apas Alberta Post-Secondary Application System

Information Technology Security Policy

Overview

The **Alberta Post-Secondary Application System Society (APAS)** is critically dependent on its information technology resources to fulfill its business responsibilities. Breaches or compromises of these resources can negatively affect the ability of APAS to fulfill these responsibilities, can cause financial and/or legal liability, and can be damaging to the reputation of APAS.

Use of APAS **information technology resources** must comply with all applicable laws, APAS policies, procedures, and guidelines.

Purpose

The purpose of this policy is to protect the integrity of APAS information technology resources against threats that include, but are not limited to, unauthorized intrusions, malicious use, and inadvertent compromise.

POLICY

1. GENERAL

Use of APAS information technology resources is permitted only to authorized members of the **APAS community**, and other **authorized guests**, who must follow the requirements set out in the Information Technology Resource Use Policy and related procedures. All members of the APAS community are responsible for the security and protection of information technology resources, including, but not limited to, any networks, computers, software, and data, over which the member has use or control. Use of APAS information technology resources outside of the APAS offices must comply with the same requirements as in-office use.

2. DATA CLASSIFICATION AND SECURITY

Data protection and safeguards must be implemented in a manner that is commensurate with its value and sensitivity.

3. PHYSICAL SECURITY

Appropriate controls must be employed to protect physical access to information technology resources, commensurate with the identified level of acceptable risk.

4. DISPOSAL OF ELECTRONIC EQUIPMENT

All electronic equipment must be disposed of in accordance with APAS policy.

5. INCIDENT RESPONSE

Anyone witnessing unacceptable use of APAS information technology resources in a manner that contravenes this Policy, or suspects an **information technology security incident**, is obligated to report it to the Executive Director: (780) 427-5718, or info@applyalberta.ca.

6. NON-COMPLIANCE AND MISCONDUCT

Non-compliance with this policy constitutes misconduct and may be pursued under the applicable APAS policy, collective agreements, contracts, or law.

DEFINITIONS

APAS Community	APAS staff, member institution representatives, member institution users, or other holders of valid IDs.
Authorized guests	Other authorized users of information technology resources may include, but are not limited to, contractors, applicants, and users of APAS public domain resources.
Information Technology Resources	Information technology resources refer to all hardware, software, and supporting infrastructure owned by or under the Custodianship of APAS that is used to create, retrieve, manipulate, transfer and/or store electronic information. This includes (but is not limited to) centrally and non-centrally supported computers, file systems attached to these computers, operating systems running on these computers, software packages supported by these operating systems, wired and wireless networks, telecommunication and hand-held devices, data stored on or in transit on the above, as well as electronic identities used to identify and authenticate the users of the aforementioned resources.
Information Technology Security Incident	Events where there is suspicion that: • the confidentiality, integrity, and availability of APAS data has been compromised • information and information technology resources are used for, or violated by, illegal or criminal activity • information technology resources have been attacked, are currently under attack, or are vulnerable to attack.