Overview

This standard is defined to protect SDCC's electronic information from being inadvertently compromised by authorized personnel connecting to the SDCC network locally and remotely via VPN.

Purpose

The purpose of this document is to define standards for connecting to SDCC's network from any host. These standards are designed to minimize the potential exposure to SDCC from damages, which may result from unauthorized use of SDCC resources.

Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical SDCC internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, SSH, and cable modems, etc.

Audience

This policy applies to all SDCC employees, volunteers/directors, contractors, vendors, and students with a computer or workstation used to connect to the SDCC network. This policy applies to remote access connections used to do work on behalf of SDCC, including reading or sending email and viewing intranet resources.

Definitions

Virtual Private Network (VPN): A private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Some VPNs allow employees to securely access a corporate intranet while located outside the office.

User Authentication: A method by which the user of a system can be verified as a legitimate user independent of the computer or operating system being used.

Multi-Factor Authentication: A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories:

- Knowledge (something they know)
- Possession (something they have)
- Inherence (something they are)

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include:

- Being logged into the corporate network via a local Ethernet connection, and dialing into AOL or another Internet Service Provider (ISP)
- Being on a SDCC provided remote access home network, and connecting
- to another network, such as a spouse's remote access
- Configuring an Integrated Services Digital Network (ISDN) router to dial into SDCC and an ISP, depending on packet destination

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

ISDN: There are two flavors of ISDN: BRI and PRI. BRI is used for home/office/remote access. BRI has two "Bearer" channels at 64kb (aggregate 128kb) and 1 D channel for signaling information.

Remote Access: Any access to SDCC's corporate network through a non-SDCC controlled network, device, or medium.

Split-tunneling: Simultaneous direct access to a non-SDCC network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into SDCC's corporate network via a Virtual Private network (VPN) tunnel. VPN is a method for accessing a remote network via "tunneling through the Internet.

IPSec Concentrator: A device in which VPN connections are terminated.

Cable Modem: Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.

Standard Detail

Network Security

Users are permitted to use only those network addresses assigned to them by SDCCD‘s IT Department. All remote access to SDCC will either be through a secure VPN connection on a SDCC owned device that has up-to-date anti-virus software, or on approved mobile devices (see the SDCC Owned Mobile Device Acceptable Use and Security Policy and the Personal Device Acceptable Use and Security Policy).

Remote users may connect to SDCC Information Systems using only protocols approved by IT. Users inside the SDCC firewall may not be connected to the SDCC network at the same time a remote connection is used to an external network. Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the SDCC network without SDCCD IT approval.

Users must not install network hardware or software that provides network services without SDCC IT approval. Non-SDCC computer systems that require network connectivity must be approved by SDCCD IT.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, SDCC users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the SDCC network infrastructure. Only the IT Department is permitted to perform these actions.

Users are not permitted to alter network hardware in any way.

Remote Access

It is the responsibility of SDCC employees, volunteers/directors, contractors, vendors, and agents, with remote access privileges to SDCC’s corporate network, to ensure that their remote access connection is given the same consideration as the user’s on-site connection to SDCC.

General access to the Internet, through the SDCC network is permitted for employees who have flat-rate services and only for business purposes. SDCC employees are responsible to ensure that they:

- Do not violate any SDCCD policies
- Do not perform illegal activities
- Do not use the access for outside business interests

SDCC employees bear responsibility for the consequences should access be misused.

Employees are responsible for reviewing the following topics (listed elsewhere in this policy) for details of protecting information when accessing the corporate network via remote access methods and acceptable use of SDCC’s network:

- Virtual Private Network (VPN)
- Wireless Communications

Dial-in modem usage is not a supported or acceptable means of connecting to the SDCC network.

Requirements

Secure remote access should be strictly controlled. Control should be enforced with Multi-Factor Authentication (MFA). SDCC employees, volunteers/directors, and contractors should never provide their login or email password to anyone, including family members.

SDCC employees, volunteers/directors, and contractors with remote access privileges:

- Must ensure that their computer, which is remotely connected to SDCC's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Must not use non-SDCC email accounts (i.e. Hotmail, Yahoo, AOL), or other external resources to conduct SDCC business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for split-tunneling or dual homing is not permitted at any time. For remote access to SDCC hardware, all hardware configurations must be approved by SDCCD IT. All hosts that are connected to SDCC internal networks, via remote access technologies, must use up-to-date, anti-virus software applicable to that device or platform.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the SDCC production network must obtain prior approval from SDCCD IT.

Virtual Private Network (VPN)

The purpose of this section is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the SDCC corporate network. This applies to implementations of VPN that are directed through an IPSec Concentrator. This applies to all SDCC employees, volunteers/directors, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN's to access the SDCC network.

Approved SDCC employees, volunteers/directors, and authorized third parties (customers, vendors, etc.) may utilize the benefit of a VPN on a SDCC device, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees. Further details may be found in the Remote Access section.

The following guidelines will also apply:

- It is the responsibility of employees or volunteer/directors, with VPN privileges, to ensure that unauthorized users are not allowed access to SDCC internal networks.
- VPN use is controlled using a multi-factor authentication paradigm.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
- VPN gateways will be set up and managed by SDCC IT.
- All computers connected to SDCC internal networks via VPN or any other technology must use up-to-date, anti-virus software applicable to that device or platform.
- VPN users will be automatically disconnected from SDCC's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- To ensure protection from viruses, as well as protection of member data, only SDCC-owned equipment or non-SDCC devices in accordance with the Personal Device Acceptable Use and Security Policy (BYOD) will have VPN and Remote Access.
- Only IT approved VPN clients may be used.
- By using VPN technology, users must understand that their machines are an extension of SDCC's network and as such are subject to the same rules and regulations, as well as monitoring for compliance with this policy.

VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a SDCC approved VPN configured to drop all unauthenticated and unencrypted traffic and will be provisioned with split-tunneling disabled. As with all SDCC computers, Windows or other OS and/or browser Internet proxy settings will be enabled to effectively route Internet access to the device through SDCC firewalls and Internet filters.

To comply with this standard, wireless implementations should maintain point to point hardware encryption of at least 128 bits, support a hardware address that can be registered and tracked (i.e. a MAC address), and support and employ strong user authentication, which checks against an external database such as TACACS+, iDiTJS, or something similar. Any deviation from this practice will be considered on a case-by-case basis.

VPN Approval, Acceptable Use Review, and Acceptance

Approval from a staff director or higher authority is required for a user's VPN access account creation. A sample acceptable use form is attached to the VPN procedure maintained by SDCCD IT and shall be reviewed and signed by each approved user to acknowledge having read and

understood the policy (see Exhibit A). This form shall in turn be approved, collected, and retained by SDCCD IT management prior to the user's VPN account use.

EXHIBIT A

SAMPLE Virtual Private Network (VPN) Agreement

This Virtual Private Network Agreement is entered into between the User and SDCC, effective the date this agreement is executed by SDCCD's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a mobile device connecting to the SDCC network is a privilege granted to the User by management approval per the Network Security and VPN Acceptable Use Policy. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to SDCC and to ensure the data remains secure.

In the event of a security breach or threat, SDCC reserves the right, without prior notice to the User, to disable or disconnect the VPN connection of the mobile device.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following SDCC policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, Anti-Virus, E-Mail, Password, Safeguarding Member Information, and Telecommuting.

User of the mobile device shall not remove sensitive information from the SDCC network, attack SDCC assets, or violate any of the security polices related to the subject matter of this agreement.

The User understands and agrees that his/her use of the VPN software is required as part of his/her employment at SDCC and is permitted to connect to internal information services in support of SDCC activities only. The User will safeguard the VPN access as well as its components (software/password) from any unauthorized use.

The VPN will be used on a company issued mobile device that is protected by a personal firewall. The company issued mobile device may be subject to scanning from the IT Department to check compliance with the contents of this Agreement.

SUPPORT

SDCC will offer support for connectivity to the SDCC network. SDCC is not responsible for ISP outages that result in a failure of connectivity to the SDCC network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the SDCC network.

The User certifies that this Agreement has been read and has an understanding of the above conditions under which the User may be provided access to SDCC computer/information systems and further that the User understands and agrees to abide by them. The User also understands that limitations on disclosure of any information covered under this Agreement shall survive the modification or elimination of the User access to SDCC computer/information systems.