

CHURCH ON THE STREET

Data Security

Document Type: Policy


Document Code: P005

Written Date: 01 May 2023

Approved by:

Name: Hannah Emmett

Role: Treasurer

Signed: 

Date: 05/05/2023

Name: Alastair Barrie

Role: Secretary

Signed: 

Date: 05/11/2023

CHURCH ON THE STREET

Contents

| | |
|-------------------------------|----------|
| Contents | 2 |
| Purpose | 3 |
| Scope | 3 |
| Security-Related Events | 3 |
| Workstation Security | 4 |
| Authorised Users | 4 |
| Safeguards | 4 |
| Appropriate measures include: | 4 |
| Software Installation | 5 |
| Password Security | 5 |
| Requirements | 5 |
| Standards | 5 |
| Protective Measures | 5 |
| E-mail Usage | 6 |
| Remote Working | 6 |

CHURCH ON THE STREET

Purpose

Church on the Street (COTS) is entrusted with the responsibility to provide various services to service users who provide us with confidential personal data. Inherent in this responsibility is an obligation to provide strong protection against theft of data and all other forms of cyber threats.

The purpose of this policy is to establish standards for the base configuration, and acceptable use of equipment and any software running on it that is owned and/or operated by COTS or equipment that accesses COTS's internal systems.

Effective implementation of this policy will reduce the risk of unauthorised access to COTS's proprietary information and technology and protect confidential personal data.

Scope

This policy applies to equipment owned/ operated by COTS, and to employees/ volunteers connecting to any COTS owned network domain or cloud applications that are used as part of projects or assignments managed by COTS.

Security-Related Events

Security-related events will be reported to the Operations Director. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Evidence of unauthorised access to privileged or non-privileged online accounts.
- Evidence of unauthorised access to privileged or non-privileged offline folders, cupboards, drawers where personal data is stored.
- Service interruptions, error messages, or other anomalous occurrences such as that are not related to specific applications on the host.
- Loss of work related equipment: phone, laptop, desktop, paper, ring binders

CHURCH ON THE STREET

Workstation Security

Authorised Users

Appropriate measures must be taken when using workstations to ensure that exposure of sensitive information is restricted to authorised users.

Safeguards

COTS will implement appropriate physical, administrative, and technical safeguards for all workstations that access data or information that is confidential or sensitive to restrict access to only authorised users.

Appropriate measures include:

- Restricting physical access to workstations to only authorised personnel.
- Configuring screen-locks to automatically lock the screen after 10 minutes of inactivity, and requiring personnel to manually enable screen-lock on workstations prior to leaving the area to prevent unauthorised access.
- Providing personnel with documentation for all password policies and procedures, and verifying personnel compliance said password policies and procedures as defined by IT management.
- Ensuring workstations are used for authorised business purposes only.
- Creating a documented list of authorised software applications for each classification of workstation determined by job requirements performed with that workstation, and providing personnel with this list that pertains to their role. Compliance should be verified by ensuring that no unauthorised software applications are installed on workstations.
- Storing all confidential or sensitive information on authorised cloud resources only.
- Securing laptops that contain confidential or sensitive information by using cable locks or locking laptops up in drawers or cabinets when not in use.
- Antivirus - All windows workstations and laptops MUST have an approved anti-virus application installed and activated that offers real-time scanning protection to files and applications.
- All anti-virus applications must have automatic updates enabled and the status of automatic updates must be periodically verified. If automatic updates are not being successfully applied, IT management must be notified immediately.

CHURCH ON THE STREET

Software Installation

Employees may not install software on COTS's computing devices owned by COTS without prior permission from the Operations Director.

Password Security

Requirements

All system-level passwords (Administrator, etc.) must be changed on a quarterly basis, at a minimum. Technical controls should be used whenever possible to prevent the reuse of passwords, and enforce minimum password complexity. All user-level passwords (e-mail, web, desktop computer, etc.) must be changed at least every six months. All user-level and system-level passwords must conform to the standards described below.

Standards

Password policy should be provided to all users at COTS in order to create awareness of how to select strong passwords. Strong passwords have the following characteristics:

- Contain at least one of each of the following character classes:
 - Lower case characters
 - Upper case characters
 - Numbers
 - "Special" characters (e.g. @!.,#\$%^&*()_+|~-=\`{}[]:;';<>/ etc)
- Have a minimum length of 12 characters
- A password manager must be used to generate a pseudo random password that conforms to the above characteristics of an arbitrary length between 12 and 30 characters. All personnel must use the password manager to store passwords and make them available on all desktop, laptop, and mobile devices.

Protective Measures

- Do not share COTS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential COTS information.
- Passwords should never be written down or stored anywhere online except in a password manager application that has been deemed acceptable by IT managers.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").

CHURCH ON THE STREET

- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the Operations Director.
- Always decline the use of the “Remember Password” feature of native applications such as browsers, and web-applications.
- Two-factor authentication (2FA) MUST be enabled on all accounts that provide such a feature, and 2FA codes MUST be stored in a 2FA authenticator mobile application that has been deemed acceptable by IT managers. 2FA backup codes should also be stored in a password manager to ensure their security, and if 2FA backup codes are provided via a downloaded file, that file must be deleted, and purged from the trash-bin.

E-mail Usage

COTS e-mail system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any COTS employee must report the matter to their supervisor immediately.

The following activities are strictly prohibited for email, telephone, or any other messaging service or application:

- Sending unsolicited messages, including the sending of “junk mail”, “spam”, or other advertising material.
- Any form of harassment, whether through language, frequency, or size of messages.
- Fraud, identity misrepresentation, or forging of email protocol header information.
- Any communication that is not related to COTS’s charitable/ operational activities.
- Using non-COTS email accounts (i.e., Gmail, Hotmail, Yahoo), or other external resources to conduct charitable/ operational activities business.

Remote Working

Any employee or volunteer that works primarily at home or on an ad-hoc basis must follow all the above guidelines as if they are working on COTS premises.

| | |
|-----------------------|--------------------------------|
| TITLE | P005 Data Security May 2023 V1 |
| DOCUMENT ID | 231223904166046 |
| DOCUMENT PAGES | 6 |
| STATUS | COMPLETED |
| TIME ZONE | Europe/London |

DOCUMENT HISTORY

| | | | |
|---|------------------|--------------------------|---|
|  | Invitations Sent | May 03, 2023 02:53 PM | Sent for signature to (hannah@cots-ministries.co.uk) IP: 188.28.106.41 |
|  | Process Started | May 03, 2023 02:53 PM | The document has been sent for signature. |
|  | Invitations Sent | May 03, 2023 02:53 PM | Sent for signature to (alastair@cots-ministries.co.uk) IP: 188.28.106.41 |
|  | Viewed | May 05, 2023 08:44 AM | Viewed by (hannah@cots-ministries.co.uk) IP: 92.17.164.120 |
|  | Signed | May 05, 2023 08:46 AM | Signed by (hannah@cots-ministries.co.uk) IP: 92.17.164.120 |
|  | Viewed | May 11, 2023 01:53 PM | Viewed by (alastair@cots-ministries.co.uk) IP: 82.132.184.221 |
|  | Signed | May 11, 2023 01:56 PM | Signed by (alastair@cots-ministries.co.uk) IP: 82.132.184.221 |

| | |
|-----------------------|--------------------------------|
| TITLE | P005 Data Security May 2023 V1 |
| DOCUMENT ID | 231223904166046 |
| DOCUMENT PAGES | 6 |
| STATUS | COMPLETED |
| TIME ZONE | Europe/London |

DOCUMENT HISTORY

| | | | |
|---|-------------------|--------------------------|----------------------------------|
|  | Process Completed | May 11, 2023 01:56 PM | The document has been completed. |
|---|-------------------|--------------------------|----------------------------------|