Password Policy

Confidentiality Statement

The policies, procedures and standard practices described in this manual are for the said process only at SG Analytics **(from here on termed as 'SGA')** and do not extend or imply to any other SGA entity. Information in this document represents guidelines only. SGA reserves the right to modify this document, amend or terminate any policies, procedures, or employee benefit programmes whether or not described in this document at any time, or to require and/or increase contributions toward these programs.

All policies contained herein have been adopted by SGA and supersede previous policies. We periodically review policies, in part or as a whole, to ensure that they continue to reflect current thinking of the organisation and are consistent with trends and legal requirements.

Document Summary

Document Reference #	SGA_PO_Password Policy_v4.0
Author	Umed Patil
Reviewed By	Umed Patil
Approved By	Susshruth Apshankar
Owner	Umed Patil
Document Type	Policy
Document Status	Approved
Document Circulation	Confidential Internal
Document View Level	Internal
Release Date (dd-mm-yyyy)	03-02-2017

Revision History

Version	Date (DD-MM-YYYY)	Author (Designation: Name)	Changes (Short Description)	Remarks
v1.0	15-12-2015	Manager IT Umed Patil	-	Initial Document
v2.0	14-03-2016	Manager IT Umed Patil	Change in password characters for standard and privileged account	Reviewed & Approved version
v3.0	06-09-2016	Manager IT Umed Patil	Added section 1.3 and 2	Reviewed Document
v4.0	03-02-2017	-	-	Reviewed Document

Content

1. Introduction

1.1 Overview

A password is a secret word/phrase that a claimant memorises and uses to authenticate the claimant's logical access. Passwords are the most commonly used authentication mechanism. This policy shall govern the creation and protection of passwords in SG Analytics to prevent their compromise.

1.2 Scope

The scope of this policy includes all SGA employees, who have and/or are responsible for an account (or any form of logical access that supports or requires a password) in any system and supporting IT facilities of SGA.

1.3 Glossary of Terms

Terms	Description
ISMS	Information Security Management System
IT	Information Technology
SGA	SG Analytics Pvt. Ltd.

2. Responsibility

IT team would be responsible for verifying the effectiveness of the process and its revision whenever required.

3. Policy

1. SGA recognises two categories of passwords as below:
    a. End-user password - The end user password includes a system domain and an email password, which is also categorized as "standard account"
    b. IT infrastructure password – IT infrastructure password includes administrator and root account password, which is also categorized as "privileged account". Such accounts are sensitive and shall have critical business impact in case of any incidence
2. As an exception, an end user can also hold and he/she can be responsible for possessing a password related to a project specific applications or systems
3. A formal password management process shall be established in SGA for the allocation of passwords. This process shall be system controlled, wherever technically possible
4. SGA's IT management team shall develop and implement administrative procedures for password creation, change, reset, and subsequently communication of initial passwords to the user concerned
5. Wherever technically feasible, a control shall be enforced to change a temporary password at the first logon by the user concerned
6. A password shall not be stored in the system in any unprotected form
7. The use of password by more than one user (sharing of password) is highly discouraged in SGA and considered a serious violation of company's policies

8. Password leakages shall be treated as serious security incidents. A deliberate attempt to leak out a password shall call for disciplinary action
9. Use of group user-ID/password shall be limited to situation dictated by operational necessity and/or under certain circumstances approved by the Business Head with a proper written approval
10. SGA's IT System Administrator shall ensure changing of all default passwords provided by vendors
11. SGA's IT System Administrator shall determine and enforce appropriate controls for password complexity, the predefined password change frequency and preventing reuse of old password
12. A password shall be changed for SGA's critical data center assets once in every 2 quarters
13. All IT infrastructure passwords shall be created, changed, reset, and managed by SGA's IT Team only
14. All critical IT infrastructure passwords should be maintained in a password-protected office document file by SGA's IT management team. The password of such office document file shall be changed once in every 2 quarters. Such office document shall be printed and kept in a company sealed envelope. This envelope shall be stored in a safe locked and its key shall be kept in the data center
15. In case of emergency, the locked envelope will be opened in presence of the ISMS team and SGA's IT management team

4. Guidelines

4.1 Password Management Guidelines

4.1.1 Password Creation

1. Passwords for a standard account shall be of minimum 8 characters
2. Passwords for a privileged account shall be of minimum 15 characters
3. A password shall be a combination of alphabets (minimum one letter in upper case), minimum 1 numeric and 1 special character. (e.g. Alpha1234! @)
4. A password and user-ID shall not be identical. A password should not contain a user's first letter or last letter
5. A password shall be significantly different from previous three passwords
6. Password history shall be enforced and last 3 passwords shall not be accepted

4.1.2 Password Modification

1. User passwords shall expire after a maximum period of 60 calendar days
2. A user password expiry notification shall be sent after 45 calendar days
3. Passwords of Server/Network devices shall be changed every 180 calendar days

4. Users shall modify/change their passwords using the 'password change' option provided in the system, in accordance with the password guidelines
5. Email passwords for Project Managers and above will be changed every 60 calendar days

4.1.3 Password Reset

1. If a user is unable to recollect his/her current password, then he/she will initiate a request though the Helpdesk portal to reset the password
2. If the request is received via the employee's ID, IT team will reset the password
3. If the request is received via other than the employee's ID, approval from the skip Manager is mandatory to initiate the request
4. The IT team communicates the new password through the ticket closure or via internal communicator

4.2 Password Protection Guideline

1. Passwords assigned during the user creation process must be changed at the first Logon. This applies to all user-IDs and email IDs
2. Use of a single password shall be avoided to access various SGA's information/IT assets
3. Details regarding User ID & password etc. should not be sent using clear text across mail systems/ SMS
4. Passwords shall not be revealed to anyone orally in person/on phone/cellphone or through fax/internet messenger services
5. Logical access to a computer or a system will be locked out after 3 unsuccessful attempts to login using invalid or inaccurate credentials
6. Passwords shall be encrypted using 128 bit SSL encryption when stored in files or database or transmitted over the internet, public networks or wireless devices. Where encryption is not possible, access to such files/databases shall be restricted
7. Format of a password shall not be revealed without authorisation
8. Passwords shall not be revealed in questionnaires or security forms
9. Passwords shall not be shared with family members and co-workers
10. The 'remember password' feature of applications shall not be used
11. Passwords shall not be written down and stored anywhere inside and outside the organisation
12. If an account or password is compromised, the password must be changed immediately
13. Protection of Super User Password/Administrator Password:
    a. All super user/administrator passwords of critical servers & critical devices should be sealed in an envelope and kept in a safe locked & its key should be kept in the data center. This will help in retrieval of the administrator password, if the password is forgotten or the person concerned leaves without surrendering passwords

b. In case, a password needs to be retrieved from sealed envelope, it should be changed immediately and a new sealed envelope shall be kept in a safe locked & the key shall be kept in the data center

c. In case, a person holding administrator/super user password resigns, the password should be changed immediately and stored in a new sealed envelope and kept in a safe locked & the key should be kept in the data center

14. In case of separation of an employee:

    a. Passwords for all accounts and possibly the user ID must be changed on separation / resignation of employees by the IT Department (Manager–IT, System Administrator)

    b. For other category of employees, the relevant accounts must be disabled/removed

    c. If a user ID is required after the separation of an employee, the Department Head concerned should request for keeping the ID live and change of password. The Department Head should also intimate as to who needs to have the new password

15. A report on password change requests shall be available with the IT Department via helpdesk, wherein the user has to fill up and submit a 'password reset form' with his/her manager's approval on it

4.3 User Responsibilities

ALWAYS USE following types of passwords:

1. Include both upper and lower case characters (e.g., a-z, A-Z)
2. Include digits and special characters as well as alphabets e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
3. Should be at least 8 alphanumeric characters long
4. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation

DO NOT USE following types of passwords:

1. Passwords based on personal information, names of family members, etc
2. A password, which is a word in any language, slang, dialect, jargon, or found easily in a dictionary
3. Never write down passwords or store them online in an unprotected way
4. Password containing less than 8 characters
5. Never use a password, which is a commonly used word such as:

    a. Names of family members, pets, friends, co-workers, fantasy characters, etc

    b. Computer terms and names, commands, sites, companies, hardware, software, etc

    c. The words "sganalytics", "sgan", "analytics" or any derivation

    d. Birthdays and other personal information such as extensions or phone numbers

e. Word or number patterns like aaabbb, gfedcba, 123321, etc

f. Do not use either of these examples as password