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 Tw -14eA8 (p)-0-e

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

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 A