
Alberta Employment and Immigration

ALBERTA WORKS ENTERPRISE SOLUTION PROJECT

MOBIUS

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	5
3.	Responsible Public Body.....	5
4.	Responsible Business Area	5
5.	Contact Person	5
6.	AWES Project	5
7.	Managing Access and System Usage.....	8
8.	Access to MOBIUS	9
9.	Requesting and Revoking Access.....	14
10.	Restricting Access to Information.....	15
	10.1 Eligibility	15
	10.2 Role	15
	10.3 MOBIUS User Security Group.....	16
	10.4 MOBIUS Sensitivity security.....	16
11.	Access to Information of Other Ministries.....	17
12.	Privacy Awareness.....	17
13.	Audit Process.....	18
14.	Mitigation of Potential Privacy Impacts.....	19
15.	Conclusion	21
APPENDIX 1	CÚRAM PIA.....	22
APPENDIX 2	Request for Mobius ID - Internal Users.....	22
APPENDIX 3	Request for Mobius ID - External Users.....	22
APPENDIX 4	Draft Acknowledgement of AppropriateUse of the Mobius System for Internal	22
APPENDIX 5	Mobius Update November 6, 2008	22

1. Background

The Government of Alberta Enterprise Architecture (“GAEA”) initiative was initiated 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.

These strategic directions and actions will ensure that government and all Albertans get the most benefit from their investment in ICT, and to make the Government of Alberta (“GoA”) a leader in innovation and electronic delivery of services to Albertans.

The GoA developed a 10-year strategic plan called “*Building and Educating Tomorrow’s Workforce*”. This strategy outlines how government, business and industry, training providers and communities must work together to meet skill and labour shortages and ensure the province remains globally competitive, and identifies 17 priority actions which require government leadership. Alberta Employment, Immigration and Industry (“AE&I”) is the lead in 13 of these priorities.

The strategy centres around four main themes:

- **Inform** Albertans and employers about education and labour market issues, initiatives, and opportunities.
- **Attract** people to Alberta.
- **Develop** the knowledge and skills of Albertans, as well as innovative work environments.
- **Retain** people in Alberta’s workforce.

Alberta Works is an AE&I initiative designed to assist Albertans find and keep jobs, assist low-income Albertans cover their basic costs of living, and assist employers meet their need for skilled workers. AE&I is repositioning, from a department that administers programs and provides financial assistance to low income Albertans, to one that works in partnership to attract Albertans to the workplace. Partners of the Alberta Government include industry, business (including the private and public sectors and the public service), labour groups, professional associations, volunteer and community agencies, education and training providers, and where appropriate, other orders of government.

This repositioning depends on the integration of a number of programs and relies on the sharing of information across the programs and services. This will enable staff to do more value added work such as helping Albertans with their action plans and working with employers. It will also improve client access to our services and programs.

Alberta Works' goals are achieved through its four program areas; Employment and Training Services, Income Support, Health Benefits and Child Support Services. These programs are brought together under the umbrella of Alberta Works.

☐
[Income Support](#)

Income Support provides financial benefits to individuals and families who do not have the resources to meet their basic needs, like food, clothing and shelter.

[Child Support Services](#)

Child Support Services helps single parents and parents living in blended families get the legal agreements or court orders they need to obtain child support.

[Health Benefits](#)

Through Alberta Works, people who are eligible for income support receive health benefits for themselves and their dependants.

☐
[Financial Support for Training](#)

Tuition, books and supplies, and living allowance may be available if you qualify as an eligible learner.

[Alberta Works...for farmers](#)

A program to help farm families through brief periods of financial difficulty.

[Alberta Works Regulations & Legislation](#)

Regulations and legislation governing the Alberta Works program.

[Alberta Works Publications](#)

Information publications related to the Alberta Works program.

In order to bring together these programs to support the GAEA initiative and Building and Auctioning Tomorrow's Workforce, AE&I required a new system that would integrate existing systems and automate many business processes.

AE&I issued a Request For Information to collect information on the availability of Enterprise Solution Software to support AE&I's Alberta Works' programs and services. Based on the information collected, AE&I submitted a Request For Proposals for the AE&I Alberta Works Enterprise Solution ("AWES") project.

IBM was the successful vendor and will be using the CÚRAM Software – Business Application Suite ("CÚRAM") that provides an integrated service management system which supports multiple programs using a consistent and standards based technology and management practices. (refer to CÚRAM PIA *Appendix 1*). AE&I has entered into contracts with IBM and CÚRAM.

AWES is expected to provide an integrated system through the implementation of CÚRAM that will support the ongoing evolution of Alberta Works' programs and services delivery model. This integrated system has been named MOBIUS. It is expected to reduce program administration time required from AE&I and Delivery Partner staff, and provide them with the automation support and information required to support this repositioning and to enhance service delivery to Albertans.

The enhancement of service delivery to Albertans aligns with the Priority Actions in Building and Educating Tomorrow's Workforce, eg.

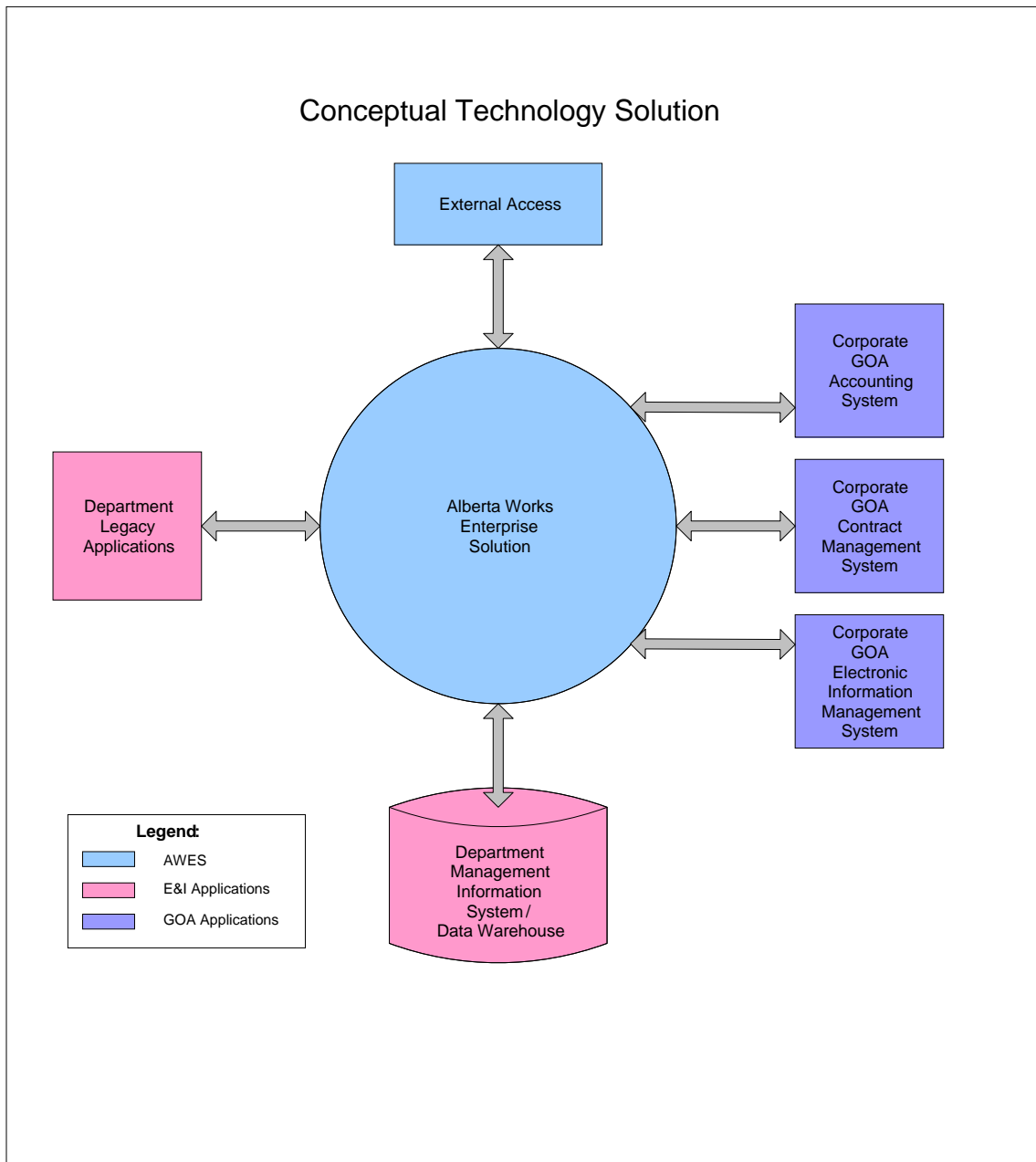
- Provide quality information to Albertans, business and industry on prominent labour force issues and human resource best practices, market opportunities and program supports.
- Provide enhanced information to Albertans regarding career, education and training opportunities, as well as resources and tools available to support career and educational decisions.

AE&I has a number of legacy applications that support specific AE&I programs and services or provide specialized functionality. They are typically standalone applications with their own database.

It is envisioned that the implementation of MOBIUS will allow for the retirement of some of the legacy applications/functionality over time. The project will be accomplished over a period of 4 to 5 years. The objectives of this project will be achieved through a phased approach.

Until the project is complete, it is expected that some standalone applications will remain and require bi-directional interfaces.

The implementation of the Enterprise Solution will probably overlap with the concurrent running of the existing legacy application(s) for certain functionality and/or access to historical data.



2. Purpose of This Review

This report describes the AWES project and the integrated system - MOBIUS, identifies potential privacy implications that may result from usage practices, and defines activities that can be undertaken to mitigate potential privacy impacts.

AE&I is one of the first ministries to adapt CÚRAM for their AWES project. This report was prepared in consultation with the CÚRAM Implementation Project Team.

3. Responsible Public Body

AE&I is the responsible public body for the AWES project and the MOBIUS integrated system.

4. Responsible Business Area

Business Innovations, Business Processes and Systems is the business area responsible for accountability decisions and for the development and implementation of policies, guidelines and/or practices.

5. Contact Person

The following individual can answer questions about the project.

Director, Projects
Information Management and Application Support
Employment and Immigration
5th Floor, Centre West Building
10035 – 108 Street
Edmonton, AB T5K 3E1
Tel. 780 644-0001

6. AWES Project

The complete AWES Project will support core functionality for three major business streams. These streams are identified as:

INDIVIDUAL SERVICE MANAGEMENT	EMPLOYER SERVICE MANAGEMENT	PROGRAM , SERVICE & BENEFIT MANAGEMENT
INFORMATION	INFORMATION	REGISTRATION AND SERVICE & BENEFIT SETUP
REGISTRATION	REGISTRATION	PROGRAM, SERVICE & BENEFIT CAPACITY PLANNING
ASSESSMENT	ASSESSMENT	PROVIDER PARTNERSHIP PLANNING
INVESTMENT PLANNING	PARTNERSHIP PLANNING	PROGRAM, SERVICE & BENEFIT ALLOCATIONS
APPLICATION, APPROVAL AND ENROLLMENT	APPLICATION, APPROVAL AND ENROLLMENT	PROGRESS MONITORING AND ADJUSTMENT
CLIENT MANAGEMENT	PLACEMENT AND PROGRAM TRACKING	PROGRAM, SERVICE & BENEFIT EVALUATION
FINANCIAL MANAGEMENT	FINANCIAL MANAGEMENT	PROGRAM, SERVICE & BENEFIT MAINTENANCE

- Individual service management** – Involves registering Individuals, performing assessments, establishing investment plans, providing benefits and services to ensure Individuals meet their needs and/or attain their goals, and managing the Individual’s participation in AE&I programs;
- Employer service management** – Involves registering employers, establishing partnership plans that reflect their labour market needs and goals, and managing the employer’s participation in AE&I programs;
- Program, service & benefit management** – Provides for the creation and maintenance of a programs and services catalogue, and supports AE&I, delivery partners, community service providers and clients in performing program and service management activities.

Programs and services will be registered and business policies and rules will be established in the system.

The business objectives of the AWES Initiative are to implement MOBIUS to:

- Significantly automate the routine functions of service delivery through application, eligibility determination, benefits calculations, financial benefits administration, and case management.
- Support a service delivery model in which Investment Plans can be created in conjunction with individuals and organizations, and the completion of those activities can be tracked and measured to ensure accountability.
- Enhance the processes of assessment, planning, and outcomes measurement, and make it possible to enhance collaboration with partners in these processes.
- Provide a comprehensive history of individual client information and all interactions with Alberta Works and affiliated partners.
- Provide a detailed comprehensive history of all interactions of household members, and changes in household composition, with Alberta Works.
- Support the department's repositioning through the capture of relevant detailed information on organizations, initially about delivery partners and in the future about employers, industry associations, and program delivery partners in support of new programs and services delivered through industry partnerships.
- Capture individual, employer, and program information once and, with the appropriate approvals and authorities, and make it available throughout the system for use in downstream processes.
- Support continuous improvement and streamlining of programs, services and processes through appropriate monitoring and outcomes reporting. Provide flexibility to support changes to program and service composition and business rules.

7. Managing Access and System Usage

AWES through MOBIUS will support delivery of programs and services which are based on the following:

- AE&I processes recognize the variety of Albertans /employers / organizations, their preferences, competencies and their diversity. Processes will recognize and leverage client capacities and support their growth towards independence and self-reliance.
- Albertans/employers/organizations will have the ability to access program information and update their personal information, assess eligibility for program entitlements, self manage, and self refer to services from government and service providers through multi-channel access (Internet, call center, Interactive Voice Recognition technology, in person, print, etc.).
- Information will be accessible by the individual Albertan / employer / organization through electronic access and safeguards based on user roles thus ensuring the appropriate level of privacy and confidentiality around that information managed by the ministry.
- Data will be utilized by many programs, subject to access rights, user roles and authority, thereby supporting the concept of “collect it once and use it many times”.
- The Case Management system is the beginning point for services and should be able to draw on and exchange data from internal and external systems to provide services to employers/industry/ organizations as well as Individual Albertans.
- MOBIUS will facilitate access to service and benefit history, existing assessment and other information produced through other AE&I program involvements.
- MOBIUS will facilitate reporting and links to other reporting environments (e.g. Strategic Information Environment).

- MOBIUS will be user friendly and adaptable, able to capture registration information, assessment of needs, an action/investment plan, eligibility determination and benefits calculation, benefit administration, a record of services provided, progress towards goals and reporting on outcomes.
- MOBIUS will be able to support workflow management and business processes (e.g. schedule events, bring forwards, monitors, file transfers, etc).
- Information provided, collected and generated is electronic based with minimal paper files/information and future imaging capability.
- Information management/information technology solutions will be robust yet flexible to respond to business programs and service changes in a timely, cost-effective manner.

8. Access to MOBIUS

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

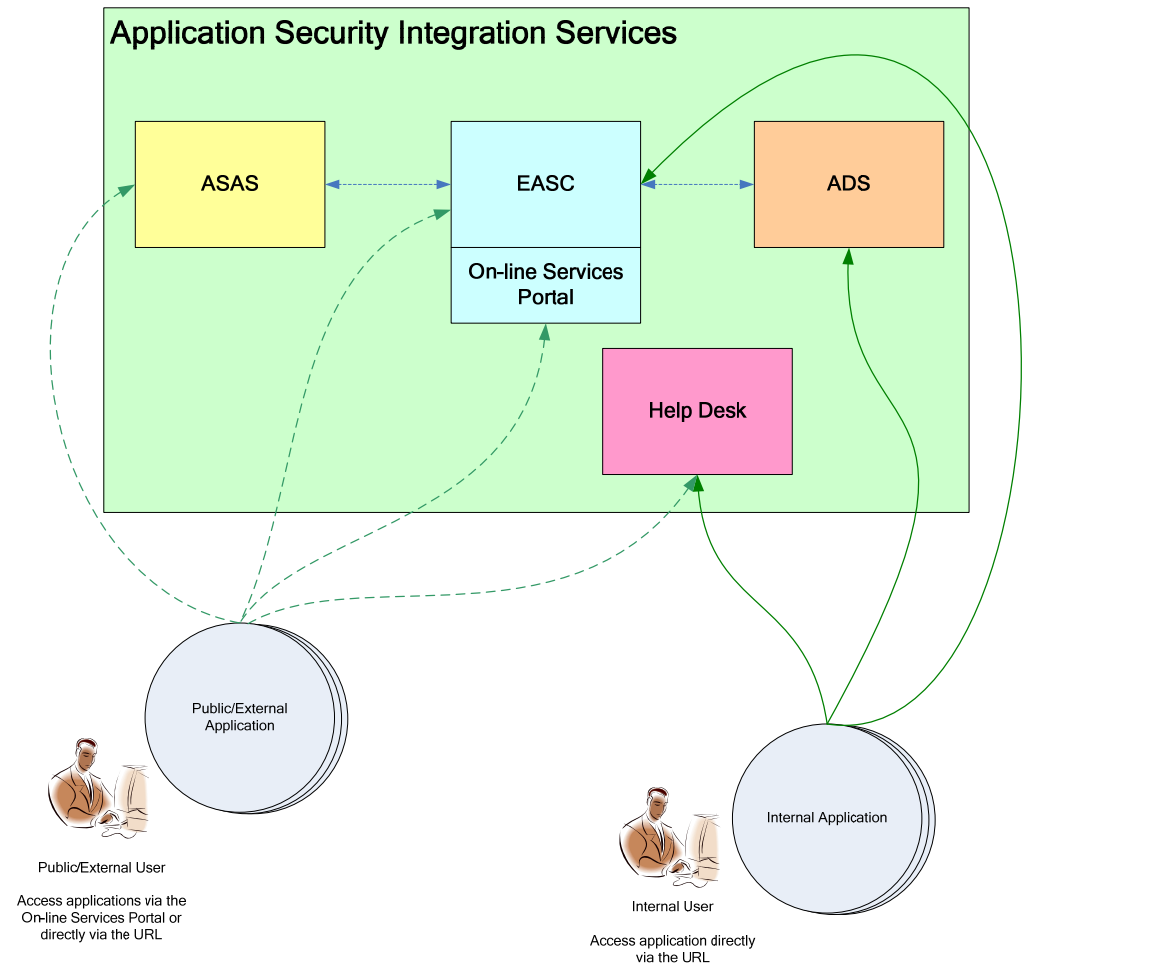
CÚRAM functionality enables an extensive list of possible user roles. These roles will be defined and applied to each user authorized to access MOBIUS. The roles will be allocated to such facilities as (but not limited to) system parameter management, security management, financial management, and approvals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

CÚRAM has the ability to provide data-level security, based on user role. This is supported by the restrictions set upon the relationships of the users to AE&I. Internal (AE&I) users are authorized to view most client information based on their user role and by the security group. AE&I's external providers' views and access to clients and their information will be restricted to a need to know basis only on their client.

An example is that the external provider must enter the Social Insurance Number (SIN) of the client in order for the provider to successfully complete the search and display criteria for the client. The SIN must be an exact match. This requirement limits the external provider's access to only their client's information. The external provider is unable to do a random search by name and therefore limits an external provider's access to the system.

To ensure authentication of an external provider the Contract Services Coordinator is responsible for ensuring external users are trained in the use of MOBIUS and expectations of the user's role and responsibilities before using login ID's. The "Request for Mobius ID – External Users" form requires the Users date of birth. The date of birth is collected by the Alberta Secure Access Services (ASAS) for user identification purpose before electronically distributing a personal Identification number (PIN) to a user which is required for the ASA enrolment process. This requirement increases the level of security for the user, the institutional and the GoA.

A key component of CÚRAM's security configuration is the Application Security Integration Services (ASIS). This is a suite of components designed for the purpose of providing identification, authentication and authorization services for on-line applications, with coarse grained (highest level of authorization available to a user being granted access) and fine-grained (level of authorization controls for functions to be carried out or viewed). ASIS provides a single unified front for applications thus removing the complexities and time required to adequately secure on-line applications for public, external and internal use.



ASIS is made up of the following components;

Alberta Secure Access Service (ASAS). Through Service Alberta ASAS provides identity and access management services for Government of Alberta web-enabled on-line services. ASAS is divided into two basic concepts – Registration and Enrollment.

Registration – sets up an account to access Government of Alberta on-line services. During the registration process the individual must provide information about themselves, who they work for, basic information for use when accessing the ASAS self-provisioning services such as retrieving a forgotten password or resetting their password.

Once the appropriate information has been entered and validated, ASAS assigns a unique username and a random 3-digit number (PIN)

Enrollment – once registered then enrollment is required to the available on-line services. The enrollment process requires your ID provided prior to the enrollment process and their PIN. These two credentials are only known by the individual and Service Alberta and thus establish their identity with the Ministry.

AE&I may utilize this facility to control access by users throughout the world-wide web. This aspect of MOBIUS will not be put in place for individual clients until such time that authentication processes are appropriate and privacy safeguarded.

CÚRAM being a web-based application, enables service providers to access AE&I's repository of services and service management facilities through the internet. By following the GoA's practices for the use of ASAS, access to MOBIUS meets the security standards defined by the GoA's security policies.

On June 1, 2004 the Office of the Information and Privacy Commissioner accepted the Office of the Corporate Chief Information Officer's Government of Alberta Information and Communications Technology Operations Privacy Impact Assessment (PIA) The PIA outlines the delivery of the Government of Alberta Secure Access Service as a result of the Government of Alberta Secure Access Project.

Enhancing the security and access rights provided by ASAS and AE&I applications, AE&I has developed the Enterprise Application Security Component.

Enterprise Application Security Component (EASC). EASC provides coarse-grained and fine-grained authorization services for custom-built and Commercial-Off-The-Shelf software products. This facility brokers 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 MOBIUS and the information allocated to the user's role.

EASC has proven to be a very robust, stable and scalable authorization service. EASC offers the following key features;

- EASC has been used to secure web-based applications, desktop-based applications and unattended batch jobs. To date, a number of custom-built applications have been secured with EASC (e.g.; Service Alberta – SHARP, EII - Appeals Information Management System, Expenditure Officer System, Learner Referrals to TOMIS, Alberta Works One View, Strategic Information Environment). Additionally, a number of COTS

products have also been secured with EASC including Microsoft SharePoint (datalink) and Curam (a Human Sector Client Management software product).

- EASC is role-based. Security rights are granted to roles (e.g.; a role of Case worker can access Forms 1 and 2, Information Products 1 and 3 and execute functions 5, 7,8 and 10). People are in turn assigned to one or more security roles (e.g.; John Doe is assigned the roles of Case Worker and Assessor). Thus, John Doe has access for Forms 1 and 2, Information Products 1 and 3 and functions 5, 7, 8 and 10. If the security for the Case Worker role is changed to allow access to Form 3 as well John Doe will automatically gain access to that form because he has been assigned to the Case Worker role. Changes to security are made to the role and any person assigned to the role in question is automatically updated.
- EASC implements a “best-of” security model. A person can be assigned to multiple security roles. The best of all roles is used to control the person’s access. Thus, a person does not have to switch between roles when using an application.
- EASC is real-time. Any changes to security take effect immediately. Users do not have to log off an application for the security settings to take affect.

Active Directory Service (ADS). Provides coarse-grained authentication services for authorized internal (GoA) staff only (not all GoA staff will be given access rights). The ADS only supports single factor authentication (i.e.; username and password).

On-line Services Portal. The On-line Services Portal content is provided by EASC. Applications a person has enrolled in or are available to enroll in are displayed on the portal. The list of applications displayed on the portal is controlled by EASC application administrators.

Help Desk. Help Desk services are provided to end users for various components. Users will typically contact the ASAS help desk first when they experience issues accessing an on-line service. The ASAS Help Desk analyst will trouble-shoot the problem and either resolve it if it’s related to the ASAS service or forward the user to the ministry help desk if the problem appears to be with the ministry application.

9. Requesting and Revoking Access

The System Administrator is responsible for managing security access to MOBIUS.

Requesting a new ID, change to ID and deleting an ID in MOBIUS for internal staff is delegated to the business area Manager for completion of the “Request for Mobius ID – Internal Users” and submitting to the Security Administrator. The form in particular details the employee’s Role/Job Title and Sensitivity Level. The Manager signs the request form which outlines in bold ‘The User must be trained prior to accessing Mobius.’ Training date(s) are recorded on the form (refer to *Appendix 2*).

Requesting a new ID, change to ID and deleting an ID in MOBIUS for external service providers is the responsibility of the E&I Contract Services Coordinator. The request form requires an external to provide their date of birth which is collected by the Alberta Secure Access Service (ASAS) for user identification purposes. Completion of the “Request for Mobius ID – External Users” is required and signed off by the Contract Services Coordinator and submitted to the Security Administrator. The form outlines in bold ‘Contract Services Coordinator must ensure the user is trained prior to accessing Mobius’. Training date(s) are recorded on the form (refer *Appendix 3*).

All internal and external users of MOBIUS must be trained prior to receiving access. Acknowledgements of appropriate use of the Mobius System forms are being drafted for sign off by the internal and external users. A copy of the drafted form for internal users is attached as *Appendix 4*.

The responsible business area Managers and Contract Services Coordinators will outline the decision making process based on the user roles and outline exceptions, if any are to be allowed. This will ensure that access request forms submitted to the Security Administrator for the granting of access to users are completed and approved appropriately.

The Privacy Impact Assessments to be completed on each legacy system to be integrated into MOBIUS as well as any new systems created will detail the decisions made for access to information based on role, user responsibilities (security group) and sensitivity. It will be imperative that the Managers and Contract Services Coordinators fully understand the scope of the role in relation to the user responsibilities and ensure the assigned role to the user meets the administrative, security and privacy requirements.

The access request forms will provide the Security Administrator 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 administration personnel can change over time.

Currently there is no automated process that alerts the Security Administrator when an individual leaves their position. The business area Managers and Contract Service Coordinators have a responsibility to notify the Security Administrator to delete an ID. As an added security, users that have not signed on to the system in the past 60 days will be inactivated (refer to Mobius UPDATE, *Appendix 5*).

The requirements for the proper maintenance of access rights to systems are detailed in the AE&I Security Policy. Security access on MOBIUS is managed to ensure adequate and appropriate security controls are consistent with requirements of the AE&I Security Policy. A User Access Policy and Procedures for MOBIUS is currently being drafted to define guidelines on usage and access. Assessment of the proper usage and access will be built into the audit process.

10. Restricting Access to Information

Access to information will be based on role, user responsibilities (security group) and sensitivity. The degree of access granted will be based on the type and amount of information. The extent of the access granted will be based on the user's job responsibilities in relation to creating, modifying, deleting or view only.

10.1 Eligibility

To be considered eligible to access MOBIUS, an individual must be one of the following:

- AE&I Employee
- Contracted External Service Provider

10.2 Role

MOBIUS access is first determined by the user's role for example:

Internal

- Service Delivery Management
- Supervisor
- Front Line User Internal
- Specialist

- Financial Analyst
- Centralized Entity (Mobius Support)

External

- Front Line User External

10.3 MOBIUS User Security Group

MOBIUS User Security Group

The security group is identified by functionality in MOBIUS and allows the restriction of access by role to create, delete, modify, view only, or no access through an assigned Security ID. For example:

	<i>Front Line User Internal</i>	<i>Supervisor</i>	<i>Centralized Entity (Mobius Support)</i>	<i>Front Line User External</i>
Employer Inf-Create	Yes	Yes	No	No
Employer Inf-Delete	Yes	Yes	No	No
Employer Inf-Modify	Yes	Yes	No	No
Employer Inf-View	Yes	Yes	Yes	No

10.4 MOBIUS Sensitivity security

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.

- Level 1 = general public (any user has access to the data)
- Level 2 = external providers (can view data at levels 1 or 2)
- Level 3 = internal staff (can view data at levels 1,2,3)
- Level 4 = supervisor and managers of delivery staff (can view levels 1,2,3,4)
- Level 5 = confidential (senior roles only – can view all levels)

AE&I has a designated Security Administrator to manage the process of 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

11. Access to Information of Other Ministries

MOBIUS will be a provider, which means that other applications may be able to communicate/link within MOBIUS through an open, standards-based mechanism that can serve to enable and enhance information sharing agreements.

Before integrating common business processes across ministries through MOBIUS consideration will be given to the implications on personal information flows, access rights, authority to access and levels of security.

12. Privacy Awareness

MOBIUS allows a greater level of openness.

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

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

- 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 and security of the personal information.
- In a manner consistent with professional conduct.
- For the sole purpose of the performance of their duties.

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

All employees of AE&I are required to have mandatory FOIP training once every three years. The Information and Privacy Office (IPO) offers a “Managing Information at Work” for employees as an opportunity to develop a good awareness about the information they are responsible for collecting, using and disclosing.

In addition, the IPO offers an “External Service Provider/Agent Training” for those working on behalf of (or under contract to) E&I and Alberta Children and Youth Services. The sessions are intended to provide general training about privacy and security expectations arising under the Freedom of Information and protection of Privacy Act and are presented with the expectation that External Service Providers and Agents will communicate and incorporate the privacy and security requirements within their individual organization such as through the use of policies/procedures/processes and training delivered to their own staff.

All internal and external users of MOBIUS must be trained prior to receiving access to MOBIUS. Training Guide materials are available electronically on the AE&I intranet site at <http://ahreintranet.gov.ab.ca/publications/awtraining/systems/mobius/index.asp>

AE&I Contract Service Coordinators are responsible for the contractual agreements with the external service providers and must ensure they understand access policy expectations.

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

13. Audit Process

Auditing is supported on most MOBIUS 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 in order to support the open system concept of MOBIUS. This requirement is designed to mitigate privacy concerns and greater awareness of the user's obligations.

14. Mitigation of Potential Privacy Impacts

The CÚRAM application for MOBIUS has been modified to remove all non-required personal information fields.

External service providers will have limited access to MOBIUS with restricted search capabilities.

The CÚRAM application has the capacity of restricting access by role, user responsibilities (security group), sensitivity and by user (through customization). AE&I has chosen to have a more open system with MOBIUS by restricting access only by role, security group and sensitivity and not by individual user.

Processes will be implemented to audit usage and access on a regular basis with a reporting mechanism of any indications of unauthorized activity. Employees will have a clear understanding as to their responsibility and authorization and the consequences of unauthorized access, use or disclosure.

The CÚRAM application has the capacity 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 AE&I has disabled these features in MOBIUS.

MOBIUS provides access to both internal staff and external service providers. Authentication and Authorization is managed externally to MOBIUS through Alberta Secure Access Service (ASAS) and for internal staff through the Active Directory Service. To enhance the security and access rights provided by ASAS and AE&I applications, AE&I has developed and implemented the Enterprise Application Security Component which registers all MOBIUS users.

MOBIUS training is mandatory before access is approved for internal and external users.

The AE&I's Privacy and Security Policies prescribe common privacy expectations across the Department. They are the foundation for department-wide processes, detailed procedures and practices at the program and service level, and individual awareness.

The reporting requirements and review process for dealing with privacy and security breaches is outlined in the Privacy Policy and the Security Policy and described in policy and procedure manuals.

All employees of AE&I are required to have mandatory FOIP training once every three years. The Information and Privacy Office offers a “Managing Information at Work” for employees as an opportunity to develop a good awareness about the information they are responsible for collecting, using and disclosing.

To provide Albertans/employers/organizations with the ability to access/update their personal information, self manage and access other service providers through multi-channel access (Internet, call center, Interactive Voice Recognition technology, in person, print, etc.), potential privacy impacts will need to be identified and addressed before implementation ie. web security, database security, strong authentication, encryption, etc.

AE&I's Information Management and Application Support, Strategic Corporate Services Division is undertaking the completion of the Information Risk Assessment.

A Privacy Impact Assessment will be completed on each legacy system to be integrated into MOBIUS as well as any new systems created.

15. Conclusion

As new systems are created and old systems are closed and integrated into MOBIUS, potential risks to individual privacy that may occur in the course of its operations will be identified and addressed. A Privacy Impact Assessment will be completed as each system is integrated or created.

AE&I 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.

The Information and Privacy Office has reviewed the AWES project and the MOBIUS integrated system and has determined with the proper training and a dedicated auditing process, a reasonable and acceptable level of personal information privacy protection will be achieved.

APPENDIX 1	CÚRAM PIA
APPENDIX 2	Request for Mobius ID - Internal Users
APPENDIX 3	Request for Mobius ID - External Users
APPENDIX 4	Draft Acknowledgement of Appropriate Use of the Mobius System for Internal
APPENDIX 5	Mobius Update November 6, 2008

**Acknowledgement of Appropriate Use of the
Mobius System**

I will use the Mobius system:

1. For the sole purpose of the performance of my duties.
2. In a manner that will protect the confidentiality and security of the information entered into the Mobius system.
3. 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*.

I am expected to exercise discretion and judgment when using the Mobius system, and will be held accountable for failure to do so. Where there are indications of abuse, my access will be revoked, and may result in disciplinary action. Serious and deliberate noncompliance of security requirements will result in disciplinary action up to and including termination of employment.

1. I am not allowed to access the Mobius system under another user's ID and password. Likewise, I must not allow anyone access to a workstation where I have logged into the Mobius system.
2. Before leaving my workstation, I must exit out of any client file and lock my workstation.
3. Workstations should have both power-on and screensaver passwords activated. For assistance with re-setting passwords or creating passwords such as power-on and screen saver passwords, I can phone my Help Desk.
4. I must notify my Security Coordinator when I no longer require access to the Mobius system.
5. I have received training for my role on the Mobius system.

Employee Name (print)

Employee Signature

Date (yyyy/mm/dd)



UPDATE

DATE: November 6, 2008

TO: Internal Users and External Users of Mobius

RE: Mobius IDs - Internal and External Users

Starting **November 24, 2008**, the Mobius system will be adhering to the Government of Alberta security standard of deleting inactive user IDs after 60 days.

If users have not signed on to the system in the past 60 days, their ID will be inactivated. This means that no work will be able to be assigned to that user. To avoid being deleted in error, ensure you sign on to Mobius on a regular basis.

The following is the instructions for obtaining or deleting a Mobius ID:

Internal Users

Access to Mobius must be approved by a Manager.

The [EMP 2007I Request for Mobius ID – Internal User](#) form must be completed for:

- New Employees
- Change to an existing employee information (name change, role change, change to ADS (My Agent))
- Delete ID - Employee leaves the department or no longer requires access to Mobius

E-mail the information to Mobius.ids@gov.ab.ca or fax it to 780-427-4310.

The user **must** be trained prior to receiving access to Mobius. If a user **does not** access Mobius for 60 days, their ID will be removed from the system. If a user does not want their access removed they must sign in at least once every 60 days.

External Users

Access to Mobius must be approved by the Contract Services Coordinator.

The [EMP 2007E Request for Mobius ID – External User](#) form must be completed for:

- New Training Provider staff
- Change to staff information (name change)



UPDATE

- Delete ID – the employee leaves the Institution/Agency

E-mail the information to Mobius.ids@gov.ab.ca or fax it to 780-427-4310

The user must be trained prior to receiving access to Mobius. If a user **does not** access Mobius for 60 days, their ID will be removed from the system. If a user does not want their access removed, they must sign in at least once every 60 days.

APPROVED FOR DISTRIBUTION BY:

Renaë Leitch

Manager

IT Business Support

Business Innovations