

## 4.9 Citizen Online Identity Authentication Policy

### Policy Statement

The Government of Nova Scotia will take appropriate measures to ensure that:

- access to online information is restricted to authorized users;
- the privacy of users is protected in the online environment;
- users cannot repudiate responsibility for their online transactions with government; and
- the integrity of government information is not jeopardized by modifications submitted by unauthorized users.

The strength of measures to control access to government information and modifications to that information by the public corresponds to the risk that the government assumes if unauthorized access is gained or the integrity of a transaction is in doubt.

### Definitions

#### **AUTHENTICATION**

Verification of a claim. In this case, the process by which the claimed real-world or electronic identity of a client is verified. Electronic identities are asserted to, and validated by, an information system using a credential issued following a registration process.

#### **ELECTRONIC IDENTITY**

A set of information that uniquely identifies a client to a computer system. Examples are a username or digital certificate in conjunction with any necessary additional information such as a PIN/password or private signing key.

#### **NON-REPUDIATION**

The ability to confirm the origin, transmission, receipt, or processing of a transaction to ensure it is not denied by the originator or the relying party.

### **REAL-WORLD IDENTITY**

A set of information that uniquely identifies a person to another person. For individuals, this may mean possession of a passport when crossing borders or a driver's licence at a traffic stop, but could simply be appearance and mannerisms when dealing with family and friends.

### **REGISTRATION**

The process by which a client gains a credential such as a username or digital certificate for subsequent online identity authentication. Registration can be associated with a real-world identity or can be anonymous or pseudonymous.

## **Policy Objectives**

The policy is designed to:

- establish how appropriate registration and online identity authentication trust levels are determined
- encourage the identification and use of best practices when meeting requirements for registration, online identity authentication, and non-repudiation.

## **Application**

This policy applies to all departments, agencies, boards, and commissions. In this policy, references to "department" or "departments" are to be read to include agencies, boards, and commissions.

## **Policy Directives**

- A. Public-facing online transactions must be evaluated to determine their sensitivity and the risks assumed by government.
- B. This evaluation shall include the registration and online identity authentication processes, and should include the non-repudiation processes when citizens are able to modify government data.
- C. The government-endorsed Authentication Worksheet must be used to support evaluations of the registration and authentication processes, so that evaluations are consistent from transaction to transaction and from business area to business area. This Authentication Worksheet distinguishes four trust levels, numbered from one to four, and defines the required level of confidence (no confidence, some confidence, high confidence, and very high confidence) in the real-world identity or the electronic identity of the user.

- D. The measures deemed to sufficiently mitigate risk of unauthorized access or modification relative to the various trust levels will be determined by individual departments.
- E. Higher trust levels require registration and authentication mechanisms that are demonstrably stronger than those used for lower trust levels.

### **Policy Guidelines**

- A. When determining how to mitigate identified risks, departments should consult the Guide to Online Identity Authentication.

### **Accountability**

- A. The deputy head of each department covered by the policy is responsible for administering the policy, and for issuing instructions to ensure implementation of the policy including, but not limited to, informing employees of the requirements of the policy and ensuring compliance.
- B. The deputy head may augment the policy with supplementary procedures and guidance regarding registration, online identity authentication, and non-repudiation particular to the unique and special responsibilities of the department and reflecting any special requirements contained in statutes governing the operations of the department.
- C. The Treasury and Policy Board is responsible for administering the policy with respect to deputy heads.

### **Monitoring**

Departments are responsible for the consistent implementation and monitoring of the policy.

Nova Scotia Economic Development will consult periodically with departments to receive feedback regarding the relevancy, usefulness, and effectiveness of the policy and materials provided to support the policy.

### **References**

#### **LEGISLATION**

*Business Electronic Filing Act*

*Electronic Commerce Act*

*Freedom of Information and Protection of Privacy Act*

**RESOURCES**

<<http://iweb.gov.ns.ca/im/authentication/>>

Authentication Worksheet

Guide to Online Identity Authentication

**Enquiries**

Corporate IM Program Director

Nova Scotia Economic Development

(902) 424-2915

---

*Approval date: May 2, 2007*

*Manual release date: August 1, 2007*

*Approved by: Executive Council*

*Most recent review:*

---