

PEACE LIBRARY SYSTEM**DATA SECURITY**

CATEGORY: Management and Operations

POLICY: M3-17

DATE APPROVED: November 25, 2017

REVIEW IN: 2022

Background

Data security is an indispensable and integral part of current technology. Peace Library System's electronic data must be protected from negligent and intentional damage. As well, timely recovery from any damage is imperative if Peace Library System is to operate with minimum business interruption.

Reasonable and prudent steps should be taken to protect System data and information systems. At no time should these steps be breached, evaded, bypassed, or circumvented.

Policy

The IT Services Manager is responsible for security for electronic data stored on the System's local area network and the regional computer network. Financial and administrative data is backed up daily to a third party server.

Data security consists of, but is not limited to the following:

Anti-Virus Software

The IT Services Manager shall develop and implement an anti-virus protocol to protect the System's data and data systems from software that can damage or otherwise corrupt valuable electronic information. This protocol includes a procedure to keep anti-virus software current for System headquarters and for the region.

Data Backup

Individual staff members are responsible for ensuring that data recorded on their local workstation that needs to be backed up is copied to the network server so that a backup is saved in the personal or shared network directories. Critical information must be backed up as per policy.

For more information on what should be stored on local workstations and what should be stored on the local area network, please see the *Internet and Electronic Mail Acceptable Use Policy*.

E-Mail

E-mail for Peace Library System staff and most member libraries is hosted by Microsoft using Office 365. Security and backup for e-mail is the responsibility of Microsoft. Administration of e-mail, including the creation and deletion of accounts, is managed locally by the IT Services Department.

Firewall

The IT Services Manager is responsible for the maintenance and ongoing upgrades of the Peace Library System firewall.

Passwords

The IT Services Manager is responsible for the administration and security of all network and administrative passwords. Passwords will be changed annually, or as need arises. User account passwords are created by the user but may be reset by IT staff as required.

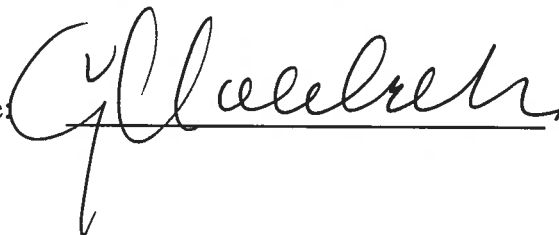
Shared Services

The Integrated Library System patron and library collection data for Peace Library System staff and member public libraries is stored on servers at Yellowhead Regional Library (YRL) and falls under YRL's security policy.

Security Procedures

System data and computer systems should only be used as authorized by the Peace Library Board. Access to information is restricted to what the individual creates on his/her local computer, in his/her individual directory and what is recorded in the "shared" directory on the network server. Release of information must comply with the System's *Confidentiality Policy* and the System's *Freedom of Information and Protection of Privacy Bylaw*. Information stored, maintained, or accessed on individual computers must comply with provincial and federal laws, including but not limited to copyright laws. Violations must be immediately reported to the System Director.

Chair's Signature:

A handwritten signature in black ink, appearing to read "G. Chalmers", written over a horizontal line.