Alberta.ca Account

Technology and Innovation

Report of the Auditor General

July 2024

Auditor General
OF ALBERTA

Auditor General
OF ALBERTA

Shane Getson, MLA Chair
Standing Committee on Legislative Offices

I am honoured to transmit my report, *Alberta.ca Account*, to the Members of the Legislative Assembly of Alberta, under Section 20 of the *Auditor General Act*.

W. Doug Wylie FCPA, FCMA, ICD.D
Auditor General

Edmonton, Alberta
July 2024

Contents

Related Reports

- Cybersecurity—Data Protection, Incident Detection and Response (December 2023, p. 163)
- Improve user access controls (November 2021, p. 136)

Appointed under Alberta's *Auditor General Act*, the Auditor General is the legislated auditor of every provincial ministry, department, and most provincial agencies, boards, commissions, and regulated funds. The audits conducted by the Office of the Auditor General report on how government is managing its responsibilities and the province's resources. Through our audit reports, we provide independent assurance to the 87 Members of the Legislative Assembly of Alberta, and the people of Alberta, that public money is spent properly and provides value.

Report Highlights

Why We Did This Audit

Alberta.ca Account (the service) lets people and businesses use a single account to quickly and securely access online government programs (programs) and funding (for example, health records and affordability payments). With over 3.7 million personal accounts and approximately 75,000 business accounts—it is fast becoming essential.

What We Looked At

Our audit objective was to assess whether the department has effective processes to manage users and provide secure access through Alberta.ca Accounts to online government programs and services.

We Found

The department:

- had automated controls for identity proofing and account management that sometimes failed, and the department didn't detect the control failures
- should strengthen its encryption controls
- had effective processes to authenticate users and manage credentials
- had ineffective processes for adding programs and setting and enforcing governance standards
- does not comprehensively monitor all systems supporting Alberta.ca Account

We Recommend

We recommend that the Department of Technology and Innovation:

- test automated controls
- strengthen data encryption controls
- improve program onboarding and governance practices
- enhance monitoring of systems

Conclusion

We conclude, based on our audit criteria, that the department has processes to manage users and provide secure access through the service to programs, but not all these processes were effective, and the department can improve them.

Why our Findings Matter to Albertans

Albertans should be confident that the department keeps their information safe and secure when they access the government's online programs through their Alberta.ca Account.

Ministry programs that rely on the service must know who they are dealing with before they grant access to sensitive information, distribute money, and serve Albertans.

Background

Albertans have a growing appetite for quick and convenient access to online government services. This has led to a significant increase in personal and business access to online government services. At the end of 2023, there were over 3.7 million personal Alberta.ca Accounts that could access 70 government online programs, services, and products using a single username and password.

Since 2015, Alberta.ca Account (Personal or Business) lets users register and manage their personal or business accounts. When users log on to their account, the service validates their credentials (username and password) then starts a session with a government program. In 2017, the department introduced a process for users of personal accounts to verify their information, including name, mailing address, date of birth, and gender, by cross-referencing it with data from Alberta's Motor Vehicle System. This verification process in combination of entering an activation code mailed to the user's address creates a "verified" account, which grants access to sensitive services, including personal health records.

The service uses single-factor authentication[1] for users to access programs and services. Ministries can choose the identity assurance level (basic, pending, or verified) for their programs. The combination of authentication and identity assurance would convey low to high levels of confidence that a person is who they claim to be when they deal with the government online. An overview of the account types, description, and population as of December 31, 2023 for each of the two services follows:

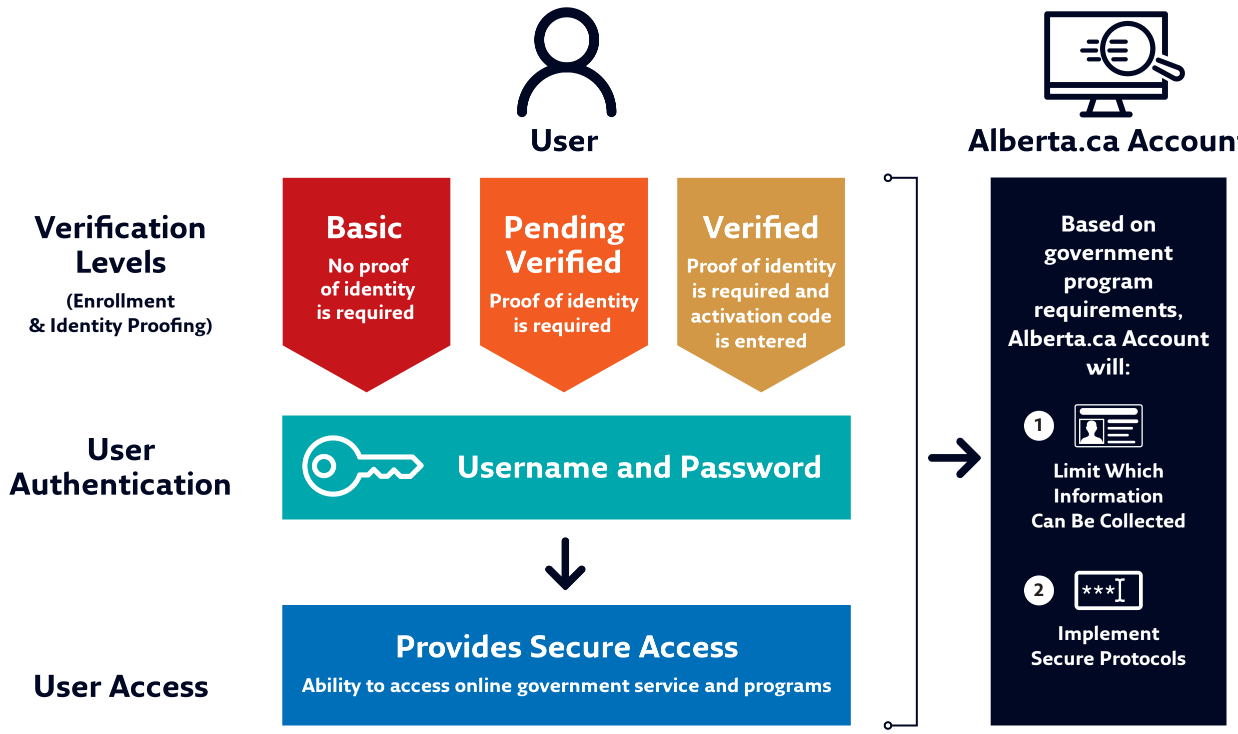
Type	Identity Verification Level	Description	# of Accounts	Example of Programs by Verification Level
Alberta.ca Account	Basic	Account has not been verified against any authoritative identity source	2,341,572	• Fire Permit System • Service Dogs Information System
	Pending Verified	Account has been verified against an authoritative record (a driver's licence or identification card)	51,659	• Alberta Affordability Payment Program • COVID-19 Emergency Isolation Support Program
	Verified	Account verified against an authoritative record and user entered activation code sent via mail to users address on driver's licence or identification card	1,350,588	• MyHealth Records • My Service Canada Account (CPP, EI, OAS, CRA)
		Total Personal Accounts	**3,743,819**	
MyAlberta Digital ID for Business[2]	Basic	Account has not been verified against any authoritative identity source	74,942 Accounts (with 81,170 authorized users)	• Small and Medium Enterprise Relaunch Grant • Water Use Reporting System
		Total Business Accounts	**74,942**	

[1] Single-factor authentication is a security process in which a user provides only one form of identification to access a system, application, or service. This involves the user providing a username or email address and a corresponding password.

[2] Rebranded as Alberta.ca Account for Organizations.

Ministries must balance delivering programs and services swiftly with verifying users thoroughly.

Alberta.ca Account Setup Process



Detailed Findings and Recommendations

Enrollment and Identity Proofing

Context

When a person or business wants to sign up for a service, they typically provide some basic information such as their name, phone number, and address. This is like filling out a form online to collect the information the service needs and to identify you uniquely. By registering for an Alberta.ca Account, people and businesses can access government programs and services without filling out form-after-form manually with the same information.

If someone in Alberta needs to prove their identity, they can use their driver's licence. The government has checked the information on the licence, so it can be trusted. And then people and businesses can confidently do things like banking and entering into agreements, knowing that people are really who they claim to be. Currently, businesses are not verified.

Similarly, the service interacts with many government programs and services that provide access to government funds and resources, so it is important to know whom they are providing services to and whether they are eligible.

Users can verify their personal information through the authoritative, automated process provided by Alberta's Motor Vehicle System. Alberta driver's licences or identification cards provided by the user must be valid and current, and cannot be within 30 days of expiry. Users must verify the account annually to maintain the verification status.

Data collected during enrollment must be secured using encryption both while the data is in transit, and at rest. The encryption must be tough to break, even if the attacker has all the time in the world to work on it. When a user no longer requires an account, the service must ensure proper offboarding by disabling the account and securely deleting data according to its retention and disposition policies.

Criteria

The department should have effective processes to enroll and verify applicants.

Our findings

Key findings

The department:

- uses automated processes to consistently enroll users and obtain their consent
- transmits identity information from Motor Vehicle System to Alberta.ca Account securely
- had automated controls for identity proofing and account management that sometimes failed, and the department didn't detect the control failures
- should strengthen its controls to encrypt some of its data

Consistent, automated process to enroll users and obtain consent

People and businesses can create an account by registering with the service. We tested the automated enrollment processes and found the service consistently collected information for program use.

We analyzed the entire user database to confirm all users completed the terms-of-use agreement to allow collection of information and completion of the account verification process.

Identity proofing process transmits accurate information securely

We tested data transmitted from the Motor Vehicle System to the service's database and reviewed the system architecture design, and found:

- only approved information is transferred and accurately transmitted
- the identity proofing process uses secure channels between the Motor Vehicle System and the service
- verification codes are sent to the user's address on the identification card or driver's licence

Automated controls sometimes failed, and the department didn't detect the failures

The department relies on a series of automated controls to enroll, verify identification, and manage users. A failure in these automated controls could cause security breaches and unauthorized access to sensitive information. Ideally, the controls work 100 per cent of the time to maintain the integrity of the service.

We reviewed the user database to find users who created or maintained verified accounts with expired or nearly expired IDs and those granted a verification period longer than allowed. Of the 1.3 million verified users, we found:

- 976 users had a verified account with an expired provincial ID or driver's licence
- four users created a verified account with a provincial ID or driver's licence within 30 days of expiry

Management is investigating what caused the problem with the automated control in the verification process.

The department's policy is to deactivate accounts that have been inactive (no login) for two years and 60 days and to dispose of sensitive data it collects when an account is closed or inactive. But our testing found over 669,000 user accounts were not demoted to inactive status because the automated script was not operating as designed. Deactivation is important because users who are not actively monitoring their accounts are easier targets for identity theft.

The department's current practice is to use automation to disable and scramble username and passwords, making the closed or inactive account inaccessible to the user. But all account data such as name, date of birth, identification card details, and corporation details remained in the database unaltered, increasing the department's exposure to breaches as more users enroll in the service. Although there is a records retention and disposal schedule established for the service, it was not adhered to, resulting in the accumulation of user data in the service's database.

NEW Recommendation:
Test automated controls

We recommend that the Department of Technology and Innovation periodically test its automated controls to ensure they are operating as intended.

CONSEQUENCES OF NOT TAKING ACTION:

When automated controls are not reviewed and do not function properly, errors in the verification process and account management may occur, leading to users maintaining verified accounts longer than they should or accounts not being deactivated when unused. This can lead to increased risk of identity theft as these dormant accounts can be exploited, ultimately eroding trust in the service.

Controls to encrypt some data could be improved

We found gaps in the department's controls for encrypting some of its data. We are not reporting these findings publicly because doing so could reveal vulnerabilities and pose a risk to the safeguarding of confidential data. Instead, we have reported them directly to the department.

NEW Recommendation:
Strengthen data encryption controls

We recommend that the Department of Technology and Innovation strengthen its data encryption controls.

CONSEQUENCES OF NOT TAKING ACTION:

Storing information without encryption or using weak encryption methods increases the impact of data breaches and unauthorized access to information.

Authentication

Context

Authentication is like locking your door with a key to keep unwanted guests out. Your username and password are your personal keys to your Alberta.ca Account. You will want your lock strong enough to keep intruders out but easy enough for you to use every day.

The right combination of lock and key will provide assurance that the user has control over their account and transactions they initiate.

The department has security measures and controls to safeguard user credentials. It requires complex passwords and limits password guessing.

The department requires users to enter a username and password, providing Level 2 confidence (see page 8) that they have maintained control of their account.

Criteria

The department should have effective processes to authenticate users and manage credentials.[3]

Our findings

Key findings

- The department effectively manages login credentials and mitigates authenticator threats through its controls.

Service manages user credentials and has controls to mitigate authenticator threats

We confirmed through our testing that the security controls to manage user credentials are effective. Additionally, our testing verified that the authenticator threat controls are also effective.

Safely Sharing User Data and Establishing Trust Relationships

Context

If you need to send a message and want to make sure only the right person can read it, you will lock it with a specific key and give the key only to the person you trust to open it. Similarly, when information is transmitted to a program, secure protocols act like locks, making sure only authorized parties with the right “key” can access the data. These protocols protect sensitive user information, ensuring that it reaches the intended recipient safely and securely.

The department sets standards for sharing information about users in a secure and controlled manner, like a master keyholder in an apartment building. It oversees and coordinates the overall governance of parties using the service by establishing rules and policies that require strong, reliable digital security measures. The department manages access to systems and data across multiple systems consistently, much like a property management office maintains the security and uniformity of all apartment locks and keys.

Before a program integrates with the service, the department vets the program to ensure it meets minimum standards. This vetting process ensures that all participants in the service can exchange information securely, reliably, and seamlessly, much like how a property management office protects all residents by maintaining secure and consistent locks and keys throughout the complex.

Criteria

The department should have effective processes for establishing and maintaining secure protocols that allow the service to share account holder information securely across government applications.

Our findings

Key findings

The department:

- uses secure protocols to protect user data exchanged with programs
- has ineffective onboarding and governance processes

[3] Credentials are pieces of information that a user provides to gain access to the service, such as a username and password.

Department protects user data exchanged with programs

We tested protocols used to exchange information between Alberta.ca Accounts and ministry programs. We found the department:

- restricts communication between the service and the programs
- encrypts data during transmission to safeguard its confidentiality and integrity
- developed guidelines and specifications to facilitate the secure exchange of information between the service and programs

Onboarding and governance processes are ineffective

When a program joins the service, it must comply with the standards established by the department. Our assessment included examining the onboarding procedures and guidelines communicated to programs using the service. We found three areas for improvement detailed below.

Onboarding documentation not consistently collected or vetted—The department has a standard onboarding process for new programs that want to use the service. It gives ministries a range of onboarding documents, such as an integration guide and a service overview including technical architecture. Program owners must confirm that they have completed the following items:

- privacy impact assessment so programs can show they can collect user information
- testing of network security
- program integration form
- FAQ document to help the service's support team

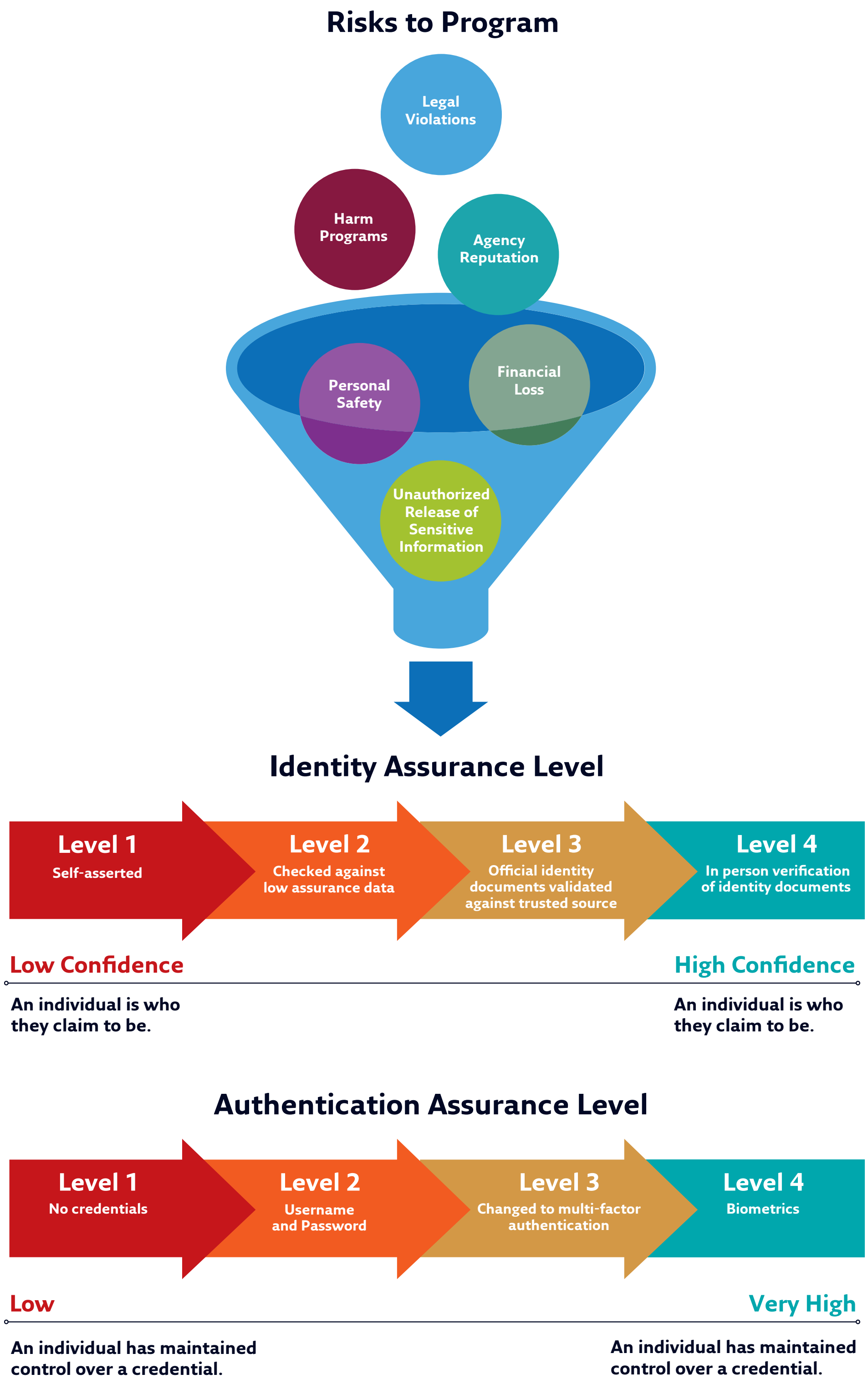
The department did not always collect and retain onboarding documentation to show it followed the process. It did not always vet the documents itself. Instead, the programs asserted that the onboarding documents were completed, and the department relied on those assertions. Of the seven programs we sampled, we were unable to confirm the completion of:

- seven network security testing reports
- five integration forms
- three privacy impact assessments

Establishing documentation procedures and conducting thorough vetting are essential to ensure seamless integration between systems and to verify that user information requested by programs aligns accurately with data provided by the service.

Risk assessments not completed—Programs do not have to complete a risk assessment to decide on the most appropriate level of identity and authentication assurance before joining the service. Best practice indicates programs should analyze potential harms to people, businesses, and the programs arising from inadequacies in the processes for granting access to accounts and verifying user identities. Choosing assurance levels that are too low may leave a program vulnerable to security breaches and unauthorized access. Alternatively, assurance levels that are too high may create unnecessary barriers for users, leading to frustration and dissatisfaction. It is essential for programs to carefully consider their requirements and align assurance levels accordingly to mitigate risks effectively.

Risk Assessment for Assurance Levels



Roles and responsibilities not defined—The department is responsible for formalizing arrangements to ensure mutual confidence in the security measures and capabilities of the service and programs. This is known as a trust relationship. To maintain transparency and accountability in a trust relationship requires clearly defined roles and responsibilities for each party in the relationship, so that they all understand their obligations.

Historically, the department would define roles and responsibilities in service agreements. But Government of Alberta programs no longer use service agreements. Instead, they are used only for programs outside of the provincial government, for example with Service Canada.

Our examination of seven programs found three instances where ministries onboarded programs to utilize the service but then unilaterally added additional programs using the existing connection without going through the department's program vetting process. The ministries did not provide assurances that these additional programs met the department's security standards. In all cases, the programs failed to encrypt user data that was securely transmitted from the service. While the responsibility for protecting user data rests with individual ministries, these observations highlight the critical importance of governance practices in establishing clear expectations for data protection and responsibilities.

NEW Recommendation:
Improve program onboarding and governance practices

We recommend that the Department of Technology and Innovation improve program onboarding and governance practices by ensuring completion and formal review of onboarding documents, developing a risk assessment process for service integration, and defining roles and responsibilities.

CONSEQUENCES OF NOT TAKING ACTION:

Inadequate vetting of programs may lead to greater security vulnerabilities and reduced functionality among systems, reducing both program and user experience. It can also undermine trust in the service and lead to a lack of accountability when issues arise.

Monitoring

Context

Effective monitoring is like having a surveillance camera watching over your home. It's crucial for keeping your belongings safe and ensuring everyone behaves properly in an increasingly digital world.

Logging user activity is like recording what each person does on your property. This way, if there's any suspicious activity, there is a record of who was involved and what they did. Making sure these logs are detailed and protected is like storing these recordings securely, so they can't be tampered with.

Regularly reviewing these logs helps you spot any unusual behaviour, like someone lurking where they shouldn't be, so action can be taken to prevent problems. Network and system monitoring ensures the continuous surveillance and health of systems to promptly detect anomalies, ensure optimal performance, and safeguard against potential security threats.

Criteria

The department should monitor user activities to confirm compliance and detect unauthorized access.

Our findings

Key findings

The department:

- generates audit logs of identity-related events
- does not comprehensively monitor some systems

Audit logs used to track identity-related events

We tested the generation of log records of user activities, including login attempts, access requests, and changes to user credential and information. Appropriate information was collected to investigate incidents.

Monitoring of systems is not comprehensive

The department uses real-time network monitoring tools to detect and respond promptly to any potential security incidents or anomalies. However, we found gaps in the department's monitoring of certain systems. We are not reporting these findings publicly because doing so could reveal vulnerabilities and pose a risk to the government's operations. Instead, we have reported them directly to the department.

NEW Recommendation:
Enhance monitoring of systems

We recommend that the Department of Technology and Innovation enhance monitoring practices for all Alberta.ca Account systems.

CONSEQUENCES OF NOT TAKING ACTION:

Cybersecurity incidents and system errors may go undetected for a long time. This could expose confidential data and cause system failures, making Alberta.ca Account and government programs and services that use it unavailable.

About This Audit

Objective and Scope

Our audit objective was to assess whether the department has effective processes to manage users and provide secure access through Alberta.ca Accounts[4] to online government programs and services.

We audited processes from January 1, 2023 to December 31, 2023 when the department performed online identity verification and account management and monitoring for Alberta.ca Accounts and provided secure protocols to transmit information to relying parties. It did not include the Government of Alberta services or programs using Alberta.ca Account services account, nor the investigation or mitigation measures performed by cybersecurity branch.

Criteria

To determine whether the department had effective processes to manage users and provide secure access through Alberta.ca Accounts to online government programs and services, we used the following criteria. The department should have effective processes to:

- enroll and verify applicant identities
- authenticate users and manage credentials
- establish and maintain secure protocols that allow online services to share account holder information securely across government applications
- monitor user activities to confirm compliance and detect unauthorized access

We developed the criteria for this audit based on the department's responsibilities and industry best practices, including:

- Public Sector Profile Pan-Canadian Trust Framework Version 1.3
- NIST SP 800-63-3 Digital Identity Guidelines
- Government of Canada Directive of Identity Management
- Government of Alberta's Information Management Technology (IMT) standards, policies, and directives

Management of Technology and Innovation acknowledged the suitability of the audit criteria on February 13, 2024.

[4] Alberta.ca Accounts (formerly My Alberta Digital ID) and for the scope of this audit includes Alberta.ca Account for Organization (formerly MyAlberta Digital ID for Business).

Audit Responsibilities and Quality Assurance Statement

Management of Technology and Innovation is responsible for management of users and providing secure access through Alberta.ca Accounts to online government programs and services.

> **Our responsibility is to express an independent conclusion on whether the Department of Technology and Innovation had effective processes to manage users and provide secure access through Alberta.ca Accounts to online government programs and services.**

All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements, set out in the CPA Canada Handbook—Assurance. The Office of the Auditor General applies Canadian Standard on Quality Management 1, which requires the office to design, implement and operate a system of quality management, including policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements. The office complies with the independence and other ethical requirements of the Chartered Professional Accountants of Alberta Rules of Professional Conduct, which are founded on fundamental principles of integrity and due care, objectivity, professional competence, confidentiality, and professional behaviour.

Auditor General
OF ALBERTA

Contact us:
info@oag.ab.ca
780.427.4222

ISSN 1919-4242 (print)
ISSN 1927-9604 (online)