Barth Syndrome UK IT Access Policy

Reviewed**: 01.07.2018 / 02.12.2019/ 0 02.12.2020 / 2 02.12.2021/ 19.04.2023/ 17.04.2024**

Next Review Date: 17.04.2025

1 Policy Statement

Barth Syndrome UK [BS UK] will establish specific requirements for protecting information and information systems against unauthorised access.

BS UK will effectively communicate the need for information and information system access control.

2 Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important asset of BS UK which must be managed with care. All information has a value to BS UK, its Service Users, and their families. However, not all this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3 Scope

This policy applies to all BS UK Board Members, BS UK Trustees, Employees of BS UK (including system support staff with access to privileged administrative passwords), and contractual third parties with any form of access to BS UK's information and information systems.

4 Definition

Access control rules and procedures are required to regulate who can access BS UK information resources or systems and the associated access privileges. This policy should be adhered to whenever accessing BS UK information in any format, and on any device.

5 Risks

On occasion, BS UK information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to BS UK information which may adversely affect day to day running of the Charity. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the Charity and may result in financial loss and an inability to provide necessary services to our customers**.**

6 Applying the Policy - Passwords

6.1 Choosing Passwords

Passwords are the first line of defence for our IT systems and, together with the user ID, help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

6.1.1 *Weak* and *strong* passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least eight characters.
- Contain a mix of uppercase, lowercase, numeric, and symbols (where possible) with at least one of each set.
- More complex than a single word (such passwords are easier for hackers to crack).
- No obvious substitutions e.g., @ for a, or $ for s.
- Should not have been previously used.

6.2 Protecting Passwords

It is of utmost importance that your passwords remain protected always. The following guidelines must be adhered to always.

- Never reveal your passwords to anyone.
- Never use the 'remember password' function, if a hint is required simply enter ‘No Hint’ or similar.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different BS UK systems.
- Do not use the same password for systems inside and outside of work.

6.3 Changing Passwords

The National Cyber Security Centre specifically advises against forcing password changes at regular intervals.

However, if you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the BS UK Board.

Users **must not** reuse the same password within 4 password changes.

7 Applying the Policy – Employee Access

7.1 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by BS UK. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

7.2 User Registration

A request for access to the Charity's computer systems must first be submitted to the Board for approval. Applications for access must only be submitted if approval has been gained from a Board Member.

When an employee leaves the Company, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the Board to ensure that suspension of the access rights occurs within the correct timescale.

7.3 User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to BS UK systems by:

- Following the Password Policy Statements outlined above in Section 7.
- Ensuring that any PC or Device they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.

8 Policy Compliance

If any user is found to have breached this policy, they may be subject to the BS UK's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the BS UK Board.

9 Policy Governance

The following table identifies who within the BS UK is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	The Board Members of the Charity
Accountable	Michaela Damin – CEO
Consulted	The Board Members of the Charity
Informed	All Trustees, All Board Members, All Employees of the Company, All contractual third parties with any form of access to the Company's information and information systems

10 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the board in conjunction with Michaela Damin – CEO.

11 Key Messages

- All users must use **strong** passwords.
- Passwords must be protected at all times and must be changed if there is any suspicion that they have become compromised.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to the Charity systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Charity's network without permission from the Board.
- Partners or 3rd party suppliers must contact the Board before connecting to the Charity network.