Password Policy

Version number	1.2
Last Approved	Dec 4, 2023
Classification	PUBLIC

Overview

The Password Policy stipulates constraints and practices that Personnel must abide by while creating and managing passwords.

Applicability

The applicability of this statement falls under the purview of the Security Documentation Overview.

Purpose

The purpose of this policy is to outline The Company's standards for using passwords so that devices, software and services are appropriately protected to ensure privacy and protection of Company and customer data.

Scope

This policy applies to all Personnel. Employees must ensure passwords conform to this policy to avoid damage to The Company and its customers. Personnel must contact a member of the IT and/or the Security Team or Management to report suspected policy violations.

Password Minimum Requirements

- All default passwords must be changed prior to use.
- Minimum password length must be at least 12 characters.
- Password contain at least 3 of the following 4 items: Upper case, lower case, numeric, special characters: `~!@#$%^&*_+=`|\(){}[]:;"'<>,.?/`
- Cannot contain any part of the user’s name or login ID.

Systems Processing Passwords

All LTG systems, including servers, applications, and websites that are hosted by or for LTG, must be designed to accept passwords and transmit them with proper safeguards. IT Services and all authorised password system designers must follow the following requirements:

- Passwords must be prohibited from being displayed when entered.
- Passwords must never be stored in clear, readable format (encryption must always be used)
- Systems storing or providing access to confidential data or remote access to the internal network must be secured with multifactor authentication.
- Password hashes (irreversible encoded values) must never be accessible to unauthorised individuals.
- Where possible, salted hashes (irreversible encoded values with added randomness) should be used for password encryption.
- Where supported, enforced SSO functionality must be configured to ensure confidentiality, integrity and availability of Company data.
- Where SSO option is not available, alternative options like enforced MFA should be deployed instead.
- All systems, supporting traditional account protection features, must be configured accordingly:
  - Lockout duration must be set to at least 15 minutes (the time after the password is locked out due to incorrect password entry before automatic unlock).
  - Account lockout observation window – 10 minutes (If the user enters the password incorrectly 5 times in 10 minutes, the account will lock out).
  - Cannot be any of the 24 most recently used passwords

User Requirements

- Passwords must meet the requirements outlined in this Policy.
- Passwords must be kept confidential. LTG individual user account Passwords must never be shared with another individual for any reason or in any manner not consistent with this document.
- Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats.
- All users are required to change initial and temporary passwords upon next login. Initial passwords must be securely transmitted to the individual. User IDs and Passwords must be communicated/distributed via separate media (e.g., e-mail and phone). For instance, using one-time-password service: https://ots.ltgplc.com.
- Passwords for LTG devices must be unique and different from passwords used for other personal services (e.g., banking).
- Users must immediately change their password and notify the IT Service Desk if they have any indication their account may have been compromised.
- Users must also change their password immediately if the IT Service Desk informs them that a password change is necessary.
- In the event of a hardware malfunction and the device needs to be handled by a third party, passwords should not be shared with an external technician or any other individual.
- When sharing passwords with users, company-approved password management systems and vaults or one-time secret passwords must be used.

Recommendations for Creating Compliant Passwords

Use a Passphrase - A passphrase is like a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with various character types is exponentially harder to breach than a shorter password. Users can add further password complexity by using Capitalisation of every word, substituting letters for numbers or symbols or incorporating spaces or substituting with a different character. For example:

- When I was 6, I learned to ride a bike
- When I Was 6, I Learned To Ride a Bike
- My-dre@m-car-is-Supra
- My_Dream_car_is_supr@

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Aleksandr Zaldak	
Author(s)	@Aleksandr Zaldak	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Dec 4, 2023
	@Aleksandr Zaldak - IT Infrastructure Manager	Dec 4, 2023
Review cycle	ANNUAL	
Next review date	Dec 3, 2024	

Version History

Date	Author(s)	Version	Changes
Nov 1, 2024	@angelina.kilmer	1.2	Changed Policy classification from Confidential to Public
Nov 8, 2023	@Aleksandr Zaldak @Art Machado	1.1	Full review of the policy. Language and content has been changed to ensure it meets the requirements of everyone within the scope of the policy.
Mar 1, 2018	@Aleksandr Zaldak	1.0	Original