netcom TRAINING

IT Security Policy

Reviewed by Adam Davies, Quality Manager

Approved by Lynne Whitehouse, Operations Director

Version date: 14/7/21

Review schedule: 14/7/22 or in line with operating procedure and/or legislative updates/requirements

Person/s responsible: SLT, all management and staff

Signed Adam Davies

Signed ……

Policy owner

Contents

Overview

This policy sets out key objectives to protect the security of the company computer network and resources and the principles and responsibilities in relation to the safe and effective management of its information management systems. Suitable levels of security will be applied to mitigate the risks of theft, loss, misuse, damage, or abuse. The policy will apply to all staff, learners and any other party accessing company information systems and networks. All users will need to be aware of the confidentiality and integrity of data they may handle

Account Security

Staff Accounts and Responsibilities

All staff (including contracted, temporary and agency staff where applicable) must agree to written terms and conditions covering the safe and acceptable use of IT before access can be granted to enable the use of the company's IT systems. (See Appendix A)

Unique user ID and login credentials observing generally agreed best practice password security measures will be provided which must not be shared with other staff. This will also enable individual usage to be tracked and monitored if there may be reason to do so to ensure the appropriate security processes are maintained and to avoid potential breaches of policy requirements.

The IT department will ensure that:

- Temporary staff accounts will be set to expire at the end of the staff contract period.
- Staff accounts will be disabled when a member of staff's employment ends or in times of an extended absence.
- Staff accounts are only assigned rights and permissions commensurate with job roles and responsibilities.

Awareness training about electronic information security and the proper use of the company's IT systems will form part of the Staff induction process.

Learner Accounts and Responsibilities

In order to use the company's IT Systems, learners must agree to written terms and conditions covering the safe and acceptable use of IT before they will be allowed access.

Awareness training about electronic information security and the proper use of the company's IT systems will form part of the Learner Induction process.

Learner accounts will be individually assigned where applicable and are not to be shared to protect the privacy of information. The same tracking/monitoring of usage processes apply as per those detailed for staff.

The company IT department will ensure that:

- Learner accounts are only assigned access rights and permissions that are appropriate to course study and assessment requirement and will be set to expire within an agreed timescale following course completion.

There is no requirement for any learner to store any personal or confidential information on the company's IT system.

Confidential Exam and Assessment Resources

Examination or assessment resources will be accessible via Cloud based services negating the need to add or remove them from the local system by an authorised person either using removable media or through a user account with a suitable level of permissions. In unforeseen circumstances where removable media may be required, it will be stored in a locked cabinet when not in use. Awarding body guidelines and procedures will be followed at all times to preserve the confidentiality of data and integrity of qualifications.

System Security

All systems, such as servers, network equipment, wireless access and workstations will have security features enabled/installed, such as firewalls, antivirus, encryption, etc. appropriate to the device, in order to harden the systems against attack. Staff will be advised to carry out any authorised security updates and installation processes when prompted to do so.

Operating systems and firmware on all devices are supported by a supplier that has regular updates and fixes for security problems. Any previously used applications that are no longer supported have been removed.

All unnecessary or unused features or facilities will be disabled or removed in order to reduce the attack surface of the systems.

All configurable devices will have a secure administration account with a secure username/password which is known only to authorised members of the IT department.

Physical Security

Servers and Networking

Cloud based virtual servers are in operation negating the need to have physical servers on site holding personal or confidential data (including exam and assessment resources). "Test" servers are located on site for the purposes of demonstrations and lab work only as part of learning programme tuition and practice use. The LAN cabinet is kept locked and only accessible to authorised personnel.

Portable Equipment

Any portable IT equipment must be either appropriately secured to prevent removal or kept in a secure locked environment when not in use. If the latter, the equipment will not be left with unsupervised learners or visitors.

Service Provider

The business will invoke a Disaster Recovery plan with its IT service provider to ensure that systems essential to the delivery or the administration of learning programmes, including apprenticeships are recovered and operational as soon as is reasonably practicable in the event of service failure/loss. Data is stored on cloud-based services and backed up as part of normal procedure to assist this objective. The service provider will commit to the following as part of the continuity agreement:

- Review incident history
- Gather diagnostics
- Propose repair/replacement/response based on the nature/scale of the incident
- Arrange technical personnel, if applicable
- Provide regular status updates
- Contact to confirm successful resolution
- Provide the Customer with DR Incident Report

Monitoring/review

The policy and procedures will be reviewed at least annually or in the light of significant changes to processes or legal requirements or policy breaches. Any such changes will be communicated at the earliest opportunity to all relevant staff, learners and other parties that may be affected.

Appendix A

Computer Systems and Internet Usage Terms and Conditions

1. Netcom Training Ltd (the Company) shall reserve the right to review all files and records and the right to periodically monitor, audit and review network, workstation, internet, and email use on the company network. No employee or learner should have any expectation of privacy as to internet access. Our IT department may request a review of internet activity to analyse usage patterns and may choose to perform detailed analysis of the data to assure the training centre network and internet access are devoted to maintaining the highest levels of productivity and security.

2. The Company will not tolerate the use of cyber-bullying of individuals using mobile phones, social networking sites or other. It is an offence to send indecent, offensive, or threatening messages with the purpose of causing the recipient distress or anxiety. Suspected or actual cases amounting to cyber-bullying will lead to investigatory proceedings and disciplinary action where applicable and staff dismissal and/or the termination of a learner's programme in the most severe instances.

3. Sexually explicit, illegal, or other potentially offensive material may not be viewed, archived, stored, distributed, edited or recorded using the training centre network. Such activities will be viewed as gross misconduct and where appropriate reported to the Police.

4. In the event of company systems being connected accidentally to a site that contains sexually explicit or offensive material, the user must disconnect from that site immediately and the line manager or tutor (in the case of learners) informed of the incident.

5. Nobody may use the company network or internet access to knowingly download or distribute pirated software or data.

6. Nobody may use the company network or internet access to knowingly propagate any virus, worm, Trojan horse, trap-door program code or malicious malware.

7. Nobody may use the company network or internet access to knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user (commonly known as 'hacking').

8. Those accessing the company network may only download licensed and registered software directly related to the user's permission requirements or

requested purpose requiring senior management approval e.g., educational activities for learners. Downloaded software must only be used under the terms and conditions of its licence. Any decision to install new company wide software or part thereof will require authorisation from the Operations Director in consultation with the IT department.

9. Nobody may use the company network to knowingly download and make use of entertainment software or games via the internet or LAN.

10. Personal devices such as laptops, smartphones and tablets are not permitted to be attached to the training centre network unless authorised by the IT department. USB and optical drives can be used for removable media where devices have been virus scanned at the point of installation and under the supervision of the trainer in the case of learners wishing to view and edit any documents for the purpose of their learning. Autorun will be disabled on USB and optical drives to reduce the risk of malware infecting computer systems.

11. Any file that is downloaded to the company's network must be scanned for viruses before it is run or accessed.

12. Unsupervised learner access to the classrooms and computers before or after class sessions or during breaks is not permitted.

13. No company desktop PC may be opened internally, or any component removed other than those machines specifically designated as 'practical workshop PCs' and then only under the direction of a technical trainer. Any hardware failure should be reported to the IT department who will troubleshoot and aim to resolve the issue.
14. Home based/mobile workers will be required to adhere to the following secure working practices in relation to data protection:
    - Follow all procedures set out within this policy and observe all terms and conditions
    - Use only organisationally approved technology(hardware and software) to provide a suitable level of protection
    - Maintain confidentiality within a home environment or other business setting
    - Avoid printing out information relating to private/confidential data unless absolutely necessary
    - Secure equipment when not in use, ideally locked away
    - Carry out company approved software security updates when required
    - Use company e mail and messaging accounts only for the transmission of personal/confidential data

15. Violations of this policy may subject the individual to disciplinary and/or legal action.

Appendix B Covid-19 business update

Since the outbreak of the Coronavirus and resulting lockdown in the UK, the company has taken the initial decision to close business premises from March 2020. The terms and conditions of users accessing company systems and networks whether on business premises or remotely remain unchanged. The training, assessment and management of learners is taking place remotely via a collaborative communication system, requiring them to gain access using their own personal equipment. All learners are informed at their induction prior to the start of learning of general e safety tips and their permissions and responsibilities when accessing the system to upload or download any files that may be required of them during their programme. They are also informed of expected conduct and etiquette when posting any information within the channel assigned to them. All other aspects of the policy are unaffected. The IT security arrangements in the centre will be reviewed as and when learners may return, pending the lifting of restrictions brought about as a result of the pandemic.