Policy - Password Management

Introduction

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of resources. All GlobalLogic's staff, including contractors and vendors with access to GlobalLogic systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1. Purpose:

The purpose of the Policy is to establish a standard for creation of strong passwords, the protection of those passwords and frequency of change.

2. Scope:

The scope of this Policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password: user account passwords, service account passwords, partner account passwords, device passwords, etc.) on any system that resides at any GlobalLogic facility, has access to the GlobalLogic network, or stores any non-public GlobalLogic information.

Abbreviations and Definitions

Abbreviation	Description
ISMS	Information Security Management System
AD	Active Directory

Description

3. Policy:

3.1 Password Creation

3.1.1 All user-level and system-level passwords must conform to the Password Requirements, set in **Annex A.**

3.1.2 Partner accounts should be created in AD per approved request only with 3 months duration period. Account extension should be requested per approved

ticket by Project Manager.

3.1.3 Project Service accounts should be created in AD per approved request only with 6 months duration period. Exception may only be service accounts, created for IT services – duration is set to 12 months. Account extension should be requested per approved ticket by Head of IT Infrastructure.

3.1.4 Users must use a separate, unique password for each of their work related accounts. Users must not use any work related passwords for their own, personal accounts.

3.1.5 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that multi-factor authentication is used for any privileged accounts.

3.2 Password Change

3.2.1 Individuals must change their initial account password, provided by IT, during the first logon to the system.

3.2.2 Passwords should be immediately changed when there is reason to believe a password has been compromised.

3.2.3 Individuals must change their passwords at least quarterly.

3.2.4 IT notifies the expiration / new password or extension through email to the owner.

3.2.5 User's manager can request IT to reset the password for his/her team members. However, users are guided to change the password on their own from the logon prompt by selecting the change password option.

3.2.6 Partners should reset their password via Password Change utility - https://changepassword.globallogic.com/ . Respective project managers shall inform and guide the partner regarding the same. Partner’s password can be reset by request of respective project manager only.

3.3 Password Protection

3.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential GlobalLogic information. Individuals must not engage in activity outside the limits of access that have been authorized for them. This includes but is not limited to:

- Sharing of passwords for project/ client group/ guest accounts can only be done on approval from respective project manager and ISO with a complete list of group members having access to such accounts.
- Revealing a password for any account, including one's own personal account.
- Permitting the use of any account, including one's own personal account, in a way that allows unauthorized access to resources (e.g. logging in for someone else).

3.3.2 Individuals must not write their passwords down or post their passwords on or near the computer.

3.3.3 Passwords must not be inserted into email messages, HelpDesk tickets, Alliance cases or other forms of electronic communication, nor revealed over the phone to

anyone.

3.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

3.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.4 Multi-Factor Authentication

3.4.1 Multi-factor authentication is highly encouraged and should be used in critical services and applications by admins.

3.5 Account Lockout

3.5.1 Account lockout threshold: 5 invalid logon attempts - User account will get locked after 5 failed logon attempts. Account lockout duration: 30 minutes - Account can be unlocked by IT or it will be unlocked automatically after 30 min.

3.5.2 Reset account lockout counter after 15 minutes - This security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts.

4. Enforcement

4.1 IT Department will regularly monitor accounts to confirm that passwords are being changed according to this document. The level at which accounts will be monitored will vary from system to system since the tools available for each system also vary.

4.2 IT Department will configure accounts for automatic password expiration and set other options to encourage or remind individuals to change their passwords. IT Department will do what they can to help employees to succeed in following the document.

4.3 Violations of these requirements may be referred for disciplinary action.

5. Restrictions

5.1 At their discretion, some departments may impose additional rules or restrictions to better improve security. Such rules have to be documented and agreed with country ISO.

Annex A

User Password Requirements

1. Minimum password length should be 8 characters.
2. Password history, last 5 passwords remembered - This means user will not be able to keep new password from his last 5 passwords.
3. Maximum password age 90 days - Password will expire after 90 days.
4. Minimum password age 1 day - This security setting determines the period of time that a password must be used before the user can change it.
5. Password must meet complexity requirements. Password should not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
6. Password must contain characters of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Numerals (0 through 9)
    - Non-alphabetic characters (such as !, $, #, %)

Administrator Password Requirements

1. The GL infrastructure Administrative passwords (both service and admin accounts) are kept in a secure way with access limited to authorized administrators only.
2. For GL infrastructure Service and admin accounts' passwords should be changed at least once a year or in case when a team member leaves within a month and complexity should be at least 12 characters including alphabets, numbers and special characters.
3. For GL Delivery project service accounts, the same process shall be followed. Any specific password requirements proposed by client may supersede the company's password guideline for that specific project after approval from respective country's ISO.

Change History

Revision	Change Description	Valid Date	Approver
1.0	Initial Version	7 March 2012	Alok Malik (CISO)
1.1	Details of passwords for AD accounts and their communication method is added to point no.1 and Format Change According to Rebranding	20 Feb, 2013	Alok Malik (CISO)
1.2	Correction in Account Lockout policy	04 June, 2013	Alok Malik (CISO)
1.3	Password change Policy for Delivery and IT Support service/admin account added and Password Pro Manager for keeping admin passwords safely added Password's reset rules for partner's accounts updated	10th Sept, 2013	Alok Malik (CISO)
1.4	Annual Review – Removed Password Manager Pro and included Google Doc with Microsoft Admins and Linux Admins having access to their infrastructure	15 Dec 2015	Alok Malik
1.5	Annual Review – Removed information about Cisco ACS	25th Oct, 2016	Alok Malik (CISO)
2.0	Annual Review. Change title from Policy to Guideline. Change Account Lock timing from 15 to 30 minutes. Delete Do's, Dont's, Suggestion sections. Link on Guideline - Secure Logon, Session Timeout And Sensitive System Isolation was added.	24th Nov, 2017	Alok Malik (CISO)
2.0	Annual Review – no changes	09th Sep, 2018	Alok Malik
2.1	6.1 changed, few minor text edits	3rd March, 2019	Alok Malik
2.2	Link to Password Change utility was updated.	09/08/2020	Alok Malik (CISO)
3.0	Guideline – Password Management was changed to Policy – Password Management due to documents re-structure project. Passwords Requirements were placed into Annex A.	01/27/2021	Alok Malik, CISO
3.1	Removed exception in section 3.3.3	09/17/2021	Alok Malik (CISO)

3.1	Annual review – no changes	09/09/2022	Alok Malik (CISO)
3.1	Annual review – no changes	09/21/2023	Denys Kudriavchenko, Head of Security Risk & Compliance