

The Chinook's Edge School Division

Request for Proposal

ERP Solution

Closing Date

10:00 AM Local Time

Friday, July 9, 2021

The Chinook's Edge School Division herein referred to as "The Division," is interested in receiving proposals from qualified parties for the supply, installation, training and technical support for an ERP solution for a period of 5 years with an option for 2 only 5 year extensions for a possible total term of 15 years.

Contents

BACKGROUND	2
CURRENT SITUATION	2
GENERAL GOALS AND REQUIREMENTS	3
PROJECT SCOPE	4
IMPLEMENTATION TIMELINES.....	9
RESPONSE REQUIREMENTS	9
DEMONSTRATION DAY	10
EVALUATION PROCESS.....	11
GENERAL TERMS AND CONDITIONS	11
SIGNATURE FORM.....	19
APPENDIX I - THIRD PARTY INFORMATION SECURITY POLICY.....	20
APPENDIX II – SECURE TRANSFER OF INFORMATION REQUIREMENTS	47

BACKGROUND

The Division is one of the largest school divisions in the province, serving over 11,000 students in 40 Central Alberta schools between Calgary and Red Deer.

Our schools are located in 13 small communities that sprawl east and west from the Highway 2 corridor, conveniently providing Chinook's Edge staff and families with the best of both worlds: a friendly, healthy and affordable small-town lifestyle combined with the proximity to big city amenities! Plus, the world famous Rocky Mountains are a short drive away.

The Division's reputation for staff and student wellness, our family-friendly communities that boast easy access to exciting cultural and recreational opportunities, and our highly regarded quality learning environments make us a desirable division in which to live, learn, work and play!

CURRENT SITUATION

Currently, the Division is utilizing the following systems to meet its Finance, Human Resources and Payroll needs:

- Serenic (Bellamy) Software (Finance/HR/Payroll/Attendance/Fixed Asset/Work Order/Costing)

- MyBudgetFile Software for budgeting
- Rycor (Student Fee Management/Online Payments)
- School Engage (Transportation Registration and Fee Management / Online Payment)
- Laserfiche (Personnel File, field trip processes and other records management)
- Various web based financial applications that require data uploads in .csv file format
 - U. S. Bank Visa
 - ASEBP (Alberta School Employee Benefit Plan) Reconciliation
 - Telus billings
 - Servus Credit Union bank transactions

GENERAL GOALS AND REQUIREMENTS

The Division invites interested parties to submit a Proposal for the provision of an Enterprise Resource Planning (ERP) system consisting of:

- Human Resources, Payroll and Financial Information System Software, including fixed assets, project costing and work order, consulting and implementation services, subject to the conditions herein.
- While the replacement of the Serenic Software is our main goal, we are open to proposals that include budgeting and student fee management/online payment software, consulting and implementation services, subject to the conditions herein.
- Licensing for 100 or more users.
- Flexible licensing for role changes.
- Strong and simple security by user role, groups, departments, sites, accounts.
- Ability to audit all areas in the program(s) for any changes, both by date and by person.
- Ability to work in more than one fiscal year or more than one fiscal month
- Must be a batching system
- Ability to import/export data to from Excel or Google Sheets
- Ability for users to have multiple sessions open
- Ability to query any data field in any subsystem
- Ability to have multiple GST accounts
- Ability to copy a prior batch
- Ability to changes employee names and address for all subsystems at one time
- Ability to electronically approve transactions such as payroll, purchase orders and accounts payable.
- Maintenance and update processes and timelines that do not interfere with data processing.

The goal is to secure a qualified successful vendor to provide consultant services for the supply, delivery, installation, configuration, support and associated training for the ERP system software solution.

The successful vendor will provide at its sole cost and expense, all staff, equipment, goods, materials, tools, resources, accommodations, technical assistance and any incidentals and assume all overhead expenses necessary to perform the services required in accordance with the scope and deliverables outlined herein. It is critical to the Division that support personnel have the ability to communicate fluently in English.

Proposals must also include the location and security features of the database servers. Because of the sensitive nature of the data being stored, servers must be located in Canada.

The successful vendor will be required to work with the Division to confirm an acceptable Privacy Impact Assessment (PIA).

The successful vendor will be required to meet the requirements outlined in the Division's Third Party Information Security Policy (Appendix I).

The successful vendor will be required to meet the requirements of the Division's Secure Transfer of Information requirements (Appendix II).

PROJECT SCOPE

DELIVERABLES

Integration with other applications

The proposed ERP software will need to integrate with the following applications and systems at the Division:

- Active Directory integration
 - Update staff HR information (location movement, roles, name changes, etc.)
 - Add new employees
 - Photo ID information
- Multifactor authentication
- Data export capabilities to SQL or other data sources
- Data import capabilities
- Laserfiche integration
- Access to historic data
- Archiving current system data
- Security encryption of data and how it flows between systems
- Google calendar and sheets integration

The following basic functions are required, listed by department as a minimum to any acceptable solution:

Human Resources

- Transfer of information – ALL historical information up to and including final transfer date including active and inactive employee data
- Demographics tracking
- External job posting
- Internal job posting
- Posting process management
- Grievance management
- Certification tracking
- AKA, maiden name and change of name tracking
- Assignment management
- Seniority and sick leave management
 - Porting of sick leave: incoming
 - Porting of sick leave: outgoing
 - Porting of seniority: incoming
 - Porting of seniority: outgoing
- Experience calculation
- Staffing requisition
- Attendance management
- Leave management
- Absence bank tracking
- Professional development event tracking
- Personnel file management
- Electronic notifications of changes between HR and Payroll and Technology Services
- Benefits enrolment
- Contract and evaluation management, notification, prompts
- Notification to employees of HR changes and contracts
- Web access for administrators based on roles and responsibilities
- Criminal record check tracking
 - RCMP
 - Child Intervention check
 - Volunteers
- Retirement tracking / years of service tracking
- Evaluation tracking and notification of dates to be completed
- Benefits administration
- Employee Onboarding and Notification and Distribution of Required Information and form filling
- Annual Network Agreement Tracking
- Employee Access for FAQ and video tutorials

- Certificate tracking
 - Teacher Qualifications
 - Other
- Substitute and casual staff booking system with integration to payroll (contact, tracking, employee access), including automated call out system
- TWINS reporting (Alberta Education requirement)

Finance

- General Ledger
 - Data conversion planning, development, testing and execution, including conversion of up to 10 years of data
 - Both adjusting and budget journal entries with the ability to scan and attach supporting documentation
 - Ability to upload .csv files into software from other software (i.e. MyBudgetFile, Rycor, School Engage, U.S. Bank Visa, Telus, etc.)
 - Accurate and robust reporting ability
 - Easily accessible G/L activity (drill down ability)
 - Customizable reporting appropriate for school divisions (financial statements, school and department reporting, etc.)
 - Ability to tag expenses by employee
 - Account structure must be a minimum of 23 characters including delimiters.
 - Ability to record entries in two fiscal years in one batch
 - Ability to reverse a prior journal entry
 - Ability to prepare a prepaid expense and deferred revenue journal entry.
- Accounts Payable
 - Data conversion planning, development, testing and execution, including conversion of up to 10 years of data.
 - Cheque writing
 - Direct deposit to vendors, with email notifications to them
 - Scanning and attaching supporting documentation to batches
 - Posting against purchase orders and work orders
 - Visa tracking, changes, approvals and upload to general ledger
 - Upload utility data from vendors
 - Ability to utilize Visa for vendor payments but maintain records in accounts payable ledger
 - Accurate and robust reporting and ability to export to Excel
 - Ability to record prepaid expense batches to future months and years
 - Ability to import CSV files to create accounts payable batches
 - Ability to copy an accounts payable batch

- Ability to create AP batches that have already been paid by direct withdrawal
- Audit for duplicate invoices for a vendor
- Sequential numbering of cheques and EFT
- T4As
- Ability to process contract AP invoices with holdbacks and GST applied correctly.
- Accounts Receivable
 - Data conversion planning, development, testing and execution, including conversion of up to 10 years of data
 - Invoicing
 - Direct deposits from customers
 - Online payments
 - Charitable receipts with electronic signatures
 - Manage permits for school rentals from inside & outside agencies including creating invoices and receiving payments
 - Ability to create, register, monitor, collect payments, provide receipts, refunds, attendance lists, etc. for workshops for both internal employees and external customers
 - Sequential number of invoices by department or site
 - Ability to print past invoices
 - Ability to add custom notes to invoices
- Payroll
 - Transfer of information – ALL historical information up to and including final transfer date including active and inactive employee data
 - Process payroll for teacher's collective agreement, division office staff, trades staff, custodians, social workers, administrative support staff, learning commons staff, educational assistants, bus drivers, trustees, cafeteria workers, and various other support staff
 - Handles staff working in multiple positions
 - Electronic timesheets and delivery of pay stubs and T4s and other communications
 - Ability for employees to update timesheets, change their personal information, enter vacation requests, etc.
 - Multiple earning codes, absence codes, banks, and overtime
 - Ability to override earnings or deductions at payroll entry
 - Ability to process retroactive pay and deductions
 - Various taxable benefit codes, calculations
 - ATRF and LAPP pension calculations
 - Ability to export data in a file compatible with LAPP and ATRF requirements
 - ASEBP benefit calculations
 - Mass salary update to ASEBP

- WCB calculations
- Statutory holiday pay calculations
- Upload and download ability to various outside sources
- T4, T5, ROEs, T4As
- Multiple Receiver General accounts
- Distribute average costing to budget centers
- Ability to split employees pay to a minimum of two bank accounts
- Ability to inquire or sort employees by group, location, position, status, etc.
- Sequential data entry into payroll batches
- Ability to process advances based on a formula
- Sequential numbering of payroll cheques and EFTs
- Operations
 - Work order system (tracking, entering costs including labour, uploading into the GL)
 - Interface with accounts payable
- Project Costing
 - The Division uses extensive project costing for the following:
 - Expenditures tracked by:
 - Student, employee, project, contract and for various other reasons
 - Asset, liability, equity, revenue and expense accounts
 - Integration with general ledger, accounts payable, work order, purchase orders
- Purchasing
 - Purchase orders
 - Interface with accounts payable
 - Inventory management
 - Contract management
 - Purchase orders that encumber the GL and projects
 -
- Fixed Assets
 - Integration with accounts payable and the general ledger
 - Reporting that includes opening, additions, disposals, amortization, accumulated amortization and year-end balances
 - Amortization calculations
 - Ability to search assets using various fields
- Banking
 - Banking information should be integrated with all appropriate subsystems.
 - Ability to upload transactions from the bank for reconciliations.
 - Electronic bank reconciliation.
 - Multiple bank accounts.

IMPLEMENTATION TIMELINES

The Division anticipates the following timelines:

- July 9, 2021 – Closing of RFP Process
- July 12-31, 2021 – initial evaluation of RFP responses
- August 3, 2021 – notify vendors of their Demonstration Day
- Week of August 23th – Presentation, interview, question and answer
- Announcement of successful vendor – September 2021

RESPONSE REQUIREMENTS

The vendor's response must include the following:

1. A brief executive summary of your organization, including a description of the ownership structure and history.
2. A fully costed proposal, in Canadian dollars, in the form of the Excel File, Proposal Cost 2021 ERP.xlsx.
3. The vendor's project team, their roles, their experience at implementation and conversions.
4. A description of project management services included in the vendor's proposal.
5. An implementation plan with the following
 - a. Phase Implementation Approach
 - Describe your phased implementation approach. Clearly identify the different tasks involved and what deliverables will be presented that clearly identifies the different phases.
 - b. Change Management
 - Describe how you will handle and guide changes as part of your solution implementation. List the steps you intend to implement to drive full adoption and transition users from the current system to the new system outlining the various transitions to be carried out in each specific phase. Identify key training and onboarding activities associated with the change.
 - c. Training Methodology
 - Identify your training methodology and plan for the various systems and components. Identify the approach for training users with varying skill sets. Availability of online manuals and ability for the Division to customize.

Training formations available (i.e. onsite, webinar, online, train-the-trainer)

d. Software Updates

- Describe your process for software updates including:
 - Notification
 - Customization and configuration testing
 - Integration testing
 - User acceptance testing
 - Performance load testing
 - Fixes to the system as a result of the update
 - Procedure to roll back the update in the event that there are issues

e. Maintenance and Support

- Describe your maintenance and support model throughout the implementation process and post implementation. Describe the different maintenance activities and the available support. Items to clarify from a support perspective include:
 - System support
 - System updates and managing updates around customization
 - System data support
- Provide any value added options that you would like the Division to consider in arriving at a decision. These options (free or for fees) will require a rationale for their value to the Division.

f. History of data breaches and / or privacy breaches.

g. References

- Provide a list of at least 5 division references currently using your software. At least one of these references must be a division who has implemented your solution in the past three years.

DEMONSTRATION DAY

Based upon initial evaluations scoring, vendors will be shortlisted and chosen to participate in a demonstration of their solution. The results of this presentation will be used to finalize the evaluation process.

These demonstrations are expected to occur at the school division office, located in Innisfail, Alberta during the week of August 23, 2021 to a group of Division evaluators. Approximately 2.5 hours will be allocated for the demonstration and a question and answer session.

This demonstration will be thorough and involve the following:

- System demonstration;
- Question and answer period from the Division evaluators arising from the original submission. The questions will be supplied to the vendor prior to their schedule demonstration;
- Clarification of capacity to meet the Division's timelines.

EVALUATION PROCESS

All responses will be evaluated based upon the following criteria:

Criteria	Key Components	Scoring
System Capabilities	Mandatory criteria, integration into the Division's Technical environment, maintenance and support process, functionality.	40
Project Team	Recent experience, references, list of recent implementations.	15
Cost	Total cost based on Excel File: Proposal Cost.xlsx	25
Innovation	Examples of change management and improvements to processes at other implementations.	10
Detailed Implementation Plan	A realistic plan that provides detailed dates of work for both the vendor and the Division.	10
Initial scoring		100
Demonstration Day	Ease of use, thoroughness of solution, the Division's questions answered	20
Final Score		120

GENERAL TERMS AND CONDITIONS

It is the practice of the Division to award contracts for goods and services to vendors who display the ability to provide the best combination of products, capability and cost effectiveness.

Proof of Alberta WCB coverage will be required for all on site trainers and technicians. The vendor shall be solely responsible for ensuring the safety and health of its employees or agents and for ensuring that its activities are in compliance with Chinook's Edge School Division health and safety policies.

The contract will be written under the laws of the Province of Alberta.

Responses Meet Requirements

All vendors must certify that their response has met all of the requirements contained in this document and any others that may be added prior to closing date and time.

Please note that any addendum will be posted to <http://www.purchasingconnection.ca/>.

It is the vendor's responsibility to continue to monitor the website to ensure that the response addresses any addendum or modification posted up to and including closing time.

Clarification of Responses

The Division reserves the right to clarify any section of a response with a vendor within 10 working days of the closing date.

Conflict of Interest

Vendors must identify any potential conflict of interest or relationship between the vendor's employees and the Division's employees. Vendors should indicate how they are addressing this in their response.

Cost of Proposals

The Division will not be responsible for any costs incurred by any vendor in the submission of a proposal. The Vendor is responsible for all costs associated with preparing and submitting a response.

Force Majeure

Delays in or failure of performance by either party under the contract shall not constitute default thereunder or give rise to any claim for damages if caused by occurrences beyond the control of the party affected, including but not limited to, decrees of government, acts of God, fires, floods, riots, wars, rebellion, sabotage, and atomic or nuclear incidents. Lack of finances, strikes, lockouts or other concerted acts by works shall not be deemed to be a cause beyond a party's control.

In the event that performance of the contract, in the reasonable opinion of either party, is made impossible by an occurrence beyond the control of the party affected, then either party shall notify the other in writing. The Division shall either terminate the contract forthwith and without any further payments being made, or authorize the vendor to continue the performance of the

contract with such adjustments as may be required by the occurrence in question and agreed upon by both parties. In the event that the parties cannot agree upon the aforementioned adjustment, it is agreed by the parties that the contract shall be terminated.

Indemnification

Notwithstanding the providing of insurance coverage by the vendor, the vendor hereby agrees to indemnify and save harmless the Division, its officers, agents, servants and employees and each of them from and against claims, demands, losses, costs, damages, actions, suits or proceedings by whomever made, brought or prosecuted and in any manner based upon, arising out of, related to, occasioned by or attributable to the negligent activities of the vendor, its servants, agents, and Sub-Consultants, in providing the services and performing the work of this contract, excepting always liability arising solely out of the negligent act or omission by the Division.

Irrevocability

Proposals are binding and irrevocable upon submission and enforceable for the 90 days from the Closing Date.

Right to Negotiate

Subject to the Irrevocability clause above, the Division reserves the right to negotiate final terms and conditions (including pricing) for any items not contained in the Proposal, and/or deemed of minor materiality.

Confidentiality and Freedom of Information and Protection of Privacy Act

Information pertaining to the Division obtained by the vendor, its employees or agents as a result of its participation in this Request for Proposal is confidential and must be disclosed by the vendor. Only use or copy such information as is necessary for the purpose of submitting a proposal.

The Division will endeavor to keep all proposals and accompanying documentation received as confidential and used only for the purposes of evaluation of the proposals. The Division provides no warranty with respect to confidentiality and shall incur no liability from any disclosure. The vendor grants the Division the right to copy any documents provided in or with the proposals for the purposes of the evaluation.

All documents submitted may be subject to protection and disclosure provisions of the *Freedom of Information and Protection of Privacy Act*. While this act allows persons the right of access to records in the Division's custody or control, it also prohibits the Division from disclosing personal or business information where disclosure would be harmful to your business interests or would be an unreasonable invasion of personal privacy as defined in Section 15 and 16 of the Act. Any information deemed to be copyright or trade secret must be identified as such in the proposal. Final adjudication of qualification for non-disclosure will be at the discretion of the Privacy Commissioner.

Insurance

The vendor shall, at its own expense, obtain and maintain during the term of this Contract, in a form and with an insurance company satisfactory to the Division, policies of:

Commercial General Liability insurance with a limit of not less than Five Million Dollars (\$5,000,000) for any one loss or occurrence and in the aggregate with respect to bodily injury, personal injury and property damage, including loss of use thereof, which policy shall by its wording or by endorsement:

- include the Division, its officers, directors, employees, agents and trustees as an additional insured with respect to the obligations assumed by Vendor under this Contract;
- provide that, in relation to the interests of each additional insured, the Insurance shall not be invalidated by an action or inaction by any other person other than the respective additional insured;
- include a "cross liability" clause which shall have the effect of insuring each entity named in the policy as an insured in the same manner and to the same extent as if a separate policy had been issued to each;
- extend to cover blanket contractual liability, including the insurable liabilities assumed by Vendor under this Contract;
- extend to cover products and completed operations; such products and completed operations coverage, whether by specific policy endorsement respecting the services or by renewal of any annual practice policy, shall be kept in force during the supply of services and for a further period of 24 months following completion of supply of the services;
- extend to cover non-owned auto liability coverage; and
- not exclude any existing property of the Division, but shall treat same as "third party property".

Employer's Liability Coverage which shall not be less than \$5,000,000 for each employee where Workers' Compensation coverage does not exist or the profession/trade has been indicated to be exempted from Workers' Compensation coverage.

Automobile public liability and property damage insurance in an amount not less than Two Million Dollars (\$2,000,000) all-inclusive covering the ownership, use and operation of any motor vehicles and trailers which are owned, leased or controlled by the Vendor and used in connection with this Contract; and

Property "All Risks" insurance covering the vendor's owned property, including the vendor's equipment, where applicable, and property of others in the care, custody, or control of Vendor or for which the vendor has assumed liability, all including while in transit or storage, on a replacement cost basis. With respect to any property of the Division, such policy shall contain a loss payee clause in favour of the Division; (collectively, the "Insurance").

The vendor shall ensure that the above Insurance policies:

- are endorsed to provide the Division with not less than sixty (60) days written notice in advance of cancellation, lapse, change or amendments restricting coverage;
- do not include a deductible that exceeds such maximum amount that a reasonably prudent business person would consider reasonable; and
- take the form of an occurrence basis policy and not a claims-made policy.

The successful vendor shall, before any services are performed, provide the Division with a copy of the certificates of insurance and, if requested by the Division, the insurance policies evidencing all the coverage stipulated above, and the Division may withhold payment of any invoice until it receives evidence of such coverage. Failure for any reason to furnish this proof at any time shall be a breach of the contract, allowing the Division to terminate the contract or at the Division's option, to supply such insurance and charge the cost to vendor. The Division may require vendor to have the Division added as an insured party to the insurance policy and/or require vendor to furnish a certified copy of the policy for such insurance.

Vendor shall not make or cause to be made any modification or alteration to the Insurance, nor do or leave anything undone, which may invalidate the Insurance coverage. Vendor shall be responsible for any deductible and excluded loss under the Insurance.

The vendor shall cause all subcontractors performing services to obtain and maintain the Insurance connected with this Contract, including without limitation:

- a) those resulting from any act or omission on the part of Vendor or its employees, agents and subcontractors;
- b) those resulting from any action, suit or proceeding brought by any third party;
- c) those brought in respect of personal injury (including injury resulting in death) or damage or destruction of tangible or intangible property, including the Division's property;
- d) those made under Workers' Compensation legislation;
- e) those legal costs and fines resulting from the failure of Vendor, its employees, agents or subcontractors to comply with any applicable laws, regulations, by-laws, rules or orders of any government, authority or body having jurisdiction, whether identified in this Contract or applicable by-law;
- f) those resulting from the release, discharge, seepage or other escape of any substance including chemicals, hazardous or toxic materials, substances, pollutants, contaminants or wastes, whether liquid, gaseous or of any other nature or for any breach of any applicable environmental legislation;

- g) those resulting from any laborers', material men's, or mechanics' liens arising from or relating to the performance of the Contract;
- h) those brought for actual, alleged, direct or contributory infringement of any patent, trade mark, copyright, trade secret or other intellectual property right, including breach of obligations of confidentiality; and
- i) any other claims, expenses, costs, and losses suffered, incurred or sustained by the Division. policies required by this Section.

The vendor agrees that the insurance coverage required to be maintained by it under the provisions of this Contract shall in no manner limit or restrict its liabilities under this Contract.

The Division reserves the right to maintain the insurance in good standing at the vendor's expense and to require the vendor to obtain additional insurance where, in Division's reasonable opinion, the circumstances so warrant.

The insurance coverage shall be primary insurance as respects to the Division. Any insurance or self-insurance maintained by the Division shall be in excess of this insurance and shall not contribute to it.

Cyber Insurance

The vendor shall have Computer Security, Privacy Liability and Cyber Liability Insurance, with limits not less than \$5,000,000 per occurrence or claim, \$5,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by (The vendor) in this agreement and shall include, but not be limited to, covering actual or alleged acts, errors or omissions committed by the (The vendor), its agents or employees. The policy shall also extend to include the intentional, fraudulent or criminal acts of (The vendor, its agents or employees). The policy shall expressly provide, but not be limited to, coverage for the following perils:

- unauthorized use/access of a computer system
- defense of any regulatory action involving a breach of privacy
- failure to protect confidential information (personal and commercial information) from disclosure
- notification costs, whether or not required by statute.

The vendor shall be responsible for all claims expenses and loss payments within the policy deductible or self-insurance retention. If the policy is subject to an aggregate limit, replacement insurance will be required if it is likely such aggregate will be exceeded. Such insurance shall be subject to the terms and conditions and exclusions that are usual and customary for this type of insurance.

If this insurance is provided on a claims-made basis, (The vendor) shall maintain continuous insurance coverage during the term of this Contract and in addition to the coverage requirements above, such policy shall provide that:

- Policy retroactive date coincides with or precedes the insureds' initial services under the Agreement and shall continue until the termination of the Agreement (including subsequent policies purchased as renewals or replacements);
- Policy allows for reporting of circumstances or incidents that might give rise to future claims; and
- Not less than a three year extended reporting period with respect to events which occurred but were not reported during the term of the policy or ongoing coverage is maintained.

The insurance policies mentioned above are to contain, or be endorsed to contain, the following provisions:

The vendor shall have the required insurance in full force and effect prior to execution of this Agreement.

The vendor shall provide the Board with evidence satisfactory to the Board of all required insurance prior to the commencement of the work in the form of the Certificate of Insurance.

Late Proposals

Proposals received after the closing time stated will not be accepted and will be returned unopened.

Acceptance / Rejection

All the terms and conditions of this tender are assumed to be accepted by the vendor and incorporated in its Proposal.

The Division reserves the right to reject any part of, or all proposals. Furthermore, the Division reserves the right to accept the proposal that the Division deems to be in their best interest and best serves their needs and budgets.

The Division reserves the right to accept any part of, or all proposals and also reserves the right to negotiate with the selected vendor to clarify and enhance the services provided under the proposal, prior to acceptance. Furthermore, the Division reserves the right to select a vendor directly from respondents to this RPF, or alternatively may elect to short list potential vendors who will be invited to participate in a "Best and Final Offer" process. Specific details of the final offer may be subject to refinement based on changing circumstances such as passage of time, new information or factors beyond the control of the Division or vendors.

Proposals which are incomplete, conditional, obscure, or in any way fail to conform to the requirements of this Request for Proposal may, at the Division's sole discretion, be rejected.

The Division reserves the right to award contracts to any one or more of the submitting vendors, at the Division's sole discretion. The Division may, at its sole discretion, award individual modules to one more vendors.

It is the vendor's responsibility to familiarize themselves with all aspects of the Division's requirements. Requests for clarification of information and requirements should be emailed to Susan Roy at sroy@cesd73.ca. Responses to Requests for Information will be issued by addendum. Verbal responses will not be provided.

The Division will not assume any responsibility or liability for any costs incurred by the vendor in preparing their response to this request for proposal.

Closing Date

Proposals signed by an authorized agent of the vendor's company must be received by 10:00 a.m., local time, on Friday, July 9, 2021 via email to Susan Roy at sroy@cesd73.ca.

SIGNATURE FORM


The undersigned company represents and warrants that it is authorized to carry on business of this nature within the Province of Alberta and that it is not disabled from performing said business by any law of the Province of Alberta. The undersigned also acknowledge receipt, understanding, and has taken into consideration, all information presented in this Request for Proposal.

The undersigned confirms and agrees that the person whose name is set out below is fully authorized to represent the company and to bind it to the terms and conditions of this Request for Proposal, including any and all addenda issued, and any subsequent contracts or purchase orders issued as a result.

The undersigned also acknowledges that the Division reserves the right to accept or reject in whole or in part, all quotations in response to the Request for Proposal.

_____ Company	_____ Date
_____ Name and Title	_____ Authorized Signature
_____ Name and Title of Witness	_____ Witness Signature

CESD ISMS Policies and Controls

	<p>Chinook's Edge School Division #73</p>	<p>Issue Date: December 2011</p>
<p>Relevant ISO 10.2.1</p>	<p>Revision #: 1 Date: January xx, 2012</p>	<p>Approved by: Ted Harvey Title: Director Technology Services</p>

Chinook's Edge Information Technology Department

CESD

Third Party Information Security Policy

Date: Jan 16, 2011

CESD ISMS Policies and Controls

Table of Contents

1	Third Party Information Security	4
1.1	Introduction	4
1.2	Scope	4
1.3	Definitions and Terms	4
1.4	Organization	5
1.5	Establishing Security Requirements	6
1.6	Third Party Approvals	7
2	General Security Requirements	8
2.1	General Audit	8
2.2	Personnel	8
2.3	Inventory, Ownership, and Classification	9
2.4	Data Storage and Handling	10
2.5	Data Transmission	11
2.6	Laptops/Workstations	11
2.7	Business Continuity Planning/Disaster Recovery	12
2.8	Incident Response	12
2.9	Third Party Workplace Security	13
2.10	Computer Room Access	14
2.11	Consumer and Regulatory Compliance	15
3	Data and Application Security Requirements	15
3.1	Data and Application Audit	15
3.2	Data Isolation and Architecture	16
3.3	Change Management	16
3.4	Server Operating Systems	17
3.5	Data Back-Up	19
3.6	Activity and Fault Logs	19
3.7	Access Controls and Privilege Management	20
3.8	User Accounts	20
3.9	Password Policy	21
3.10	Application Security	21
4	Network Connectivity Security Requirements	23
4.1	Third Party Type and Audit	23
4.2	Third Party Network Transport Requirements	23
4.3	Basic Third Party Access Requirements	23
4.4	Trusted Third Party Access Requirements	24
4.5	Trusted Third Party Network Architecture	25
4.6	Trusted Third Party Outbound Proxy Servers	Error! Bookmark not defined.

CESD ISMS Policies and Controls

4.7 Trusted Third Party Email Servers 26

5 Appendix.....26

5.1 Appendix A: CESD Data Classification Standard 26

5.2 Appendix B: CESD Acceptable Use Guidelines 27

5.3 Appendix C: CESD Supplier Security Risk Analysis Checklist 27

CESD ISMS Policies and Controls

1 Third Party Information Security

1.1 Introduction

CESD recognizes that information protection requires a partnership between CESD and its suppliers, vendors, partners, and clients. This document outlines CESD's security policies designed to safeguard CESD information, and information belonging to Third Parties, from unauthorized or accidental modification, corruption, destruction, or disclosure.

1.2 Scope

This policy addresses technical security and compliance concerns with respect to CESD on-site, remotely connected and Virtual Desktop-connected contractors, CESD data housed or hosted by external service providers, site-to-site customer-facing network connectivity, and general connections into the CESD internal network from non-CESD sites. Specially designed CESD external customer services DMZ's with no inbound access to CESD internal networks are out-of-scope.

The basis for the control objectives and controls is compliance with applicable law and CESD general policies, primarily the CESD security policy. However, most of this document's procedures go beyond technology concerns and have wider applicability. For example, information protection applies to data in electronic form as well as printed or paper documents.

CESD may periodically update its security policies based upon newly reported vulnerabilities and threats. In addition, CESD already has an extensive network of existing Third Party Connections, e.g. PASI which bring additional joint risk. To minimize this residual risk, third parties or contract renewals should be brought in line with the latest documented policy. All third parties should have all gaps identified, then brought into compliance or mitigated.

1.3 Definitions and Terms

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

Basic Third Party Connection: A site-to-site connection between Third Party network and CESD internal network that requires minimal firewall rules and NAT of CESD internal addresses. Used for outbound-initiated connectivity into the Third Party network, or a specific set of inbound IPs/ports/protocols acceptable to CESD.

CESD ISMS Policies and Controls

BCP/DR: Business Continuity Planning/Disaster Recovery.

GDC: Global Development Center – a Trusted Third Party with additional management controls and oversight sponsored by CESD Corporate to service multiple business contracts. A

CESD Worker: CESD and Third Party employees, their consultants, contractors, and vendors for any CESD engagement. Will generally apply to customers with remote or on-site access to CESD facilities.

Hosting: Third Party providing Internet-facing servers and applications accessible by the public or CESD customers; Most Hosting Third Parties will also have Housing of CESD data as part of the application.

Housing: Third Party that stores or processes CESD data such as data processing applications, data center services and backup tape storage facilities. Housing includes CESD data storage whether accessible to the Internet or not.

Minimal Access: The minimum required access rules necessary to achieve function required; used to describe “locked-down” firewall rules.

NAT: Network address translation; used to convert CESD internal addresses to numbers routable on the Third Party’s network; required for Basic Third Party connectivity.

Remote VPN: Individual Internet-based access to the CESD internal network using two-factor authentication such as SSL-VPN or IPsec. Because a token is required, it is not suitable for access by automated processes.

Third Party: Vendor, supplier, partner, contractor, service provider, or customer with connectivity to CESD’s internal network or access to CESD data. This includes joint ventures without majority CESD ownership.

Third Party Manager: The individual at the vendor responsible for the CESD/Third Party relationship.

Vendor Project Manager: Appointed by the vendor Manager with notification to the CESD Sponsor and CESD Technology Services Director to supervise and coordinate security activities within the organizations. Assumes role as primary point of contact with CESD in case of security incident response.

Trusted Third Party Connection: A physically isolated segment of the Third Party network connected to CESD internal network in a manner identical to a CESD remote office. Organization

CESD Sponsor: Every Third Party should have a CESD Sponsor, responsible for owning the business relationship and overall performance

CESD ISMS Policies and Controls

including adherence to compliance and security requirements. The CESD Sponsor should be guided by local business definitions, legal or regulatory requirements and the specifications of the CESD Information Sensitivity Classification Standard (see Appendix) and security program.

CESD Technology Services Director: The CESD Technology Services Director should assess Third Party risks for the CESD Sponsor, and ensure the Third Party implements security controls appropriate to the classification of the data and access required. The CESD Technology Services Director should work closely with the vendor Project Manager to maintain adequate incident response/audit, and provide updates to any ongoing changes to CESD security practices.

Vendor Manager & Vendor Project Manager: The vendor Manager must identify a Vendor Project Manager responsible for adherence to CESD security policies. The vendor Project Manager is responsible for preparing and implementing a security program that promotes compliance and assists workers in practicing sound security principles, reviewing security plans periodically and updating them as necessary, reporting security incidents, and scheduling periodic audits as directed in this policy. The vendor Manager is responsible for notifying the CESD Sponsor of any subcontracts/outsourced work and maintaining Third Party subcontractor security levels and agreements that ensure CESD information security requirements and audits are met. The Project Manager interfaces with the CESD Technology Services Director.

1.4 Establishing Security Requirements

This information security policy document is organized in three sections. Based upon CESD assessment of business access needs, then language addressing one, two or all three sections should be included in supplier agreements.

Section 2. **General:** All Third Parties must comply with General security requirements

Section 3. **Data and Application:** Additionally applies if Third Party is Hosting/Housing CESD data

Section 4. **Network Connectivity:** Additionally applies if the Third Party has direct access to CESD networks

The business need to access CESD data, networks, and systems is a decision based upon assessment by the CESD Sponsor and CESD Technology Services Director of the Third Party status, work performed, number of CESD users served and type of access.

CESD ISMS Policies and Controls

Examples (Note: CESD Sponsor and CESD Technology Services Director will adjust based upon business need and data classification)	2. General Security Requirements	3. Data and Application Security Requirements	4. Network Connectivity Security Requirements
On-site with No Sensitive Access Remote VPN L1 Helpdesk Basic Third Party L1 Helpdesk/Device Support	Yes		
Remote Hosting/Housing On-site Development/Data Processing Basic Third Party Development/Data Processing	Yes	Yes	
Trusted Third Party L1 Helpdesk/ Device Support/Network Management	Yes		Yes
Trusted Third Party Development/ Data Processing/Hosting/Housing	Yes	Yes	Yes

1.5 Third Party Approvals

All Third Party access should be sponsored, reviewed and approved by the sponsoring business with:

- **CESD Sponsor:** Approves request as a business need and ensures the security reporting structure is in place.
- **CESD Legal Team:** Approves contract as meeting CESD and legal standards.
 - Master Services Agreement: reviewed and approved by the appropriate CESD legal department with necessary signatures from both parties.
- **CESD Technology Services Director:** Approves request as meeting security requirements specified in this document and the CESD Information Security program including:

CESD ISMS Policies and Controls

- Control: Personnel, physical, software, information asset ownership, access control and identity management responsibilities.
- Physical Security: Access to workplace, computer rooms, systems, and media/documents
- System Security and CESD Metrics: System and application configurations and vulnerabilities with periodic metrics reporting to the CESD Technology Services Director
- BCP/DR and Crisis Management: BCP/DR preparedness and management of CESD or Third Party events include information security incident response.
- Business Access and Network Security: Type of Third Party Connection (Basic/Trusted), network access details and termination dates

2 General Security Requirements

2.1 General Audit

- 2.1.1 Specific language covering periodic General or industry-specific audits should be included in agreements between CESD and the Third Party. Scope for compliance must be agreed upon with CESD sponsor but will vary based upon industry and regulatory (such as School Technology Framework) requirements.
 - 2.1.1.1 Third Party must review with CESD Technology Services Director all risk items identified through infrastructure reviews and audits that Third Party does not remediate within five business days.
 - 2.1.1.2 Third Party must be prepared to provide necessary confirming documentation in support of CESD's external audits upon CESD request.
 - 2.1.1.3 In addition to any audits provided for in CESD contractual agreements, the Third Party must permit CESD to request and/or perform, at the expense of CESD, up to two security assessments per year, including but not limited to, review of policies, processes, and procedures, on-site assessment of physical security arrangements, network, system, and application vulnerability scanning, and penetration testing. Such assessments will be communicated at least one-quarter year in advanced and conducted at a time mutually agreed upon between the Third Party and CESD, and CESD will provide the results to the Third Party.

2.2 Personnel

- 2.2.1 Specific language must be included in agreements to ensure Third Party has conducted a criminal record check and child intervention

CESD ISMS Policies and Controls

background check for Third Party CESD Workers in CESD engagements.

- 2.2.2 Vendor Manager must ensure employees are aware of the fact that they are not entitled to privacy protection in the use of their company computers and networks, since these resources may be monitored. Vendor Manager must define a formal process for responding to a security policy breach by Third Party CESD Workers.
- 2.2.3** All Third Party CESD Workers, contractors, and relevant third parties with access to CESD networks and data must read and accept the *CESD Acceptable Use Agreement* (see document in Appendix).
- 2.2.4 The Third Party must employ designated staff whose job responsibilities include information security and information risk management.
- 2.2.5 The vendor Manager should ensure that Third Party personnel added to the CESD account (in-processing) and removed from the CESD account (out-processing) are completed in a timely, consistent manner auditable by CESD.

2.3 Inventory, Ownership, and Classification

- 2.3.1 CESD reserves the right to audit Third Party's CESD inventories.
- 2.3.2 Data Inventory: Third Party must maintain an inventory of all CESD information assets including:
 - 2.3.2.1 Name, location, retention, and CESD-assigned data classification level (as described in the *CESD Information Sensitivity Policy* of the information asset such as a database or file system.
 - 2.3.2.2 A knowledgeable individual owner of each information asset with the default owner of an information asset is its creator.
 - 2.3.2.3 Computer systems that house CESD data and storage encryption status.
- 2.3.3 Application Inventory: Third Party must maintain an inventory of Applications that provide access to CESD data and transmission encryption status with correlation to computer systems.
- 2.3.4 Assign access controls based upon classification and individual "need to know"
- 2.3.5 CESD reserves the right to examine CESD data and all data stored or transmitted by CESD computers or communications systems that are the property of CESD. (This may exclude data specifically owned by any government agency or other businesses where CESD is the "caretaker" rather than owner).

CESD ISMS Policies and Controls

- 2.3.6 Physical Inventory: Third Party must maintain an inventory of physical computing assets used in the performance of the CESD engagement.
 - 2.3.6.1 Physical assets and equipment must have asset tags or recorded serial numbers.
 - 2.3.6.2 Assign a knowledgeable individual owner and usage requirements to each asset.
 - 2.3.6.3 Include purpose or project, locations authorized, and current location.
 - 2.3.6.4 For CESD-supplied equipment, record CESD authorization (CESD provides a template) and return date.
- 2.3.7 Software Inventory: Third Party must maintain an inventory of software used in the performance of the CESD engagement: those licensed and issued by CESD, procured by the Third Party and reimbursed by CESD, and those procured by CESD.
 - 2.3.7.1 Include license date, purpose/locations authorized, and return date.
 - 2.3.7.2 Record the CESD authorization (CESD provides a template) and usage compliance.

2.4 Data Storage and Handling

- 2.4.1 Third Party must, at a minimum, follow the *CESD Information Sensitivity Procedure* (see Appendix) directives when storing CESD data. The following best practices meet these requirements.
 - 2.4.1.1 Non-public information can be stored as locked, password protected/encrypted, or under direct user control. At no time may CESD data be left unattended.
 - 2.4.1.2 Follow a clear desk policy to securely store CESD documents. *CESD Confidential* and *Confidential Private* (as described in CESD Information Sensitivity Procedure) printing jobs must not be left unattended. The Third Party security team must audit and confiscate unattended documents.
 - 2.4.1.3 Passwords and challenge response answers must not be stored in clear text, but can be stored using a one-way hashing algorithm (e.g. MD5).
 - 2.4.1.4 *CESD Confidential* or *Personal* information can be only printed if attended.
 - 2.4.1.5 Before computer magnetic storage media is sent to a vendor for trade-in, servicing, or disposal, all *CESD Confidential* and *Personal* information must be physically destroyed, or erased using tools for hard disk overwrite.
 - 2.4.1.6 All waste copies of *CESD Confidential* and *Personal* data generated in the course of copying, printing, or otherwise handling such information must be destroyed.

CESD ISMS Policies and Controls

- 2.4.2 Do not make copies of *CESD Confidential* or *Personal* information without the permission of the CESD information owner.
- 2.4.3 CESD data at the Third Party in any form must not be stored or replicated outside the Third Party without special agreement; obtain approval from the CESD Sponsor before transmitting CESD data to a subcontractor or any non-CESD entity. The vendor Manager must maintain an inventory of the non-CESD entities that are receiving the data, the purpose of the data transmission, the transmission and encryption/protection method or protocol, the data that is transmitted and the CESD approver and CESD Technology Services Director who has authorized the transmission with these controls.
- 2.4.4 Upon conclusion or termination of the work agreement, the Third Party must provide CESD with copies of all CESD information maintained under the work agreement, as well as all backup and archival media containing CESD information.
- 2.4.5 Upon conclusion or termination of the work agreement, the Third Party must use mutually agreed upon data destruction processes to eliminate all CESD information from the Third Party systems and applications.

2.5 Data Transmission

- 2.5.1 Third Party must at a minimum follow the *CESD Information Sensitivity policy* and Secure Transfer of Policy when transmitting CESD data.

2.6 Laptops/Workstations

- 2.6.1 Third Party is responsible for the infrastructure that supports user compliance with the *Acceptable Use of CESD Information Resources* (see Appendix). The policy applies to laptops, desktop PCs, Unix workstations, and mainframe terminals.
- 2.6.2 Third Party must maintain laptop and workstation security through demonstrated provisioning, patching, and antivirus processes. Personal firewall and anti-virus are required for all Windows systems. Laptop disks should be encrypted.
- 2.6.3 Systems with direct access to the CESD internal network must follow monthly reporting to the CESD Technology Services Director in the form of the CESD Information Security Metrics. They may be restricted or removed for compliance failure or compromise.
- 2.6.4 CESD data must not be stored on laptop computers or other portable computing devices. Although laptops should primarily be used for access, not storage, specific exceptions may be granted by the CESD Technology Services Director for systems running CESD-

CESD ISMS Policies and Controls

licensed software, with patching, anti-virus, encryption, and personal firewall conforming to CESD security requirements with justified business need.

2.7 Business Continuity Planning/Disaster Recovery

- 2.7.1 Specific language must be included in agreements to ensure Third Party has a tested and sufficient BCP/DR plan and reporting process. So that the business processes may be quickly re-established following a disaster or outage, the Vendor Project Manager must maintain an updated inventory of all critical production systems and supporting hardware, applications and software, projects, data communications links, and critical staff at both the primary and secondary sites.
- 2.7.2 Vendor Project Manager must ensure preparation, maintenance, and regular test of the BCP/DR plan that allows all critical computer and communication systems to be available in the event of emergency or a disaster, and meet service level and recovery time and recovery point objectives.
- 2.7.3 BCP/DR test results must be periodically reported to CESD Technology Services Director.
- 2.7.4 Any emergency event-related disruption of business activities must be reported to the CESD Sponsor.
- 2.7.5 Ensure backup site security requirements meet *CESD Third Party Information Security Policy*.

2.8 Incident Response

- 2.8.1 Vendor Manager or Vendor Project Manager must maintain an up-to-date information security incident response plan including mobilization contact/call trees, bridge numbers, severity assessment, log recording steps, evidence collection and process diagrams.
 - 2.8.1.1 Vendor Project Manager must review test results of periodic drills with CESD Technology Services Director. Violation of CESD Information Security policies, virus/worm attacks, spam, data compromise, and physical asset loss must be covered.
 - 2.8.1.2 The Third Party, at the request of CESD, must provide copies of any log files maintained by the Third Party (including firewall, intrusion detection, system, and application log files) to support any investigation or legal action that may be initiated by CESD.
- 2.8.2 Specific language must be included in agreements to ensure Third Party has a tested and sufficient incident response and CESD reporting process. Vendor Manager must notify and update the CESD Sponsor and/or CESD Technology Services Director without

CESD ISMS Policies and Controls

- unreasonable delay of any actual or threatened unauthorized access or release of *CESD Confidential* or *Confidential Private* data or to the systems holding or providing access to such data. Final notification must include detailed incident log and root cause analysis within five days of closure that describes actions taken and plans for future actions to prevent a similar event from occurring in the future. The Third Party Information Security Leader must negotiate process with CESD Technology Services Director, but expectation is within two hours of discovery and mutually agreed upon updates for agreed upon high-impact incidents.
- 2.8.2.1 Third Party must report all occurrences of viruses and malicious code, not handled by deployed detection and protection measures, on any workstation or server used to provide services under the work agreement, to CESD without unreasonable delay. CESD expectation is within four hours as negotiated with the CESD Technology Services Director.
- 2.8.3 Specific language must be included in agreements to ensure Third Party has a tested and sufficient CESD disclosure approval process. Third Party must take action immediately to identify and mitigate an incident, and to carry out any recovery or remedies. Third Party must first secure CESD approval of the content of any filings, communications, notices, press releases, or reports related to any security breach prior to any publication or communication thereof to any third party. The Vendor Project Manager must maintain a well-understood reporting procedure for security incidents and train Third Party CESD Workers on CESD contracts.

2.9 Third Party Workplace Security

- 2.9.1 Entry to the Third Party area with CESD data access must be restricted to personnel authorized for access including an access termination procedure and periodic audit.
- 2.9.2 Visitor logbooks must be maintained which includes clear description of the visitor, arrival and leaving time, and CESD-relevant business purpose. A Third Party employee must always escort visitors within the Third Party area.
- 2.9.3 A security guard or electronic access control must protect entry to Third Party area. Entry and exit logging are preferable. Software-based access control systems must be secured, have proper backups and be highly available. Entry logs must be maintained for at least six months.
- 2.9.4 Ensure windows or any other auxiliary entry points are secured. If not staffed 24x7, alarms and entry point security cameras must be

CESD ISMS Policies and Controls

installed for off-hours access monitoring with recordings retained for at least one month.

2.10 Computer Room Access

- 2.10.1** All computer room doors must be secured to prevent access into the room unless otherwise authorized by the Vendor Project Manager.
- 2.10.2** Each computer room door must have signs on both sides indicating it is to be closed and locked with a contact to notify if it is found unsecured.
- 2.10.3** An identification badge or card reader must control all entrances into the computer room. Any other doors must be exit-only. The entrance and exit doors must be alarmed such that if left unsecured longer than one minute, the Security Office will be automatically notified. The Security Office must investigate the cause of the alarm, arrange to have it corrected, and notify the vendor Project Manager of incidents.
- 2.10.4** Identification Systems must generate a log of each entry. All door openings must generate a log entry, and every time the identification reader is used, it must log date, time, room location, and user.
- 2.10.5** Anyone needing badge/card access to any computer room must follow a defined procedure approved by the vendor Project Manager. The Third Party Security Office must not configure any badge for computer room access without being authorized by the vendor Project Manager or designated team members.
- 2.10.6** Employment termination must result in badge access termination. The vendor Project Manager must confirm that the badge access list is validated every quarter to verify those on this list still require access. Any discrepancies found must be corrected.
- 2.10.7** Badge access must only be given to individuals who require long-term access (those who are responsible for continuous administration or maintenance of the equipment located in the room).
- 2.10.8** Anyone having badge access to a computer room must not give or loan their badge to another to gain access to a computer room.
- 2.10.9** If it is necessary to leave a computer room door open for a specific time period for individuals who do not have access:
 - 2.10.9.1** The vendor Project Manager or designated team members must authorize the unsecured door request for a specific time period and document such in the access logs.

CESD ISMS Policies and Controls

- 2.10.9.2 A badge contact must be assigned to monitor the unsecured area and ensure the door is secured at the end of the specified time. Posted signs are recommended.

2.11 Consumer and Regulatory Compliance

- 2.11.1 Specific language must be included in agreements to ensure Third Party protects CESD student and employee privacy. Third Party must not disclose, market or otherwise contact CESD students or employees/contractors outside of their work on behalf of CESD, either electronically or through other media, using information gathered from Third Party web sites or CESD data.
- 2.11.2 Specific language must be included in agreements to ensure Third Party complies with industry and regulatory policies applicable to CESD data and security controls such as FOIP. If one of the above stated policies is in conflict with a governmental regulation, the issue must be presented to the CESD Technology Services Director for investigation and resolution.

3 Data and Application Security Requirements

3.1 Data and Application Audit

- 3.1.1 A Third Party Housing or Hosting *CESD Confidential* or *CESD Restricted* data must have infrastructure reviews performed by a third party at least annually.
- 3.1.2 Third Party must periodically conduct external security audits of their Internet-facing applications that make available *CESD Confidential* or *CESD Restricted* information, and the infrastructure that holds or transmits CESD data. A sanitized version of these results must be provided to CESD.
- 3.1.3 Perform a source code review of all non-static application logic changes before they are moved into production or perform an application penetration test at least twice yearly.
- 3.1.4 Third Party must conduct regular periodic and change-related internal audits of networks and systems.
- 3.1.5 Third Party must review with CESD all high-risk items identified through infrastructure reviews, code reviews and audits (internal or external, security and otherwise) that Third Party does not remediate within 10 business days.
- 3.1.6 Based upon CESD business access type and security requirements established, ensure the *Data and Application Security Requirements* (and Appendix checklist) to assess application security controls are audited.

CESD ISMS Policies and Controls

- 3.1.6.1 The Third Party upon request must provide copies of relevant security policy, process, and procedure documents to CESD for review and audit purposes. CESD should review and recommend reasonable changes, and supplier must amend the policies or respond with mitigating controls and responses.

3.2 Data Isolation and Architecture

- 3.2.1 CESD data must be stored in a separate system or database instance from data belonging to or accessed by other companies. If this is not possible, adequate controls must be documented and approved by the CESD Technology Services Director to ensure that a compromised database must not yield any CESD data.
- 3.2.2 CESD data must be backed up on separate tapes/drives than data belonging to or accessed by other companies. If this is not possible, adequate controls must be documented and approved by the CESD Technology Services Director to ensure that a compromised database must not yield any CESD data.
- 3.2.3 At no time may CESD data be housed on a server shared by companies other than the contracting vendor. For example, a shared web server that is used by several companies and maintained by an Internet Service Provider must not be used to house CESD data.
- 3.2.4 Internet facing web servers must be dedicated to this task, and must not host internal (intranet) applications for the Third Party.

3.3 Change Management

- 3.3.1 Third Party must have a documented change management procedure for applications and networks that support CESD processes or for Housing CESD data.
- 3.3.1.1 Third Party change management process must have clear separation of duties.
- 3.3.1.2 Third Party must have a documented source code versioning procedure.
- 3.3.2 Third Party must have a demonstrable process for keeping servers and software updated with the latest patches and service packs as recommended by the OS and software vendors.
- 3.3.3 Third Party must have separate development, staging, and production environments.
- 3.3.4 Production CESD data must not be used in the Third Party's development or staging environment without approval from the CESD Sponsor or CESD Technology Services Director. If a production extract is used, the Third Party must de-identify the

CESD ISMS Policies and Controls

CESD data or use a tool to obfuscate the CESD data before it is inserted into these environments.

3.4 Server Operating Systems

3.4.1 Antivirus must be installed on all Microsoft Windows systems.

3.4.1.1 Antivirus definitions must be updated at least once a day.

3.4.1.2 Do not install any freeware and shareware software before consulting Vendor Project Manager for review and approval.

3.4.1.3 Avoid installing plug-ins from Internet sites or using servers for General browsing.

3.4.2 The latest critical operating system, application, database, and network patches as defined by the CESD Information Security Metrics and Third Party's risk management process must be installed.

3.4.2.1 Third Party must demonstrate a security bulletin risk assessment process to react to emerging attacks and newly discovered vulnerabilities.

3.4.2.2 Systems must have weekly change windows for emergency and maintenance patching.

3.4.2.3 Latest "Critical" security and operating system patches should be installed within a seven-day change window to stem targeted attack or outbreak unless otherwise agreed upon with the CESD Technology Services Director. Other patches should be assessed and applied during periodic maintenance windows.

3.4.3 Lock down the server operating system. The following minimum requirements must be expanded upon based upon industry best practices.

3.4.3.1 Only the minimum/necessary set of applications and services should be installed.

3.4.3.2 Source code of server-side executables and scripts should not be viewable by external users.

3.4.3.3 Packet filters (such as host-based firewall and TCP wrappers) should be installed to restrict connections to necessary hosts on necessary services and log incoming requests.

3.4.3.4 Synchronize time to a trusted time service.

3.4.3.5 Services that require different access should use different accounts IDs.

3.4.3.6 No SNMP accessibility from the Internet. It is recommended to disable all SNMP.

3.4.3.7 There should be legal notice warning of unauthorized access penalties where applicable.

3.4.3.8 The password database should be encrypted.

CESD ISMS Policies and Controls

3.4.4 Lock down the web server using industry best practices.

- 3.4.4.1 The server's web root should be a unique directory from all other server files (i.e. all interpreters, shells and configuration files should be located outside of web server directory).
- 3.4.4.2 Directory browsing (indexed directories) should be turned off at the web server as to not reveal the presence of unlinked files.
- 3.4.4.3 The web server should run with minimum privileges necessary (not root or Administrator).
- 3.4.4.4 The web server host should not be a domain controller (NIS or Windows).
- 3.4.4.5 The web server host should not be configured as a router or packet sniffer.
- 3.4.4.6 The web server identification should be removed from the returned HTTP server field.

3.4.5 Lock down administration using industry best practices.

- 3.4.5.1 If Third Party has the capability to remotely administer servers, the remote connection must take place over an encrypted tunnel, and must require two-factor authentication.
- 3.4.5.2 All administrator accounts should have IP address restrictions, two-factor authentication or be limited to console login.
- 3.4.5.3 All administrative traffic should be encrypted. Encryption level should be defined based on the needs of the application.
- 3.4.5.4 All default accounts should be renamed or removed and all default passwords changed.
- 3.4.5.5 Access to devices involved in the provision of services should be granted only on a "need to have" basis. Server administration permissions are typically granted to a limited number of individuals within an organization.
- 3.4.5.6 More than one person should approve the granting of new administrator account access, and the addition/removal of account access should be auditable.
- 3.4.5.7 Shared administrative accounts should not be used. Instead, use individual accounts with an auditable method to escalate privileges for administration (example: sudo) where possible. Admin passwords can also be "checked out" for a period of time then reset.
- 3.4.5.8 System and service account passwords used by automated and batch processes should only be granted restricted access. The account should be single purpose, non-interactive login, from controlled sources such as a fixed source IP as a second login factor. If account should have more access, the CESD Sponsor should be made fully aware of their account responsibilities with the account description field annotating the contact.

CESD ISMS Policies and Controls

- 3.4.6 At the initial user sign-on to any system, server, device, and/or application used to provide services under the work agreement, the Third Party must display a warning banner advising users that the system they are accessing is a private computer system and is for authorized use only and activities are monitored and recorded. The warning message should include content that advises prospective users that unauthorized and/or malicious use of the system is prohibited and violators may be prosecuted to the fullest extent of the local and international law and that by logging on, the user has read and understood these terms.

3.5 Data Back-Up

- 3.5.1 Third Party must have well-documented procedures for information backup.
- 3.5.2 *CESD Confidential* or *CESD Private* data and Third Party systems critical to CESD operational processes must be backed up and stored in physically secured area with periodic notification to the CESD Technology Services Director of location and status.
- 3.5.2.1 Third Party must maintain all backup and archival media containing CESD information in secure, environmentally controlled storage areas owned, operated, or contracted for by The Third Party and approved by CESD Technology Services Director.
- 3.5.2.2 Third Party must limit access to backup and archival media storage areas and contents to authorized Third Party staff members with job-related needs.
- 3.5.3 Validity of backed-up data must be checked on a periodic interval not more than quarterly to ensure data is available when required.
- 3.5.4 CESD data must not be stored on removable media other than physically secured retention media expressly used for the purpose of backup or data retention for BCP/DR purposes.
- 3.5.5 Third Party must maintain adequate access and encryption controls on electronic backups as outlined in the *CESD Data Classification Standard*.
- 3.5.6 If the Third Party uses off-site tape storage then Third Party or their subcontractor must use an auditable tape check-in/check-out process and locked storage for transportation.

3.6 Activity and Fault Logs

- 3.6.1 Success and failure for all user account logins, system logins, and administrative requests must be logged.

CESD ISMS Policies and Controls

- 3.6.2 General server event logs, utilization logs, and application events and errors must be periodically verified as functioning in case of a forensics investigation.
- 3.6.3 The Third Party must maintain record for all hardware problems and operating system crashes.
- 3.6.4 Authentication failures and successes must be reviewed (at least weekly) for security violations.
- 3.6.5 Unless required otherwise by law, the Third Party must, at a minimum maintain logs for a period of no less than 180 days from origination.

3.7 Access Controls and Privilege Management

- 3.7.1 All CESD Data must be protected via access controls. The information must be protected from improper access, disclosure, modification and deletion. See *CESD Data Sensitivity Policy*.
- 3.7.2 CESD data must not be disclosed to unauthorized personnel. Access to CESD data must be approved on a business need basis. Access to servers must be restricted to authorized staff based on function (e.g., employees working in development must not have access to production servers).
- 3.7.3 The users must be given access privileges with the minimum requirements as per their job requirements. Non-administrative users must not have access to administrative system software or utilities. Privileged or administrative accounts must only be given to the persons responsible for managing systems, databases and applications.
- 3.7.4 Ensure procedures are in place to add, remove, and modify user access, including details on control of user administration rights.

3.8 User Accounts

- 3.8.1 General user account requirements
 - 3.8.1.1 Every user must have a unique user ID. No shared accounts must be used beyond built-in and system accounts where individual usage can be tracked.
 - 3.8.1.2 The account owner is responsible for protecting data and resources that are proprietary to CESD, respecting privacy considerations where appropriate, operating ethically, and following security and legal procedures.
 - 3.8.1.3 Account settings should be configured such that files owned by that account are not world-accessible or other-accessible (for reading, write, or executing) by default. The account owner can modify accessibility as needed.

CESD ISMS Policies and Controls

- 3.8.1.4 Upon employment termination, all accounts belonging to exiting CESD Workers must be disabled or deleted on their departure date.
- 3.8.1.5 When an account is removed, files associated with the account must be transferred as instructed by the request. If specific instructions were not received, the files must be archived on tape or other approved backup media and then deleted from the system.
- 3.8.1.6 On a quarterly basis all user accounts must be reconciled. Any account that is not owned must be removed. Any account that is not sponsored, is not valid, or has not been accessed during the prior 90 calendar days or longer must be disabled.
- 3.8.2 CESD Sponsored user accounts including SSO
 - 3.8.2.1 A CESD employee should sponsor all accounts on CESD-managed systems assigned to Third Party CESD Workers
 - 3.8.2.2 The full name of the CESD employee sponsoring the account should be included in the account profile in readable form such that the account can be easily identified as the responsibility of that employee.
 - 3.8.2.3 The CESD account sponsor is jointly responsible with the owner for protecting CESD data and resources.
 - 3.8.2.4 When a Third Party CESD Worker leaves or is no longer actively engaged on a CESD project, it is the responsibility of Third Party to inform the CESD Sponsor to initiate account termination activities.
 - 3.8.2.5 Disabled accounts must not be re-enabled until sponsored by a CESD employee.

3.9 Password Policy

- 3.9.1 For CESD systems, <http://security.CESD.com/> explains the password policy. Third Party account access must match or exceed CESD or industry standard password management, and include audits for:
 - 3.9.1.1 Minimum password length and complexity .
 - 3.9.1.2 Account login failure lockout (example: 5 failures, timeouts).
 - 3.9.1.3 No shared or group passwords.
 - 3.9.1.4 Required encryption during network transmission.
 - 3.9.1.5 One-way hash if stored (example: SHA-1).
 - 3.9.1.6 Two-factor authentication is preferred and may be required for some applications such as remote access.
- 3.9.2 When an administrator assigns a temporary password to an account, the user should be forced to change the password at the first sign-on.

3.10 Application Security

- 3.10.1 Third Party must incorporate information security testing checkpoints into the software development lifecycle.

CESD ISMS Policies and Controls

- 3.10.2 Third Party must train developers in application information security and provide quantitative feedback on common vulnerabilities found along with prevention and remediation measures.

3.10.2.1 Follow the *CESD Application Security Guidelines* (see *CESD Application COE SupportCentral* and *Appendix checklist*) and stay informed of common vulnerability types at OWASP (owasp.org).

- 3.10.3 Third Party must follow standard application account security procedures.

3.10.3.1 A secure process should be in place for distributing first-time passwords. First time password should be unique, randomly generated, not publicly available, and may only function one time.

3.10.3.2 The system should force a password change upon a user's first login. The permanently selected password may not be the same as the first time password.

3.10.3.3 An account lockout should be in place whereby the user's account is locked after a certain number of unsuccessful attempts.

3.10.3.4 A user may reset or reactivate their password by answering a challenge/response or requiring that a new one-time use password be sent to the user's e-mail address. The username should not be present in this e-mail.

3.10.3.5 Auditing and logging procedures should be in place for all account access.

3.10.3.6 A process should be in place for account disablement. Third Party should have a process to immediately disable an account in an emergency situation (within 10 minutes) as well as a process for normal account retirement.

3.10.3.7 Password aging should be in place for all accounts, with password changes forced at least yearly.

3.10.3.8 After the third set of failed login attempts, the account should be permanently disabled and the user should contact the customer service/help desk to reestablish the account.

3.10.3.9 Administrative accounts should be automatically disabled when an administrator no longer requires access to systems or applications or terminate employment with the Third Party.

3.10.3.10 Third Party should perform administrative account audits at least quarterly. Audits should identify and disable accounts that are not actively administering the system or accounts that no longer require access to the systems or networks.

3.10.3.11 At CESD's request, Third Party should provide an inventory, for each application or system that accesses CESD Data, of all

CESD ISMS Policies and Controls

application roles, a description of each role and how many active users are assigned to each role.

4 Network Connectivity Security Requirements

4.1 Third Party Type and Audit

4.1.1 Based upon CESD business access type and security requirements, use the *Secure Transfer of Information Policy* to assess access security controls are adequate and can be audited.

4.1.1.1 The Third Party upon request must provide copies of relevant security policy, process, and procedure documents to CESD for review and audit purposes. CESD should review and recommend reasonable changes, and supplier must amend the policies or respond with mitigating controls and responses.

4.1.2 Each Third Party Connection should have a termination date that is not more than 18 months from the start of the connection. The CESD Sponsor is responsible for reviewing and either renewing or terminating the connection prior to the termination date. If the connection needs to continue after the termination date, a review of the connection should take place to ensure the correct security measures are in place to meet any new or updated business needs and to utilize new technology. This review should take place prior to the termination date to ensure continued service.

4.2 Third Party Network Transport Requirements

4.2.1 Dedicated Supernet connection or site-to-site VPN from the Third Party parent network to the CESD internal network leveraging existing ISP Internet connectivity is acceptable. Other options such as MPLS require special review and approval by the CESD Technology Services Director. The following are the site-to-site requirements.

4.2.1.1 Use a screening device that allows only VPN IPSec protocols (IP 50/UDP 500/ping) to the Third Party-side termination point. This may be a firewall or router ACLs.

4.2.1.2 Periodic audit should include external scans of the Internet-reachable devices used to build the VPN tunnel

4.2.1.3 No unencrypted sensitive CESD traffic transits over the Internet.

4.3 Basic Third Party Access Requirements

4.3.1 A site-to-site connection between the Third Party network and CESD internal network should have a firewall.

CESD ISMS Policies and Controls

- 4.3.1.1 The CESD firewall should be on the CESD network in a CESD-controlled facility. Since it is a CESD internal firewall, it must not be visible to the Internet.
- 4.3.1.2 The interface between the Third Party and CESD should be monitored for inappropriate activity using intrusion detection or preferably prevention systems (NIDS/NIPS) or monitored firewall IDS/IPS.
- 4.3.1.3 It is recommended that the Third Party protect its internal network from CESD by implementing a Third Party-managed firewall with Least Access rules.
- 4.3.2 Access to and from CESD to the Third Party network should be reviewed and approved by the CESD Technology Services Director
 - 4.3.2.1 Rules should specify IP-to-IP access with specific ports and protocols.
 - 4.3.2.2 Third Party and CESD should not use NetBIOS protocols (for example 135/137/138/139/445).
 - 4.3.2.3 CESD should not allow Basic Third Party access to corporate shared resources such as internal instant messaging, email, DNS, and shared web portals.
- 4.3.3 A site-to-site connection between Third Party network and CESD internal network requires NAT of CESD internal addresses.
 - 4.3.3.1 CESD internal address space (such as 10.0.0.0/8) may not be routed into the Third Party network. NAT CESD addresses to either RFC1918 or CESD-assigned address.
 - 4.3.3.2 Third Parties address space should not be translated. It should be registered address space that is not accessible from the Internet. This enables simpler identification of network traffic.

4.4 Trusted Third Party Access Requirements

- 4.4.1 Outbound Gateways (Internet access) and Inbound Gateways (Hosting)—subscribe to an existing CESD shared service, e.g. Supernet VLAN.
- 4.4.2 Wireless LAN—Third Party should follow the CESD Wireless LAN Policy.
- 4.4.3 Vulnerability detection and prevention—anti-virus with updates no more than a day old for all Windows systems, personal firewall for all desktop/laptop, patching for all systems.
- 4.4.4 CESD Security Metrics—report monthly through the CESD Technology Services Director of security defects and opportunities

CESD ISMS Policies and Controls

(contact CESD Technology Services Director for details and process).

- 4.4.5 Physical Security—access restricted to Third Party CESD Workers assigned to CESD contracts and briefed on CESD acceptable use policies.

4.5 Trusted Third Party Network Architecture

- 4.5.1 All current and new connections between the Trusted Third Party network and any other network, including the Internet and other companies, should be managed by CESD and should meet CESD standards and requirements for these types of connections.
- 4.5.2 The Trusted Third Party Network by default is a standalone group of subnets with no physical or logical connectivity to any network other than the CESD network. Where practicable, the business network of the Third Party should not share layer-2 switches. CESD has approved outbound connections to a CESD-dedicated parent email server on a case-by-case basis using a CESD-managed Basic Third Party firewall separating the Third Party CESD network from the Third Party parent network.
- 4.5.3 Firewall filtering rules are recommended between the Trusted Third Party Network and the CESD network to limit the access from the Trusted Third Party Network to only the systems needed to implement the business function. These filters should also ensure that all traffic destined for the CESD network originated on the Trusted Third Party Network.
- 4.5.4 The address given to the Trusted Third Party Network is dependent on the work being done by the Trusted Third Party for CESD and the access needed.
 - 4.5.4.1 If the work is being performed for a for a specific function or service then use addresses that are registered to the Third Party but not publicly routed
 - 4.5.4.2 Although discouraged, a CESD address can be provided. A joint venture managed and treated as a part of a CESD business is an example.
- 4.5.5 It is recommended that the interface between CESD and the 3rd party be monitored for inappropriate activity using intrusion prevention/detection technology.
- 4.5.6 Physical access to the network devices (routers, hubs, switches, etc.) should be protected to allow access only by CESD approved network administrators and CESD-approved Third Party staff.
- 4.5.7 The Trusted Third Party should scan their network and systems at least weekly. All machines with vulnerabilities should at a minimum

CESD ISMS Policies and Controls

be updated with. Security metrics for systems on the network should be reported monthly to the CESD Technology Services Director.

- 4.5.8 Network ownership for reporting and incident response should be assigned to the CESD IT department.
- 4.5.9 Remote access is only allowed through the CESD virtual desktop infrastructure.
- 4.5.10 Modem access (dial-up or ISDN) to the Trusted Third Party Network is prohibited except for CESD out-of-band management access of critical systems, in conformance with CESD guidelines.

4.6 Trusted Third Party Email Servers

- 4.6.1 Manage attachment types in email, with periodic updates to be issued by the CESD Technology Services Director. Restrictions may be placed on the types of email file attachments that should be permitted when using company email. The restrictions apply to incoming and outgoing messages, both internal to CESD and to/from external addresses. Attachments of most of the common file types are permitted. These include: Word (.doc), Excel (.xls), PowerPoint (.ppt), Images (e.g., .jpg) and PKZIP (.zip). HTTP links embedded in the email pointing to internal or external web addresses are also permitted.
 - 4.6.1.1 Third Party should block
ade;adp;app;asf;asx;bas;bat;bz2;chm;cmd;cnt;com;cpl;crt;dll;eml;exe;fxp;hlp;hta;inf;ins;isp;js;jse;lnk;mdb;mde;mht;msc;msi;msp;mst;pcd;pif;prg;rar;reg;scr;sct;shb;shs;url;vb;vbe;vbs;wmd;wsf;wsc;wsh.
- 4.6.2 CESD internal service email servers are preferred for *CESD Confidential* Private business processes. These accounts have chinooksedge.ab.ca email addresses.
- 4.6.3 For internal administrative or automated email, CESD can provide a CESD shared email server on the Trusted Third Party Network for non-sensitive communications and business processes. The CESD Technology Services Director should approve use.
- 4.6.4 The CESD Sponsor or CESD Technology Services Director should set up a process for email account creation/deletion for CESD mailboxes.

5 Appendix

5.1 Appendix A: CESD Standard

[Link to Information Sensitivity Classification](#) below

CESD ISMS Policies and Controls

5.2 Appendix B: CESD Acceptable Use Guidelines


[Link to CESD Acceptable Use Guidelines below](#)

5.3 Appendix C: CESD Supplier Checklist

[Link to CESD Supplier Checklist below](#)

Please find these Appendices at
https://drive.google.com/drive/folders/1MJui2AKvrf_smmmapGjmXTymOpe4_Xfvh?usp=sharing

The Chinook's Edge School Division*ISMS Procedures and Controls***Secure Transfer of Information**

Reference No. xx	Revision No. 1	Relevant ISO Control No. 10.8.2	
Issue Date: January 20, 2012			
Revision Date: January 20, 2012			
Approved by: Ted Harvey Title: Director, Technology Services			

Version History

Version #	Version Date	Author	Summary of Changes
1.0	20 Jan 2012	Ted Harvey	Document Creation

Approvals

Name	Title	Date of Approval	Version No.
Ray Hoppins	Associate Superintendent, System Services		

Distribution

Name	Title	Date of Issue	Version No.

Document Control

Document Title	Secure Transfer of Information
Document Location	http://xxx.cesd73.ca/

Table of Contents

1.0. Overview.....	3
2.0. Purpose.....	3
3.0. Scope	3
4.0. Risks	4
4.1. Is the transfer legal and necessary?	4
4.2. Is it Personal information?	4
4.3. Before you make any transfer you must:	4
5.0. Policy Detail	5
5.1. User responsibilities.....	5
5.1.1. IT Auditor	6
5.1.2. Departmental Managers.....	6
5.1.3. Individual employees	6
5.1.4. Departmental Information Management Specialists.	6
<i>For example, Records Manager, Student Information Manager, etc.</i>	6
5.2. Requirements for Transferring Personal or Confidential Information.....	6
5.2.1. Electronic Mail	6
5.2.2. Electronic Data Transfer (FTP, Secure FTP, Edulink)	7
5.2.3. Electronic memory (CD, DVD, Floppy, USB drive, Memory Card)	7
5.2.4. FAX Transmission	8
5.2.5. Delivery by Post or by Hand.....	8
5.2.6. Telephone/Mobile Phone	9
5.2.7. Internet Based Collaborative Sites	9
5.2.8. Text messaging (SMS), Third Party Instant Messaging (IM)	9
6.0. Enforcement.....	10
7.0. Policy Governance	10
8.0. Definitions.....	11
9.0. References	11
Appendix 1 - The principles of data protection	12

1.0. Overview

2.0. Purpose

There are many occasions when information is transferred between departments, to third-party service providers, to other public bodies, commercial organizations and individuals. This is done using a wide variety of media and methods, in electronic and paper format.

In every transfer there is a risk that the information may be lost, misappropriated or accidentally released. The Division has a duty of care in handling information. Recent high-profile losses have highlighted this.

For legal reasons such as confidentiality or data protection, and to maintain the trust of our users and partners it is essential that transfers are performed in a way that adequately protects the information. It is the role of the Sender to assess the risks and ensure that adequate controls are in place. This policy outlines the responsibilities attached and the minimum-security requirements for transfer.

3.0. Scope

This policy states the minimum-security requirements for physical transfer of information into, across and out of the organization, in any format.

For the purpose of this document, Information refers to both textual information (e.g. word-processed documents, reports and spreadsheets), and raw unformatted data (e.g. backup tapes), in any format and on any medium.

This policy applies to all employees of CESD and any Third-party that processes the organization's information.

Exclusions

This policy does not cover the transfer of information via the internally created automated Student Information Framework, which has its own automated security controls.

4.0. Risks

The sender's responsibility

With any information transfer there is a risk that the information may be lost, misappropriated or accidentally released. It is the responsibility of the sender to assess all risks and ensure that adequate controls are in compliance with this policy. This section contains some of the things that must be considered before transferring information.

If in doubt, contact your FOIP Officer or CESD IT department.

4.1. Is the transfer legal and necessary?

It is dangerous to assume that because someone asks for information that they are necessarily authorized or legally entitled to have it. If you are in doubt then you should check with your Principal or department head.

Once you are sure that the transfer is legal and necessary then you must decide what kind of information you are dealing with. This will determine what security is appropriate. Information classification can be determined by consulting the Information Sensitivity Procedure.

To transfer personal or confidential information without these checks may leave the Division open to Legal and Reputational damage and the sender may be subject to disciplinary and legal action.

4.2. Is it Private information?

Private information is about a living, identifiable individual. It could contains details of racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission of offences, court appearances and sentences.

Anything we do with private personal information must comply with the Alberta Freedom of Information and Privacy Protection Act. Basic requirements of the Act are listed at the Alberta FOIP website at <http://www.servicealberta.ca/foip>. If in doubt contact the FOIP Officer.

4.3. Before you make any transfer you must:

- Where appropriate, ensure the Communications Officer approves transfers to any Media organizations.
- Obtain and document the approval of the Data Owner for transfer.
- Ensure that the transfer is legal (in particular under the FOIP Act).
- Ensure that the transfer is necessary (is there a less intrusive way)

Remove or redact anything that is not essential for the recipient's purpose
Have a documented agreement in place to ensure the recipient understands their responsibilities under the law, particularly what to do with the transfer file after they have extracted the information to their system. Recommend destruction of sent file after extraction of the information.

5.0. Policy Detail

The organization recognizes its responsibility to process its information correctly and in line with all legal, regulatory and internal policy requirements.

It is the Sender's responsibility to risk assess what they are intending to do and ensure that all associated risks are adequately understood and covered, and that the transfer is properly authorized. The baseline security requirements for various methods are listed below.

The IT department will monitor compliance with this Policy.

If a user is found to have breached this policy, they may be subject to disciplinary procedure. If they have broken the law then they may be subject to prosecution.

If a user does not understand the implications of this policy or how it may apply to them, they should seek advice from, either their principal, the Director of Technology Services or the FOIP officer.

5.1. User responsibilities

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

- The Sender The Sender is responsible for ensuring the following requirements of this Policy are met:
 - Assessing the information to be sent is in accordance with this policy.
 - Ensuring that the identity and authorization of the recipient has been formally confirmed and documented.
 - Obtaining the consent of the Data Owner for the transfer.
 - Ensuring that the information is sent and tracked in an appropriate manner in compliance with this policy.
 - Follow up to make sure recipient is in receipt of information. (Triple check email address in destination box!)

5.1.1. IT Auditor

The IT department will monitor and audit departments to ensure compliance with all statutory and regulatory obligations, and internal policies.

5.1.2. Departmental Managers

Principals and department managers are responsible for ensuring that this Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing or funding are communicated back to their liaison superintendents in a timely manner.

5.1.3. Individual employees

Individual employees will be responsible for familiarizing themselves with this Policy and ensuring that any information transfer for which they are responsible is done in a compliant manner.

Individual employees must report any suspected or actual security breaches related to data transfer in line with the Organizations Incident Management Policy.

5.1.4. Information Management Specialists.

For example, Records Manager, Student Information Manager, etc.

The IT department will provide first line advice to departments on Information Transfer related issues.

5.2. Requirements for Transferring Personal or Confidential Information

Having decided what kind of information you have, and prepared it for transfer, the sender must consider the various methods of transfer available and whether they are appropriate. This section lists the main methods and sets out any restrictions and the requirements for secure transfer of Personal or Confidential information.

For all transfers of Personal or Confidential information, it is essential that the sender has authenticated the identity and authorization of the recipient.

5.2.1. Electronic Mail

Information must be enclosed in an attachment and encrypted using 7-zip (a product approved by the Division) set at a minimum encryption level of AES (256 bit).

- Any password must be to CESD standard. Further details of the password policy can be found in the CESD Password Policy document.
- Any password to open the attached file must be transferred to the recipient using a different method than the same e-mail, or a telephone call to an agreed telephone number, closed letter, etc.
- E-mail message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipients. This can be included within the sender's signature.
- An accompanying message and the filename must not reveal the contents of the encrypted file.
- Check with the recipient that their e-mail system will not filter out or quarantine the transferred file.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to the IT department immediately.

5.2.2. Electronic Data Transfer (FTP, Secure FTP, Edulink)

Standard FTP without encryption is inherently insecure and should not be used for transmitting private or confidential information.

SFTP (secure FTP) file transfers are acceptable but such transfers must be set up and administered by the Information Technology department.

External secure transmission systems such as the Edulink system are designed to be secure provided that they are implemented configured and used correctly. However, it is the responsibility of the sender to ensure that the use of such a system is appropriate for the use they propose. If in doubt, advice should be sought from the system owner.

5.2.3. Electronic memory (CD, DVD, Floppy, USB drive, Memory Card)

- Information in a file or the media must be encrypted using a product approved by the Division
- Any password must be to CESD standard. Further details of the password policy can be found in the CESD Password

Procedure document.

- Any password to open the attached file must be transferred to the recipient using a different e-mail, or a telephone call to an agreed telephone number, closed letter, etc.
- An accompanying message should contain clear instructions on the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.
- An accompanying message and the filename must not reveal the contents of the encrypted file.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

5.2.4. FAX Transmission

FAX is inherently insecure and is not recommended for transfer of sensitive information. However it is acknowledged that certain circumstances demand it.

- Sender must check that the Fax number is correct and that the receiver is awaiting transmission.
- For high sensitivity information the number must be double-checked by a colleague before transmission, or pre-stored in the machine and telephone contact should be maintained throughout transmission.
- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine, and a clear requirement to securely destroy the message when no longer required.
- The message should contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipients.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their principal or manager.

5.2.5. Delivery by Post or by Hand

It is essential that the file, whether electronic or paper is kept

secure in transit, tracked during transit, and delivered to the correct individual.

- An appropriate delivery mechanism must be used.
- Package must be securely and appropriately packed, clearly labelled and have a seal, which must be broken to open the package.
- Package must have a return address and contact details.
- The label must not indicate the nature or value of the contents.
- Package must be received and signed for by addressee.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their principal or manager.

5.2.6. Telephone/Mobile Phone

As phone calls may be monitored, overheard or intercepted either deliberately or accidentally, care must be taken as follows.

- Transferred information must be kept to a minimum.
- Private or Confidential information must not be transferred over the telephone unless the identity and authorization of the receiver has been appropriately confirmed.
- Phone calls transferring Personal or Confidential information must be conducted in a private location that prevents eavesdropping.

5.2.7. Internet Based Collaborative Sites

Must not be used for Personal or Confidential information.

5.2.8. Text messaging (SMS), Third Party Instant Messaging (IM)

Must not be used for Personal or Confidential information.

Certain departments are free to use an Internal CESD supplied Instant messaging solution, i.e. Jabber.

5.2.9 Printing When printing to a photocopier, use copiers print password feature.

Do not leave Private or confidential hard copies unattended.

6.0. Enforcement

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

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

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

7.0. Policy Governance

The following table identifies who within Chinook's Edge School Division is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

Responsible – the person(s) responsible for developing and implementing the policy.

Accountable – the person who has ultimate accountability and authority for the policy.

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

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

Responsible	Director Technology Services
Accountable	Superintendent System Services
Consulted	Technology Committee, Technology Advisory Group, COLT
Informed	All Employees, All Students, All Temporary Staff, Volunteers, All Contractors.

8.0. Definitions

Requester - Any individual that requests records from a School or CESD department. They may be another department, a service provider, supplier, or an external Agency.

Sender - The Sender is the individual acting for the division that initiates a Data Transfer. They must have the authority, and the sufficient knowledge of the nature of the data to determine whether it should be sent, and that it is sent securely. Where the final actual task is delegated to administrative, untrained or inexperienced staff, the original Sender remains responsible for ensuring the Transfer complies with this policy.

Information Owner - Every major type of record (e.g. Invoices, Purchase Orders, Adoption case files) must be assigned an owner within the Council who will be responsible for it throughout its lifecycle. This Owner may work in any department but must have sufficient ability, authority and experience to understand the contents and approve the processing of the record. Record owners must be formally documented.

9.0. References

List any reference material used

CESD Password Policy

More Content

Appendix 1 - The principles of data protection

Data Protection Guidelines state that anyone processing personal information must comply with Eight Principles of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary for that purpose or those purposes.
6. Shall be processed in accordance with the rights of data subjects under the FOIP Act.
7. Shall be kept secure i.e. protected by an appropriate degree of security.
8. Shall not be transferred to a country or computer system in territory outside of Canada, unless that country or territory is recognized as a safe harbor for data protection.

In most cases the consent of the data subject is required.