

CVS POLICY & PROCEDURE MANUAL

Policy Area: **Operational Policies - General**

**Policy # &
Policy Name:** **3.3 Technology**

Group: All Staff, Board of Directors, Volunteers

Purpose:

To ensure appropriate use of technology in achieving the goals of CVS.

Policy Statement:

CVS shall develop, implement and maintain a technology plan and policy.

Practice Standards:

Annually develop a technology plan to include:

- ? an assessment of the role of technology in the CVS;;
 - ? an inventory of the hardware and software;
 - ? an inventory of policies, procedures & standards for use;
 - ? an inventory of technology competencies;
 - ? a set of technology project recommendations to meet the needs of CVS staff, volunteers, consumers, and Board; and
 - ? implementation, monitoring and renewal of the technology plan.
-

Policy Audit: March Annually

Date Issued: March 2004

Date Revised:

Position

Responsible: Executive Director

References: Technology Plan

CVS POLICY & PROCEDURE MANUAL

CVS Technology Policies

E-mail Policy

Use of **CVS** communication systems must be lawful, ethical and consent with **CVS** professional reputation, standards, policies, procedures and guidelines. In using all communications systems, each staff member must exercise good judgment and follow the spirit of this Policy.

Communications systems include e-mail, voice mail, the Internet (while on **CVS** premises, or remote access via **CVS** Internet accounts) computer programs and files, as well as any other form of communication.

Issue: Public nature of E-mail and the mistaken belief regarding E-mail's informal nature.

Policy: Always keep in mind that e-mail and the Internet are public methods of communication. When information is sent by e-mail or otherwise made available on the Internet there is a possibility that unauthorized individuals will view the information.

E-mail sent via **CVS** communications systems reflects the image of users and the organization. Accordingly, all e-mail messages must be consistent with **CVS** professional reputation and standards.

Content of all communications should be accurate. Users should use the same care in drafting e-mail and other electronic documents as they would any other written communication. Anything created on the computer may, and likely will be reviewed by others.

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful, unethical or inappropriate may not be sent by e-mail or other forms of electronic communication, or stored on the Community Ventures Society (CVS) computers. Staff, directors or consultants, encountering or receiving this kind of material must immediately report the incident to their immediate supervisor or the Executive Director.

Issue: Privacy

There is no privacy regarding the use of communications systems or the data contained in the communications systems, including e-mail and voice mail.

Communications systems and all data contained in the communications systems, including e-mail and voice mail, are the property of **CVS**.

CVS may access, inspect, retrieve, review, read, copy, store, archive, delete, destroy, distribute or disclose to others (including courts and law enforcement authorities) all communications systems data and uses, including e-mail, voice mail and Internet use, without any further notice as may be considered necessary or appropriate. **CVS** has no obligation to monitor communications systems use and data.

CVS POLICY & PROCEDURE MANUAL

Users who want their Internet use or e-mail or voice mail communications to be private should not use **CVS** communications systems.

Issue: Third party access

Policy: Non-employees are not permitted to use or access the communications systems, including the organization's Internet and e-mail accounts, without prior written authorization from the Executive Director or his/her delegate.

Issue: Personal uses

Policy: Communications systems may be used for personal purposes (e.g., to send and receive e-mail, voice-mail messages of a personal nature, to access the Internet for personal use); provided that in the opinion of the Executive Director, those uses do not interfere with the organization's business and do not compromise the integrity and efficiency of **CVS** communications systems, the organization's professionalism or its reputation.

All personal uses of the communications systems must comply with this policy and the organization's other policies, procedures and guidelines.

It should be carefully noted that all communications systems, data and uses, including e-mail, voice-mail and Internet, are not private and are subject to **CVS** access and control.

Issue: Confidential Communications

Policy: Internal E-mail

Internal e-mail is confidential and for internal use only. Internal e-mail may not be distributed to persons outside the organization unless such distribution is clearly authorized by the author of the e-mail.

External E-mail

External e-mail and data transmission is not secure or private unless it is encrypted. E-mail and other data sent externally will pass through many computers and systems that are not under **CVS** control, and may be subject to unauthorized access. For this reason, confidential e-mail or other data should not be sent or received via external e-mail unless it is secured by encryption software authorized by the Executive Director.

CVS POLICY & PROCEDURE MANUAL

Issue: Accidental Addressing.

Policy: A standard "footer" for e-mail, similar to that used on a Fax should be used on all e-mail. "This communication may contain confidential material. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited. If you have received this communication in error please contact ___ by phone at _____."

Issue: Inappropriate material in e-mail or acquired from the Internet.

Policy: CVS reserves the right to monitor any and all aspects of the computer system, including, but not limited to, reviewing e-mail sent and received by users, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users to the Internet."

Issue: E-mail signatures can add to the presentation of an email message and gives a very professional image of an organization.

Policy: The use of E-mail signatures will be standardized and used on all E-mail messages sent.

Issue: Prohibited Uses

Policy: The following uses of the communications system are prohibited:
Distributing e-mail chain letters;
Political activities, solicitation of funds, or advertising goods or services;
Other commercial or business uses;
Unauthorized access to other users' e-mail, data or communications;
Uses that infringe copyright or other intellectual property rights;
Unsecured disclosure of confidential or privileged information;
Unauthorized use of data encryption; and
Uses that may compromise system integrity or degrade system performance.

Financial Reporting and Analysis Policy

Issue: The use of specialized spreadsheets and financial programs.

Policy: Ensure the tools used are adequately documented, backed up, and that alternate staff are knowledgeable in their ongoing use and function.

Issue: Security of information generated.

Policy: Information is accessed by the use of passwords for security purposes, and any paper reports are clearly marked as confidential,

CVS POLICY & PROCEDURE MANUAL

and when no longer need, shredded. If the information is available on the network, appropriate staff must ensure that appropriate network security features are enabled.

Issue: Ensuring the input information is reliable.

Policy: Designated staff ensure the appropriate controls for the generation of the source information are in place and reviewed regularly.

Virus Policy

Issue: The proliferation of viruses including Microsoft Word macros

Policy: Documents received as e-mail attachments, downloaded from the Internet, or by other means must be closely examined for (1) knowledge of and confidence in who the sender is (2) the presence of viruses and or "macros" in the Document."

Files obtained from sources outside the company, including disks brought from home; files downloaded from the Internet, newsgroups, or other online services, files attached to e-mail; and files provided by members or vendors that may contain dangerous viruses are under no circumstances to be introduced to CVS computers. If a user suspects that a virus has been introduced into CVS computers, they should notify the Executive Secretary (939 8070) immediately.

The Internet

Some of these issue areas have been covered above.

Issue: The Internet is used as an avenue for malicious attack.

Policy: The Internet is to be strictly used by staff, directors, consumers and consultants in the performance of CVS business and under no circumstances will any other usage be permitted.

Back-up Policies and Procedure:

Issue: System recovery following a computer or technology failure.

Policy: To ensure adequate system back-ups and documentation are required to enable a replacement device to be put promptly back into service.

Procedure: Back up systems will be required for each computer on a weekly basis and will be carried out as follows:

Staff with server access will ensure all documents located on their hard drive (i.e. "C Drive") are copied to the server folder made available to them for this purpose.

Staff without access to the server will ensure that a copy of all documents located on their hard drive is kept on one or more disks

CVS POLICY & PROCEDURE MANUAL

and that the disks are kept in a fire proof cabinet if on site. Should a fire proof cabinet not be available the disks should be secured off site.

Miscellaneous Issues and Policies

Issue: Passwords and the purpose of passwords.

Policy: Use of passwords to gain access to the computer system, or to particular files or messages, does not imply the user should have the expectation of privacy in the material they create or receive. Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. No user may access the computer system using another user's password or a group password that is not expressly for their use. A secure central password list shall be maintained by the Executive Director or designate.

Computer Care

In order to help look after this equipment we ask you to:

- ? Keep the computer, keyboard and monitor clean;
- ? Be cautious with food and drink around the keyboard to prevent damaging it;
- ? Ask for help if you are having difficulty; and
- ? Ensure that all documents created for CVS use have a footer created which shows the path, file name, date created, creator's name, date updated.

Employment Termination

Employees who leave **CVS** no longer have any right to any communications systems data, including e-mail messages; nor will they be allowed access to the organization's communications systems and its Internet accounts.

Amendments, Revisions, and Compliance

This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

Violations of this policy will be taken seriously and may result in disciplinary action, including but not limited to termination, civil and/or criminal liability.

Use of the communications systems is governed by this policy as well as all other policies that guide the conduct of staff. This policy is part of the employment terms and conditions for all employees.

Use of the communications systems is a privilege that must not be abused. Use of the communications system may be revoked at the

CVS POLICY & PROCEDURE MANUAL

organization's sole discretion. Failure to comply with this policy may have serious ramifications and result in disciplinary action.