MSLA International Latinamerican Lists	***Identity and Access Management Policy***

Overview

This document is for exclusive use by MSLA.

Version	Responsible	Author	Creation date	Approved by	Date approval
1.6	Hugo Flores	MSLA IT Department	11/24/2023	Luis Rios	11/27/2023

Table of Contents

1.0 PURPOSE

This policy defines the requirements for establishing, maintaining and deleting account settings for all privileged user accounts on any MSLA computer and communications system.

2.0 SCOPE

This policy applies to all information security analysts and system administrators responsible for the maintenance of accounts and password management systems on MSLA electronic information resources.

3.0 POLICY

3.1 SYSTEM APPROVAL AND AUTHORIZATION

3.1.1 Default Password Changes - All vendor-supplied default passwords must be changed before any computer or communications system is used for MSLA business.

3.1.2 Privileged User ID Review - Before any production multi-user computer operating system is installed at MSLA, all privileged user IDs that are not assigned to a specific employee or job role must have their passwords changed to large random values and these should be recorded in the privileged account management system with appropriate permissions for the administrators responsible for managing these accounts.

3.1.3 Unnecessary Software - Software features that could be used to compromise security, and that are clearly unnecessary in the MSLA computing environment, must be disabled at the time when software is installed on multi-user systems.

3.2 PASSWORD CATEGORIZATION

Passwords fall into two categories:

User Account Passwords – First, a password is a secret that allows the use of an account. An account may represent a human being and therefore that password determines a human identity, for example, an Active Directory user account. The Active Directory user account password is the secret known by the human that identifies that human to the system. These types of passwords are known as user account passwords and they need to be memorized by the human whose identity they represent. A goal is to strive for as few user account passwords per human user as possible, ideally a single user account password per human user. .

Privileged Account Passwords – Privileged account passwords are passwords where the account does not represent a human being – this could be a system account like UNIX root or a service account. The passwords on these accounts do not typically provide for any identity of a human and therefore do not need to be memorized. These passwords can be set to very large values and stored in the privileged account management system.

The focus of this Privileged Password Security Policy document is on the second type of password, Privileged Account Passwords. However, because User Account passwords often have elevated or administrative privileges attached to them, both types of passwords are described in many of the guidelines in this policy.

3.3 PASSWORD COMPOSITION

3.3.1 Role-Based Password Length - The minimum length for fixed passwords, or passwords created by users, must be set to six for handheld computers, eight for all network-connected computers, and ten for administrator and other privileged user IDs.

3.3.2 User Account Password Complexity - All user-chosen passwords for user accounts must meet the following complexity requirements:

- Must contain at least one alphabetic, one numeric and one symbol character.
- Must be at least 8 characters in length.
- Ideally passphrases should be used to increase length. Increased length provides more security than complexity and is easier for a human to memorize.
  For example:
  1) lf@j7asFd! versus 2) Blue5Chandelier2@
  The seven extra characters in (2) make it 64 trillion times stronger than (1).

3.3.3 Privileged Account Password Complexity – These passwords should be optimized for security since no human needs to memorize these passwords. They can be optimized for the maximum lengths of the platform. For example: Recent versions of Windows allow for up to 127 characters for the password – therefore random passwords should be generated between 80 and 127 characters in length to provide the maximum security. The following requirements should be followed for Privileged passwords:

- Should maximize the possible length of password for each platform.
- Should not be memorized.
- Passphrases should not be used since memorization is not desirable.
- Should have a complete mix of upper case, lower case, numbers, and symbols.

3.3.4 Seed for Generated Passwords for Privileged Accounts - If system-generated passwords are used, they must be generated using the low order bits of system clock time or some other very-frequently-changing and unpredictable source.

3.3.5 Null Passwords Always Prohibited - At no time, may any Systems Administrator or Security Administrator enable any user ID that permits password length to be zero (a null or blank password).

3.3.6 Enforce Password Complexity - All passwords must meet the above complexity requirements and this complexity must always be checked automatically at the time that the password is created or changed.

3.4 PASSWORD HISTORY AND CHANGE INTERVAL

3.4.1 User Account Password Changes – Users must be required to change their password at least once every 90 days. It is better to have good passwords that can be memorized than frequent changes of these passwords. More frequent changes will lead to more forgotten passwords or weaker passwords being chosen with little security benefit.

3.4.2 User Account Maximum Password Changes – Users must not be permitted to change their password within 7 days of their previous change. This requirement is only helpful for passwords that users are memorizing (user accounts) and is used to prevent users from changing the password multiple times back to a previously used password (therefore defeating the requirement to change the password).

3.4.3 Privileged Account Password Changes – All privileged accounts must be automatically required to change their passwords at least once every 90 days. This time interval should be set based on an internal risk assessment for any potential disruption to the business. For example: A service account password change can be highly disruptive if it is part of a mission critical system and therefore this password change could be once every 90 days. However a Domain Admin account password change would have zero disruption to the business and is very high risk – these accounts should have their passwords changed as often as possible – ideally after every use to reduce exposure to abuse, misuse or exploits such as Pass the Hash attacks.

3.4.4 Password History - On all multi-user MSLA computers, system software or security software must be used to maintain an encrypted history of previously chosen fixed passwords. This history must contain at least the previous thirteen passwords for each user ID.

3.5 ACCOUNT LOCKOUT AND COMPROMISED PASSWORDS

3.5.1 Maximum Login Attempts - All MSLA computer systems that employ fixed passwords at log on must be configured to permit only five attempts to enter a correct password, after which the user ID is deactivated.

3.5.2 Lockout Duration – All accounts that have been disabled for incorrect logon attempts must remain inactive for at least 15 minutes.

3.5.3 Lockout Notification – All disabling of accounts for incorrect logon attempts must be notified to the security team so that investigation can occur if necessary and anomalies can be detected.

3.5.4 Password Changes After Privileged User Credential Compromise - If a privileged user credential has been compromised by an intruder or another type of unauthorized user, all passwords on that system and any related systems must be immediately changed.

3.5.5 Fixed Password Change Confirmation – System administrators must be immediately notified when fixed passwords are changed or updated outside of the central privileged account management system.

3.6 ACCEPTABLE USE PRIVILEGED ACCOUNTS

3.6.1 User Account Password Sharing – User Account Passwords must never be shared or revealed to anyone other than the authorized user. If they are shared then they are no longer a User Account since the identity of the user is not known.

3.6.2 Privileged Account Password Sharing - Passwords for privileged accounts can be shared among administrators as long as controls are in place to know which administrator is using the account at any one time. This must include full auditing and non-repudiation mechanisms. Each system must have a unique password.

3.6.3 Password Display And Printing - The display and printing of account passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. Any display of a privileged account password to a user must be audited and the password should be changed after it has been used.

3.7 PRIVILEGED ACCOUNT APPROVAL

3.7.1 Privileged Account Requirements – All privileged accounts on MSLA systems must employ greater security than non-privileged accounts. This includes longer, more secure passwords and greater audit accountability.

3.7.2 Privileged User Account Approval – The creation or modification of privileged user accounts must be approved by at least two individuals: The System Owner and an authorized member of the Information Technology department.   System administrators must not be allowed to create other privileged accounts without authorization.

3.7.3 Number of Privileged User IDs - The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

3.7.4 Role Based Account Privileges – To facilitate secure management of systems, wherever possible, privileged accounts must be defined based on the specific role of the system administrator.

3.8 PRIVILEGED ACCOUNT CONSTRUCTION

3.8.1 Privileged User ID Construction- All privileged user IDs on MSLA computers and networks must be constructed according to the MSLA user ID construction standard, and must conform to one of the following:

- Must clearly indicate the responsible individual’s name.
- Must clearly define the purpose of the account (i.e. purpose of the account, type of account, etc.

- Must be managed in a system which can clearly associate a single User Account to each use of the Privileged Account in order to document accountability for the use of the Privileged ID

3.8.2 Generic User IDs - User IDs must uniquely identify specific individuals and generic user IDs based on job function, organizational title or role, descriptive of a project, or anonymous, must be avoided wherever possible. User IDs for service accounts and other application accounts should also follow the MSLA naming convention and requirements outlined in section 3.8.1 above.

3.8.3 Re-Use Of User IDs - Each MSLA computer and communication system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a worker or customer terminates their relationship with MSLA.

3.8.4 Separate Systems Administrator User IDs - System administrators managing computer systems with more than one user must have at least two user IDs, one that provides privileged access and is logged, and the other that provides the privileges of a normal user for day-to-day work.

3.9 PRIVILEGED ACCOUNT MANAGEMENT

3.9.1 Central Automated Management – All privileged accounts on MSLA systems must be managed by a central system. This system must provide an audit trial that tracks specific additions, changes, and deletions.

3.9.2 Integration with Native Directories – Any privileged account management system must integrate with native operating system account management systems or directory services (such as Active Directory)

3.9.3 Integration with Strong Authentication Methods – Any privileged account management system must integrate with strong authentication methods (such as multi-factor authentication) to ensure the identity of the user in addition to their directory authentication.

3.9.4 Password Vault – MSLA system administrators must have access to a vault system that enables the temporary provisioning of access to privileged accounts and passwords (aka FireID) for emergency maintenance.

3.9.5 Password Vault Encryption – MSLA must maintain any credentials stored in a central management system within an encrypted password vault, using strong encryption algorithms that meet compliance and/or regulatory requirements.

3.9.6 Privileged Account Inventory – MSLA must maintain an inventory of all accounts with privileged access on production information systems. These include, at a minimum, local administrator accounts and service accounts.

3.9.7 Account Inventory Update – The privileged account inventory must be updated at least quarterly to identify new or changed accounts.

3.9.8 Inactive Account Maintenance - All inactive accounts over 90 days old must be either removed or disabled.

3.9.9 Disaster Recovery – Any privileged account management system must be configured to utilize robust backup, recovery and availability methodologies in order to ensure resiliency and availability of the credentials stored within the system as well as the timely recovery of the system in the event of a system failure.

3.10 THIRD PARTY PRIVILEGED ACCOUNTS

Third Party User ID Expiration - Every privileged user ID established for a non-employee or third party application must have a specified expiration date, with a default expiration of 30 days when the actual expiration date is unknown.

3.11 APPLICATION DEVELOPMENT

3.11.1 Special Application Accounts – All production applications that require privileged access must use special application accounts that are created specifically for the given application. Applications must never use default administrator accounts.

3.11.2 Secret IDs or Passwords - Developers must not build or deploy secret user IDs or passwords that have special privileges, and that are not clearly described in the generally available system documentation.

3.11.3 Hard-Coded Passwords In Software - Passwords must never be hard-coded in software developed by or modified by MSLA workers.

3.11.4 Test Account Removal - Test data and accounts used during development and testing must be removed before a production system becomes active.

3.12 PRIVILEGED ACCOUNT LOGGING

3.12.1 Privileged System Commands Traceability - All privileged commands issued on computer and communication systems must be traceable to specific individuals through the use of comprehensive logs.

3.12.2 Privileged User ID Activity Logging - All user ID creation, deletion, and privilege change activity performed by Systems Administrators and others with privileged user IDs must be securely logged.

3.12.3 Privileged User ID Activity Log Review - All logs recording privileged ID activity must be reviewed at least quarterly via periodic management reports.

3.12.4 Privileged User ID Activity Log Correlation – All logs recording privileged ID activity must be aggregated into a central log management or Security Information and Event Management (SIEM) tool in order to correlate privileged ID activity to other security events, log entries and related non-privileged ID activity.

3.12.5 Privileged User ID Session Logging – In addition to event logging, all activity on privileged accounts must be logged via session or keystroke recording.

3.13 DISABLING INACTIVE OR TERMINATED USERS

3.13.1 The following are the MSLA User Termination Best Practices:

- Disable the departing employee’s account in Active Directory immediately; after 30 days, remove it.
- Disable the user’s email login; forward email to the user’s manager for as long as needed.
- Terminate VPN and Remote Desktop access.
- Terminate access to remote web tools (web apps, Office 365, e-mail, etc.).
- Terminate access to voicemail. Forward phone and voicemail to the user’s manager, and delete them at the manager’s convenience.
- Disable access to business applications such as SAP.
- Change all shared account passwords that the departing user knows.
- Move the user’s personal share data and email archive to the manager’s account; delete them at the manager’s convenience.
- Reset the “FAX/SCAN to e-mail” setting on multi-function printers.
- Remove the user from email group lists, distribution lists, internal phone lists and websites.
- Connect to the user’s workstation and shut it down.
- Retrieve or disable all company-owned physical assets (computer, laptop, phones, tablet, etc.) assigned to the user, and update the IT inventory.
- Copy all needed local data from employee’s computer to manager’s one.
- Change any access codes the user knows, such as PINs for accessing secured rooms.
- Remove any personal belongings from the user’s work area.
- Inform company staff that the user is no longer employed there.

4.0 VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. MSLA reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. MSLA does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or in the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, MSLA reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

5.0 DEFINITIONS

Account (User ID or Username) - A unique string of characters assigned to a user by which a person is identified to a computer system or network. A user commonly must enter both a user ID and a password as an authentication mechanism during the logon process.

Fixed Password – A password created by a user for an account or credential.

Least Privilege - Least privilege means that for each task or process, the administrator is granted the minimum rights required to perform the task.

Password – An arbitrary string of characters that is used to authenticate an account when attempting to log on, in order to prevent unauthorized access to the account.

Privileged Account – An account that can either be a user account on any system that has system privileges beyond those of a normal user or an account that does not represent a human use. Privileged accounts are typically not assigned to a user, but can, in some cases, be dedicated user accounts which are given more permissions than a typical user account. Root, local administrator, domain admin and enable passwords are all examples of privileged accounts that have elevated access beyond that of a normal user. Passwords for privileged accounts should be randomized, not memorized by anyone, and changed frequently.

System Administrator – An employee or partner who is responsible for managing a MSLA multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

Third Party – Any non-employee of MSLA who is contractually bound to provide some form of service to MSLA.

User - Any MSLA employee or partner who has been authorized to access any MSLA electronic information resource.

User Account – An account that represents a single human user. They are the only person to ever use the account and it is their way of authenticating into MSLA systems. The password for this account is something they would memorize and would not be shared with any other user.