## Systems Malware Protection Procedure

<table>
<thead>
<tr>
<th>Reference No.</th>
<th>Revision No.</th>
<th>Relevant ISO Control No.</th>
<th>Issue Date</th>
<th>Revision Date</th>
<th>Approved by</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx</td>
<td>1</td>
<td>10.4.1</td>
<td>January 22, 2012</td>
<td>January 22, 2012</td>
<td>Ted Harvey</td>
<td>Director, Technology Services</td>
</tr>
</tbody>
</table>

### Version History

<table>
<thead>
<tr>
<th>Version #</th>
<th>Version Date</th>
<th>Author</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Jan 22 2012</td>
<td>Ted Harvey</td>
<td></td>
</tr>
</tbody>
</table>

### Approvals

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date of Approval</th>
<th>Version #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ray Hoppins</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Distribution

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date of Issue</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Document Control

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Server Malware Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Location</td>
<td><a href="http://xxx.chinookedge.ab.ca/">http://xxx.chinookedge.ab.ca/</a></td>
</tr>
</tbody>
</table>
Table of Contents

1.0 Overview...............................................................................................................................4

2.0 Purpose.................................................................................................................................5

3.0 Scope ....................................................................................................................................6

4.0 Risks......................................................................................................................................7

The risks associated with the Procedure subject............................................................

5.0 Procedure Detail ...................................................................................................................8

Detailed Procedure statements .........................................................................................

6.0 Enforcement .......................................................................................................................10

If any member of IT staff is found to have breached this Procedure, they may be subject to
disciplinary action..............................................................................................................

If any user is found to have breached this security Procedure, they may be subject to disciplinary action... 10

Any violation of the Procedure by a temporary worker, contractor or supplier may result in the
termination of their contract or assignment................................................................. 10

7.0 Procedure Governance........................................................................................................11

8.0 Definitions ..........................................................................................................................13

9.0 References ..........................................................................................................................15

List any reference material used.........................................................................................
1.0 Overview

Chinook’s Edge Technology Services is entrusted with the responsibility to provide professional management of the organization servers. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this Procedure will limit the exposure and effect of common malware threats to the systems they cover.
2.0 Purpose

The purpose of this Procedure is to outline which server systems are required to have anti-virus and/or anti-spyware applications.
3.0 Scope

This Procedure applies to all servers that Chinook’s Edge Technology Services is responsible to manage. This explicitly includes any system for which a third party external supplier has a contractual obligation to administer. This also includes all server systems setup for internal use by Chinook’s Edge, regardless of whether Chinook’s Edge retains administrative obligation or not.
4.0 Risks
Non-compliance with this policy could have a significant effect on the efficient operation of the School Division and may result in financial loss, exposure of private and confidential data to unauthorized users and an inability to provide necessary services to our staff and students.
5.0 Procedure Detail

Chinook’s Edge operations staff will adhere to this Procedure to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

5.1 ANTI-VIRUS

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- NBT/Microsoft Share access is open to this server from systems used by non-administrative users
- HTTP/FTP access is open from the Internet
- Other “risky” protocols/applications are available to this system from the Internet at the discretion of the Chinook’s Edge Security Administrator

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Outbound web access is available from the system
- Email attachments can be executed or opened from the system.

5.2 MAIL SERVER ANTI-VIRUS

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.
5.3 ANTI-SPYWARE
All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own

5.4 NOTABLE EXCEPTIONS
An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions apply to this system:

- The system is a SQL server
- The system is not a Windows based platform
6.0 Enforcement

Infection of servers may cause business information to be disclosed or accessed illegally. Compromised systems and user actions, may allow external users to fake correct authorization and clearance so they may gain unauthorized access to confidential and private information which may adversely affect day to day business and student privacy. This policy is intended to mitigate that risk.

The responsibility for implementing this Procedure belongs to all operational staff at Chinook’s Edge. Responsibility for ensuring that new and existing systems remain in compliance with this Procedure resides with the Chinook’s Edge Technology Director.

If any user is found to have breached this security Procedure, they may be subject to disciplinary action.

Any violation of the Procedure by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.
7.0 Procedure Governance

The following table identifies who within CESD is Accountable, Responsible, Informed or Consulted with regards to this Procedure. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the Procedure.

- **Accountable** – the person who has ultimate accountability and authority for the Procedure.

- **Consulted** – the person(s) or groups to be consulted prior to final Procedure implementation or amendment.

- **Informed** – the person(s) or groups to be informed after Procedure implementation or amendment.

<table>
<thead>
<tr>
<th>Responsible</th>
<th>Core Team - Technology Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable</td>
<td>Director Technology Services</td>
</tr>
<tr>
<td>Consulted</td>
<td>Technology Committee,</td>
</tr>
<tr>
<td>Informed</td>
<td>All Technology Department Employees, All Contractors.</td>
</tr>
</tbody>
</table>
8.0 Definitions

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>For purposes of this Procedure, a server is any computer system residing in the physically secured data center owned and operated by Chinook’s Edge. In addition, this includes any system running an operating system specifically intended for server usage as defined by the Chinook’s Edge IT/IS Manager that has access to internal secure networks. This includes, but is not limited to, Microsoft Server 2000 and all permutations, Microsoft Server 2003 and all permutations, any Linux/Unix based operating systems that external users are expected to regularly connect to and AS400 systems.</td>
</tr>
<tr>
<td>Malware</td>
<td>Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words &quot;malicious&quot; and &quot;software&quot;. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.</td>
</tr>
<tr>
<td>Spyware</td>
<td>Broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.</td>
</tr>
<tr>
<td>Anti-virus Software</td>
<td>Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).</td>
</tr>
</tbody>
</table>
9.0 References

“Malware.” Wikipedia, The Free Encyclopedia. 22 Jan 2012,
<http://en.wikipedia.org/wiki/Malware>


<http://en.wikipedia.org/wiki/Anti-virus>