Acceptable Use Policy

1. **Introduction**

1.1 This policy defines the acceptable use of INA Prime Solutions' information assets and those assets provided to Goway by partner organizations. It is known as the "Acceptable Use Policy" or "**AUP**".

1.2. This policy applies to all INA employees including temporary workers, independent consultants and suppliers/contractors who need to use INA information assets, as part of/to carry out their duties. These people are referred to as "users" in the rest of this document.

1.3. Acceptable use means that access to information is legitimate, it is used only for the intended purpose(s), the required standards of practice are in place to protect the confidentiality, integrity and availability of information, and the use complies with relevant legislation and regulation.

1.4. INA aims at all times to conduct its business in a professional manner and to provide the highest possible level of service, both internally and to its customers. Any loss, compromise, or misuse of INA information and associated assets, however caused, could have potentially devastating consequences for INA and may result in financial loss and legal action.

2. **Definitions**

2.1. An information asset is any data, device, or other component of the environment that supports information-related activities. Assets include hardware (e.g. laptops), software and confidential information (e.g. a person's record).

2.2. Inappropriate use of information assets exposes INA and the service users who entrust us with their data to risks.

2.3. A data subject is a person or organisation to whom data relates.

2.4. A data controller is a person or organisation who is legally in charge of a data asset. INA is the data controller for many of the assets it holds.

2.5. A data processor is a person or organisation who is tasked by a data controller with using a data asset.

2.6. A user is any person or organisation accessing information assets.

2.7. Personal data is data that relate to an individual. For example, name, address and date of birth are examples of personal data.

2.8. “PC” means any computer device such as a tablet, laptop or desktop.

2.9. “mobile” means any portable device with a mobile network connecting including smart phones, standard phones, Personal Digital Assistants. Note that some tablet devices (e.g. a tablet with a mobile network connection) fall into both the PC and mobile category and rules for both must be followed.

3. **Policy Statements**

3.1. It is the responsibility of all INA users to know this policy and to conduct their activities accordingly. Breach by any user could result in disciplinary action or other appropriate action being taken.

3.2. INA information facilities are provided for business purposes only, with limited personal use permitted as defined elsewhere in this document. Use of information facilities for personal use must be authorized by the employees manager.

3.3. Any use of INA facilities for unauthorized purposes may be regarded as improper use of facilities. INA IT systems must display an appropriate warning notice to this effect when users log on.

3.4. Users should be aware that any data they create on INA systems (including anything pertaining to themselves) is deemed to be the property of INA. Users are responsible for exercising good judgment regarding the reasonableness of personal use and to be compliant with the Employee Code of Conduct.

3.5 For security and network maintenance purposes, authorized INA staff may monitor equipment, systems and network traffic at any time. INA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.6. The policy is not designed to be obstructive. If any INA user believes that any element of this policy hinders or prevents them from carrying out their duties, they can contact the IT department or Human Resources.

3.7. This policy is supported by a number of other policies which should be read in conjunction with it.

4. **Use of Personal Data**

4.1. INA Prime Solutions has access to a wide range of personal data entrusted to us by our clients and others. This data must be used and accessed in accordance with the law.

4.2. Users must only use personal data in accordance with the agreed and published purposes for the collection of data. Using personal data in any manner requires a clear legal basis or consent from the data subject. Merging personal data with other sources, for example, is not permitted unless a legal basis or consent is present, and the use of the data correctly authorized.

5. **Information System Security**

5.1. Security of INA's information assets is paramount. Information assets must be treated as confidential.

a. Security Controls and Reporting

i). INA has implemented security systems to safeguard information assets. These include controls over viruses, offensive and illegal material, disruption to our systems, and unauthorized access. Bypassing or attempting to bypass these security systems is a breach of policy.

ii). To be effective, all users must support and use these systems and must assist in identifying and eliminating threats to information security. Any breach or suspected breach of this policy must be regarded as a security incident. Users must report security incidents to the IT department immediately.

b. Use of Downloaded Programmes

i). Under no circumstances may users use any programme that is not already installed on a PC or download programmes from the Internet for use on INA Information and Communications Technology (ICT) systems. For mobile devices, only applications from approved app stores should be installed.

c. Passwords

i). Users are responsible for the security of their passwords and accounts. Passwords must be kept confidential and not shared with others.

ii). Passwords should be changed at regular intervals or based on the number of accesses. The reuse of old passwords is not permitted.

iii). Temporary passwords must be changed at the first log on. Passwords must be changed whenever there is any indication of possible system or password compromise.

iv). If legitimate access to an absent person's system or data is required, then written or email authority must be provided by a senior manager of the employee to the IT General Manager.

v). All PCs accessing resources must be secured with a password protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

6. **Internet Usage**

6.1. INA Prime Solutions provides access to the information resources on the Internet to help users carry out their functions. The provision of Internet access is at INA's discretion and users provided with internet access are required to read and adhere to this policy.

6.2. Internet access for personal use is at INA's discretion and should not be assumed as a given. Any misuse of this facility can result in it being withdrawn. Limited personal use of the Internet is permitted outside of normal working hours.

7. **Email Usage**

7.1. The email system is for INA business use only. Users should use personal email facilities wherever possible and web mail systems are allowed from INA devices for this reason. However, INA understands that users may on occasion need to send or receive personal emails using their work address. Users wishing to send personal email must seek the prior permission of their manager. Auto forwarding of email to external email accounts (non INA) is expressly forbidden.

7.2. Emails that users intend to send should be checked carefully. Email should be treated like any other form of communication and, as such, what is normally regarded as unacceptable in, for example, a letter is equally unacceptable in an email communication. The sender of the email is responsible for the safe arrival of information at its intended destination and it is the sender who is usually liable for any breach of security and confidentiality.

7.3. Sending emails internally is secure. Sending emails externally is not generally secure and they can be intercepted and viewed by unauthorized people. Secure email must be used when emailing information to external agencies or individuals when the content of the e-mail includes:

- Personally identifiable client or third party information
- Financial, sensitive or other information that could cause detriment to INA or to an individual
- Personal or sensitive business information must not be sent to an email address outside of INA, unless it is absolutely necessary and the transmission is secure.
- Staff must be vigilant with attachments to emails and links to documents downloaded from other locations as they may contain viruses. Users who suspect a possible virus attack must report it to the IT Department immediately.

7.4. Staff must be aware that email is easy to forge and that attacks based on this are common. Always treat emails asking for unusual actions with suspicion. For example:

- Any email asking to move money should be confirmed in person or by telephone.
- Any email asking for a password or to click on a link which then asks for username, password or bank details even if it appears to be from ICT may be fake – ICT will never ask for these details.
- Emails containing urgent invoices are likely to be fake – invoices should be checked by the Accounting Department

7.5. For further information regarding secure information exchange (e.g. via email & Cloud Storage) please refer to the *Data Protection Policy* & *Information Classification and Handling Policy*.

8. **Responding to Security Incidents & Malfunctions**

8.1. Any perceived or actual information security weakness or incident must be reported to the IT Department immediately. Examples of a security incident include unauthorized access to information assets, misuse of information assets, loss/theft of information assets, virus attacks, denial of service attacks, suspicious activity.

9. **Computer Viruses & Other Harmful Code**

9.1. All PCs and servers directly connected to resources, whether owned by INA or not, must be continually executing approved virus scanning software with a current virus signature file except where this is not technically possible.

9.2. It is a crime to deliberately introduce malicious programmes into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc). Users must not use INA facilities for intentionally accessing or transmitting computer viruses or other damaging software or software designed for creating computer viruses.

9.3. When the PC is not connected directly to the INA network, users should scan any material received/downloaded from the Internet to make sure it is virus free using the approved anti-virus protection system and should not distribute any material that has not been scanned using the approved system.

9.4. If a user is in doubt about any data received or suspects a virus has entered their PC, they must log out of the network immediately, stop using the PC and inform the IT Department immediately. Users are required to follow the instructions that the IT Department issues about virus attacks.

10. **Hacking and Associated Activities or Breaches of Policy**

10.1. It is a crime to enter into another computer system without authorisation.

10.2. INA IT facilities must not be used in any way that breaks the law or breaches standards. Such actions could result in disciplinary action being taken.

10.3. Users must not use INA facilities for:

- Sending threatening, offensive or harassing messages
- Creating or sending obscene material
- Accessing or transmitting information about, or software designed for, breaking through security controls on any system.
- Effecting security breaches or disruptions of network communication. These include, but are not limited to:
- Accessing data to which the user is not an intended recipient without permission, even if it is not protected by security controls
- Logging into a server or account that the user is not expressly authorized to access
- Network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- Port scanning or security scanning (unless prior authorisation has been granted)
- Executing any form of network monitoring which will intercept data not intended for the user (unless prior authorisation has been granted)
- Circumventing user authentication or security of any host, network or account
- Interfering with or denying service to any user (for example, denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's communication session, by any means, locally or via the Internet or Intranet

10.4. Users may be exempted from some of the above restrictions during the course of their legitimate job responsibilities (e.g. systems administration employees may have a need to disable the network access of a host if that host is disrupting production services). Such exemptions should be approved and documented by the IT Department General Manager.

11. **Copyright & Encryption**

11.1. It is illegal to break copyright protection. Users could break copyright if they download, transmit or copy protected material.

Users must not:

- Transmit copyright software from their PC or allow any other person to access it from their PC unless the controls/license so permits
- Knowingly download or transmit any protected information/material (including, but not limited to, digitisation and distribution of photographs from magazines,

books or other copyrighted sources and copyrighted music) that was written by another person or organization without getting permission
- Copy/install copyright software from/to their PC for any purpose not approved by the license and for which INA or the user does not have an active license
- Transmit software, technical information, encryption software or technology, in violation of international or regional export control laws.

11.2. The IT General Manager should be consulted prior to export of any material that is in question and all information in this respect should be documented accordingly.

12. **Unattended User Equipment**

12.1. Users must not leave their workstation unattended without ensuring that sensitive information is not visible on their screen or left on their desks and/or access to any open sessions are closed.

12.2. Users accessing sensitive information must position their workstation in such a way that the information is not visible to unauthorized users.

12.3. Screen savers or equivalent tools must be installed and enabled as part of a Standard Operating Environment (SOE).

12.4. To protect against unauthorized access, equipment must be locked (generally, this can be achieved via holding the Windows key and pressing L) when not attended.

12.5. No paper copies of data, memory sticks or other portable media may be left on desks when unattended.

12.6. Lockable cabinets need to be available to store sensitive documentation when a desk is unattended.

13. **Hardware Usage**

13.1. All INA owned computer equipment and software remain the property of INA. Any user who leaves INA employment / engagement is required to return all hardware and software that has been provided to them.

13.2. Only hardware provided by INA is authorized for use for INA business. Users must not attempt to attach any other equipment to INA hardware or to network or telephone sockets.

14. **Software Usage**

14.1. INA Prime Solutions is committed to the use of authorized software within its computer

systems. It is expressly forbidden for users to load or operate software gained from the Internet or other sources. INA is also committed to using software for which it has current licenses.

14.2. It is the responsibility of all users to ensure that they do not introduce viruses into computer systems. Users should take care when receiving electronic information from unknown sources, including attachments within Email. Where there are reasons to access information from questionable source(s), active virus checking must be performed, preferably on a standalone computer and/or test server, thus having no communication links to other systems.

14.3. The following provisions, which apply to the use of all computers, govern all users:

- Only software purchased by INA and approved by the IT Department may reside on INA computer equipment including PCs and mobiles.
- The IT Department will undertake to purchase licenses for all products used by INA and will control the allocation of licenses for products that are distributed as single media items and licenses for multiple instances of that one distribution.
- Only IT Department authorized technical staff may install or remove software on INA computer equipment.
- Software includes source code, object code and intermediate code that can be firmware as well as software.
- Downloading of "shareware" and/or "freeware" is prohibited irrespective of the fact that a license may or may not be needed unless the IT Department has approved the product to be downloaded and installed.
- The installation of personal software including screen savers is prohibited.
- Upgrades to software products will be treated as new products.
- All software media is to be held and securely stored by the IT Department
- IT Department staff may copy software media only if they are legally allowed to do so. This is in accordance with Copyright laws and the terms and conditions of the relevant software license. Software media may not be copied under any other circumstances.

15. **Mobile Computing**

15.1. When using computing and communication facilities outside of the secure office environment, special care should be taken to ensure that information is not compromised. Protection must be in place to avoid unauthorized access to or disclosure of information including ensuring your screen cannot be seen by others and that equipment is not left unattended.

15.2. If a device is lost or stolen, the IT Department must be contacted as soon as possible.

16. **Access from Overseas**

16.1. Access to the INA's network from overseas is subject to additional controls to ensure compliance with relevant legislation and this may place additional personal liability on users.

16.2. The facility to remotely access the INA network from other countries will only be permitted in exceptional circumstances and should not be assumed. A written request including a business case must be submitted to the IT Department for considerations at least two weeks in advance of any planned travel.

16.3. The user should seek advice from the IT Department before taking any INA supplied ICT equipment outside of North America. The equipment may not be covered by the INA's normal insurance against loss or theft.

17. **Fax**

17.1. All faxes must include a non-disclosure statement and security classification.

17.2. All users must ensure that confidential faxes are protected during transmission and only sent when the recipient is aware of the transmission and is instructed to protect its content.

17.3. Confidential faxes must be removed as soon as the transmission has ended.

18. **Telephones**

18.1. Personal calls should be kept to a minimum and not interfere with performance of duties. I reserve the right to check, review and monitor telephone calls made using any INA telephone or telephone system.

18.2. Where INA provides a user with a mobile phone, it is to ensure that the user is contactable when away from the office. Therefore, INA mobile phones should be switched on or directed to voicemail or an alternative phone at all times during working hours.

18.3. Voicemail should be checked regularly and greetings updated as necessary. Voicemail users should secure their messages with a minimum four-digit pin code and clear down messages on a frequent basis.

18.4 To ensure that a mobile phone cannot be used fraudulently, it should be protected by using a PIN number. If a INA mobile phone is lost or stolen it must be reported to the IT Department immediately.

19. **Legislative Requirements**

19.1. Under no circumstances are users allowed to engage in any activity that is illegal under local, national or international law while utilizing INA resources.

20. **Monitoring Use**

20.1. INA Prime Solutions reserves the right to monitor, review and record the use of all information and telephone systems and all documents stored on information systems, including documents profiled as private and confidential.

20.2. INA reserves the right to monitor email traffic within the corporate email system and to access mailboxes and private directories without notification to the individual concerned that the right is being exercised.

20.3. INA may exercise this right in order to establish facts relevant to INA business and to comply with:

- Regulatory practices and procedures
- To prevent or detect crime
- To ensure compliance with INA policies
- To investigate or detect unauthorized uses of the system or to ensure the effective operation of the system (e.g. to check if viruses are being transmitted)

20.4. Therefore, users do not have the right to privacy when using INA information systems or in relation to any communications generated, received or stored on INA information systems.

21. **Policy Compliance**

21.1. INA Prime Soltions expects that all users will achieve compliance to 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.

22. **Exceptions**

22.1. 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 any person
- 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 user 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 nonconformance report

- Ensure that the situation is reported to the IT Department as soon as possible.

Failure to take these steps may result in disciplinary action.

In addition, the IT 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. INA will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

23. **Penalties**

23.1. 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 or partner organization
- 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 or partner organization 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 Department or senior management.
- Any violation or non-compliance with this policy may be treated as serious misconduct.
- 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 **Acceptable Use 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 Acceptable Use Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.