IT Security Policy

Contents

Introduction

OCN London takes security very seriously. All staff are made aware of security procedures to be followed in the handling or personal information. Please note that Internet e-mail is never a 100% secure communication medium. By using it you agree that you will send any information by e-mail at your own risk. Whilst OCN London will take all reasonable precautions to ensure that other organisations with whom we deal have good security practices, we are not responsible for the privacy practices of those organisations whose websites may be linked to the site.

Status of this Policy

This policy does not form part of the formal contract of employment for staff but it is a condition of employment and will abide by the rules and policies made by OCN London from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Scope

The scope of this document applies to any electronic data handled by any OCN London staff member, or consultant hired by OCN London, that relates to the work for OCN London.

Key Information Assets

OCN London's key information assets are grouped as follows:

- Centre information
- Learner information
    - Registration
    - Achievement
    - Assignments
- Qualification and unit information

All key information is stored on the main Quartz database.

Information pertaining to Learner assignments is held on the OPAL and OPT systems.

Physical security

- The premises are accessed with a key and fob system.
- A log must be kept of all keys and fobs in circulation.
- Physical data records must be kept in a locked cabinet on the premises.
- Physical IT equipment must be kept in a locked room.

Hardware

LAPTOPS AND DESKTOPS

- Local firewall on all machines
- AntiVirus on all machines,
- Automatic updates on all machines
- All Operating Systems kept up to date
- Secondary AntiVirus software installed on all machines for secondary ad hoc malware scans

SERVERS

- All on-premise servers non-internet facing and behind Hardware Firewall
- Local Firewall on all machines
- Operating Systems kept up to date.

NETWORK EQUIPMENT

- Hardware Firewall to prevent any outside connections.
- WiFi access points with firmware kept up to date and protected with passwords.

Passwords

OCN London follows the following guidance regarding a successful password policy:

- Maintain an 8-character minimum length requirement (longer isn't necessarily better)
- Don't require character composition requirements. For example, *&(^%$
- Don't require mandatory periodic password resets for user accounts
- Ban common passwords, to keep the most vulnerable passwords out of your system

- Educate your users to not re-use their organization passwords for non-work related purposes
- Enforce registration for multi-factor authentication
- Enable risk-based multi-factor authentication challenges

Office365 and Google password controls follow the above guidance.

In the case of Quartz, passwords expire after 90 days.

Remote Access

Remote access is only allowed by arrangement with IT.

Remote users are required to access with multi-factor authentication. They must set up MFA by adding their own mobile phone numbers as authentication phones and another number (i.e. their office phone) as secondary authentication numbers.

An exception is made to MFA in the case of emails on staff members mobile phones.

In all cases, where a work account is being accessed from a non-work device (eg work emails on a personal mobile phone), that device must itself be protected by a password, pin code or biometric data.

RESPONSIBILITIES OF STAFF REGARDING REMOTE ACCESS

- Don't save Passwords on non-work devices, except emails/calendars on phones
- Always sign out after a session
- Do not save confidential information in folders local to the remote machine, e.g. the desktop.
- Secure all non-work devices that are used to access work with passwords.

Responsibilities of staff

- Don't open unsolicited attachments
- Exercise common sense for suspicious emails
- Remote PCs - do not install anything without consulting IT.
- No sharing of folder and files with non-OCN London staff without prior consultation with IT. If files in the cloud need to be shared with non-OCN London staff, should be sent as an email attachment.
- Do not attempt to amend Firewall or Windows Defender settings

Back-up Policy

The key data assets covered by the back-up policy are:

- Files and folders
- Emails
- Databases

- Websites

OCN London takes a layered approach to back-ups that is tailored depending on the asset being protected. Assets are backed up continually in the location in which they sit to enable easy retrieval. The second layer is an online back-up in a separate cloud based location. These back-ups are taken nightly and kept indefinitely. The third layer is a hard disk back up taken monthly.

Back up methods are detail in the *Detailed Back-up Policy.*

Data Retention Policy

20. OCN London has a duty to retain some staff and learner personal data for a period of time following their departure from OCN London, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Different categories of data will be retained for different periods of time. The exact details of retention periods and purposes are set out in the Records Retention Schedule.

The data protection officer is responsible for implementing and monitoring compliance with this policy. They will undertake an [annual] review of this policy to verify that it is in effective operation.

All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

Hard copy and electronically-held documents and information must be deleted at the end of the retention period.

Hard copy documents and information must be disposed of by shredding.

Retention of data is detailed in the Record Retention Schedule.