Secure Use of McGill Administrative Systems

Issued by: Chief Information Officer
Issue date: June 5, 2020
Effective date: June 5, 2020

This document provides compliance requirements for users of McGill's **Administrative systems** ("**Administrative users**") who manage or access other people's Regulated data (personal information).

Payment Card Industry (PCI) data is subject to more stringent requirements that can be found in the McGill Merchant (PCI) Policy and Procedures and the PCI DSS standard.

Terms and Definitions

For the purposes of this directive, the following words and expressions have the respective meanings described below.

1. **"Administrative system"** is an IT service whose primary role is to support the operation of the University and contains large amounts of Regulated data (personal information).
2. "**Administrative user"** is someone with elevated privileges having access to other people's Regulated data (personal information).
3. "**Institutionally owned or managed device"** is a device owned by McGill or its researchers, or a device that McGill has been granted authority to manage.
4. "**Regulated data**" means information whose protection and use is mandated by law, regulation, or industry requirement (e.g., personal information, personal health information, and payment card data). Regulated data are confidential.

Related Documents and Resources

1. Responsible Use Policy: https://mcgill.ca/secretariat/responsible-use-it
2. Policy on Enterprise Data Governance: https://www.mcgill.ca/secretariat/files/secretariat/policy_on_enterprise_data_governance.pdf
3. Standard on Enterprise Data Classification: https://mcgill.ca/secretariat/files/secretariat/standard_on_enterprise_data_classification.pdf
4. Standard on Enterprise Data Governance: https://mcgill.ca/secretariat/files/secretariat/standard_on_enterprise_data_governance.pdf
5. Cloud Directive: https://mcgill.ca/it/files/it/cloud_data_directive.pdf
6. Cloud Service Acquisition Process: https://mcgill.ca/cloud-directive
7. Merchant (PCI) Policy and Procedures: https://mcgill.ca/financialservices/policies/merchant

The provided guidance is not mandatory for those who are only using the **Administrative system** to access their own personal data (Self-Service). McGill imposes fewer limitations regarding how you access and handle your own data, but the controls provided are recommended for your own protection.

McGill's **Administrative systems** that contain large amounts of Regulated data are subject to this directive. They contain the personal information of thousands of individuals and that information could be leveraged to perform various abuses such as identity theft and fraud. A failure to follow proper security practices (or an equivalent control) when accessing our **Administrative systems** and manipulating their data could result in a data breach affecting a large part of the McGill community.

This document lists requirements over and above what is contained in the Responsible Use Policy. Unless specific exceptions are formally granted by the CIO, **Administrative users** must comply with the following controls (or equivalent approved controls):

1. Secure access to Administrative systems

1.1 You may only use **Institutionally owned or managed devices**, including computers and mobile devices that are managed by McGill and are located on the McGill network, to access back-office **Administrative systems** (when working remotely, **Administrative systems** must be accessed through a secured communication channel such as VPN).

1.2 These devices have been designated for your work use and must not be shared with others including family members.

1.3 You must keep all deployed controls that have been applied to these devices (device password, authenticated screensaver, automatic updates, and antivirus protection) active.

1.4 Only licensed software may be installed on institutionally managed devices.

1.5 The operating systems and applications on institutionally managed devices must be maintained at supported versions.

2. Secure handling of Regulated data (personal information)

McGill **Administrative systems** contain a large volume of Regulated data (personal information) that the McGill community entrusts **Administrative users** to safeguard. This data must reside only within authorized systems that have been properly secured and approved.

2.1 Storage

2.1.1 Local copies of Regulated data (personal information) may only be <u>temporarily</u> stored on institutionally managed devices and must be securely deleted in a punctual manner. Controls commensurate with the source system must be implemented to restrict access to the data.

2.1.2 Regulated data (personal information) may only be stored in approved locations:

- The **Administrative system** itself
- Documentum D2 – Official source of record and archive
- SharePoint – Collaboration solution across teams (only if all users with access are registered to McGill 2FA)
- Microsoft Teams – Collaboration solution within a restricted team (only if all users with access are registered to McGill 2FA)
- OneDrive for Business – Personal storage and draft versions of files (only if the user is registered to McGill 2FA)
- Approved downstream applications – A downstream application is an application that receives data from some authoritative source.

2.1.3 Where there is a business need to use removable media (e.g., USB Drive) the media must be protected by strong encryption.

2.1.4 No other existing solution is permitted for storage of Regulated data (personal information) without approval of the appropriate data trustee.

2.1.5 Any new cloud solutions must be vetted through the McGill Cloud Service Acquisition Process.

2.1.6 Regulated data (personal information) must not be sent by email unless employing strong encryption. When it is appropriate to share such data, the use of the approved collaboration tools is preferred.

2.2 Printing

2.2.1 Regulated data (personal information) may only be printed if there is a business need to print.

2.2.2 Regulated data (personal information) may only be printed using uPrint Secure Release or a physically restricted printer where all users with physical access to the printer have authorized access to the data printed.

2.2.3 Printed documents with Regulated data (personal information) must have a written label of "Confidential" at the top of each page or bear some form of labeling to inform people with access of the data sensitivity.

2.2.4 Printed documents with Regulated data (personal information) must not be left unattended.

2.2.5 Printed documents with Regulated data (personal information) must be kept in a locked cabinet or in a secure room.

2.2.6 Printed documents with Regulated data (personal information) can only be taken out of McGill by authorized users.

2.2.7 Printed documents with Regulated data (personal information) must not be shared with anyone that does not have authority to see it.

2.2.8 Sending printed documents that contain a large amount of Regulated data (personal information) must be sent internally through authorized personnel or externally through a courier.

2.2.9 To dispose of documents with Regulated data (personal information) they must be securely shredded and cannot be put in a garbage or recycling bin.

2.3 Access management

When using the different approved solutions to store, process and/or transmit Regulated data (personal information), the following controls are required.

2.3.1 Granular access controls must be set to ensure that people can only access the data that they need and for which they have been authorized.

2.3.2 Any ad hoc sharing of data should be done on a business need basis for a restricted period of time. **Administrative users** are accountable for revocation of access.

3. Secure use of mobile devices

Because mobile devices are more frequently used on untrusted networks, additional controls are needed when used in the context of **Administrative users**.

3.1.1 Wherever supported, biometric authentication (fingerprint or facial recognition) should be enabled as this provides an additional layer to protect the authentication and data encryption.

3.1.2 From a mobile device, screen captures of Regulated data (personal information) must not be taken, stored or shared.

3.1.3 Mobile applications relating to McGill's **Administrative systems** must be kept up to date, as new upgrades are made available.

3.1.4 If the device is used over an untrusted wireless network, it must first connect to VPN before accessing **Administrative systems**.

3.1.5 The device must have a screen lock enabled (equivalent to an authenticated screensaver).

3.1.6 Mobile devices allow you to configure applications to bypass the screen lock: this must be minimized and care must be taken not to bypass the lock for any applications that could expose Regulated data.

3.1.7 Applications are installed only from an official repository (Apple Store, Google Play Store and Microsoft Store).

4. Secure access from personal devices

The use of unmanaged personal devices to access McGill's **Administrative systems** as **Administrative users** is authorized only under the following conditions.

- Regulated data (personal information) must not be stored beyond the duration of the connected session (this includes screen captures)
- The device must first connect to VPN with McGill 2FA before accessing Administrative systems
- The device must have a password set, authenticated screensaver, most current application and operating system updates applied and antivirus protection enabled
- IT credentials used to access the administrative systems must not be saved on these devices

Contact IT Services for any questions and clarifications (www.mcgill.ca/itsupport/servicedesk**)**