

---

Government of Alberta

# CÚRAM

Privacy Impact Assessment

---

Final Report

March 2009

Submitted by:  
Information and Privacy Office  
Employment and Immigration

## Table of Contents

1.	Background .....	1
2.	Purpose of This Review .....	2
3.	Managing Access and System Usage.....	2
4.	Responsible Business Area .....	3
5.	Access to CÚRAM .....	3
6.	Requesting and Revoking Access.....	4
7.	Restricting Access to Information.....	4
8.	Access to Information of Other Ministries.....	6
9.	Information Format.....	6
10.	Privacy Awareness.....	6
11.	Audit Process .....	7
12.	Mitigation of Potential Privacy Impacts.....	8
13.	Conclusion .....	9

## 1. Background

Historically, each ministry has implemented its own systems to support programs, services, provide specialized functionality and financial functions of the Government of Alberta (“GoA”). It is also recognized that each ministry performs similar activities in managing service delivery and financial activities.

The Government of Alberta Enterprise Architecture (“GAEA”) initiative was formed to analyze cross-government business, data, security, privacy, application and technology needs to create a set of ongoing corporate investment/design guidance, blueprints and processes necessary to steer Information and Communications Technology (“ICT”) solutions towards support of corporate strategic goals.

This strategic direction and action will ensure that government and all Albertans realize the most benefit from their investment in ICT, and to make the GoA a leader in innovation and electronic delivery of services to Albertans.

It is envisioned that the implementation of an enterprise solution will allow for the retirement of some of the legacy applications/functionality and integrate common business processes across ministries.

CÚRAM is a Software – Business Application Suite (“CÚRAM”) that provides an integrated service management system which supports multiple programs using consistent and standards based technology and management practices. It will allow ministries to phase out old, stand-alone systems and become more efficient and streamlined. This initiative will simplify processes and improve service to Albertans.

CÚRAM is also web-enabled software that will empower Albertans. It is envisioned that Albertans will have the ability to access program information and update their personal information, assess eligibility for program entitlements, and receive the results of an assessment of eligibility and benefit entitlement for some programs.

CÚRAM is being used around the world to support the delivery of social services. As enhancements are made in other parts of the world to reflect best practices, the GoA will have the opportunity to implement those best practices without having to change current systems or build new ones.

Several GoA ministries have expressed interest in and are working towards implementing CÚRAM. CÚRAM can and likely will be a provider, which means that other applications can communicate with CÚRAM through an open, standards-based mechanism that can serve to enable and enhance information sharing agreements.

It will be critical that as the ministries move forward with their implementation of the software, that attention be paid to a number of areas, including: the need to review and enhance information sharing agreements, and in some cases implement new ones; to the implications on personal information flows as enterprise solutions are considered; and that some thought be given to the implications of the setting up of access rights, and the ability to access information based only on an authority to access, and enhanced by the various levels of security.

A series of programs and their systems will be phased into using CÚRAM across ministries. It is recommended that individual PIAs be completed on a modular basis. The implications on other systems, including cross-government systems and linkages, such as the government Integrated Management Information System (IMAGIS), will need to be reviewed with a view to privacy mitigation.

## **2. Purpose of This Review**

It is each ministry's responsibility to determine its use of the various capabilities built into CÚRAM and to customize and establish policies and practices that support each system being implemented.

This report describes the CÚRAM product, identifies potential privacy implications that may result from usage practices, and defines activities that can be undertaken to mitigate potential privacy impacts.

Alberta Employment and Immigration (AE&I) will be one of the first ministries to adapt the CÚRAM application. This report was prepared in consultation with the CÚRAM Implementation Project Team.

## **3. Managing Access and System Usage**

CÚRAM will be purchased by individual ministries. Each ministry will be responsible for managing implementation, access, security and determining system usage.

AE&I have assessed that CÚRAM meets the GoA Security Standards. As programs and their systems are phased in using CÚRAM it is recommended that ministries undertake the completion of an Information Risk Assessment.

Through customization CÚRAM has the capacity to restrict access to some or all components of a file to only specified roles and/or users.

System administration responsibilities, such as controlling user permissions and the access privilege process, monitoring system usage, training and orienting system users, and dealing with security breaches are typically assigned to a system business sponsor.

Unauthorized collection, use, disclosure and disposition of personal information are considered breaches of privacy.

Security and privacy breaches would be handled in accordance with each ministry's policies and procedures.

#### **4. Responsible Business Area**

It is crucial to identify a business area as responsible for accountability decisions and for the development and implementation of policies, guidelines and/or practices.

#### **5. Access to CÚRAM**

Access to and the use of CÚRAM's various functionalities can be based on roles, user responsibilities (security group) and sensitivity.

CÚRAM enables an extensive list of possible user roles. These roles can be defined and applied to each user authorized to access CÚRAM. The roles can be allocated to such facilities as (but not limited to) system parameter management, security management, financial management, and approvals of client action items.

External providers' views and access to clients and their information may be restricted to a need to know basis. That access can be limited by ensuring that the external provider has a means of validating that they are only accessing information for clients that they are providing a service to. An example is that the client must have provided such information as to authenticate their identity (program ID number, birth date, etc), to the provider, in order for the provider to successfully complete the search and display criteria.

Each ministry will define the roles and make a determination on the openness or restriction of information. Access based on user-roles has to take into consideration the authority of the user to access, and their need-to-know, the personal information.

While CÚRAM has the ability to provide data-level security, based on user role, further restrictions would be available through customization. Ministries will therefore need to determine whether the out-of-the-box provisions sufficiently mitigate any privacy/security concerns. If not, additional processes may need to be put in place, including areas such as heightened auditing processes.

## **6. Requesting and Revoking Access**

Each ministry should develop a 'User Access Policy and Procedures' which outlines the process and responsibility for requesting and revoking access to CÚRAM for ministry staff and third parties. Such a document must be reviewed by staff from privacy and security perspectives as well as a program based need.

A User Access Policy and Procedures would help to ensure that the practices to be followed for the granting or revoking of access to CÚRAM are known by those who have the responsibility for approving the request.

If the ministry has no automated process that alerts those responsible for revoking access to CÚRAM when an individual leaves their position, added security may be invoked by inactivating users that have not signed on to a system in the past 60 days.

At a minimum, the responsible business area should outline the decision making process, generally predicated on the user roles, but also outlining exceptions, if any are to be allowed. This will help to ensure that request forms for the granting of access to users are completed and approved appropriately.

An access request form may provide those responsible for granting access to CÚRAM with the necessary information to assign the proper access role to an individual or group. This information is useful for maintaining consistent access practices as CÚRAM administration personnel can change over time.

## **7. Restricting Access to Information**

Access to information can be based on role, user responsibilities (security group) and sensitivity. The degree of access granted should be based on the amount of information that can be viewed, updated and accessed.

The extent of the access granted should be based on the user's job responsibilities and authority to access and use the personal information.

As separate programs are brought into CÚRAM a determination will need to be made as to whether the information is required to be maintained separately.

Sensitivity security provides a means of securing all data that must be reserved for viewing by a small number of users. This is accomplished by assigning a sensitivity level to the sensitive data. Users are only permitted to view the secured data if their sensitivity level is equal to or higher than the specific data. By definition, personal information is sensitive, so it will be important that each ministry determines the level of sensitivity that needs to be attached to the information elements.

The end result will be a matrix approach to the management of the personal information in a way that offers appropriate protection from a security and privacy perspective.

Each ministry is responsible to designate Security Administrators to manage the approval process, and monitor the accuracy of the setup and removal of access to the system.

System security processes both in the application and the network prevent unauthorized access to information. This includes:

- Physical server security
- Multi-tiered zones of network access controlled by firewalls
- Strict access controls
- Stringent password requirements
- Use of 128-bit SSL for browser communication
- Continual intrusion detection monitoring
- Logging of access and user activities, including read or view only access

A key component of CÚRAM's security configuration is the use of the GoA's Alberta Secure Access Service (ASAS). This facility can be utilized to control access by users throughout the world-wide web. CÚRAM being a web-based application, enables service providers to access ministry repository of services and service management facilities through the internet. By following the GoA's practices for the use of ASAS, access to CÚRAM meets the security standards defined by the GoA's security policies.

To enhance the security and access rights provided by ASAS a ministry can create an application security component to broker web requests to the

applications required by the web user that entered the system via ASAS. This ensures that the web user has been granted the rights to access CÚRAM and the information allocated to the user's role.

## **8. Access to Information of Other Ministries**

At this time Ministries will only be able to access the personal information that their ministry is responsible for.

CÚRAM can and likely will be a provider, which means that other applications can communicate with CÚRAM through an open, standards-based mechanism that can serve to enable and enhance information sharing agreements. It will be critical that as the ministries move forward with their implementation of the software, that attention be paid to a number of areas, including: the need to review and enhance information sharing agreements, and in some cases implement new ones; to the implications on personal information flows as enterprise solutions are considered; and that some thought be given to the implications of the setting up of access rights, and the ability to access information based only on an authority to access, and enhanced by the various levels of security.

## **9. Information Format**

To streamline the efficiencies of sharing information for common program information sharing agreements between ministries, good business practice would be a collaboration of ministries on the format of information being collected to insure an effective interfacing in the future.

## **10. Privacy Awareness**

GoA employees and individuals deemed employees under the *Freedom of Information and Protection of Privacy Act* or the *Health Information Act* have an obligation to ensure that discretion and judgment is exercised when using information. Those obligations are reflected in the "A Guide for Government of Alberta Employees".

Unauthorized collection, use, disclosure and disposition of, personal information are considered breaches of privacy. Staff should use CÚRAM:

- In accordance with the *Code of Conduct and Ethics for the Public Service of Alberta*, the *Official Oath* and the *Freedom of Information and Protection of Privacy Act*. The URLs are:  
<http://www.pao.gov.ab.ca/Practitioners/?file=legreg/code/titlepage>

<http://www.pao.gov.ab.ca/staff/oath/Official-Oath.pdf>  
<http://foip.gov.ab.ca/>

- In a manner that will protect the confidentiality of the personal information.
- In a manner consistent with professional conduct.

Where there are instances or indications of unauthorized access, use, or disclosure, individual access will be revoked. Depending on the severity of the circumstances, disciplinary actions up to and including dismissal, or contractual sanctions, may be taken.

GoA IT Baseline Security Requirements document is being updated and will be available at <http://www.sharp.gov.ab.ca>

## 11. Audit Process

Auditing is supported on most CÚRAM entity operations with the exception of some batch processes which, normally, have built in audit functions. The information captured by table level auditing is stored in the database audit table.

Table level auditing is enabled by switching on this database function. This causes the generated data-access code to record audit information for an operation. The type of audit information is configurable and can include a trace of the SQL operations (purely technical) or be extended to include the information of the new and old versions of the records.

The following information is captured within the audit log as needed:

- Date and time - The date and time of the transaction.
- User ID - The ID of the user who invoked the transaction.
- Table name - The name of the database table which was modified.
- Program name - The FID of the function which invoked the transaction.
- Transaction type - Indicates whether the transaction was online / batch /deferred / etc.
- Key info - The key which was provided to this operation. Note that this may identify one or many records.
- Details of changed data - These details are logged in an XML format.
- Operation type - Indicates whether the operation was one of: create, read, update or delete.

A regular audit process and reporting mechanism is required with dedicated resources if a ministry chooses an open system concept where access is only restricted by role and sensitivity and not by individual user.

## **12. Mitigation of Potential Privacy Impacts**

CÚRAM has the capability of restricting access by role, sensitivity and use by user. Access restriction by individual or by file would require customization of the application. If a ministry chooses to have an open system with restricted access by only role and sensitivity and not by individual user or by file, processes should be in place to regularly audit usage with a reporting mechanism. There would need to be a clear understanding by staff as to their responsibility and authorization and the consequences of unauthorized access, use or disclosure.

The CÚRAM application has the capability of using the back button to return to previous information, allows several windows to be opened with information active on the desktop and provides an auto-fill sign in. For security purposes ministries may choose to disable these features.

Any ministry that uses or implements CÚRAM should develop and implement a Privacy Framework that at a minimum outlines training, consults, Privacy Impact Assessments, monitoring and breach reporting.

The development of a 'User Access Policy and Procedures' is recommended that outlines the process for requesting and revoking access, privacy and security policies, and the audit process if implemented.

A Privacy Impact Assessment should be completed on each legacy system being integrated into CÚRAM and any new systems created.

### **13. Conclusion**

Technical safeguards and good intentions are not enough to ensure the appropriate use of CÚRAM and the protection of personal information.

As old systems are closed and created using CÚRAM each ministry should identify and address potential risks to individual privacy that may occur in the course of its operations. Conducting a Privacy Impact Assessment on each system to be integrated or created is good business practice.

The GoA is committed to protecting the security, confidentiality, integrity and availability of information resources. The GoA supports the principle that security is a responsibility shared by all users of the system. Awareness of privacy and security features reduces the risk of human error, theft, fraud and the misuse of information.