Password Policy

1. **Introduction**

1.1. The purpose of this document is to provide specific guidance to users of INA Prime Solutions systems and applications in relation to passwords. This is because passwords are an important aspect of information security, and a poorly chosen password could result in INA data being lost or stolen.

2. **Policy statement**

2.1. This Policy applies to all employees and independent contractors of INA Prime Solutions worldwide. Its purpose is to advise all company personnel of their password obligations and to ensure compliance by everyone. It also provides guidance on identifying potential risks, dealing with challenging situations and reporting when those situations violate or may lead to a violation of this Password Policy

2.2. All users with access to INA's systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3. **Roles and Responsibilities**

3.1. The following roles and responsibilities apply in relation to this Policy where appropriate:

3.1.1. **Vice President - Technology & Operations**

- To review and approve the policy on a periodic basis

3.1.2. **IT General Manager**

- To ensure the Policy is reviewed and approved by the VP - Technology & Operations
- To enforce compliance with password standards
- To consult as appropriate with members of the management teams
- To liaise with th VP - Technology & Operations on information received in relation to potential breaches of the policy
- To ensure the appropriate standards and procedures are in place to support the policy

3.1.3. **Staff**

- To adhere to the practices contained in this document
- To report suspected breaches of this policy to their manager

- If you have any queries on the contents of this policy, please contact it@inaprime.com

4. **Scope**

4.1. This standard applies to all users who are allocated an account (or any form of access that supports or requires a password) on any system that has access to INA's network, stores any personal data or private non-personal INA data, or has been authorized as a INA service including, but not limited to, external cloud services.

4.2. Where users are required to access sensitive personal data as part of their assigned duties, additional password requirements will apply. Details on these are available in *Section 5.2.*

4. **Supporting Standards & Procedures**

4.1. The Policy should be read in conjunction with the following INA Prime Solutions policies and Users should ensure compliance with these policies in addition to this policy:

- Data Protection Policy
- Data Retention Policy
- IT Operations and Network Security Policy
- Acceptable Use Policy

5. **Password Standards**

5.1. Password standards for accessing **personal data or private non-personal data** should meet the requirements below to the maximum allowable by the device or application.

5.1.1. Password Complexity

- Passwords must be at least 14-characters. A longer passphrase is recommended. (A passphrase is a sequence of words or other text, e.g. 2Day is a g00d day#.)
- Passwords must contain both upper and lower case letters, at least one number, and one special character (e.g. @, #, $, etc.)

5.1.2. Password Protection

- The user is the sole custodian of the password, and must protect the password at all times
- Passwords must be physically secured if written down, and must be encrypted if stored or transmitted digitally

- Passwords must not be shared, unless used for a documented and approved shared account (e.g. it@inaprime.com)
- System administrators must use a separate account for performing administrative tasks. The username for such accounts should clearly identify the assigned user
- Passwords used for INA accounts must not be used with non-INA systems, for example, social media sites such as LinkedIn, Twitter, and Facebook. INA email addresses should only be used on social media for work-related purposes
- After five failed login attempts the account will be automatically locked. The account will unlock after 15 minutes
- After 10 minutes of inactivity, the session must automatically lock, and require the appropriate password to be input for continued access

5.1.3. Password Changes

- Passwords must be set to expire *at least* annually
- Passwords must not be reused for the next 10 password changes.
- Passwords must be changed immediately when:
    - The password is a default or temporary password created by someone other than the user. This includes vendor-supplied and IT Department default passwords
    - The password, or a system, service or application storing, processing or transmitting the password, is suspected to have been shared or compromised
    - Where a INA system is incapable of supporting the requirements identified in this standard, an exemption with remedial action plan must be approved by the VP - Technology & Operations

5.2. Password standards for accessing **sensitive personal data** should meet the requirements below to the maximum allowable by the device or application.

5.2.1. Password Complexity

- Passwords must be at least 16-characters. A longer passphrase is recommended. (A passphrase is a sequence of words or other text, e.g. 2Day is a g00d day#.)
- Passwords must contain both upper and lower case letters, at least one number, and one special character (e.g. @, #, $, etc.)

5.2.2. Password Protection

- The user is the sole custodian of the password, and must protect the password at all times
- Passwords must be physically secured if written down, and must be encrypted if stored or transmitted digitally
- Passwords must not be shared, and generic accounts must not be used for accessing sensitive personal data
- System administrators must use a separate account for performing administrative tasks. The username for such accounts should clearly identify the assigned user
- Passwords used for INA accounts must not be used with non-INA systems, for example, social media sites such as LinkedIn, Twitter, and Facebook. INA email addresses should only be used on social media for work-related purposes
- After five failed login attempts the account will be automatically locked. The account can only unlock following intervention by the INA IT department
- After 10 minutes of inactivity, the session must automatically lock, and require the appropriate password to be input for continued access

5.1.3. Password Changes

- Passwords must be set to expire *at least* every 60 days
- Passwords must not be reused for the next 24 password changes.
- Passwords must be changed immediately when:
    - The password is a default or temporary password created by someone other than the user. This includes vendor-supplied and IT Department default passwords
    - The password, or a system, service or application storing, processing or transmitting the password, is suspected to have been shared or compromised
    - Where a INA system is incapable of supporting the requirements identified in this standard, an exemption with remedial action plan must be approved by the VP - Technology & Operations

6. **Exceptions Process**

6.1. In circumstances where compliance with some or all of this standard is not practically achievable in the immediate term, an exception must be documented and approved. This will require completion of an Exception Request form detailing the nature of the exception, and any steps that can be taken to mitigate the resulting risk. This form shall be approved and retained by the appropriate manager for the duration of the exception.

Review and update of this document will take place when changes require revising the **Password Policy**. Such modifications may relate to changes in roles and responsibilities, release of new legislation or the identification of a new policy area, in consultation with appropriate members and their approval on all revisions to this Password Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.