ACCESS CONTROL POLICY

Introduction

The objective of this Policy is to protect the confidentiality, integrity and availability of the Organisation's information by controlling access to its IT and paper-based systems. The Data Protection Policy is to be regarded as integral to this Policy.

Responsibilities

1. All staff are responsible for ensuring that this Policy, along with the Data Protection Policy, is fully complied with.

2. Overall responsibility for the security of the Organisation's networks rests with the CEO, assisted by the Head of Operations (ISMS Manager), who may delegate day-to-day technical issues regarding access control.

3. All of the Organisation's employees are responsible for controlling access to Organisation information in accordance with this Policy and the Data Protection Policy at all times.

Network Access

The following instructions apply to all users of the Organisation's IT systems:

1. Access to the Organisation's network is controlled by means of individual user logins and passwords. Login names are allocated by the Internal IT Manager, who also issues the initial password for each user

2. Immediately on receiving a login and password, the user must change the Password to one that they have created in accordance with the Password Policy. Thereafter, the operating system automatically prompts for a password change at intervals controlled by the Internal IT Manager.

3. Access to accounting and operations software is controlled by means of login and password. This information is given only to users who need to work with the respective packages, and their level of access is controlled by permissions allocated to the various login identities

4. Logins and passwords are not to be revealed to anyone, even a colleague, supervisor or manager. The exception to this rule is set out in the Password Policy

5. Users may access the network and their own files by logging on to any PC on the system. However, access to network objects is limited by individual logins that are authorised on the basis of operational requirements

6. User rights are decided by the Internal IT Manager only and are not to be changed. This instruction is reviewed at the ISMS Management Review meetings

7. User rights are kept to the minimum necessary for efficient working. Anyone who feels that they would work more efficiently with increased user rights must justify this to their line manager and this will be implemented through our change management process.

8. Users must not allow other users to access any systems via their login, either by logging in deliberately on the other's behalf or by logging in and leaving the PC unattended

9. Monitoring is implemented on all systems to record login attempts and failures, successful logins and all changes made

10. Remote access to the Organisation's systems (if applicable) is subject to particularly careful control. This is addressed in the Remote Access and Mobile Computing Policy that is set out in this Management System

11. Currently no third party (other than those approved by the ISMS Committee) has any access rights to the Organisation's networks

12. Anyone who suspects there may have been a breach of network access rules must report it immediately to the Internal IT Manager. If the breach involves the possibility of unauthorised access to Personal Data, this must be reported immediately to the Data Protection Officer.

Access to online information

1. The Organisation's electronic information can be made available to all users, to certain defined users, or to the creator only. This is determined by the selection of the appropriate access rights.

2. Sensitive information that is kept on the network, e.g. financial records, is to be protected by the removal of all unnecessary access permissions, including those of Administrators.

3. Should a hacker gain access to the network, every password that stands in their way will offer some protection to sensitive data. Therefore, directories and documents containing such data are not to be named in such a way as to make them easily identifiable. Names indicating Confidential, Top Secret etc. are not to be used.

4. Without appropriate permission, no files are to be created on the Network that are password protected. Should this need arise then specific permission must be given by the CEO / Senior Developer / Head of Operations (ISMS Manager). Details of the authority and the password issued will be securely recorded.

Access to paper-based information

1. Sensitive information on paper, such as personal or financial data, is accessible only to authorised persons.

2. Access must be controlled by means of locked cabinets.

3. Sensitive information is not to be left lying on desks overnight.

4. All waste paper containing business information is shredded.

Premises Security

Physical access to the Organisation's premises and thus to the information systems is controlled as follows:

1. Access to the building is by means of a locked front door, which includes an access fob system, with telephone intercom to the main 1st floor office area

2. In addition, a Warehouse access door is kept closed and secured at all times when access is not immediately required

3. All visitors are required to sign in and out, and are required to accompanied at all times

4. Access to the Organisation's offices on the second floor is via an unsecured access door at the head of the stairs

5. Access to the server equipment is controlled at all times by means of restricted access using a locked server room door

6. Filing cabinets and personal desk-drawsare locked using keys o and are kept locked outside of normal working hours

7. CCTV is in place, which covers the car park and public areas of the site.

Further measures to prevent unauthorised access to information

Apart from the measures outlined above, access to the Organisation's premises, information systems and information is further limited by the following general instructions:

1. No employee who is entrusted with an access fob, combination code or a Password of any kind is to reveal or share this with a fellow employee

2. In the case of equipment destined for repair or disposal, information stored on a hard disk or other storage media is to be protected as follows:

    - Any hard disk intended for repair or contained in equipment being sent away for repair is fully backed up or cloned before dispatch

    - If the disk contains sensitive information, the directories or files containing the information are removed before dispatch

    - Any storage media containing Organisation information, including hard disks, tape cartridges etc. that are faulty or no longer required are rendered unreadable before disposal

3. Disposal of computer equipment is to be carried out by a reputable specialist disposal firm and disposal records are kept for both Information Security and Environmental reasons.

4. Should data be required to be sent or transmitted from the Organisation's premises then information stored on hard disk or any other medium is to be protected by the following means:

    - No computer equipment is to leave the Organisation's premises unless specific permission has been obtained from the (nominated ISMS representative).

    - The exception to the above is the Mobile Computing Facilities. The Remote Access & Mobile Computing Policy covers this.

    - Transportation is only undertaken by reputable carriers or by the Organisation's employees.

    - The Organisation's employees who are transporting computer equipment or storage media take precautions to protect such items from theft, as detailed by the (nominated ISMS representative).

5. When employees leave the Organisation, the following action is taken:

    - The employee's access rights to all IT systems are revoked

    - The relevant e-mail account is disabled

    - Employees are required to reveal all passwords they may have used to protect documents or files created or processed in the course of their duties

    - Employees are required to return all intelligent keys to doors entrusted to them

- Combinations on the filing cabinets only need to be changed if the Organisation feels that there is a potential future risk

The responsibility for arranging these measures lies with the HR Department.

General

Although the Organisation has taken reasonable technical and material precautions to prevent unauthorised access to its information systems, every individual employee can make a decisive contribution to the Organisation's security. Access control of all kinds depends to a great extent on the employee's active participation, watchfulness and consistent compliance with the spirit of this Policy.

Policy Sign-off

Date of Issue:	26/10/2020
Date of Next Review:	
Name:	
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	30/09/2020	Jo Holloway	
2.0	26/10/2020	Jo Holloway	Update to responsibilities