INFORMATION TECHNOLOGY POLICY

ALMA MATER SOCIETY

OF QUEEN'S UNIVERSITY

Responsibility	President
Approved by	Board of Directors
Date initially approved	April 19, 2012
Date last revised	March 27, 2018

QUEEN'S UNIVERSITY
AMS
STUDENT GOVERNMENT

Table of Contents

Purpose 1
Terminology and definitions 1
Statement 2
Scope 2
Roles and Responsibilities 2
Policy 3
Access 3
Acceptable use 3
Administration 5
Websites 5
Security 6
General 6
Personal devices 7
Monitoring 8

Purpose

The purpose of this policy is to provide users with a clear and concise set of directions regarding the proper use of information technology (IT) at the Alma Mater Society of Queen's University Incorporated (AMS).

Terminology and definitions

“AMS Office 365” means the Microsoft Office 365 account that is attached to an AMS email account.

“AMS network file server” means the central location where all AMS business files are stored and accessed.

"Bitlocker" is a data protection feature that may be installed on the hard drives of computers.

“ITSC” means the information technology steering committee of the AMS.

“IT resources” means any and all hardware and software that is owned or under contract by AMS for the purpose of conducting AMS business.

“Office 365” means a set of Microsoft online tools that are available for users to work remotely on AMS business that is saved to the AMS server.

“Password” means a combination of characters that are chosen by the user and only known by the user.

“Password protected” means a document where the author has created a password to access and provide access to other people who have been provided the password for the document.

“Personal access code” means a combination of characters that are entered for access to a machine, device or software that is only known by the individual in question and/or the director of information technology.

“Personal device” means any and all computers, laptops and mobile devices that are owned by an individual who uses that device for conducting the business of the AMS.

“Term of office” means the period from May 1 to April 30 of each year.

"VPN" means a virtual private network that is made available to users for access to the AMS network file server to work remotely on AMS business.

Statement

Information technology is critical for conducting the daily business of the AMS. It is essential that all users of the system follow the policy directions outlined here to ensure uninterrupted IT services. Adherence to this policy is a condition of employment. Use of IT resources by AMS employees must not hinder the administration, access and security of information at the AMS. IT resources must be used in a responsible manner that is ethical and does not breach legal agreements.

Scope

This policy applies to all AMS executives, officers, directors, commissioners, salaried and part-time employees, volunteers, as well as permanent staff and contractors. All hardware and software that is owned by the AMS and personal devices used for conducting AMS business are within the scope of this policy.

Roles and Responsibilities

All users of information technology resources have the responsibility to comply with this policy and to bring any gaps in this policy that they become aware of to the attention of the director of information technology.

The executive (president, vice-president of operations, vice-president of university affairs) has a responsibility to follow directions in this policy, to actively promote compliance with this policy and ensure that AMS information technology resources are adequately funded.

The general manager has a responsibility to consult with the executive, the director of information technology and the information officer to provide administrative direction and to actively promote compliance with this policy.

Directors, officers and commissioners are responsible for supporting, promoting and adhering to this policy and ensuring that any and all hired employees and volunteers comply with the policy.

The director of information technology is responsible for overseeing all aspects of the management and maintenance of IT resources at the AMS including risk analysis and management. The director is responsible for maintaining this policy in collaboration with the information officer. The director is also responsible for training, administration and otherwise informing users of this and other IT governance documents, while monitoring users to ensure compliance with this policy.

The information officer has the responsibility to ensure that AMS electronic information is maintained in an organized, secure and accessible environment. The information officer also has the responsibility to maintain this policy in collaboration with the director of information technology. The information officer also will monitor users for compliance regarding this and any other policy that has an impact on the integrity of information at the AMS.

Managers are responsible for ensuring that employees are following IT policy and are using AMS information technology resources only for business purposes. Managers also have the shared responsibility with their supervisor to ensure that any contract, temporary or part-time staff are in compliance with this policy.

The Information Technology Steering Committee (ITSC) has the responsibility to conduct business as outlined in the committee terms of reference. The committee is comprised of the president, vice-president operations, vice-president university affairs, general manager, and director of information technology, information officer and controller.

The director of human resources has the responsibility ensure that all salaried employees are aware of the contract clause that confirms that employees have read, understand and will comply with this policy.

Policy

Access

Acceptable use

1. AMS IT resources shall be used exclusively for the administrative and operational purposes for which they are intended.
2. Users shall be restricted to accessing solely those IT resources for which they have received authorization, unless those resources are intended to be generally available to all AMS members and/or the broader Queen's community.

3. Authorized users shall not compromise the integrity or reliability of AMS IT resources and nor shall they access AMS IT resources in a manner that interferes with the normal operation of IT resources within the AMS and Queen's University.
4. Authorized users of AMS IT resources shall not hinder or otherwise adversely affect the ability of others to use IT resources within the AMS and Queen's University.
5. Authorized users of AMS IT resources shall not violate the rights of others and will not contravene the law.
6. Employees, volunteers, as well as ratified clubs and approved member societies are granted email accounts, which are administered by the director of information technology under the supervision of a designated member of the executive.
7. AMS email accounts are to be used for AMS business only and are not for personal use. Users of AMS email accounts shall not have any expectation of privacy regarding content of email accounts and shall not send, receive or store any personal content using an AMS email account.
8. Files attached to emails and the textual content of emails are the property of the AMS. Unapproved transfer of AMS information via email to a personal account is prohibited and will be considered a breach of the AMS confidentiality and non-disclosure agreement with its provisions for disciplinary actions.
9. AMS network file servers are to be used for AMS business only and must not be used for personal content. All files on the server are the property of the AMS. Users of AMS network file servers shall not have any expectation of privacy regarding content of files and shall not send, receive or store any personal content on the AMS network file server.
10. All files and folders must be accessed on the AMS network file server or through Office 365. Use of an external portable storage device to transfer information must be approved by the information officer and the executive. Unapproved transfer of content from the AMS network file server by any means will be considered a breach of the AMS confidentiality and non-disclosure agreement with its provisions for disciplinary actions.
11. Remote access through personal devices to AMS email accounts, document storage and collaboration are provided through the use of AMS Office 365. Remote access through personal devices to AMS network file servers may be obtained through a virtual private network (VPN).
12. On request, the director of information technology shall grant the executive, general manager and information officer access to employee AMS email accounts and files without notifying the employee for the purpose of monitoring compliance with this and other policies.
13. Downloading and installation of unauthorized software, applications or programs is prohibited. Users may request the purchase of products by submitting an IT project approval form. The decision to purchase is reserved for the ITSC with approval of the executive.

Administration

1. Maintenance of hardware, software and procurement is under the administrative duties of the director of technology.
2. Records of IT assets are to be maintained by the IT office, including schedules for replacement of hardware, the updating and licencing of software packages and names of users.
3. Development and implementation of applications must be approved by the ITSC and are to be managed by individuals appointed by the ITSC.
4. The only system administrator will be the director of information technology and selected personnel from Queen's Information Technology Services (QITS).
5. Local administrators will be the director of information technology and information technology support staff.
6. Requests for routine IT services submitted by email, phone, text or any other method will not be addressed. Users must use the AMS IT office ticketing system at https://www.queensu.ca/itrack/AMS/ams.php
7. Requests for extraordinary IT issues such as a network outage, computer failure or any other circumstances that prohibit the use of the ticketing system may be reported by calling the IT service desk.
8. Remote control support may be required at times to address issues. The IT office must contact and receive the permission of the user to assume remote control of the computer.
9. Servers will be backed up following a regular schedule that is managed by Queen's ITS. The back up schedule will ensure that the AMS server is backed up every twenty-four (24) hours by Queen's ITS.

Websites

1. Creation of new websites must be approved by the ITSC and managed by the director of information technology or designated authorized IT support staff. Users are not permitted to design and implement websites.
2. Design and structural changes to websites will be restricted to once every three years, unless the change is urgent and is approved by the ITSC.
3. Changes to websites must be submitted to the ITSC using the IT Project Approval Form (link).
4. Website content may be edited and updated by authorized users as required.
5. Addition, deletion, restructuring and/or redesign of webpages and/or sections of websites constitutes a major change and must be introduced using the prescribed form to gain approval by the ITSC.

6. In the case of a website that has been in operation for more than three years and requires major changes or there is a change in industry standards, the director of information technology will have the discretion to determine that a complete website design is required.

Security

General

1. **All salaried and permanent staff shall sign an AMS confidentiality and non-disclosure agreement.** Signed confidentiality and non-disclosure agreements will be retained in electronic and/or paper form by the general manager or their designate.
2. All executives, officers, directors, commissioners, salaried full-time and part-time employees, as well as permanent staff must take a cyber security course offered by Queen's University Information Technology Services and administered by the director of information technology. The director of information technology will ensure that all incoming executives, officers, directors, commissioners, salaried full-time and part-time employees must take the course as part of mandatory training week at the beginning of their term of office or employment contract. Permanent staff must take the course once every two (2) years or more often should new courses be available and confirm that they have taken the course with the director of information technology.
3. Users shall report suspected, known or observed IT or information security risks or exposures to the director of information technology. Failure to report shall be considered a violation of this policy.
4. All information exposures must be reported.
    a. Personal information exposures of students or AMS staff must be reported to the director of information technology who will immediately inform the executive, the general manager and the information officer; the executive will inform the following Queen's University officials, if applicable:
        i. chief information officer;
        ii. chief privacy officer.
    b. Corporate information exposures must be reported to the director of information technology who will immediately inform the executive, general manager, and information officer. Depending on the nature of the exposure and after consultation with the executive, the general manager and the information officer; the executive may report the exposure to any one of or all of the following Queen's University officials:
        i. chief information officer;
        ii. chief privacy officer.

5. Personal information of students collected by Queen's University and provided to the AMS shall be protected as prescribed by a binding agreement with Queen's University. For clarity, the requirements of the agreement include:
    a. Information must be maintained on AMS network file servers that are under the care and control of Queen's ITS and are Bitlocker encrypted.
    b. Information must be password protected.
    c. Information must not be backed up, transferred or copied onto any other media.
    d. Information must be solely in the care and control of the AMS president, who has ultimate responsibility for the security of personal information provided by Queen's University.
6. All AMS computers must be equipped with Bitlocker security technology.
7. All AMS salaried and permanent staff must use only AMS approved platforms that are administered by the director of information technology for conducting AMS business. Approved platforms may include social media (Facebook, Twitter, etc.) and productivity tools (Google docs, Dropbox, Slack, etc.). **Use of a personal account on any platform to conduct AMS business will be considered a breach of the AMS confidentiality and non-disclosure agreement with its provisions for disciplinary actions.**
8. Passwords on all accounts for all platforms are mandatory. Passwords will be administered by the director of information technology. User passwords shall be a minimum of eight (8) characters in length and users will prompted to change passwords every ninety (90) days. Passwords must contain at least three (3) of the four (4) following character types:
    a. Upper case character (e.g. A, B, C, etc.);
    b. Lower case character (e.g. a, b, c, etc.);
    c. Numeric character (e.g. 1, 2, 3, etc.);
    d. Special character (e.g. $, *,], etc.).
9. Passwords must not contain more than three (3) consecutive letters that appear in a username. For example, if a username is "itmanager", the password must not contain the letters "itm" or "man" in combination.
10. As a security precaution, passwords that are attempted more than five (5) times will be locked out for a period of thirty (30) minutes. Users must submit a password reset request at myams.org/support to obtain a new password.

Personal devices

1. Users shall acquire and maintain familiarity with all applicable AMS and Queen's Information Security Policies, Standards and Guidelines.
2. All personal devices used by AMS staff for AMS business must have a personal access code that is verified by the director of information technology.

3. All personal devices must use tools provided by the AMS to conduct all AMS business. AMS documents must not be mailed to personal email accounts or downloaded to personal devices. AMS documents and email accounts accessed on personal devices must use AMS Office 365 tools as installed and administered by the director of information technology.
4. Access to AMS network file servers on a personal device may be gained through a VPN that is installed and administered by the director of information technology.
5. All AMS information including emails and documents shall be deleted from personal devices used for AMS business at the end of the term of office. Removal of AMS accounts and deletion of documents will be verified by the director of information technology.
6. All AMS staff using personal devices for AMS business must ensure that the device has the most up-to-date operating system and security updates. The director of information technology has the authority to inspect any personal device that is suspected of being a security risk.
7. All AMS staff using a personal device for AMS business must report the loss or theft of that device to the director of information technology and to the service provider immediately. Loss of a personal or AMS owned device containing AMS business information is considered an information exposure. AMS staff will be advised that all data, including personal data, will be remotely deleted.

Monitoring

This policy must be reviewed annually by the director of information technology and the information officer.

Monitoring for compliance with this policy will be carried out by the director of information technology and designated support staff. The information officer will monitor and report any contraventions of this policy or potential issues to the director of information technology.

All AMS email accounts and files are subject to monitoring by the director of information technology, IT support staff and the information officer to ensure compliance with this policy.

Contact person	Director of information technology
Date of next review	March 2019
Related policies, procedures and guidelines	Information and Records Management Policy
Policies superseded by this policy	Information and Technology Policy (2012), amended 2016