN or password protection, is required ~~in any instance where the latter does not lead to factory reset of the device after a finite number of failed password attempts~~.

Backups and Resiliency

Data that is critical to the mission of the University ~~should~~shall be backed up ~~to prevent~~or resiliently stored to reduce the risk of accidental loss. Backup copies of ~~Sensitive~~University Electronic Data shall be protected to the same standards set out in this policy. For guidance regarding backups, consult your campus IT Service Desk or IT-Classified Staff.

Physical Security

Appropriate controls must be employed to protect physical access or proximity to Computing Resources and University Technology Resources, commensurate with the acceptable risk considering data type and physical exposure of the environment.

Disposal

~~Sensitive~~University Electronic Data must be securely deleted from reassigned and/or surplus ~~computing resources~~Computing Resources in accordance with ~~the principle of least privilege and~~ the *Data Removal* Policy. *(Updated below)*

Use of Non-University-owned Equipment

~~Sensitive~~University Electronic Data ~~preferably should~~is not to be stored on non-University-owned equipment. ~~If such data must be stored on non-University-owned equipment,~~ Please refer to the ~~Authorized User is responsible~~Electronic Data Security Standards *(Updated below)* for ~~Information Technology Services shall provide information and training to members of the~~ university ~~community as it pertains to this policy.~~ provided file storage solutions.

Deviations:
Requests for ~~exemption should~~deviation are to be submitted ~~in writing to the head of the campus information technology service.~~using the Electronic Data Security Deviation Request Form. *(To be added)* This form is to be submitted by IT Classified Staff on behalf of~~r~~ requestors. Requests ~~should~~are to detail which subsection of the policy ~~for~~ which the ~~exemption~~deviation is being sought, and proposed compensating controls outlined, if any. Requests for ~~exemption~~deviation must be endorsed by the director/head of the requestor's Unit.

Non-compliance:
Units and Authorized Users who act in good faith and execute their responsibilities with a reasonable standard of care shall not be subject to disciplinary action in the event of a data security breach. Breaches arising from non-compliance with this policy may result in disciplinary action up to and including dismissal or expulsion.

Procedures and Standards

- ~~Procedure for Laptop Disk Encryption~~
- ~~Procedure for Managing a Privacy Breach~~
- ~~Procedure for Reporting Suspected Security Incidents~~
- Electronic Data Security Standards *(Updated below)*
- Procedure for Managing a Privacy Breach
- Procedure for Reporting Suspected Security Incidents
- IT Onboarding for New Employees
- Procedure for Managing University Records of Exiting Employees
- Process for Exiting Employees
- Security and Information Protection Assessments
- Elevated Account Privileges for Desktop Administration Request
- Certificate Signing Request (CSR) Certificate Request
- IT Procurement Order Process

For inquiries related to this policy:

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

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

Category: Operations