Access Control Policy

1. **Purpose**

1.1 The objective of this policy is to minimize accidental or unauthorized access to INA Prime Solution and/or partner connected systems, networks, applications, and information. It is applicable to all forms of logical access.

1.2. This document supports INA's Information Security Policy and Code of Conduct for INA employees. It provides direction and support for the implementation of information security and is designed to help INA employees carry out the business of INA Travel in a secure manner. By complying with this policy, the risks facing INA are minimized.

2. **Introduction**

2.1. Individuals who are not explicitly granted access to INA information or information systems are prohibited from using such systems.

2.2. Individuals employed by or under contract to INA Travel shall be granted access only to information and information systems that are required to fulfill their duties.

2.3. Access will be granted only to those staff who have formally agreed to comply with INA's Information Security Policy and have signed INA's Code of Conduct (for INA employees) or a confidentiality/non-disclosure agreement (contractors/consultants).

2.4. This policy applies to:

- All employees including temporary workers, independent consultants and contractors.
- Third party organizations who require access to INA's information systems and facilities should also be aware of the contents of this policy.

2.4. The policy is not designed to be obstructive. If any INA employee believes that any element of this policy hinders or prevents them from carrying out their duties, they need to contact department heads in either the IT or Human Resources departments.
This policy should be read in conjunction with the following documents:

- Acceptable Use Policy
- Information Classification and Handling Policy
- Physical and Environmental Security Policy
- Third Party Access Policy

3. **Physical Access Control**

3.1. Control of entry into INA Prime Solutions buildings, sites and locations is important for the security of the INA's information systems (both computerized and manual) and its employees.

3.2. Appropriate entry controls must be provided to ensure that only authorized employees are allowed access. When the offices are closed this is achieved by using INA's security system/pass system. Access control must be rigidly enforced in areas housing sensitive information assets.

3.3. In buildings where IT facilities are located and where there is public access, special measures for access enforcement, particularly after normal office hours, must be taken.

3.4. For further details, please see INA's Physical Security Policy.

4. **IT Operations and Network Access Control**

4.1. Access to information and information systems will be controlled on the basis of business and security requirements.

4.2. An access management process for every system/database must be created, documented, approved, enforced and communicated to all relevant employees and partner organizations.

4.3. Each business application run by, or on behalf of INA, will have a nominated system administrator who is responsible for managing and controlling access to the application and associated information.

4.4. Access to information must be based on "need to know" and segregation of duties and roles. The appropriate information, system, database, or application owner is the only individual that can authorize a systems administrator to grant or update access via the formal access management process.

4.5. INA's IT General Manager must monitor the process to ensure that access control is appropriately implemented according to 'business need to know' and 'segregation of duty and role' principles.

4.6. Special attention is given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

5. **User Access Management**

5.1. User access management covers all stages of user access, from initial registration, through changes in role, to deregistration and revocation of access.

5.2. The security of systems, networks, applications and databases is heavily dependent on the level of protection of user IDs, passwords, and other credentials that provide access to it. Hence, protecting the credentials that provide access to information is indirectly protecting the information.

5.3. Identification and authentication of users and systems enables the tracking of activities to be traced to the person responsible.

5.4. All employees shall have a unique identifier (user ID) for their personal and sole use. Shared, group and generic user IDs are not permitted. INA employees must be educated that they are not permitted to allow their user ID to be used by anyone else. All employees must be made aware of this and how to store them.

5.5. A process must exist for issuing and revoking the user IDs. Redundant user accounts must be monitored and managed.

6. **User registration**

6.1. A process for user registration and granting access rights exists and includes:

- Unique user IDs assigned so that access and modifications can be traced
- Authorized users are aware of their responsibilities for the protection of information within the application and where applicable users sign an appropriate agreement
- Ensuring access is granted once authorisation is obtained
- Maintaining a record of all registered users

7. **Change of Role**

7.1. Where an employee changes role within INA the following process is followed:

- Managers must inform all relevant system administrators of the names of employees that have transferred to different job/roles within 24 hours of transfer.
- A process must be in place for the HR department to communicate transfers to system administrators.
- System administrators must review the transferee's access rights to their systems to ensure that they are still valid.

8. **Review of Access Rights**

8.1. Managers should review access lists to ensure they are still applicable. Necessary modifications must be sent to system administrators for correction.

8.2. The data owner must approve access rights prior to set up by the system administrator. The system administrator does not have the authority to decide who should have access to what information. This is a business decision.

9. **Removal of Access**

9.1. On resignation of employment, managers, in conjunction with HR, will undertake a risk assessment and determine whether existing access rights of an individual should be reviewed and reduced whilst working out their notice. Hostile terminations must be communicated to system administrators immediately and access immediately disabled.

9.2. Managers must inform system administrators of the names of employees that will be leaving INA employment at least 48 hours before the end of their last working day.

9.3. Access rights should be disabled by 5.00 pm on the employee's lasting working day. It is the responsibility of managers to ensure that leavers return their entry keys and pass codes at the end of their last working day and to return it for deactivation as well as return all INA equipment that could be used to gain network access.

10. **Password Management and Multi-Factor Authentication**

10.1. To identify users, usernames must require another access token in order to login. This can be a biometric, a time-sensitive generated password, a hardware token, a user-managed password or a combination of these.

10.2. Where practicable, system access should require more than one access token - multi-factor authentication (MFA).

10.3. All systems must use passwords for access. The following controls will be in place to ensure strong password management.

- Password length must be a minimum of 16 characters.
- Where the software solution allows the password complexity will be as follows (or at minimum a combination containing at least three of the following conditions):
- One Numeric (0123456789)
- One uppercase (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
- One lowercase (abcdefghIjklmnopqrstuvwxyz)
- One special character (*!#.@#$%^&*,)
- The password will be changed every 60 days (where the application allows this to be enforced, otherwise users will be required to change the password manually).
- Users should not repeat the same password within a cycle of 20 password changes
- When an invalid password is entered three times in a row, the system revokes user access and must be reset. In some systems, users can do this for themselves

using validation such as messages to mobile or secret questions. In others, system administrators must validate the request before resetting the password. Passwords stored on a computer are encrypted and protected from unauthorized access or deletion.

- Passwords must not be displayed on screen at any time.
- All default passwords must be changed following the installation of any new software or hardware
- Users can reset their own passwords in some systems, in others, only system administrators are permitted to reset passwords or assign new passwords
- New passwords and reset passwords are random and force immediate change after first login by the user. System administrators must ensure that they divulge new or reset passwords only to the authorized user of that ID.
- When it is known or suspected that a user ID has been compromised the system administrator must be immediately informed in order to have it revoked.
- System passwords, including administrator passwords that are used to access data that is required by the business, must be stored in secure locations such that in the advent of a business requirement the passwords can be recovered.
- There is a process in place to allow for the prompt resetting of passwords.
- A process is in place for the allocation and removal of system administration level access or increased user privilege and includes the following controls:
    i). Every level of privilege within each application and the categories of staff to which they need to be allocated are identified and recorded
    ii). Privileges are allocated to an individual as an event requires
    iii). Authorisation is recorded for each allocated level of privilege and only granted once authorisation is obtained
    iv). The development of system routines are identified and implemented to avoid the use of privileged access
    v). Privileges are assigned to a different user ID from those used for normal business use and where possible a log of increased user privilege is recorded.

11. **Monitoring System Access and Use**

11.1 Systems will be monitored to detect deviation from the Access Control Policy and record events to provide evidence in case of security incidents.

11.2. The application business owner/system administrator must establish the logging and monitoring requirements for business auditing purposes. Designated employees responsible for the following areas must establish the logging and monitoring requirements for the relevant purposes:

- Security
- Incident investigations
- Audit
- Fraud

- Legal

11.3. A process for capturing logging and monitoring requirements must be developed. Audit and event logs will need to be adequately secured, possibly centrally and separately from privileged-level employees (separation of duties). Tools may be required for log analysis.

12. **Security of Third Party access**

12.1 *See Third Party Security Policy*.

13. **Access from overseas**

13.1 Access to INA Prime Solutions' network from overseas is subject to additional controls to ensure compliance with relevant legislation and this will place additional personal liability on users. Please refer to the Acceptable Usage Policy for details.

14. **Access to Secure Areas**

14.1 All network equipment (including, but not limited to WAN service termination equipment, routers, switches, cabling patch panels) will be kept in appropriate locked facilities whenever practicable. All network equipment outside of designated communication rooms must be kept securely. Staff must ensure that communications cabinet and communications room doors are secured when they are left unattended. All keys must be limited to staff who need them to carry out their duties. If any key is lost or mislaid, or any door found unlocked, then this must be reported immediately as an IT security incident.

14.2 All physical servers must be kept physically secure in an area for authorized individuals only. A process of allocating and monitoring access to server rooms must be implemented – this may include electronic access control or the use of signing in books as appropriate.

14.3 For cloud servers and services, the supplier must have a suitable Cloud Security Assessment.

14.4 For further information see the *Physical Security Policy.*

15. **Policy Compliance**

15.1 INA Prime Solutions requires that all employees comply with the directives presented within this policy. This policy will be included within the Information Security Internal Audit

Programme, and compliance checks will take place to review the effectiveness of its implementation.

16. **Exceptions**

16.1 In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would lead to physical harm or injury to a member of staff
- If complying with the policy would cause significant damage to the company's reputation or ability to operate
- If an emergency arises
  In such cases, the staff member concerned must take the following action:
- Ensure that their manager is aware of the situation and the action to be taken
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non- conformance report
- Ensure that the situation is reported to the LBE Service Desk as soon as possible.

16.2. Failure to take these steps may result in disciplinary action.

16.3. In addition, the IT General Manager maintains a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified
- Minor breaches that are not considered to be worth rectifying
- Any situations to which the policy is not considered applicable.

16.4. INA will not take disciplinary action in relation to known, authorized exceptions to the information security management system.

17. **Penalties**

17.1. Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorized disclosure or viewing of confidential data or information belonging to INA
- Unauthorized changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law,

regulation or reporting requirements of any law enforcement agency or government body

- The exposure of INA to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the IT General Manager or senior management.

17.2. Any violation or non-compliance with this policy may be treated as serious misconduct.

17.3. Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.

Review and update of this document will take place when changes require revising the **Access Control 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 Access Control Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.