QUEEN'S UNIVERSITY
AMS
STUDENT GOVERNMENT

INFORMATION AND TECHNOLOGY POLICY MANUAL

Information and Technology Policy

(Created by the Board of Directors as a separate policy manual on April 19, 2012. Last amended November 2016).

Table of Contents

IT Governance

IT Oversight Body

There shall be an IT Oversight Body consisting of the Executive that supervises the IT Officer, the General Manager, IT Officer, and IT Support Officer and a member of the Board that shall be responsible for IT risks, policies, and management. This oversight body will deal with these issues with the help of the Queen's Information Security Office (QISO) as required.

Risk Management

Since every IT operation inherently has risk associated with it, the IT Officer will be expected to work with the IT Support Officer to decide if a risk analysis is required before proceeding. When a new project is presented or suggested which involves the IT Office, the IT Support Officer will discuss the risks that are associated with this project. They will decide whether to proceed or not, documenting and communicating the decision. It will be the responsibility of the IT Officer and IT Support Officer to decide if it warrants further discussion with the IT Oversight Body.

Risk Registry

Risk Registry will be completed on a per project basis and include major changes to the Infrastructure that will involve the IT Oversight Committee. It is the intent of the Risk Registry to document both one-time type projects and recurring projects in order to act as both a planning and management document. Each project will include information about nature of project, individual(s) assigned, recurring nature, whether the IT Oversight Body is required and will be rated as high, medium and low risk.

Policy Management

IT Policy shall be the responsibility of the IT Officer and the Executive responsible for the IT office. New policy or revision to existing policy shall be the responsibility of the IT Oversight Body. They shall approve the changes (keeping in mind that the permanent staff member serves as memory as to why the policies were initially created and the conditions as to why they were created). These additions and changes shall than be approved by the Board of Directors, while keeping Assembly informed of the changes. Additionally, the Queen's Information Security Officer will be informed of any significant changes that are proposed in order to solicit their advice as well as keep them informed of our operations.

Acceptable Use Policy

AMS IT resources shall be used exclusively for the academic and administrative purposes for which they are intended. 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 Alma Mater Society members and/or the broader Queen's community. IT resources may not be utilized for personal commercial activities unless such activities have been authorized in writing by the AMS Executive, and have been determined not to adversely impact other users, or introduce risk to either the security of personal or confidential information or the AMS or Queen's IT infrastructure.

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, or externally. 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, or externally.

Thesecurityandprivacyofsensitiveinformationshallbeprotectedandnevercompromised. Therefore, users shall adhere, at all times, to the following practices:

- authentication credentials, such as user accounts and passwords or similar authentication credentials, shall be securely maintained in a manner such that they cannot be used by others;
- *secure passwords shall be chosen for all user accounts;*
- confidentiality shall be preserved for all AMS or university information to which users have access in the course of their employment or academic activities;
- privacy shall be preserved for all personal or confidential information relating or belonging to other individuals, to which users have access in the course of their employment or academic activities;
- necessary and appropriate precautions shall be identified and taken in order to prevent theft or unauthorized use of computers, storage devices, and information.

IT resources shall be utilized in a manner which is consistent with all applicable AMS and University policies and which does not facilitate or cause damage to the AMS or University. Users shall acquire and maintain familiarity with all applicable AMS and Queen's Information Security Policies, Standards and Guidelines. Users shall seek information and clarification from the AMS IT Office about any elements that are unclear. Users shall adhere to the terms of any contractual agreements or arrangements between the AMS and external service providers or organizations, and use such resources solely for the intended academic and/or administrative purposes.

Users shall not violate the rights of others or contravene the laws of Canada and/or the Province of Ontario in their use of IT resources. More specifically, users shall:

- respect the copyright and intellectual property rights of others, whether within the AMS, the University or elsewhere;

- respect the licensing agreements and terms for all software, and only install and use software as permitted in the license agreement for that software;
- respect the licensing agreements and terms for all electronic resources including databases, journals, books and other print, audio and video content;
- not use AMS IT resources for any activities or actions which are illegal or do not comply with Canadian or Ontario legislation;
- not use AMS IT Resources to do anything that is a violation of the rights of others, such as displaying or distributing obscene, harassing, defamatory, or discriminatory material or messages.

Users shall report suspected, known or observed IT or information security risks or exposures, thought to be of a serious nature, to the AMS IT Office. Any failure to comply with these responsibilities shall be considered a violation of this policy.

IT Management

The IT Officer shall be responsible for the communication, compliance, and enforcement of IT Policies. They shall also ensure that policies are easily available to all IT users. Furthermore, the Human Resources Officer shall ensure that all employee contracts include a clause that confirms the employees understanding and acceptance of the IT Policies and Acceptable Use Policy.

The IT Officer and Executive responsible for the IT office shall approve all contracts of IT confidentially working with the General Manager of AMS

IT Security Training

The IT Officer will have a training session, held in coordination with Human Resources, for all incoming student leaders that will cover the following topics:

1. IT Policies & Practices
    a. iTrack System and when to best email or call
    b. Moving computers and phones
    c. Downloading programs and what you can download
    d. Standardization and exceptions
    e. Web Development
    f. Business Accounts vs Personal Accounts (Google and Microsoft)
2. IT Security Training
    a. Phishing and where viruses come from
    b. Where the AMS File Server is, how it works, and when it backups
    c. Where to save IDs and Passwords
    d. Password changes

The IT Officer shall also provide awareness of certain conditions (e.g. e-mail phishing attacks, large virus infections, etc.) through use of alert e-mails or other forms of communication. These awareness efforts shall be delivered through May training week and volunteer chair and coordinator training in the fall.

Organization and Management

Change Management Controls

- Write description of change and the risk associated
- Impact of change to other systems and users
- Identify the communication strategy
- Get the right approvals of the change
- Identify testing strategy for testing the change and back out plan in case change fails
- Document the result of the change
- Deploy the change
- Complete change request with results of change deployment and close the ticket

Severity of Changes

- Severity 1 – Routine changes
- Severity 2 – More localized impact
- Severity 3 – Wide spread impact
- Severity 4 – Emergency change

Physical and Environmental Controls

The physical and environmental responsibilities of the IT Office Server & Network Architecture are the responsibility of Queen's IT Services. The minimum service provided shall ensure the physical security of the infrastructure using constant access control (whether it be locked doors, or electronic access cards, surveillance) and an alarm system that is activated during off-business hours. The location should have enough power, ventilation, and cooling capacity to ensure no damage is done to the infrastructure. The service shall also provide a form of uninterruptable power supply (UPS) which will allow enough of a period to safely shutdown the infrastructure. Finally, the location of the servers shall contain proper fire prevention and suppression systems that would cause minimal damage to the infrastructure. This responsibility is documented via a service contract between Queen's IT Services and AMS and is negotiated on an annual basis (February).

Each deployed workstation must be placed in a location that is locked when the room is unattended. If a workstation is to be deployed in a more public location, it must be physically secured with a computer lock. However, no personal and/or confidential information will exist on workstations or laptops left in public areas. For higher risk areas (e.g. IT Office, Services, Point-Of-Sale (POS) locations), they must be alarmed on off-business hours.

Spare or unused workstations and inventory shall be placed in a location that is behind locked doors when it is unattended and an armed alarm system during off-business hours. Alarm access codes will be maintained confidentially, kept in a secure location and not shared.

Software Controls

The IT Office shall be the only group authorized to install business related and needed software on workstations. Software to be installed on servers shall be managed by the Information Technology Support Officer. The following is a list of approved software that does not require additional authorization by the IT Oversight Committee. The IT Oversight Committee does not need to be involved if free software is added to this list by either the IT Officer or IT Support Officer.

- Window Operating System
- Device Drivers
- Microsoft Office Suite (e.g. Word, Excel, Outlook, etc.)
- Internet Explorer
- Firefox
- Google Chrome
- Kaseya
- Adobe Reader (for PDF viewing)
- Adobe Suite of Software (e.g. Acrobat Professional, Creative Suite, Photoshop, etc.)
- Malwarebytes (to be uninstalled after use)
- System Center Endpoint Protection (SCEP)
- 7zip
- GIMP
- Java 8 Runtime
- KeePass 2
- Various word document fonts and updates

Since certain services require specialized software, the IT Officer shall compile and keep a list of software that is regularly used by each service. All requests for new and unapproved software need to be made to the IT Office, who shall perform an assessment to determine compatibility with existing software and hardware. If they are unable to reach a conclusion independently, then they shall consult the Oversight Committee, and the Queen's Information Security team.

The IT Office shall track all licenses for all software, ensuring never to install the software when it will exceed the number of licenses that has been purchased.

Update Process

All computers & software should be set to auto-update without requiring user input whenever possible. In addition, the IT Office shall ensure that approved critical and security Operating System and software updates are maintained on a current basis and completed by the use of a monitoring and reporting tool such as Kaseya.

Hardware Controls

The IT Office will review the acquisition of new or used hardware for compatibility and support purposes. This review should be conducted before large purchases are presented to the Board of Directors for approval, such as capital expenditures.

Computer Procurement Policy

This section provides standardization guidelines regarding the purchase, refresh and decommissioning of all AMS desktops, laptops and tablet computers. The Alma Mater Society supports specific makes and models of computers. These systems shall normally be selected in consultation with the University to ensure that value in price and quality is maximized. Dell Computer hardware has been standardized by the AMS for the value and onsite hardware warranty that is offered.

The Information Technology Officer and Information Technology Support Officer shall maintain records of all computers within the AMS and when these computers should be replaced. The AMS shall comply with the industry standard that sets three years as the useful life of a computer and thus shall normally replace computers every three years, pending resources. Computer systems shall be refreshed before the end of the fiscal year in which they have been determined to be end-of-life.

Documentation and Testing Controls

Asset Management

The IT Office shall maintain a list of all server, workstations laptops, mobile devices, and any other AMS owned or operated equipment and associated specifications for each system. Furthermore, for each workstation, a detailed list of software that is installed, the location, and the primary user of the workstation shall be noted.

Consistent audits will be done to validate the workstation's owner and the software that is installed on each workstation to ensure compliance. Kaseya or a similar program will be used to track software.

The exception to this is any managed service contracts we have. This includes but is not limited to the OT Group for copier management/maintenance for the P&CC and RHCB Services for POS management/maintenance. We contract with these vendors for maintenance and support.

Provisioning of Access

AMS Domain & E-Mail Accounts

Any employee or volunteer of the AMS is entitled to a user account on the AMS domain with access to an e-mail account if deemed necessary by the IT Officer or Executive responsible for IT office.

Any AMS ratified club will be entitled to one AMS email, faculty clubs and other non AMS ratified clubs do not receive email. The AMS also provides email access and support to student societies on campus which include, but are not limited, to ASUS, CESA, NSS, PHESKA and ENGSOC. Support includes ensuring the account is active and the correct username and password is provided. It is at the discretion of the IT Officer and IT Oversight Committee to decide which faculty societies, groups, clubs, etc. are allowed this email access/support.

Email Naming Practices

Any emails that do not belong to AMS paid positions will receive generic display names for their email accounts that will not change yearly. For example, a club called AMS Club with a Club President of John Smith will have his first and last name listed as "AMS Club" not "John Smith" as changing this on a yearly basis is very time consuming.

System Administrators

The only system administrator on the IT Infrastructure shall be the IT Officer, IT Support Officer and selected personnel from Queen's IT Services.

Local Administrators

The local administrators for the IT Infrastructure (AMS Computers) shall consist of the IT Officer, IT Support Officer and support staff.

De-provisioning of Access

Once a user account is no longer necessary, the IT Officer will ensure that all relevant files and folders on the account have been backed up for historical record reasons (if required by the IT Oversight Committee). The IT Officer will then receive approval from either the President or IT Oversight Committee and delete the user account from the Active Directory, ensuring that the Exchange account and mailbox are successfully deleted.

De-provisioning of Devices

For AMS owed devices, the IT Officer shall retrieve the device and ensure that it is completely wiped before it is re-assigned or disposed of. For personal devices and upon completion of their term, users are responsible for deleting business data.

Those positions identified in the “Confidential Position List” shall come to the IT Office and show the IT Officer they are deleting the email account and mail off their phone.

Security exposures.

All personal information exposures shall be reported to Queens Information Security Officer and appropriate notification to users whose personal information has been compromised is disseminated by AMS responsible body.

Any personal information used in the course of elections, Qfrosh week shall be kept encrypted at all times and accessed by authorized individuals on a need to basis and who signed a confidentiality agreement.

All of Queen’s information security standards are considered a resource supporting this policy.

In areas of uncertainty, the AMS policy should defer to Queen’s information security policy, Network and Systems Security Policy and Acceptable Use of Information Technology Resources

Review cycle:

This policy shall undergo a review and approval every 3 – 5 years, with the next annual review in 2019

Application System and Database Controls

Before development can begin on a web application, it must be approved by the IT Oversight Committee.

If the application requires a database and it has been approved by the IT Oversight Body to use an internal database, then it shall have its own database account and a separate database from other applications (unless the application must share information with another application and this purpose has been allowed by the oversight committee).

Each database account shall only have access to its own database and to no other database. The only exception shall be the root account, which shall only be used by the IT Officer and the Web Application Developer for database maintenance. The user IDs and password for all database accounts shall be provided to the IT Officer and General Manager for confidential and strict dissemination. The root account shall never be used by a web application except one that allows database administration activities (e.g. PHPMyAdmin).

Application Development

All application development shall occur on the Test / Development server before deployment to the Production server. All source code developed for the AMS, whether by student employees, permanent staff or web developers under contract with the AMS, shall be solely the intellectual property of the AMS.

Application Testing & Deployment

After each application is developed, but before it is deployed, the application shall go through various forms of testing (e.g. functional, regression, unit, etc.) by the Web Application Developer. At the conclusion of the application, the application shall go through security assessment by the IT Office and QISO. After the security assessment, all issues and risks especially high level risks must be resolved before the application is allowed to go live.

Application Server (https://webapp.queensu.ca)

The IT Officer and IT Support Officer shall have admin access to the Application Server, and provide no other staff with access to it.

Web Development

Standardization

Changes to the AMS website wireframes and core structure shall not occur more frequently than once every three years unless approved by the Board of Directors. This restriction applies to complete

overhauls of websites including themes, CMS changes and web server changes. Website content may be edited and updated by authorized users as frequently as required. Where the website is older than three years and there is either a major feature request or a change in industry standard design strategies, the Information Technology Officers shall have the discretion to determine that a complete website redesign is required.

Although users other than the Information Technology Officer and Information Technology Support Officer shall have authorization to directly edit existing pages, the addition of new pages must be designed in consultation with the Information Technology Officer or Information Technology Support Officer.

New Website Creations

All web site creation shall go through the IT Office directly, with no exception. This ensures that all websites are hosted with the AMS IT Office, meeting AMS requirements. Users are not permitted to created websites on their own with any other provider unless permission is given from the IT Officer, IT Support Officer or IT Oversight Committee.

Information Security Controls

Confidential & Non-Disclosure Agreement

Any person who accesses and manages confidential or personal information shall sign the QISO non-disclosure and confidentiality agreement to ensure the confidentiality and protection of that information. All individuals will be reminded of their obligation yearly should they extend beyond a yearly engagement

Password Policies

These password policies shall apply to all AMS User accounts as well as any other accounts that are used for business purposes (e.g. Facebook account, Eventbrite, Twitter Account, YouTube Account, etc., the IT Support Officer must have these passwords as well). In addition, the IT Officer will maintain a list of which external accounts are under the purview of the AMS and the user(s) that have access and are responsible for that account.

User Password Policy

User passwords shall be a minimum of eight characters in length and shall be changed every 90 days. They shall contain at least three of the four following types of character:

1. Upper case character (e.g. A, D, G, etc.)
2. Lower case character (e.g. a, w, h, etc.)
3. Numeral character (e.g. 1, 6, 8, 0, etc.)
4. Special Character (e.g. $, *,], ?, etc.)

Furthermore, the password shall not contain more than three consecutive letters that appear in the username (e.g. if the username is “itmanager”, the password may not contain “itm”). Finally, a new password may not be the same as the previous 10 passwords.

After five unsuccessful attempts, a user accounts will be locked out for a period of 30 minutes.

Administrator Password Policy

An administrator password must follow the same rules as the user password policy, but it must be at least 12 characters in length.

Strong Key Password (Passphrase) Policy

Strong key passwords (used for SSL certificate passwords, encryption passwords, etc.) must contain one of all four types of characters covered in the User Passwords Policy. It also must be at least 20 characters in length. These encryptions keys shall be backed up on a secure media and under lock and key with the IT Support Officer

User File and E-Mail Policy

AMS employees shall have no expectation of privacy with respect to AMS e-mail accounts assigned for AMS use and user files stored on the AMS network. All AMS computer systems are subject to monitoring to ensure compliance with this policy.

AMS employees are assigned AMS e-mail accounts and file server privileges in order to conduct AMS business. These resources are not to be used for personal use. User files and e-mails that are stored on their respective servers shall be considered the property of the AMS. All AMS files shall be stored on the AMS file server. No other storage shall be permitted.

Users with subordinates shall have access to the files and e-mails of those they manage upon request, and without need to notify the employee, for purposes relating to the business of the AMS.

For Queen's listserv usage refer to the Listserv contract that has been signed between the AMS and Queen's University on the AMS Listserv usage.

Smartphone Policy

All smartphone users must connect to the AMS Mail Server through Microsoft ActiveSync so that policies may be applied to their personal phones. By connecting their phones to the server, they agree to this policy and the technical policies that are applied on their phones.

Positions listed below are subject to more strict security enforcement policies. These positions have been identified to have confidential data entrusted to them.

Confidential Position List

- AMS Secretariat
- Judicial Affairs Manager
- Director of Human Resources
- Director of Information Technology
- Commissioner of Social Issues
- Director of Hospitality and Safety Services
- QSC Service Managers
- Chief Returning Officer
- Chief Electoral Officer
- President
- Vice-President (Operations)
- Vice-President (University Affairs)
- General Manager
- Controller
- Administrative Assistant
- AMS Board of Directors

Password Policy

We recommend all smart phones have a password set on them that restricts unauthorized people from accessing business data. The phone must also auto-lock after 5 minutes of inactivity after which the password would have to be entered to access business data.

This policy is enforced for the confidential position list.

Encryption

The AMS does not encourage the storage of personal and confidential information related to AMS operations on smartphones or computers. However, as it may sometimes be necessary for business operations, any confidential and business data must be encrypted on the device to ensure its security. When possible this should be done with the built-in encryption methods. If a native application is not available, then a suitable third party application must be used to encrypt the sensitive data.

This policy is enforced for confidential position list

Update

For AMS owned phones, it should be kept as up-to-date as possible as advised by the IT Officer. For personal phones, the software shall be kept as up-to-date as best as possible with particular attention to security patches and encryption rules. When personal smart phones are used, the user would be required to securely delete all data on the smartphone related to AMS once their term is over.

Cases of Lost or Stolen Devices

Shall a smartphone that is connected to the AMS Mail Server become lost or stolen and the user is part of the “Confidential Position List” the user must notify the AMS IT Officer as soon as possible. The IT Officer shall then send a remote signal to wipe all of the data on the smartphone. In addition, the service provider that the phone was registered to shall also be notified by the user. For all other users this is an optional service provided by the IT Office.

3rd Party Application

Before the installation of a third party application, the user shall do their due diligence to ensure that the application will not create security vulnerabilities.

Methods of Support

All employees of the AMS and affiliates will use the AMS work order system for all help requests. If unable to access the system for any reason, staff and affiliates will then be permitted to call or email the

AMS IT Helpline directly for support. A first attempt should always be made to use the work order system.

Remote Support

The Information Technology office staff shall be permitted to use remote support such as Kaseya to control and view what is happening on AMS computers during a support session. An attempt must be made to contact the user prior to taking control of the computer. In the event the user cannot be contacted prior to a remote session, no remote session is permitted unless otherwise approved by the user, ie. *The user tells the IT staff in the morning to login to the computer at 12:00PM because the user will be on lunch and the computer will be free.*

The Human Resources computer will be forced to accept the remote support request prior to the staff being able to take control.

AMS Server Backup Policy

All data stored on AMS servers and web servers are backed up nightly at 12:00AM. We keep 14 revisions (2 weeks) worth of modifications before overwriting the oldest version with a newer version. This ensures that we can restore files that were deleted or changed within 14 days of the deletion or change. For the AMS file server, we also keep a 3 month archive to ensure we can restore files that may have been deleted up to 3 months prior.

Google Account Policies

In light of some concern arising from Google privacy policies, the AMS requires all Google accounts that will be used to store AMS related files to be setup and provisioned by the AMS IT Office through the AMS Google Apps for Education account. This requirement is to ensure that the data stored on the Google account is owned by the AMS and is supported by the AMS IT Office. Under no circumstance may any AMS files be stored on personal Google accounts.

No confidential information related to students or the AMS shall be permitted on Google, or any other storage provider. All confidential information must remain on the AMS file server.