DISABILITY POSITIVE ACCESS CONTROL POLICY

Revision History

Version	Revision Date	Revised by	Section Revised
1.5	22/11/2018	JF	No Changes Made
1.6	12/11/2019	LT	4, 5 onwards – personnel change
1.7	05/12/2019	LT	5.2.3 - MFA
1.8	23/11/2020	LT/MC	4, 5.2.1, 5.5
	30/11/2021	Annual Review – no changes	
1.9	30/11/2022	MC/LT	8

Document Control

Document Owner:	**Document No:**	**Status:**	**Date Approved:**
LT	**8.2**	Approved	**30/11/2022**
Security Classification:	**Next Review Date:**	**Version:**	**Department:**
Medium	**30/11/2023**	V1.9	Operations

1 POLICY STATEMENT

It is the policy of **Disability Positive** *(hereinafter referred to as the **"Company"**)* to protect and secure the information and systems within our remit and we take this function very seriously. We have developed and implemented several physical, logical and procedural measures and controls to enforce our approach. We understand that it is vital to protect the systems and information held and used by us from unauthorised use or access and are fully aware of how such access can affect security, personal information and individuals. ***The types of measures and controls used by the Company are: -***

- **Physical Access Controls** ensuring the availability of systems and information is restricted to authorised persons only, thus preventing locations and information from being accessible to non-authorised individuals. This includes industry standard locks, intruder alarms, restricted access areas, and limited key control.
- **Logical Access Controls** utilise tools and protocols for identification, authentication and authorisation of our computer information systems (*including remote access, laptops and phone systems*). The Company's logical access controls enforce access measures to our systems, programs, processes, and information and include password protocols, user authentication methods, data and authentication credentials encryption and network, system and user-level firewalls.
- **Procedural Access Measures** include our defined policies and procedures that are followed by all staff and third parties and provide the steps for areas such as access control, information security, password protocols and clear desk measures.

2 PURPOSE

The purpose of this policy is to ensure that system based and physical access to any information, location and/or system is controlled and where applicable restricted using controls and procedures that protect the associated information systems and data. The Company is committed to the security of the information and assets within our remit and enforce and stress test all access measures to ensure their functionality, effectiveness and purpose.

This Access Control Policy aims to restrict access to controlled information and/or systems to only those staff or third parties who are authorised or have written permission from the Company. Where temporary and/or partial access to information or systems is required, we follow strict protocols to only enable access to the information or for the duration required by the activity.

3 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 OBJECTIVES

The Company is committed to ensuring compliance with the rules, standards and regulations as laid out by its regulating and governing bodies and confirms that it has developed and implemented the appropriate procedures, systems, controls and measures to manage and mitigate against risk.

For systems containing restricted personal information and data, password controls are in place to limit authorised access.

As a company, we have a full understanding of the compliance standards that we are obligated to meet and confirm that we have in place effective and efficient tools and controls for meeting these obligations under the current regulatory system.

The Company's objectives regarding compliance are: -

- Generic logons are not permitted across the Company systems, however, use of generic accounts under 'controlled' circumstances can be permitted at the discretion of the Chief Executive Officer.
- To ensure relevant company, contractual, regulatory and legislative security standards are met and adhered to, employee screening checks, including references and DBS, are undertaken if required.
- The appropriate level of access to systems and information will be determined based on the user-level, role-based requirements and ad-hoc job functions and roles.
- If authorisation to use systems and information is granted, unique logon credentials and password will be provided to the employee, utilising the strong password controls detailed in this policy.
- Access for remote users shall be subject to receipt of a completed and signed Company Equipment form.

5 PROCEDURES, CONTROLS AND MEASURES

It is pivotal to operating our business and providing services to clients that the Company use computers, telephone systems, software, hardware devices and data storage systems. Due to the nature of our business, such systems are often used to store information and assets that are of a personal and confidential nature. It is therefore essential that we protect and secure such information and therefore access to the systems using a variety of access controls and measures.

We take a multi-tiered approach when securing systems and restricting access and detail in this policy the procedures and methods used throughout the Company. This information is disseminated to all employees and forms part of our information security program.

5.1 LOGICAL ACCESS CONTROL

Access to systems within the Company are governed by our tiered logical access control measures. Access to any system is classified as one of the below access levels and restrictions are implemented at the user level. Levels can be changed at the discretion of a Senior Manager or the Chief Executive Officer. ***Considerations for granting access is assessed based on: -***

- An employee or user's need of access to complete their job and/or task
- Duration of access
- Level of access

- Information types located on the system in questions
- Security measures in place if access is granted
- Ability to remove access at a predetermined time
- Access is decided and allocated on a case by case basis and can only be assigned by Management.

5.1.1 ROLE-BASED ACCESS

Users are identified as being part of a group (*such as employee)* and their level of access is generic to all required areas. This level of access is inherited by all group members and is controlled by Management. Such group access is considered necessary for each employee to enable them to carry out their job and includes access to areas such as email, printers, the Company collection system and phone system. The Senior Management team or Chief Executive Officer can assign role-based access.

5.1.2 MANAGER ACCESS

System access is granted at a higher level for managers and senior managers who can access more system areas than generic employees. Such access is deemed essential to their oversight role and enables managerial staff to carry out functions and processes that require access to personal information, secure systems or data. Manager access is not inherited by the group and only the Senior Management team or Chief Executive Officer can assign Manager Access.

5.1.3 INDIVIDUAL ACCESS

System access is granted at the required level based on a business and/or legal requirement and is only granted to the individual(s) who require access (*i.e. if an employee is granted extended access, this is not inherited by any other role-based group member*). Individual Access is usually granted for a limited period by Management and is deactivated after a set period. Such access may include a role-based user needing access to sensitive information or restricted systems to perform a task or one-off project.

5.2 PASSWORDS

Passwords are a key part of the Company's protection strategy and are used throughout the company to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third parties who are responsible for one or more account, system or have access to any resource that requires a password.

5.2.1 PASSWORD CREATION & CHANGE

Only those authorised to access specific devices, information and systems are provided with the relevant passwords and such provisions are reviewed monthly to ensure that access is still valid and required. Employees may never share their passwords with anyone else in the company, including co-workers, managers or IT staff and unique passwords are used for all employees and access to systems and devices.

Employees are made aware that strong passwords are required for all systems and user-access and that a strict non-disclosure protocol applies to passwords. Where applicable to the system or device being used, The Company utilises software to enforce the use of strong passwords. Employees are not allowed to share or disclose any password.

Strong passwords are enforced on systems and by users and must be: -

- More than 8 characters
- Include letters, numbers and at least 1 special characters
- Not be easily recognisable *(i.e. no names, dates of birth, places etc*)
- Must include upper and lowercase letters

All passwords are changed 3-monthly, and users are not permitted to reuse the same password within a 3-month period. This is forced using software on all systems and a password change is automatically promoted 5 days before password expiry. This change is enforced within 5 days of the change reminder being shown.

If a password is forgotten, only Senior Management/Chief Executive Officer can request that the IT Support service reset the passwords. Passwords that have been forgotten are changed by default and cannot be reset to use the same password. A force change of password is also affected if the user suspects that the password has been compromised.

Where a password is reset, the individuals identify is first verified. This is essential where remote access passwords are changed or reset, and the Senior Manager is not able to physically verify the identity of the user. A two-step identification process is used in such instances with user-known variables being asked and answers verified prior to passwords being reset and disclosed.

5.2.2 DEFAULT PASSWORDS

It is occasionally necessary to set up a default password. This is usually only when a new system or user are being set up and a password change will be promoted from the first user use. Default passwords are changed as soon as is possible and where applicable, access to information is restricted until a strong password has been created.

Where new systems, devices or software is purchased, default passwords are immediately changed and reset to use the strong variables indicated above.

5.2.3 PROTECTING PASSWORDS

The Company is aware that viruses, software and phishing scams can attempt to obtain passwords at a user level. Whilst Firewalls are used to secure and protect systems and software, employees are instructed to never disclose their passwords in a physical or online environment. This includes not disclosing passwords to third-parties, clients or representatives who may have a legitimate need to access a system.

Password fields are always displayed in a hash or star format (*i.e. ### or ****) so that clear text is not present when a password is typed. This helps to prevent unauthorised access or password disclosure by copy & paste or electronic printing methods.

Writing down or storing passwords in any written or digital format is forbidden and all employees are made aware of this. Disclosure or unintentional loss of a password that has been written down in any format will result in disciplinary action being taken.

If a user fails to use the correct username and/or password when logging in to a system or device, we utilise generic failure messages that do not disclose the exact nature of the login error. After 3 failed attempts, the system will advise that login has failed, however it will not disclose if this is due to the username, password or both being incorrect. This aids in preventing brute force attacks or a non-authorised user being aware of which field is incorrect, which then increases their login attempts.

Where login fails, we operate a three-strike approach, and the system will become unavailable for 15 minutes before the login can be re-tried. This protects against external ‘bot’ attacks and brute force.

Multi Factor Authentication is also utilised for Outlook. New sign ins to Multi Factor Authentication enabled accounts will require a verification method to be setup when logging in.

A user can add a mobile number for verification as part of the process which will receive a verification text if a new login is attempted. All the Multi Factor Authentication enabled accounts will then receive a verification text to the designated number each time a new login is detected which will need to be entered before access to the account will be granted. This would mean that if someone tried to access another user's account, even if they have the correct password, they would not be able to, without having direct access to the mobile device as well.

5.3 USER ID’S AND BADGES

The Company has ID badges for all employees, visitors and third-parties who are in our office building. Such badges are specific to those they are assigned to and ID’s or badges not in use are stored in a secure, locked area.

Employees must wear their ID badge at all times whilst in the building or whilst visiting third-party offices and are not allowed to share or copy their badge. Visitors to the Company are

given '***Visitor ID Badges'***. Visitors are accompanied on the premises at all times and are required to log in and out of the building and are assigned a company employee who is responsible for them during their visit.

5.4 PRIVILEGED ACCOUNTS

The Company understands the extreme importance of securing and restricting access to privileged accounts. Such accounts enable direct access to our network, servers, firewalls, routers, database servers, systems and software and as such are treated with the utmost security and protection. Employees and third-parties are never given access to privileged accounts, unless they have been assigned responsibility for a direct function. If this the case, access is only given to the exact system or infrastructure required to complete their tasks.

5.5 AUTHORISED ACCESS

As the Company is a small company, many roles are carried out by the Senior Management or validated staff, which means that having separate roles for areas such as authorised access or setting up accounts is not always possible. However, all requests for access are verified by the Senior Management and employees are never allowed to set up their own access, disclose credentials or bypass validations. An access request is completed by management for all individual access requirements and submitted to to the I.T. Support service. The request is verified by a Senior Management/Chief Executive Officer before being authorised.

5.5.1 LOGIN CONTROLS

Systems can only be accessed by secure authentication of user validation, which consists of a username and password at the role-based user level. All computers have an active firewall and default to a lock screen with user authentication required after 10 minutes of inactivity. All staff are aware that if they leave their workstation, their monitor is to be turned off and their system locked. Credentials & Roles

Access to any systems within the Company (*including sending email*), utilises authentication based on the valid credentials being used. Each user is assigned unique credentials and are not allowed to share or disclose them to any other employee or third-party. It is necessary for credentials to be stored so that when they are used to access a system, database or send an email, the authentication process works. All authentication credentials are encrypted when stored and transmitted and access is restricted to the Senior Management.

5.6 PHYSICAL ACCESS CONTROLS

Access to the Company building, office sections and secure rooms are protected by our building access controls. These increase building, information and employee security and safety and ensure that no unauthorised access is possible.

5.6.1 Door & Window Controls

The Company has 4 doors providing access to the building/office, which are secured via Secure Locks and alarms.

All windows are fixed shut. Visitors are escorted at all times in non-public areas during a visit and are given a Visitors badge. Where a visitor is required to carry any bag with them (*including laptops*) and access non-public areas, we reserve the right to search them on entering and leaving the building.

5.6.2 Outside Opening Hours

When the building has been vacated at the end of working hours, the alarm system is activated and secures all windows and doors. The main office within the building is *'locked down'* after **17:00** and any alarm trigger will immediately notify the Senior Management or Chief Executive Officer.

5.6.3 Direct Access

The use of keys to any buildings, rooms, secure cabinets, safes etc are always controlled and recorded and keys are only provided to employees who require them for business and/or legal reasons. When not in use, keys are stored in a secure, locked cabinet and only **Management/Senior Management** have access. Locations of keys are known at all times and if there is any suspicion that a key has been lost or compromised, lock and access points are changed immediately and monitored until the change is affected.

Visitors are not permitted to access server, network or confidential information areas without prior authorisation. Where authorisation has been given, the Office Manager oversees the work and access.

5.7 Leavers & End of Contract

As the Company is a small company, monitoring end of contracts with third-parties and identifying employees who are leaving or are on annual leave is straightforward. We operate an immediate deactivation process of any credentials and access rights on termination and reactivation is only possible via **Senior Management** authorisation.

Leavers are required to turn in their ID badge before exiting the building. Hard copy ID's are destroyed and where applicable, any electronic ID's are deactivated with immediate effect. It is the line manager's responsibility to ensure that ID badges are returned

Where a project or service contract ends, any access or credentials provided during the contract are deactivated.

Where an employee is on annual leave, we can suspend their credentials and access rights and reactivate on their return. This reduces the risk of unmanned access points, but also prevents having to reset up new credentials and access levels

6 RESPONSIBILITIES

The Senior Management team are responsible for ensuring that all staff and managers are aware of security policies, including access control and secure passwords and the Company operates a top-down approach. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems and attend annual mandatory training.