Overview

Acceptable use of BYOD (bring your own device) at SDCC must be managed to ensure that access to SDCC's resources for business are performed in a safe and secure manner for participants of the BYOD program. A participant of the BYOD program includes, but is not limited to:

- Employees
- Students
- Contractors
- Board of Directors
- Volunteers
- Related constituents who participate in the BYOD program

This standard is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

Purpose

This standard defines the practices, procedures, and restrictions for end users who have legitimate business requirements to access corporate data using their personal device. This policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the SDCC BYOD program which contains stored data owned by SDCC, and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any non-SDCC owned mobile device capable of storing corporate data and connecting to an unmanaged network

This standard addresses a range of threats to, or related to, the use of SDCC data:

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee

Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware, and other threats could be introduced via a mobile device
Compliance	Loss or theft of financial and/or personal and confidential data could expose SDCC to the risk of non-compliance with various identity theft and privacy laws

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This standard is complementary to any other implemented standards dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the SDCC network.

Audience

This standard applies to all SDCC constituents, including administrators, faculty, staff, students, vendors, and other agents who utilize personally owned mobile devices to access, store, backup, relocate, or access any organization or member-specific data. Such access, to this confidential data is a privilege, not a right, and forms the basis of the trust SDCC has built with its constituents. Consequently, employment at SDCC does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Standard Detail

This standard applies to:

- Any privately owned wireless and/or portable electronic handheld equipment, hereby referred to as BYOD. SDCC grants potential participants of the BYOD program the privilege of purchasing and using a device of their choosing at work for their convenience.
- Related software that could be used to access corporate resources.

This standard is intended to protect the security and integrity of SDCC's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The Audience, as defined above, must agree to the terms and conditions set forth in this standard to be able to connect their devices to the company network. If users do not abide by this standard, SDCC reserves the right to revoke this privilege.

The following criteria will be considered initially, and on a continuing basis, to determine if the Audience is eligible to connect a personal smart device to the SDCC network.

- Management's written permission and certification of the need and efficacy of BYOD for that Employee
- Sensitivity of data the Audience can access
- Legislation or regulations prohibiting or limiting the use of a personal smart device for SDCC business
- Must be listed on the Information Technology Department's list of approved
- mobile devices
- Audience's adherence to the terms of the Bring Your Own Device Agreement and this policy and other applicable policies
- Technical limitations
- Other eligibility criteria deemed relevant by SDCC or IT

Responsibilities of SDCC

- IT will centrally manage the BYOD program and devices including, but not limited to, onboarding approved users, monitoring BYOD connections, and terminating BYOD connections to company resources upon the users leave of employment or service to SDCC.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable.

- IT reserves the right to refuse, by non-physical means, the ability to connect mobile devices to SDCC and SDCC-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts SDCC's systems, data, users, and members at risk.
- IT will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to the SDCC infrastructure. To find out if a preferred device is on this list, an individual should contact the SDCC IT department Service Desk. Although IT currently allows only listed devices to be connected to the SDCC infrastructure, IT reserves the right to update this list in the future.
- IT will maintain enterprise IT security standards.
- IT will inspect all mobile devices attempting to connect to the SDCC network through an unmanaged network (i.e., the Internet) using technology centrally managed by the IT Department.
- IT will install the Mobile VPN software required on Smart mobile devices, such as Smartphones, to access the SDCC network and data.

SDCC's IT Department reserves the right to:

- Install anti-virus software on any BYOD participating device
- Restrict applications
- Limit use of network resources
- Wipe data on lost/damaged devices or upon termination from the BYOD program or SDCC employment
- Properly perform job provisioning and configuration of BYOD participating equipment before connecting to the network
- Through standard enforcement and any other means deemed necessary, to limit the ability of end users to transfer data to and from specific resources on the SDCC network

Responsibilities of BYOD Participants Security and Damages

All potential participants will be granted access to the SDCC network on the condition that they read, sign, respect, and adhere to the SDCC standards concerning the use of these devices and services (see Exhibit A). Prior to initial use on the SDCC network or related infrastructure, all personally owned mobile devices must be registered with IT. Participants of the BYOD program and related software for network and data access will, without exception:

- Use secure data management procedures. All BYOD equipment, containing stored data owned by SDCC, must use an approved method of encryption during transmission to protect data.

- Be expected to adhere to the same security protocols when connected with approved BYOD equipment to protect SDCC's infrastructure.

SDCC data is not to be accessed on any hardware that fails to meet SDCC's established enterprise IT security standards.

- Ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied to BYOD use.
- Utilize a device lock with authentication, such as a fingerprint or strong password, on each participating device. Refer to the SDCC password standard for additional information.
- Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.
- Passwords and confidential data should not be stored on unapproved or unauthorized non-SDCC devices.
- Exercise reasonable physical security measures. It is the end user's responsibility to keep their approved BYOD equipment safe and secure.
- A device's firmware/operating system must be up to date to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of the owner.

Any non-corporate computers used to synchronize with BYOD equipment will have installed anti-virus and anti-malware software deemed necessary by SDCC's IT Department. Anti-virus signature files must be up to date on any additional client machines – such as a home PC – on which this media will be accessed. IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.

If A) any BYOD device is lost or stolen, immediately contact SDCC IT; and, if B) any BYOD device is scheduled to be upgraded or exchanged, the user must contact IT in advance. IT will disable the BYOD and delete associated company data. BYOD equipment that is used to conduct SDCC business will be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's access.

Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with SDCC's overarching security standard. Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.

The user agrees to and accepts that his or her access and/or connection to SDCC's networks may be monitored to record dates, times, duration of access, etc. This is done to identify unusual usage patterns or other suspicious activity, and to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains SDCC's highest priority.

Employees, Board of Directors, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of SDCC owned and installed hardware or software without the express approval of SDCC's IT Department. The end user agrees to immediately report to his/her manager and SDCC's IT Department, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of SDCC resources, databases, networks, etc.

Third Party Vendors

Third party vendors are expected to secure all devices with up-to-date anti-virus signature files and anti-malware software relevant or applicable to a device or platform. All new connection requests between third parties and SDCC require that the third party and SDCC representatives agree to and sign the Third-Party Agreement. This agreement must be signed by the Vice President of the sponsoring department, as well as a representative from the third party who is legally empowered to sign on behalf of the third party. By signing this agreement, the third party agrees to abide by all referenced policies. The document is to be kept on file. All non-publicly accessible information is the sole property of SDCC.

The IT Department can supply a non-SDCC Internet connection utilizing a US Cellular hot spot if needed.

Help and Support

SDCC's IT Department is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

Organizational Protocol

SDCC may offer a reimbursement of expenses to employees if they choose to use their own mobile devices in lieu of accepting a SDCC-issued device. This may vary on the employees' function within the district and will be in accordance with a schedule in the associated procedure.

EXHIBIT A

SAMPLE Bring Your Own Device (BYOD) Agreement

This Bring Your Own Device Agreement is entered into between the User and San Diego City College (SDCC). Effective the date this agreement is executed by SDCC's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a supported smart device owned by the User in connection with SDCC business is a privilege granted to the User, by management approval, per the Personal Device Acceptable Use and Security Standard. A supported smart device is defined as an Android- or IOS-based cell phone or tablet running a manufacturer's supported version of its operating system. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The standards 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 some or all BYOD services related to connection of a personal smart device to the SDCC network.

REIMBURSEMENT CONSIDERATIONS

SDCC may offer a fixed reimbursement (stipend) to eligible Users starting the month following BYOD enrollment. Contact Human Resources for possible reimbursement schedule. The User is personally liable for the device and carrier service.

Accordingly, SDCC will NOT reimburse the User, over and above the monthly reimbursement, for any loss, cost, or expense associated with the use or connection of a personal smart device to the SDCC network. This includes, but is not limited to, expenses for voice minutes used to perform SDCC business, data charges related to the use of SDCC services, expenses related to text or other messaging, cost of handheld devices, components, parts, or data plans, cost of replacement handheld devices in case of malfunction whether or not the malfunction was caused by using applications or services sponsored or provided by SDCC, loss related to unavailability of, disconnection from, or disabling the connection of a smart device to the SDCC network, and loss resulting from compliance with this Agreement or applicable SDCC standards.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following SDCC standards published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, Personal Device Acceptable

Use and Security, and other related standards including, but not limited to, Anti-Virus, E-Mail, Network Security, Password, Safeguarding Member Information, Telecommuting.

The User of the personal smart device shall not remove sensitive information from the SDCC network, attack SDCC assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

SDCC may offer the following support for the personal smart device: connectivity to SDCC servers, including email and calendar, and security services, including policy management, password management, and decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), or change of ownership. SDCC is not able to provide any additional assistance on any personally owned device and is not responsible for carrier network or system 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 the SDCC network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data, or which render the smart device inoperable.

DISCLAIMER

SDCC expressly disclaims, and the User releases SDCC from, all liability for any loss, cost, or expense of any nature whatsoever sustained by the User in connection with the privilege afforded the User under the terms of the Agreement.