Disaster Recovery Procedure

Last Update Status: *Updated June 2017*

Natural Disasters, although rare, could likely cause an extended delay of service and should be planned for accordingly. This procedure defines the requirement for a baseline disaster recovery plan to be developed and implemented by PCSD that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a minor or major outage. In the event of an actual emergency situation, the Incident Response Team (IRT) may make modifications to ensure the physical safety of our people and data.

The principal objective of the disaster recovery procedure is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations.

Contact Information

In the event of a disaster or crisis, Technology Department Employees will have a clear understanding of who should be contacted. Contact information is included in the Google Doc: Data Center Maps. Other information regarding systems is included in the CSI folders. Other employees of the District should contact the help desk.

DRP Exercising/Drills

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens. The IRT will plan drills on a needed basis for training purposes.

Responsibilities of the IRT

- Respond quickly to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Ensure employees are notified and allocate responsibilities and activities as required.
- Recover key systems within 8.0 to 24.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- A financial assessment may be required. These items could include, loss of financial documents, theft of financial information, cost of machine or hardware replacement or services needed to restore functionality.

Contingency Plans

The following contingency plans must be created:

- **Computer Emergency Response Plan**: Systems are divided up into Operational Groups (OpGroups). Each OpGroup is led by an OpGroup Coordinator. The contact information of these

individuals and their backups can be found in the Google Doc “Data Center Maps” and their corresponding CSI folders. When these individuals cannot be contacted [this happens, etc]… What immediate actions must be taken in the event of certain occurrences?

- **Data Study**: Detail the data stored on the systems, its criticality, and its confidentiality.
- **Data Backup and Restoration Plan**: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data will be recovered.
- **Equipment Replacement Plan**: Describe what equipment is required to begin providing services, list the order in which it is necessary, and note where to purchase the equipment.
- **Data Center Map**
    - Server data will include: Hostname, IP, Software, OpGroup Responsible, Criticality
    - Contact Information will include: OpGroup Coordinator, their backup person, phone #, alternate contact info, email address
- **Critical Systems Instructions:** Documentation must include:
    - Detailed list of what data is stored on the system.
    - The criticality of the system, this shows priority so machines can be brought back up in order of importance.
    - If Switch, all necessary information for it.
    - Location of installation software and OS
    - Backup frequency and storage locations, detail of what data (detailed list) is stored in these backups. In case of restoration, the appropriate backup can be restored quickly. Failover servers and failover locations are included in this list. Daily, Monthly, Quarterly.
    - Steps to restart, reconfigure, and recover the system.
    - Username and passwords
    - Support phone numbers
    - Power up and power down procedures.
    - Equipment age
    - Server Specifications (disk space,RAM,CPU,disk type,disk quantity,raid config)
    - Model and serial numbers
    - Warranty and maintenance contract information
    - Software licensing information and storage location
    - IP and MAC addresses
    - Supplier contacts for sources of expertise to recover systems. These might include vendors that sell/support the products, or the manufacturers themselves. Contact Person, phone, email, tech support phone number for company
    - Contacts can include Facilities, Power Company, Telecom companies, Insurance company, HVAC, Generator maintenance, etc
    - Website username and password
    - Server username and password (root, admin, etc)
    - List of users with access to the system.
    - Maps, diagrams, charts, etc.
    - Any username/password for any system where relevant information exists to recover systems (manufacturer website username and password, server passwords, call-in information, etc.)

- Data will be stored outside the vault in the event local servers become inaccessible.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Tabletop exercises should be conducted. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, be reviewed an updated on an annual basis.

Encryption Procedure

Last Update Status: *Updated September 2015*

The purpose of this procedure is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this procedure provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States. Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data and hence, compromise of the data. While users may understand it is important to encrypt certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys. This procedure outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

This procedure applies to any encryption keys listed below and to the person responsible for an encryption key. The encryption keys covered by this procedure are:

- Encryption keys issued by PCSD
- Encryption keys used for PCSD business
- Encryption keys used to protect data owned by PCSD

*__Public keys contained in digital certificates are specifically exempted from this procedure.__

All encryption keys covered by this procedure must be protected to prevent unauthorized disclosure and subsequent fraudulent use.

- Secret Key Encryption Keys

  Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in PCSD's *Acceptable Encryption Procedure.* If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

  Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

- Public Key Encryption Keys

  Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

- PCSD's Public Key Infrastructure (PKI) Keys

  The public-private key pairs used by the PCSD's public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents the InfoSec Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with
  PCSD policies.

  Access to the private keys stored on a PCSD issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

- Other Public Key Encryption Keys

  Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the requirements for protecting the private keys are the same as those for private keys associated with PCSD's PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.

  The InfoSec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with PCSD *Password Procedure*. InfoSec representatives will store and protect the escrowed keys as described in the PCSD *Certificate Practice Statement Procedure*.

- Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

  In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

- PGP Key Pairs

  If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart

card. Since the protection of the private keys is the passphrase on the secret key-ring, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

- Hardware Token Storage
  Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in PCSD's *Physical Security procedure*, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

- Personal Identification Numbers (PINs), Passwords and Passphrases
  All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in PCSD's *Password Procedure.*

- Loss and Theft
  The loss, theft, or potential unauthorized disclosure of any encryption key covered by this procedure must be reported immediately to The InfoSec Team. InfoSec personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

- Key Agreement and Authentication

- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

- End points must be authenticated prior to the exchange or derivation of session keys.

- Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known, trusted provider.

- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

Router and Switch Security Procedure

Last Update Status: *Updated September 2015*

The purpose of this procedure is to describe the minimal security configuration required for all routers and switches connecting to a production network or used in a production capacity at or on behalf of PCSD. All employees, contractors, consultants, temporary and other workers at PCSD must adhere to this procedure. All routers and switches connected to PCSD production networks are affected.

Every router/switch must meet the following configuration standards:

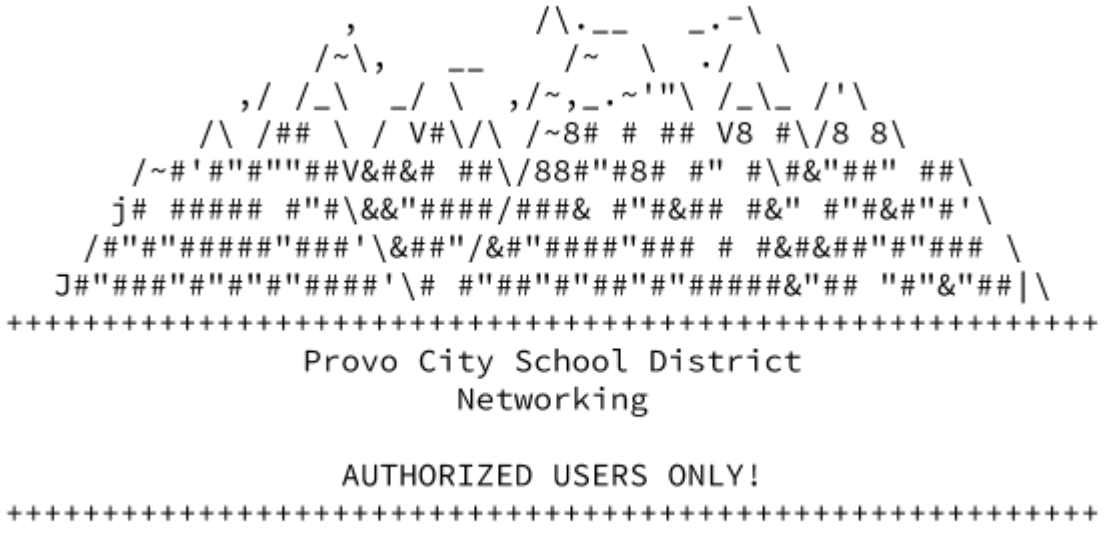
- Only one local user account is configured on the router/switch, used for backup if an external authentication source is not reachable. Routers and switches must use RADIUS for all user authentications.
- The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
- Only authorized tech support employees are allowed to login to a router or switch. The Network Engineer can give an employee rights.

The following services or features must be disabled:

- IP directed broadcasts
- Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
- TCP small services
- UDP small services
- All source routing and switching
- All web services running on router
- Cisco discovery protocol on Internet connected interfaces
- Telnet, FTP, and HTTP services
- Auto-configuration (SMART Install)
  The following services should be disabled unless a business justification is provided:
- Dynamic trunking
- Scripting environments, such as the TCL shell

The following services must be configured:

- Password-encryption
- NTP configured to a corporate standard source
- All routing updates shall be done using secure routing updates.
- Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems, at least v2.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- Access control lists for transiting the device are to be added as business needs arise.
- Each router must have the following statement presented for all forms of login whether remote or local:



- Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
- Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
- The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
  - IP access list accounting
  - Device logging
  - Incoming packets at the destination router with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    Router console and modem access must be restricted by additional security controls

Server Security Procedure

Last Update Status: *Updated May 2017*

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well. The purpose of this procedure is to establish standards for the base configuration of internal server equipment that is owned and/or operated by PCSD. Effective implementation of this procedure will minimize unauthorized access to PCSD proprietary information and technology.

General Requirements

- All internal servers deployed at PCSD must be owned by an Operational Group (OpGroup) that is responsible for system administration. Approved server configuration guides must be established and maintained by each OpGroup, based on business needs and approved by the InfoSec Team. OpGroups should monitor configuration compliance and implement an exception procedure tailored to their environment. Each OpGroup must establish a process for changing the configuration guides, which includes review and approval by the InfoSec Team. The following items must be met:

- Servers must be registered with the inventory management system and a CSI (Critical System Information) document must be created. At a minimum, the following information is required:
  - Server contact(s) and location, and a backup contact and location
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
  - Serial number
  - HW address
  - Purchase information
  - Support information
  - Vendor information
    - Information in the inventory management system and CSI must be kept up-to-date.
  - For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Procedure*.
  - Configuration Requirements
  - Operating System configuration should be in accordance with approved InfoSec guidelines
  - Services and applications that will not be used must be disabled where practical
  - Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible
  - The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with teaching and instruction
  - Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient
  - Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do
  - If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec)
  - Servers should be physically located in an access-controlled environment
  - Servers are specifically prohibited from operating with unauthorized devices and networks
  - Monitoring
  - All security-related events on critical or sensitive systems must be logged
  - Security-related events will be reported to the InfoSec Team, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host

Website Services Security Procedure

Last Update Status: *Updated September 2015*

District and school websites are an online representation of Provo City School District. They reflect the

goals and values of the district. Websites are a first impression and a gateway to the many valuable services offered through the district. Without proper security, websites can be attacked, hacked and misused for nefarious purposes, including: malware and virus distribution, backdoor entry, human exploitation and false, misleading or inappropriate content. The purpose of this procedure is to provide a baseline standard for the building and maintaining of websites in a secure manner. This procedure covers all Provo City School District websites, including elementary school websites, secondary school websites, and district level websites. This does not include Social Media e.g. Facebook, Twitter

- Website Server Software and Hardware Restrictions
  - All District Authorized school and district websites will be hosted on server hardware in a location accessible and controlled by District Technology Support
  - District Technology Support shall have the ability to edit, change, disable and/or enable school and district websites at any time
  - District Authorized school and district websites, including teacher and staff web pages, are not to be hosted outside District Technology Support control
  - Server installation and security procedures must be followed when installing or changing server hardware and software
  - Only District Technology Support will have access to maintain the server hardware and software
- Website Content Management
  - Only trained district and school personnel who are selected to manage website content will have access to edit school and district websites
  - One (1) Content Manager from each school and/or department will be selected and trained to manage website content
  - Content Managers are responsible to maintain and monitor content on assigned websites and/or web pages
  - Content Managers can request to have content contributors assist them. Content Contributors are only allowed access to designated web page(s) and do not need to be trained. Content Managers are responsible for any content posted by contributors
  - Every teacher has, or will have, an official web page hosted on their school website. Training is not required for teachers to access and use this web page, however, teachers will be required to read and understand the standards and ethics found in the document: 'Web Page Guidelines for Administrators, Teachers and Staff'
- Access to website content management systems
  - All websites in Provo City School District are maintained through a Content Management System (CMS). This allows trained teachers and staff to access and edit content without understanding code and back end processes. The following processes are employed to keep each CMS secure
    - CMS users shall maintain a strong password and not share the password with any other person
    - CMS users may only upload the following file types to the media library. All other file types are prohibited:

      - PDF
      - JPEG
      - GIF
      - PNG
      - XLS
      - MP4
      - MOV
      - MP3

    - CMS users must properly compress and resize images and movies that are uploaded to the

media library according to procedures listed below

- For detailed procedures, see the following documentation:
  - Web Services Security Procedure
  - Website Access Procedure
  - Web Server Installation and Configuration Procedure
  - Web Page Guidelines for Administrators, Teachers and Staff
  - Content Manager Responsibilities

Wireless Infrastructure Communication Procedure

Last Update Status: *Updated September 2015*

Proper configuration and deployment of wireless infrastructure devices is essential to the PCSD network. Incorrectly configured wireless infrastructure devices can provide an attacker easy access to a network. Poorly deployed wireless infrastructure devices can disrupt/degrade wireless communication between devices. This procedure specifies the technical requirements that wireless infrastructure devices must satisfy to connect to the PCSD network. Only those wireless infrastructure devices that meet the requirements specified in this procedure or are granted an exception by the InfoSec team are approved for connectivity to the PCSD network.

Network devices including, but not limited to controllers, routers, switches, firewalls, remote access devices, or wireless access points, must be installed, supported, and maintained by PCSD Network Team.

All employees, contractors, consultants, temporary and other workers at PCSD, including all personnel that maintain a wireless infrastructure device on behalf of PCSD, must comply with this procedure. This procedure applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

The InfoSec Team must approve exceptions to this procedure in advance.

PCSD Wireless Device Requirements

- All wireless infrastructure devices that connect to a PCSD network or provide access to Confidential, Highly Confidential, or Restricted information must:
  - Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
  - Use Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
  - Be configured and deployed by PCSD Networking.
  - All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

- Lab and Isolated Wireless Device Requirements
  - Lab device Service Set Identifier (SSID) must be different from PCSD production device SSID.