NIDA

# NIDA Password Policy

| | |
|---|---|
| Policy Number | Tech01-1 |
| Approving Authority | Executive Team (ET) |
| Date Implemented | September 2022 |
| Current Version | September 2022 |
| Date of Review | September 2024 |
| Contact Officer | Head of Technology |
| Related Policies, Procedures and Documents | |

## 1.0 OVERVIEW

Passwords are a critical aspect of Computer and Information Security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of The National Institute of Dramatic Art's (NIDA) entire network. As such, all NIDA employees, contractors, and vendors with access to NIDA systems are responsible for complying with this policy.

## 2.0 PURPOSE

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

## 3.0 SCOPE

The scope of this policy includes anyone who has or is responsible for a NIDA account (or any form of access that supports or requires a password) on any system that resides at any NIDA domain, has access to the NIDA network, or stores any non-public NIDA information.

## 4.0 POLICY

### 4.1 General

- NIDA IT or any other admin staff will not request NIDA Username and password at any time and as such you should not reveal your NIDA Username and password (including your Multi Factor Authentication (MFA) token) to anyone.
- Single Sign On (SSO) via Azure using NIDA logins should be used where applicable over a standalone email account and password.
- MFA must be enabled on all systems where applicable.
- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 365 days or when a key staff member departs.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 180 days and cannot be reused. This will be enforced via the NIDA systems.
- All production system-level passwords must be part of the Information Technology administrated NIDA password management database.

- Passwords for shared access (when unavoidable) to external systems for NIDA purposes must be stored and the lifecycle managed with a NIDA password management database.
- Usernames and Passwords must not be inserted in the one message (email/sms/…). Passwords should be communicated via the NIDA password management database.
- All user-level, system-level, and service access level passwords must conform to the guidelines described below.
- Default passwords shall be changed immediately on all equipment by respective business owners of the devices with assistance from NIDA IT.

### 4.2 Password Construction

A Password must:

I. Be a minimum length of ten (10) characters on all systems.
II. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
III. Expire within a maximum of 180 calendar days.
IV. Not be transmitted in the clear or plaintext outside the secure location (Password Manager).
V. Not be displayed when entered.
VI. Ensure passwords are only reset for the authorised user

### 4.3 Password Deletion

All access that are no longer required must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a staff member retires, quits, is reassigned, dismissed, etc.
- Contractor accounts, when no longer needed to perform their duties.

When access is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her point-of-contact (POC).
- NIDA POC will contact NIDA IT or remove the user's access and delete or suspend the user's account.
- NIDA IT Staff will check to ensure that the password has been deleted and user account was deleted or suspended.

When a staff member leaves the organisation, the following procedure should be followed:

- Access to the staff member's account is disabled by NIDA IT
- Manager to notify NIDA IT of any auxiliary accounts used by the staff member.
- NIDA IT or Manager to disable auxiliary accounts.
- Manager to change any shared passwords the employee may have had access to and then notify NIDA IT of a confirmation this has been done (NIDA IT do not need to know the password)

### 4.4 Password Protection Standards

It is vital to create and secure passwords to prevent unauthorized access to the system. Passwords should not be shared with anyone, including NIDA IT, administrative assistants, or secretaries. All passwords are to be treated as sensitive, confidential NIDA information.

Here is a list of "do not's":

- Don't use your User ID as your password
- Don't reveal a password over the phone to anyone
- Don't reveal a password in an e-mail message
- Don't reveal your individual password to managers
- Don't share a password with family members
- Don't reveal a password to a co-worker while on vacation
- Don't use the "Remember Password" feature of applications

- Don’t talk about a password in front of others
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t write passwords down and store them anywhere in your office.
- Don’t store passwords in a file on ANY computer system unencrypted.
- Don’t reveal a password on questionnaires or security forms

If someone demands a password, refer them to this document or have them call NIDA IT for further discussion. If an account or password is suspected to have been compromised, report the incident to NIDA IT and change all passwords.

### 4.5 Service Accounts

All service accounts must be stored securely in the Information Technology administrated global password management database and follow the life cycle outlined below.

- Password to be changed when key staff members leave the organisation
- Access to these passwords should be audited and access monitored
- Should not store passwords in clear text.
- Should not be communicated via email to Vendors or Contractors
- Should use Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

### 4.6 Remote Access Users

Access to the NIDA networks via remote access is to be controlled by using either a Remote Gateway Server or Virtual Private Network (VPN) with a form of advanced authentication (i.e. MFA, Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

## 5.0 PENALTIES

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 6.0 CHANGE HISTORY

| Date | Change Description | Reason for Change | Author/s | Version |
|---|---|---|---|---|
| 2022-08-25 | New | | Head of Technology | 0.8 |
| 2022-08-29 | Minor Changes | Approved by Exec Team | Executive Team | 1.0 |