Secure Logon Access to Operating Systems

<table>
<thead>
<tr>
<th>Reference No.</th>
<th>Revision No.</th>
<th>Relevant ISO Control No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx</td>
<td>1</td>
<td>8.1.1</td>
</tr>
</tbody>
</table>

Issue Date: July 17th 2012
Revision Date: July 17th 2012
Approved by: Ted Harvey
Title: Director, Technology Services

Version History

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Version Date</th>
<th>Author</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 17th 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 No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ray Hoppins</td>
<td>Associate Superintendent,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Services</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>

Personal Communication Devices
Document Control

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Secure Logon to Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Location</td>
<td><a href="http://xxx.chinooksedge.ab.ca/">http://xxx.chinooksedge.ab.ca/</a></td>
</tr>
</tbody>
</table>
# Table of Contents

1.0 **Overview** ...................................................................................................................................3

2.0 **Purpose** ....................................................................................................................................3

3.0 **Scope** .......................................................................................................................................4

4.0 **Risks** .......................................................................................................................................4

5.0 **Procedure Detail** .....................................................................................................................4

   **Mandy Can you fix this???**

6.0 **Enforcement** ............................................................................................................................7

   6.1 Compliance ...............................................................................................................................7

7.0 **Procedure Governance** ...........................................................................................................7

8.0 **Definitions** ...............................................................................................................................8

9.0 **References** ..............................................................................................................................8
1.0 Overview

The Access to Operating Policy is intended to help employees understand the security requirements for accessing Chinook’s Edge Operating Systems.

This policy shall define a standard for accessing computers based on education, business and security requirements.

2.0 Purpose

Access to Operating Systems controls are put in place to protect information by controlling who has the rights to access Chinook’s Edge Systems and by guarding against unauthorized use.

All employees should familiarize themselves with the Secure logon Access to Operating Systems Procedures

It should be noted that even though the Secure Logon requirements are defined below all users with access to Information should use common sense steps to protect Chinook’s Edge Confidential information (e.g, Chinook’s Edge Confidential information should not be left unattended on Computers in classrooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your Principal. Questions about these guidelines should be addressed to Technology Services.
3.0 Scope

This policy applies to all CESD students, employees (including Technology Services staff with access to privileged administrative passwords), contractual third parties and agents of CESD with any form of access to CESD’s information and information systems.

Secure Logon procedures are required to regulate who can access CESD information systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing CESD information in any format, and on any device.

4.0 Risks

5.0 Procedure Detail

5.1 Implementation

The procedure for logging into an operating system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.

A good log-on procedure should:

a) Ideally not display system or application identifiers until the log-on process has been successfully completed;

e) limit the number of unsuccessful log-on attempts allowed, e.g. three to five attempts, and consider:

1) recording unsuccessful and successful attempts;

2) forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization;

3) disconnecting data link connections;
4) sending an alarm message to the system console if the maximum number of log-on attempts is reached;

5) setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected;

5.2 User Access Management

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Policy and the Password Policy. The login procedure must also be protected by:

. Not displaying any previous login information e.g. username.

. Limiting the number of unsuccessful attempts and locking the account if exceeded.

. The password characters being hidden by symbols.

. Displaying a general warning notice that only authorized users are allowed.

. All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

. System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

The screen should display, after a successful log-on, details of the date and time of the previous successful log-on (so that an authorized user can see whether the previous log-on was someone else or not) and details of any unsuccessful log-on attempts (so that the user can immediately report this a security incident).
The screen should display no system or application identifiers until the log-on has been successfully completed.

5.3 User Registration

A request for access to the division’s computer systems must first be submitted to People Services for approval. Applications for access must only be submitted by school administrators or division office department heads.

When an employee leaves CESD, their access to computer systems and data must be suspended at the close of business on the employee’s last working day. It is the responsibility of their principal or department manager to request the suspension of the access rights by Technology Services by email to helpdesk@chinookedge.ab.ca.

5.4 Applying the Policy

Ensuring that any PC they are using that is left unattended is locked or logged out as outlined in the 11.3.2 Unattended User Equipment procedure

Leaving nothing on display that may contain access information such as login names and passwords.

Following good practices to ensure usernames and password are not shared or left in hard copy format where they may be accessible. (e.g. post it notes)

Informing Technology services of any changes to their role and access requirements.

Informing Technology Services of any suspected identity theft.
6.0 Enforcement

Compliance

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

Penalty for deliberate disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Any violation of the Procedure by a temporary worker, contractor or supplier may result in the termination of their contract or assignment and possible civil and/or criminal prosecution to the full extent of the law.

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>Director Technology Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable</td>
<td>Associate Superintendent, System Services</td>
</tr>
<tr>
<td>Consulted</td>
<td>Technology Committee, FOIP Officer, Communications Officer</td>
</tr>
<tr>
<td>Informed</td>
<td>All CESD Employees, All Contractors, All temporary workers.</td>
</tr>
</tbody>
</table>
8.0 Definitions

Certain terms are used throughout this policy; in order to avoid misinterpretation, several of the more commonly used terms are defined below.

TERM / DEFINITION

Appropriate measures - In order to minimize risk of Chinook’s Edge computer use by unauthorized personnel must be restricted so that, in the event of an attempt to access Chinook’s Edge corporate information, the amount of information at risk is minimized.

Information System - Any electronic system that stores, processes, or transmits information.

Information Assets - Definable pieces of information in any form, recorded or stored on any media that is recognized as “valuable” to the Division.

Principle of Least Privilege - Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.

Principle of Separation of Duties - Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

9.0 References