

IT0113-Acceptable Technology Use Policy

Introduction

Information Resources are strategic assets of SJRCC that must be managed as valuable resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Audience

The SJRCC Acceptable Use policy applies equally to all individuals granted access privileges to any SJRCC Information Resources.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of SJRCC are the property of SJRCC.

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of SJRCC are not private and may be accessed by SJRCC IT employees at any time without knowledge of the Information Resources user or owner. Electronic file content may be accessed by appropriate personnel as directed by the SJRCC administration.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the agency's internal and external point of contact for all information security matters.

User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

IT0113-Acceptable Technology Use Policy

Information Resources Acceptable Use Policy

- Users must report any weaknesses in SJRCC computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on SJRCC systems for which they do not have authorization or explicit consent.
- Users must not divulge VPN connection (remote computer use) information to anyone.
- Users must not share their SJRCC account(s), passwords, Personal Identification Numbers (PIN), or similar information or devices used for identification and authorization purposes.
- Users must not use non-standard shareware or freeware software without SJRCC Information Resources management approval unless it is on the SJRCC standard software list.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized SJRCC user access to a SJRCC resource; obtain extra resources beyond those allocated; circumvent SJRCC computer security measures.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, SJRCC users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on SJRCC Information Resources.
- SJRCC Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which SJRCC may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the SJRCC official processes for dealing with academic ethical issues).
- Access to the Internet from an SJRCC owned, home based, computer must adhere to all the same policies that apply to use from within SJRCC facilities. Employees must not allow family members or other non-employees to access SJRCC computer systems.
- Users must not otherwise engage in acts against the aims and purposes of SJRCC as specified in its governing documents or in rules, regulations and procedures adopted from time to time.
- Users of the College's Computing Resources who download any software, files, materials or information of any type using the College's Computing Resources:
 - Must comply with all terms of any software license agreements, end user license agreements, terms of use, privacy policies and any other agreements or policy that a User has notice of (collectively "License Agreements").
 - Must be aware that copyright protection includes, but is not limited to, computer software, recordings of songs, graphic art, photographs, images, films, videos, and that using

material that is protected by copyright is illegal, unless the User has received express permission from the owner of the copyright, or if the material is explicitly labeled as being in the Public Domain.

- Must not copy or download any materials protected by copyright, such as software, songs, image files or other similar materials, for any purpose outside those allowed by the License Agreement that pertains to such software, songs or image files.
- Must not make software, songs, image files or other similar materials available for others to use or copy in violation of the License Agreement.
- Must not accept software, songs, image files or other similar materials from any third party which has not been licensed for your use.
- Must not install or direct others to install illegal copies of software, songs, image files or their similar materials onto any College-owned or operated Computing Resources.
- Must not download, install, use or direct or assist others to download, install, or use software specifically designed to share or download material.
- It shall be a violation of this Policy for a User to use the College's Computing Resources for any unauthorized or improper purpose including but not limited to the following:
 - Any activity or behavior that violates any of the College's codes or policies, including this Policy.
 - Using any computer as a server without authorization from the College.
 - Any commercial advertising or commercial purpose not expressly authorized by the College.
 - Using any Computing Resource to harass anyone.
 - Sending chain letters, spamming, (distributing unsolicited email or advertisement to users) or denial of service attacks.
 - To attempt to defeat any security on any computer or system or to spread any computer virus.
 - Any conduct that violates local, state or federal law.
 - Any unethical or immoral conduct, such as using the College's Computing Resources to access child pornography.
 - Unauthorized reproduction or use of any College, names, trademarks and/or logos.
 - Accessing or reviewing the files, information, or data of other individuals for improper purposes or without the required authorization.

IT0113-Acceptable Technology Use Policy

Incidental Use

As a convenience to the SJRCC user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to SJRCC approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to SJRCC.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, SJRCC.
- Storage of personal email messages, voice messages, files and documents within SJRCC's Information Resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on SJRCC Information Resources are owned by SJRCC, may be subject to open records requests, and may be accessed in accordance with this policy.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of SJRCC Information Resources access privileges, civil, and criminal prosecution.

