Chelsea Theatre Bring Your Own Device Policy

Overview

Acceptable use of BYOD at Chelsea Theatre must be managed to ensure that access to Chelsea| theatre's resources for business are performed in a safe and secure manner for participants of the Chelsea Theatre BYOD program. A participant of the BYOD program includes, but is not limited to:

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

This policy 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 policy defines the standards, 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 Chelsea Theatre BYOD program which contains stored data owned by Chelsea Theatre 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-Chelsea Theatre owned mobile device capable of storing corporate data and connecting to an unmanaged network

This policy addresses a range of threats to, or related to, the use of Chelsea Theatre 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 Chelsea Theatre 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 policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the Chelsea Theatre network.

Audience

This policy applies to all Chelsea Theatre employees, including full and part-time staff, Board of Directors, volunteers, contractors, freelancers, and other agents who utilize personally-owned mobile devices to access, store, back up, 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 Chelsea Theatre has built with its members, suppliers, and other constituents. Consequently, employment at Chelsea Theatre does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy applies to:

- Any privately owned wireless and/or portable electronic handheld equipment, hereby referred to as BYOD. Chelsea Theatre 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 policy is intended to protect the security and integrity of our 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 policy to be able to connect their devices to the company network. If users do not abide by this policy, Chelsea Theatre 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 Chelsea Theatre 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 Chelsea Theatre 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 Chelsea Theatre or IT

Responsibilities (Richard Lucas LTD)

- 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 Chelsea Theatre
- 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 Chelsea Theatre connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts Chelsea Theatre'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 Chelsea Theatre infrastructure. To find out if a preferred device is on this list, an individual should contact the Chelsea Theatre IT department Service Desk. Although IT currently allows only listed devices to be connected to the Chelsea Theatre 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 Chelsea Theatre 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 Chelsea Theatre network and data.

Our 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 Chelsea Theatre employment, volunteering or trusteeship.

- Properly perform job provisioning and configuration of BYOD participating equipment before connecting to the network

- Through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the Chelsea Theatre network

Responsibilities of BYOD Participants Security and Damages /R

- All potential participants will be granted access to the Chelsea Theatre network on the condition that they read, sign, respect, and adhere to the Chelsea Theatre policies concerning the use of these devices and services.

- Prior to initial use on the Chelsea Theatre 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:

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

o Be expected to adhere to the same security protocols when connected with approved BYOD equipment to protect infrastructure.

• Chelsea Theatre data is not to be accessed on any hardware that fails to meet established enterprise IT security standards.

o Ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied to BYOD use.

o Utilize a device lock with authentication, such as a fingerprint or strong password, on each participating device. Refer to the Chelsea Theatre password policy for additional information.

o Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.

o Passwords and confidential data should not be stored on unapproved or unauthorized non-Chelsea Theatre devices.

o Exercise reasonable physical security measures. It is the end users responsibility to keep their approved BYOD equipment safe and secure.

o A device's firmware/operating system must be up-to-date in order to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of the owner.

o Any non-corporate computers used to synchronize with BYOD equipment will have installed anti-virus and anti-malware software deemed necessary by our 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.

o 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.

o If A) any BYOD device is lost or stolen, immediately contact Chelsea Theatre management; 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. /R

o BYOD equipment that is used to conduct Chelsea Theatre business will be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's access.

o Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with the overarching security policy.

o 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.

o The user agrees to and accepts that his or her access and/or connection to Chelsea Theatre'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 amongst our highest priorities.

o Employees, Board of Directors, trustees, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of Chelsea Theatre owned and installed hardware or software without the express approval of Chelsea Theatre's Management.

o The end user agrees to immediately report, to his/her manager any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of Chelsea Theatre 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 Chelsea Theatre require that the third party and Chelsea Theatre 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 Chelsea Theatre

Help and Support

Chelsea theatre 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.