Document Control

Policy Title	Password Standards Policy
Policy Number	100
Owner	Information & Communication Technology Manager
Contributors	Information & Communication Technology Team
Version	1.0
Date of Production	01 October 2014
Review date	01 October 2016
Post holder responsible for review	Information & Communication Technology Manager
Primary Circulation List	Shared Drive
Web address	n/a
Restrictions	None

Version Control

Version Number	Owner	Description	Circulation
1.0	Information & Communication Technology Manager	Review	Shared Drive

1.0 POLICY:

Passwords are one of the primary mechanisms that protect critical Sunbeam House Services (SHS) information systems and other resources from unauthorised use. Constructing secure passwords and ensuring proper password management are essential. Poor password management and protection could allow unauthorised access to SHS's Information Technology (ICT) resources, which in turn could lead to the inappropriate disclosure and use of confidential or sensitive SHS information. The purpose of this policy is to define a standard for the creation of secure passwords for use on SHS's ICT resources.

2.0 SCOPE:

This policy represents SHS's position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All SHS Information Technology (ICT) resources which include equipment, systems, and applications including cloud based applications.
- All users, and uses of SHS Information Technology (ICT) resources;
- All connections to (locally or remotely) SHS network (Local Area Network (LAN)/Wide area network (WAN))

3.0 ROLES & RESPONSIBILITIES:

3.1 Users

Each user of SHS's ICT resources is responsible for:-

3.1.1 Complying with the terms of this policy and all other relevant SHS polciies, procedures, regulations and applicable legislation.

3.1.2 Respecting and protecting the privacy and confidentiality of the information they process at all times.

3.1.3 When prompted to change their password either by ICT Member of staff or by SHS computer system to change it to do so as soon as possible.

3.1.4 Complying with instructions issued by the ICT Manager on behalf of SHS.

3.1.5 Reporting all misuse and breaches of this policy to their Senior Manager.

3.2 Senior Managers

In addition to each user's responsibilites, Senior Managers are directly responsible for:-

3.2.1 The implementation of this policy and all other relevant SHS policies within the business areas for which they are responsible.

3.2.2 Ensuring that all SHS employees who report to them are made aware of and are instructed to comply with this policy and all other relevant SHS policies.

3.2.3 Consulting with the ICT Manager in relation to the appropriate procedures to follow when a breach of this policy has occurred.

3.3 ICT System Administrators & Developers

Each SHS System Administrator & Developer is responsible for:-

3.3.1 Complying with the terms of this policy and all other relevant SHS policies, procedures, regulations and applicable legislation.

3.3.2 Ensuring the network administration password is secure.

3.3.3 Complying with instructions issued by the ICT Manager on behalf of SHS.

3.4 ICT Manager

In addtion to the above responsiblities the ICT Manager ensures that all system developers (including third party contractors) who are responsible for developing systems for SHS, must ensure that their systems contain the following security features:-

3.4.1 They must support authentication of individual users and not just groups.

3.4.2 They must not store passwords in clear text or in any easily reversible form

3.4.3 They must provide for some sort of role management, such that one user cant take control of the functions of another without having a knowledge of the other users passwords.

4.0 GUIDELINES:

All passwords must meet the following guidelines:-

4.1 Password Length

All passwords must be a minimum of 8 characters in length

4.2 Password Complexity

4.2.1 Passwords should contain a combination of letters (both upper and lower case, numbers (0-9) and symbols e.g ! @ # $ ^ & * ( ) _ - + = [{] } ; : | . / ?

4.2.2 Passwords must not be left blank

4.3 Password Bad Practice

When resetting a password please consider the following as bad practice:-

4.3.1 Any common keyboard sequences - (for example: qwerty);

4.3.2 Any personal information related to a user – such as date of birth, etc;

4.3.3 A sequence of consecutive numbers or letters (for example: 12345678, abcdefgh, abcd1234);

4.3.4 The following sequence of letters - passwrd, passwd, pwrd, paswd, passwd;

4.3.5 Common acronyms (for example: aka, 24/7, asap, fyi, sob, tlc).

4.4 Password History

No password may be re-used by a user within a 12-month period

4.5 Password Aging

SHS network will require you to change your password every 90 days please note that password changes must be made manually on mobile devices.

5.0 ENFORCEMENT

5.1 SHS reserves the right to take such action as it deems appropirate against users who breach the guidelines of the policy

5.2 Breaches of this policy by a third party, may lead to the withdrawal of SHS information technology resources to that third party and/or the cancelleation of any contract(s) between SHS and the third party.

5.3 SHS will refer any user of its ICT resources for illegal activities to the appropriate law enforcement agencies.