Information Technology Resource Use Policy

Overview

The **Alberta Post-Secondary Application System Society (APAS)** strives to foster and maintain an environment in which members of the APAS community can access and create **information**, carry out APAS business functions, and collaborate with colleagues and peers. As part of this effort, APAS is committed to maintaining an information technology environment that is free from harassment and is accessible to its members.

Such an environment can only exist when all members use and manage the **information technology resources** responsibly, respectfully, and in a manner that reflects high ethical standards, mutual respect and civility.

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 define APAS expectations and requirements for the use and management of APAS information technology resources.

POLICY

1. APAS information technology resources are to be used primarily for activities related to the mission of APAS, including, but not limited to applications, transcript transfers, and administration. Limited personal use (i.e., use not related to the mission of APAS) is permitted provided it complies with this Policy, does not compromise the business of APAS, does not increase APAS costs, does not expose APAS to additional risk, does not damage the reputation of APAS, and does not unduly impact APAS business uses. All other uses are prohibited.

2. Information technology resources must be used and managed in a responsible manner. Use of these resources for disruptive, fraudulent, harassing, threatening, obscene (including but not limited to racist, profane, and pornographic in nature), or malicious purposes is strictly prohibited. Use of information technology resources for commercial purposes is prohibited unless authorized by the Board of Directors.

3. Use of APAS information technology resources, including **electronic identities**, is permitted only to members of the **APAS community** and **authorized guests**. Requests for authorized guest use must follow the APAS enrollment process, unless the resource requested is in the public domain, such as public websites. Unless otherwise stated, such access, including the use of electronic identities, is authorized only on an individual basis and may not be shared by multiple individuals. Anyone granted authorization to use an electronic identity must make all reasonable efforts to keep such identification private and secure.

4. Information technology resource users must stay within their authorized limits and refrain from seeking to gain unauthorized access to information technology resources beyond their permissions and privileges.

5. Any individual using information technology resources to create, access, transmit or receive APAS-related information must protect that information in a manner that is commensurate with its value, use, and sensitivity.

6. Users must respect the rights of other users. They must not encroach on other users' rights to use, access, and privacy.

7. All forms of electronic communication are expected to reflect high ethical standards and mutual respect and civility. Users must refrain from transmitting to others inappropriate images, sounds, or messages which might reasonably be considered harassing, fraudulent, threatening, obscene (e.g. pornographic), defamatory, or other messages or material that are a violation of applicable law or APAS policy.

8. Users must be sensitive to the open nature of public spaces (for example, open-plan work areas, computer labs and classrooms) and take care not to display in such locations images, sounds or messages that are harassing, threatening, obscene (e.g. pornographic), defamatory, or that are a violation of applicable law or APAS policy.

9. Users must respect intellectual property, copyrights, and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

10. APAS will protect information against unauthorized disclosure. APAS reserves the right to access, monitor and record both stored or in-transit data and the usage of information technology resources when there is suspected or alleged impropriety, a business need for access in the absence of an employee, a request under the *Freedom of Information and Protection of Privacy Act*, or as otherwise required by law. APAS has the right to use information gained in this way in disciplinary actions as prescribed in APAS policies, and to provide such information to appropriate internal and external investigative authorities.

11. 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.

12. APAS reserves the right to withhold and revoke access to its information technology resources to any individual if there are reasonable grounds to suspect that their continued access to the resources poses a threat to the operation of the resource or the reputation of APAS.

13. **System administrators** of information technology resources have the responsibility to investigate and take action in the case of suspected or alleged unacceptable use. With the approval of the Executive Director or the Board of Directors, and with due regard for the rights of users' privacy and the confidentiality of users' data, system administrators have the right to suspend or modify users' access privileges to information technology resources. System administrators have the responsibility to take immediate action in the event APAS is at imminent risk. System administrators may examine files, passwords, accounting information, data, and any other material that may aid in an investigation of possible abuse.

14. Non-compliance with this policy constitutes misconduct and may be handled under the applicable APAS policy, 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.
Electronic identity	An electronic identity is any means by which a person may be identified and authenticated to access an information technology resource. This includes, but is not limited to, an account name and password, encryption keys, proximity cards, swipe cards, smart cards, or other forms of identification.
Information	Data, or aggregate data, created using APAS information technology resources.
Information technology resources	Information technology resources refers to all hardware, software, and supporting infrastructure owned by or under the custodianship of APAS that are 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.
System administrator	System administrator refers to the person or persons responsible for configuring, installing, maintaining, and supporting information technology resources for APAS. A system administrator of an information technology resource may also be a user of that resource.