REGIONAL DISTRICT OF OKANAGAN-SIMILKAMEEN
BOARD POLICY

POLICY: Information Systems Appropriate Use

AUTHORITY: Board Resolution dated September 7, 2023.

POLICY STATEMENT

Regional District of Okanagan-Similkameen (RDOS) Staff and elected officials maintain high standards of ethical conduct when using Information Systems Resources.

PURPOSE

This policy is meant to help Staff and elected officials understand their obligations when using Information Systems Resources and managing government information.

DEFINITIONS

Confidential Information means information that could reasonably harm the interests of individuals or organizations, including the RDOS, if disclosed to persons who are not authorized to access the information.

Device means an Information Systems resource that can connect (wired, wireless or cellular) to the RDOS Network, including but not limited to desktop computers, laptops, tablets, cellphones, smartphones, portable storage devices, and access cards.

Information Systems Resources means information and communication technologies that include but are not limited to information systems (network infrastructure, servers, internet, remote access, corporate software, and databases), devices, and the RDOS Network.

Portable Storage Device means a portable (or removable) device that is primarily designed to store digital information (e.g. an external hard drive or a USB flash drive).

RDOS Network means a computer system in a data centre that has met the approved security requirements for the storage of Confidential Information. This does not include the hard drives of computers, laptops, tablets, smartphones, or other devices.

Staff means all employees and officers of the RDOS as defined in all collective agreements and employment bylaws and also includes volunteers performing unpaid services for the RDOS.

RESPONSIBILITIES

1. The Board of Directors shall:
    a. make such revisions, additions, or deletions to this Policy as may be required.
    b. investigate allegations and inquiries relating to unethical conduct relating to this Policy by elected officials and the CAO and take appropriate action.

2. The Chief Administrative Officer (CAO) shall:
    a. make such revisions, additions or deletions to this Policy as may be required by law.
    b. investigate allegations and inquiries relating to unethical conduct relating to this Policy by Staff and Volunteers and take appropriate action.

3. The Information Services Department shall:
    a. maintain overall security and integrity of the Information Systems Resources.

4. Managers shall:
    a. ensure that each employee in their department is familiar with this policy.

5. Users shall:
    a. comply with this policy and any related procedural documents that may be issued.
    b. not use Information Systems Resources for activity that could expose the RDOS, themselves, or colleagues to potential criminal, ethical, or any legal proceedings.
    c. take reasonable steps to not compromise the performance and/or affect the integrity of Information Systems Resources.
    d. follow security measures and restrictions that are in place.
    e. report to the Information Services Department if something potentially negative happens, or anything suspicious is noticed, in regard to Information Systems Resources.

PROCEDURES

1. Regional District Information

Staff and elected officials must follow applicable legislation, policies, and standards for managing information in the course of their work.

General

Staff, Elected Officials

1.1 Staff and elected officials must use RDOS-provided accounts (e.g. email) when conducting RDOS business.

1.2 Staff and elected officials must use a secure portal when accessing information on the RDOS Network.

1.3 Staff and elected officials must save Regional District information (e.g. documents, emails) in accordance with the RDOS' Records Management Policy.

1.4 Staff and elected officials must only dispose of Regional District information in accordance with the RDOS' Records Management Policy.

1.5 Staff and elected officials must dispose of transitory information that they manage when the information is no longer of value.

1.6 Staff and elected officials must not, with the intent to evade either a Freedom of Information (FOI request or request for legal discovery:
    a. willfully alter, falsify, conceal, or dispose of Regional District information (including transitory information); or
    b. direct another person to willfully alter, falsify, conceal, or dispose of Regional District information (including transitory information).

1.7 Staff and elected officials must respect intellectual property rights of the Regional District and third parties. For example, Staff must not use, reproduce, modify, or distribute intellectual property without the owner's permission.

Managers

1.8 When a Staff member starts a new job, their manager must ensure they are made aware of the policies, standards, processes, and procedures that they must follow when accessing and managing information.

1.9 Managers must ensure that Staff are made aware when a significant change occurs respecting their access to Regional District information or Information Systems Resources, including but not limited to:

a. access to a new information database;
b. an approved change in their workplace; and
c. when a new or updated version of this policy or other information management or information technology policy or standard directly relevant to their work is issued.

1.10 Managers must ensure that Staff receive information management and information technology training appropriate to their positions.

1.11 Managers must ensure that Staff have the appropriate level of access to information, including Confidential Information, that is required to perform their duties.

1.12 Managers must ensure that a Staff member's access is promptly modified or removed when the Staff member no longer needs the access to perform their duties.

Confidential Information

The Regional District is the steward of a significant amount of Confidential Information, including personal information, which is managed in accordance with the *Freedom of Information and Protection of Privacy Act*. All Staff need to do their part to protect Confidential Information.

1.13 Staff and elected officials must actively protect Confidential Information, especially when handling Confidential Information in public places (e.g. on a bus, in an airport). This includes ensuring that information is not viewable or accessible by unauthorized persons.

1.14 Staff must secure Confidential Information in the workplace. This may include storing confidential paper records in locked drawers or cabinets, using strong passwords, and safeguarding devices used to save or access Confidential Information (e.g. locking or signing out of Devices when they are not in use).

1.15 When sending Confidential Information by mail or courier, Staff must use a trackable process. Decryption passwords must not accompany any encrypted storage devices that are mailed or couriered.

1.16 Staff must limit the amount of Confidential Information, particularly personal information (which is subject to legal restrictions), that is circulated, including through email or other communications such as instant messages, letters, faxes, etc.

1.17 Staff must dispose of Confidential Information using secure methods that protect confidentiality. For example, confidential paper records must be disposed of in locked shredding bins.

1.18 Managers must review Staff's access to Confidential Information annually to ensure the access remains necessary and appropriate.

2. Information Systems Resources

2.1 Staff and elected officials must securely manage and protect any Information Systems Resource in their use. For specific information on mobile device management, please refer to the Personal Device Usage Agreement and Electronic Mobile Communication Device policies.
2.2 Reasonable personal use of Information Systems Resources by Staff is permitted. Personal use is reasonable provided it is lawful, in line with the Employee Code of Conduct, and:

a. is limited during core business hours and does not interfere with Staff's duties and responsibilities;
b. does not compromise the security of Information Systems Resources or RDOS information, specifically Confidential Information; and
c. is not used for personal financial gain.

2.3 To protect personal privacy, and to reduce the RDOS' digital storage costs, Staff must limit the amount of information that they store on the RDOS Network for personal reasons (e.g. family photos, personal documents).

2.4 Staff and elected officials must not willingly or knowingly allow viruses (e.g. malware, phishing), spam/junk email, or other malicious content to be introduced to Information Systems Resources, including Devices and the RDOS Network.

2.5 Staff and elected officials must securely manage and protect the usernames and passwords they use to access Information Systems Resources. This includes not:

a. sharing credentials with colleagues or managers;
b. divulging passwords for technical support; or
c. replicating their RDOS passwords to access non-RDOS applications (e.g. Facebook, Twitter, LinkedIn).

2.6 Staff and elected officials must immediately notify the Information Services Department if they know of or suspect potential harm or risk to the RDOS Network or any Information Systems Resources (e.g. account compromise, cyber attack, phishing).

2.7 Staff and elected officials must report any lost or stolen Information Systems Resources to the Information Services Department.

2.8 Staff and elected officials must only use Information Services Department-approved Portable Storage Devices.

3. Applications and Software

3.1 If a Staff member or elected official wishes to use an Information Services Resource to access or download an application or software that is on the pre-approved list of applications and software provided by the Information Services Department, they may do so without requesting permission from the Information Services Department.

3.2 If a Staff member or elected official wishes to use an Information Systems Resource to access or download an application or software that is not on the pre-approved list of applications and software provided by the Information Systems Department, they must first obtain permission from the Information Services Department.

3.3 Staff and elected officials must not download or use applications or software that:

a. present unacceptable privacy or security risks;
b. impose terms and conditions, such as indemnification clauses, that are unacceptable to the Regional District.

4. Monitoring and Investigations

4.1 Any collection, access, use, transmission, or disposal of Regional District information or use of Information Systems Resources, including personal use, may be audited, inspected, monitored, and/or investigated to:

a. maintain, repair, and manage Information Systems Resources for the efficient operation of corporate systems;
b. meet legal requirements to produce information, including litigation document discovery;

c. ensure accessibility of Information Systems Resources for the continuity of work processes;
d. improve business processes and manage productivity; and
e. ensure compliance with legislative and policy requirements, including the Employee Code of Conduct and Code of Ethics.

4.2 Allegations of inappropriate access, collection, use, disclosure, or disposal of government information or inappropriate use of Information Systems Resources may be investigated. Investigations may include, but are not limited to, the search and/or seizure of Information Systems Resources.

4.3 Staff who inappropriately access, collect, use, disclose, or dispose of Regional District information or inappropriately use Information Systems Resources may be subject to disciplinary action, including dismissal, contract cancellation, and/or legal remedies.

4.4 Elected officials who inappropriately access, collect, use, disclose, or dispose of Regional District information or inappropriately use Information Systems Resources may be subject to remedies as outlined in the Elected Officials Code of Conduct Policy.