

CRESCENTA VALLEY WATER DISTRICT

2700 FOOTHILL BOULEVARD
LA CRESCENTA, CALIFORNIA

Agenda for the
Meeting of the Policy Committee
of the Crescenta Valley Water District
To be held on Friday, February 24th, 2017 at 9:00 AM

Posted on January 22nd 2017 at 3:30 p.m.

Call to Order

Adoption of Agenda

Public Comments

At this time members of the public shall have an opportunity to address the committee on items of interest that are within the subject matter jurisdiction of the Committee. This opportunity is non-transferable and speakers are limited to three (3) minutes each.

Action Calendar

1. Review of draft Electronic Use Policy
2. Review of exhibits and scope for future presentation on Information Technology procedures, policies and emergency planning.

Committee Member's Request for Future Agenda Items

Adjournment

CRESCENTA VALLEY WATER DISTRICT

STAFF REPORT

February 22 2017

To: Policy Committee
From: Mark E. Hass – IT Manager
Subject: **Discussion of Draft Electronic Use Policy and Future Technology Presentation**

1. Discussion of Director Erickson's request to have a presentation on current state of IT and related systems, their disaster recovery plans, documentation and budget planning.

- A. Review of "Electronic Use" Policy (EUP) draft. Staff requests feedback and direction of any topics beyond what is currently being addressed in the working revision of the EUP. (See Electronic Use Policy_draftv8 – attached)
- B. Review of exhibits and information included in presentation. Discussion with Directors on scope of presentation and a possible "closed session" portion to discuss confidential security aspects of the District's "Disaster Recovery and Prevention" plan.

Topics proposed for the presentation for the complete Board of Directors are:

- Disaster Recovery Basic Workflow (attached)
- Basic Network Flow Summary A (attached)
- Voice Communications Summary (attached)
- Business and Telemetry Inventory Summary
- Capital and Expense budgets. Future planning scope recommendations for budget discussions.
- Transition process review for unplanned personnel loss including temporary vendor support.
- Asset location review for all technology related components.
- District vulnerability review.
- Explanation of security countermeasures in closed session.

Crescenta Valley Water District Electronic Use Policy

Crescenta Valley Water District (CVWD) has a network and computer system that can provide access to resources internal to the District from within and in some cases remotely as authorized. Access is provided to facilitate work on behalf of the District's business needs and the needs of its customers.

Any access rights or use of District assets or systems requires that individual users act responsibly and within District's policies and rules and regulations established by management and the Board of Directors. Users must respect the rights of other users, respect the rights of customers, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, handbooks, MOUs and contractual obligations.

District, employee, and public concerns on safety, privacy, and professional work environment should be addressed and reasonable safeguards should be in place both physically and by policy including electronic and computer related activities and systems.

Index

1. Overview
2. Purpose
3. Scope
4. Policy
5. Rights of Employees
6. Compliance
7. Glossary of Terms
8. Review and Frequency

1. Overview

The District's intentions for publishing an Electronic Use Policy are to define responsibilities of the employees, management, Board of Directors, and those acting as delegates of the District.

Crescenta Valley Water District is committed to protecting Board Members, employees, customers and the District's assets and systems from illegal or damaging actions by individuals or companies, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, controllers, voicemail, mobile devices, cameras, software, operating systems, storage media, network accounts and their associated electronic mail, web browsing, web sites, and files, are the property of Crescenta Valley Water District. These systems are to be used for business purposes only in serving the interests of the District and of our customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Crescenta Valley Water District employee who deals with information and/or information systems connected devices. It is the responsibility of every individual user to know these guidelines and policies and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer and electronic equipment at Crescenta Valley Water District. These rules are in place to protect the Board members, employees and its customers. Inappropriate use exposes Crescenta Valley Water District to risks including virus attacks, compromise of network systems and services, loss of data, exposure of sensitive information, and potential legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Crescenta Valley Water District business or interact with internal networks and business systems, whether owned or leased by Crescenta Valley Water District, the employee.

Employees, contractors, consultants, temporary employees, and other personnel at Crescenta Valley Water District are responsible for exercising good judgment regarding appropriate use of information, electronic and computing devices, and network resources in accordance with District policies and rules and regulations, and federal and state laws and regulations.

4. Policy

4.1 General Use and Responsibility of Employees

- 4.1.1 Employees have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Crescenta Valley Water District files, equipment, or security information (including user accounts or passwords). Employees learning of any unacceptable use of any District systems or violations of this policy should notify their supervisor or management immediately.
- 4.1.2 Employees may access or use Crescenta Valley Water District information only to the extent it is authorized and necessary to fulfill your assigned job duties. Exceptions shall be authorized by management policies and memos.
- 4.1.3 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Management is responsible for creating guidelines beyond this document concerning personal use of information, electronic and computing devices, and network resources. In the absence of such policies or if there is any uncertainty, employees should consult their supervisor or manager.
- 4.1.4 For security and computer network maintenance purposes, authorized individuals within Crescenta Valley Water District may monitor equipment, systems, and network traffic at any time per the District's "Electronic Use Policy".
- 4.1.5 Crescenta Valley Water District reserves the right to audit District networks, workstations and appliances on a periodic basis to ensure compliance with this policy. All systems are subject to logging of activities and recording of activities (with the exception of audio) noted in section 4.3.
- 4.1.6 Employee personal use for personal reasons is permissible only within reasonable limits. Employees should not exceed whatever their supervisor allows or common practice of what "reasonable time" is. Employees should remember that all e-mail messages, voicemail, or any other information stored, compiled, or collected on computers, computer disks, databases, hard drives, networks or otherwise ("Electronic Information") are the property of the District and the District may use, inspect, destroy, delete, publish or otherwise dispose of such Electronic Information as the District determines to be in the District's best interest.

- 4.1.7 Printing, copying, and using other physical media for personal reasons should be limited. Any bulk or on-going use of printing and/or copying media (such as toner or paper) for non-District related business will not occur unless pre-approved by management.
- 4.1.8 Any employee personal storage (such as USB sticks, CD/DVDs, portable hard drives, and shared connections like “Dropbox”, “OneDrive” and “Google Drive”) will be scanned upon connection to the District’s network resources. Any loss or changes made to personal files due to “quarantine” or removal is at the user’s risk.
- 4.1.9 Guest Wi-Fi networks are offered to Board members, employees, consultants, contractors, and other temporary non-district visitors. Professional practices should be observed on guest networks such that they do not co-mingle with secure District resources. Access will only be granted to guest network by permission of supervisors, management, or the IT Department for non-employees.

4.2 Security and Sensitive Information

4.2.1 All mobile and computing devices that connect to the District’s internal network must comply with this *Electronic use policy*. Personal devices granted access will have modified requirements as defined by the IT Department and Management.

4.2.2 System level and user level passwords must comply with current password policies as defined by IT Department procedures. Providing access to another individual user, either deliberately or through failure to secure its access, is strictly prohibited. If certain CVWD business requirements necessitate a password to be shared, it should be reset immediately after completing the associated task or notify your supervisor of the exception.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. Employee must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a Crescenta Valley Water District e-mail address to a news outlets, social media, or external sites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Crescenta Valley Water District, that will be provided by the IT Department, unless the posting is in the course of business duties as authorized by the General Manager. No external social media or communication methods should be established on behalf of the District unless authorized by the IT Department or General Manager.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders which may contain malware. If employee believes any links or attachments are suspect, it should be reviewed first by IT Department before opening.

4.3 Audio and Video Recording

Audio recordings may be performed in the course of District business, if all parties are aware of the recording being performed. No publication of recordings externally to the District is authorized, with the exception of public meetings, without approval of the Board of Directors and the General Manager.

Video recordings may be performed in the course of District business as long as the recording are not accomplished in a covert manner and used is for District business, training, or approved publication by the General Manager.

4.3.1 The District will not record audio of employees or visitors via cameras unless a sign is posted and in the course of a public meeting or event that it has been disclosed and pre-approved by all parties. Security cameras will not capture or record audio.

4.3.2 The District will maintain video surveillance systems for the protection of employees, customers, and District assets. Camera locations will be disclosed to employees, however their placement will be at management discretion and be sensitive to privacy and comply with all privacy and labor laws.

4.3.3 Video recording will be used for policy, procedural, and safety compliance and training. Reproduction of video recordings external to the District will occur only in the course of legal actions or authorized activities with approval of the General Manager.

4.4 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., Authorized IT personnel, consultants, or contractors).

Under no circumstances is an employee of Crescenta Valley Water District authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Crescenta Valley Water District-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Crescenta Valley Water District.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Crescenta Valley Water District or the end user does not have an active license is strictly prohibited.
3. Accessing District data, a server, or an account for any purpose other than conducting Crescenta Valley Water District business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology in violation of international or federal or state export control laws is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, malware, e-mail phishing links/attachments, etc.).
6. Revealing your account password to others employees or allowing use of your account by others employees. This includes family and other household members when work is being done at home.
7. Using a Crescenta Valley Water District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws as set forth by regulations or laws, MOUs, or handbooks.

8. Making fraudulent offers of products, items, or services originating from any Crescenta Valley Water District account.
9. Using District resources to gain unauthorized access to any computer systems.
10. Effecting security breaches or disruptions of network communication, backups, or normal functions. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited and any software/hardware, either District or privately owned, is also only authorized by the IT Manager.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is being performed by authorized IT personnel or contractors.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, loggers, or similar technology on the Crescenta Valley Water District network except where approved by management in the course of assigned duties.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack on other companies' websites).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Crescenta Valley Water District employees to parties outside Crescenta Valley Water District except where required by other agencies or legal requests.
18. Deliberately wasting District network bandwidth, storage, or computing resources.

4.3.2 Email and Communication Activities

When using District resources to access and use the Internet, users must realize they represent the District. Whenever employees state an affiliation to the District, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the District". Questions may be addressed to the office of the General Manager.

1. Sending unsolicited email messages, including the sending of "junk mail" or other unnecessary material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information. Representing other agencies or companies without their permission.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Crescenta Valley Water District's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service not hosted by Crescenta Valley Water District or connected via Crescenta Valley Water District's network unless approved by management.
7. Posting the same or similar non-business related messages to large numbers of social media or email recipients (spam).

4.4.3 Social Media and External posting of Information

1. Posting of pictures, information, or activities by employees, whether using Crescenta Valley Water District's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy during performance or assigned duties.
2. No activities performed in the course of District business will be recorded and reproduced or posted externally without management approval including audio, video, and pictures.
3. Use of Crescenta Valley Water District's systems to engage in blogging/social media is acceptable for business purposes, provided that it is done in a professional and responsible manner, does not otherwise violate Crescenta Valley Water District's policy, is not detrimental to Crescenta Valley Water District's best interests, and does not interfere with an employee's regular work duties. Blogging from Crescenta Valley Water District's systems is also subject to monitoring. Any public facing sites or web blogs posting should be approved by the General Manager or delegate as they could be viewed as formal District opinion or policy.
4. Crescenta Valley Water District's use policy also applies to forum, blogging, and site posting. As such, Employees are prohibited from revealing any District confidential information, customer information, or any other activities being performed during the course of District duties without prior appropriate management permission.
5. Employees shall not engage in any posting to social media or transmitting information that may harm or tarnish the image, reputation, and/or goodwill of Crescenta Valley Water District and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when posting or transmitting or otherwise engaging in any conduct prohibited by Crescenta Valley Water District's *Non-Discrimination and Anti-Harassment* policy.
6. Employees may also not attribute personal statements, opinions, or beliefs to Crescenta Valley Water District when engaged in social media or posting of information. If an employee is expressing his or her beliefs and/or opinions in blogs, websites, or social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Crescenta Valley Water District. Employees assume any

and all risk associated with related posts and not infer that they are based on District policy or opinion.

7. Apart from following all laws pertaining to the handling and disclosure of sensitive, security or private information, Crescenta Valley Water District's logos and any other Crescenta Valley Water District intellectual property or letterhead, may also not be used in connection with any social media or blogging activity unless operating in an approved role.

5. Rights of employees

5.1 Access to records

Employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. The same standard will be met such as paper documents based on all MOUs, Policies, and Rules and Regulations.

5.2.1 Privacy

Files may be subject to search under a court order. In addition, IT Department may access user files as required to protect the integrity of computer systems or on behalf of a management requests. For example, following organizational guidelines, IT Department may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged. This also includes other systems such as email, voicemail, video, and call logs (both landlines and District provided wireless devices).

5.2.2 All employee records or sensitive information will be protected from unauthorized parties access or review. All standards at District, State, and Federal levels will be adhered to as responsible custodians of personnel records.

6. Policy Compliance

6.1 Compliance Measurement

The IT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback from employees, consultants, contractors and customers.

6.2 Exceptions

Any exception to the policy must be approved by the IT Department or the General Manager in advance.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment per the District's MOU.

7. Glossary of Terms

Definitions of terms found in this document to ensure of clarity and purpose of statement with in this document.

Spyware: Computer programs that typically track your use and report this information to a remote location. The more malicious spyware programs may capture and report keystrokes, revealing passwords, and personal information. Users are often tricked into installing spyware programs without their knowledge. Spyware is sometimes referred to as adware.

| SCADA: Supervisory control and data acquisition -is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers to interface to the process plant or machinery. For example valve positions, lift station status and reservoir levels.

User: One who uses a computer, computer program, or online services.

Network: A system of computers interconnected by telephone wires or other means in order to share information.

Computer: A device that computes, especially a programmable electronic machine that performs high-speed mathematical or logical operations or that assembles, stores, correlates, or otherwise processes information. They are typically referred to as workstation, laptop, tablet or smart phone.

System: In general, any interrelated group of electronic components, e.g. hardware and/or software, that works as a coherent entity. With respect to information security breaches, a system is any computer readable collection of information that contains electronic data in an organized form such that information about a particular subject can be distinguished from information about other subjects.

Virus: Computer viruses are small, self-replicating computer programs that interfere with computer operation. The effect of viruses can range from negligible to devastating, depending on what the virus program does when it runs. A virus might, for example, corrupt or delete data on a computer, spread itself to other computers, or even install a malicious program.

Internet: A term to describe connecting multiple separate networks together. Typically used to refer to the shared “cloud” or uncontrollable, interconnected that is used worldwide.

Intranet: A computer network, especially one based on Internet technology, that an organization uses for its own internal and usually private, purposes and that is closed to outsiders. Typically it is hosting email, files, databases, and other secure resources.

Extranet: A website or connected resource that allows controlled access to partners, vendors and suppliers or an authorized set of customers. Public facing offerings, such as “online billing”, but accesses a portion of internal resources is an example.

Host: A computerized device that has access to other computers on the network. This can be a desktop, mobile device, or auxiliary machine such as a copier, PLC, controllers for security, or heating and Air Conditioning.

File: An intact or partial file, document, photo, video, database, table or any object found in a digital form on District network resources

Blog: A website that displays postings by one or more individuals in chronological order and usually has links to comments on specific postings.

Forum: A medium for open discussion or voicing of ideas, such as a newspaper, a radio or television program, or a website.

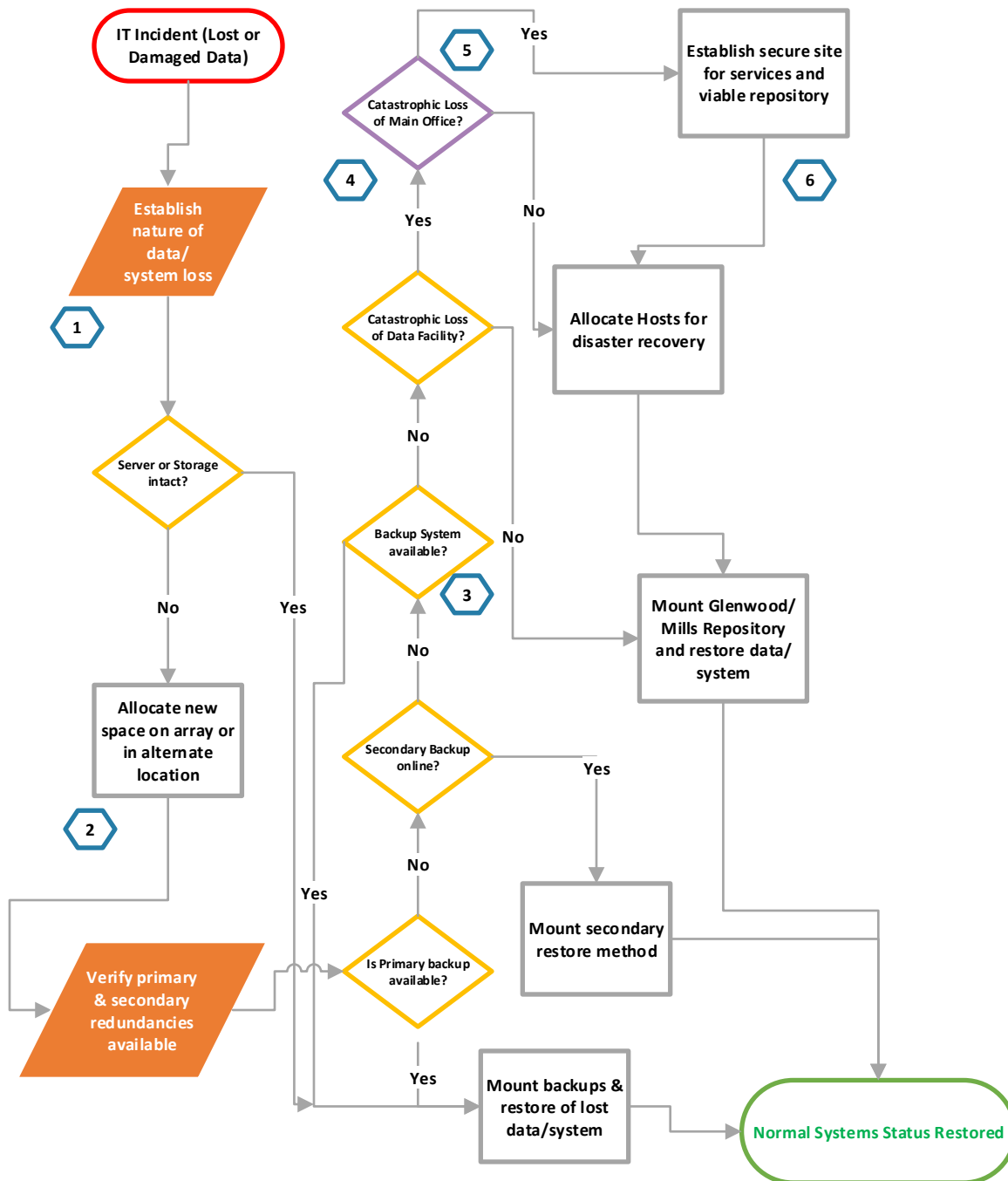
Social Media: The websites and applications considered as collectively constituting a medium by which people share messages, photographs, and other information.

Phish(Phishing): To request confidential information over the internet or by telephone under false pretenses in order to fraudulently obtain credit card numbers, passwords, or other personal data.

8. Review of Policy

This policy should be reviewed for applicable changes at least once annually by CVWD management team and the Board of Directors. Internal input from IT Staff, Management, Legal Counsel and employees and their representatives should occur upon any changes impacting employees and for the protection of the District and the employee.

Crescenta Valley Water District Systems and Data Disaster Recovery Basic Workflow



Process Comments

1 Loss types could be individual files or folders due to deletion, corruption, virus, or hardware failure. Full volumes of data, databases, drives or arrays. Physical or virtual servers are also accounted for this is step.

2 Virtual Standby space and live servers are available under normal conditions for quick recovery

3 In case of main DR systems or a total loss at the main IT office, repositories are synced at Glenwood and Mills facilities.

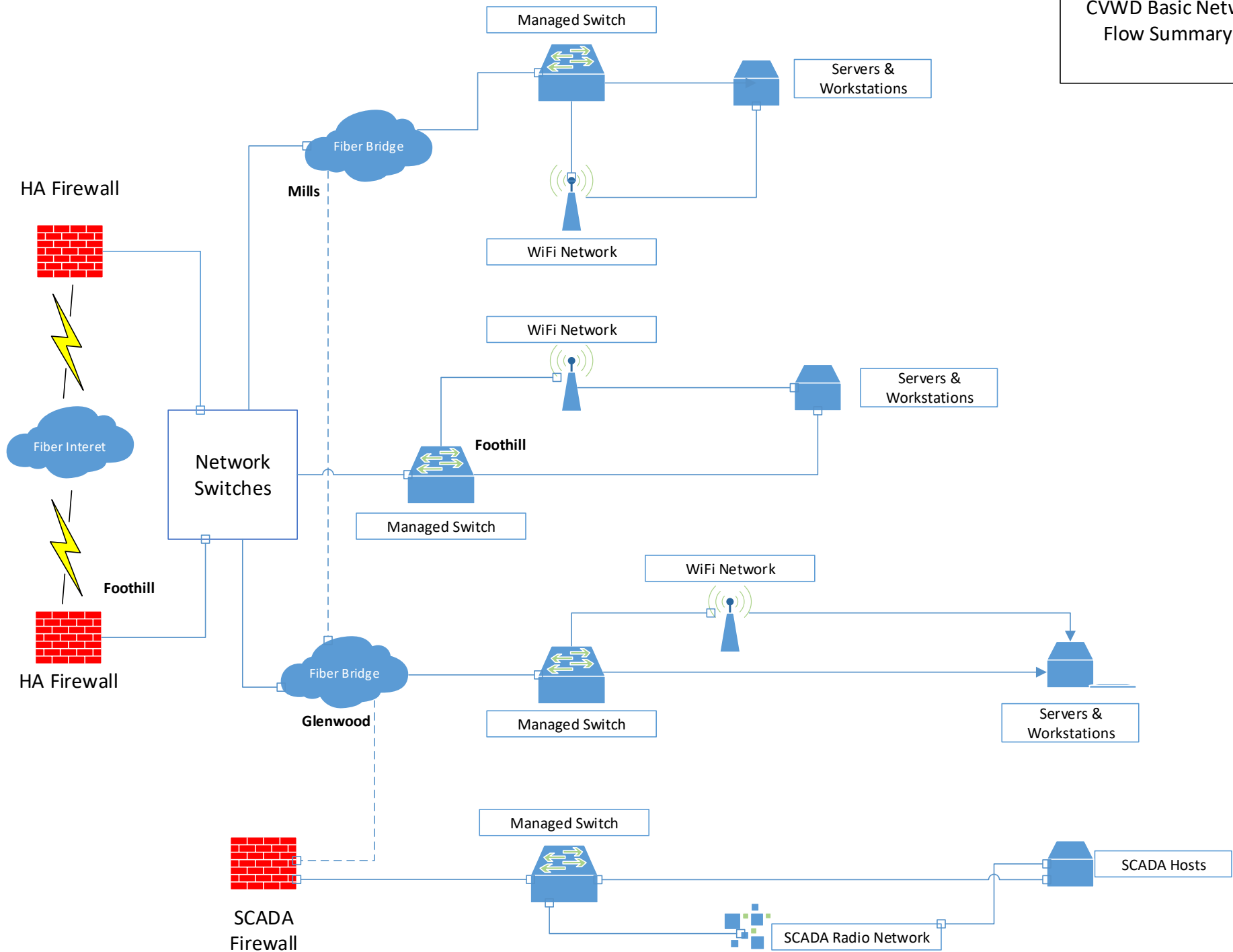
4 Loss of main office viability also triggers redundant data circuit options and procedures

5 Upon loss of the Foothill office, temporary hosts are available at other sites for files, data and services

6 Once a site is selected, DR system, Hosts and other user PC/printers can be placed

7 Normal Systems status is achieved Not when everything is replaced. Normal is achieved when all required services and data are available, email, phones and public access options are online.

CVWD Basic Network
Flow Summary A



CVWD Voice Communications
Summary

