Information Security Policy

1. **Introduction**

1.1. Next to our clients and our staff, information is INA Prime Solutions' most important asset. The information we use exists in many forms: printed or written on paper, stored electronically, transmitted using electronic means, or spoken in conversation. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

1.2. Information security is characterized here as being concerned with guaranteeing availability (ensuring that authorized users always have access to information when they need it), integrity (safeguarding its accuracy and completeness), confidentiality (ensuring that sensitive information is accessible only to those authorized to use it), and authenticity. It must also address proper methods of disposal of information that is no longer required. Security is essential to the success of almost every staff and management activity. Effective security is achieved by working within a proper framework, in compliance with legislation and INA policies, and by adherence to approved procedures and codes of practice.

1.3. The objectives of this information security policy are to:

- ensure that all of INA's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that this protection is cost-effective;
- ensure that all users are aware of and fully comply with this policy statement and all associated policies, and are aware of and work in accordance with the relevant procedures and codes of practice;
- ensure that paper records are kept securely and managed effectively;
- ensure that all users are aware of and fully comply with the relevant legislation;
- create across INA an awareness that appropriate security measures must be implemented as part of the effective operation and support of information management systems;
- ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle;
- ensure that information is disposed of in an appropriately secure manner when it is no longer relevant or required.

1.4. The policy applies to all staff of INA Prime Solutions and all other computer, network or information users authorized by INA. It relates to their use of any INA-owned facilities (and those leased or rented by INA), centrally managed or otherwise; to all private systems when connected to the INA network; to all INA-owned or licenced data and programs (wherever stored); and to all data and programs provided to INA external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of INA business.

1.5. The INA Prime Solutions Senior Management Team has approved this policy statement and delegated its implementation to each Department Head and Division.

1.6. Those requiring information, explanation or training about any aspects of the policy which relate to computer security should discuss their needs with the INA Information Technology team. Questions about the creation, classification, retention and disposal of records (in all formats) should be taken to the IT General Manager. The INA Information Technology team will in the first instance be responsible for interpretation and clarification of the information security policy.

2. **Responsibilities for Information Security**

2.1. All who make use of INA Prime Solutions' systems and information have responsibility for protecting those assets. Individuals must, at all times, act in a responsible and professional way in this respect, and will refrain from any activity that may jeopardize security.

2.2. The Information Technology team is responsible for defining an information security policy and for ensuring it is implemented by all departments and divisions through the respective Vice Presidents/General Managers.

2.3. Vice Presidents/General Managers of all departments are required to implement this policy in respect of both paper and electronic systems operated by their Departments and are responsible for ensuring that staff and other persons authorized to use those systems are aware of and comply with it and associated codes of practice. They should ensure adequate oversight of security (in consultation with the Information Technology team), and are responsible for ensuring the policy is fulfilled.

2.4. Operational responsibility for records management is delegated to the General Manager - Information Technology, who is responsible for the development of procedures, advice on good practice and promotion of compliance with the INA Prime Solutions Records Management Policy, which applies to all records in any format.

2.5. The Information Technology team is responsible for regularly reviewing the policy for completeness, effectiveness and usability. They will from time to time make available supplementary procedures and codes of practice, and promote them throughout INA; once approved by Senior Management these will also become INA policy and will be binding on departments.

2.6. The Information Technology team, in addition to its involvement in policy making, provides relevant operational services. These include incident response and coordination, and dissemination of security information.

2.7. It is the responsibility of each individual to ensure his/her understanding of and compliance with this policy and any associated procedures or codes of practice.

2.8. Staff with supervisory responsibility should make their staff aware of best practice.

2.9. Staff who process or who are responsible for the processing of personal data, as defined in INA Prime Solutions' Data Protection Policy, are additionally required to understand and comply with all obligations placed upon them under agreements with external parties, including but not limited to information security, integrity and perpetual confidentiality.

3. **Risk Assessment and Security Review by Departments/Divisions**

3.1. Senior Management should adopt a risk-based approach to assessing the value of information handled, its sensitivity and the appropriateness of security controls in place or planned. Without proper assessment of the value of information assets, and the consequences (financial, reputational and otherwise) of loss of data or disruption to service, efforts to improve security are likely to be poorly targeted and ineffective. Similarly, periodic review is necessary to take into account changes to technology, legislation, business requirements and priorities; security arrangements should be revised accordingly.

3.2. Vice Presidents/General Managers of Departments should establish effective contingency plans appropriate to the outcome of any risk assessment. They are also required to re-evaluate periodically the security arrangements for their information management systems - at least once every three years, and additionally in response to significant departmental changes (such as turnover of key staff, commissioning of new systems etc.).

4. **Breaches of Security**

4.1. Any individual suspecting that the security of a computer system has been, or is likely to be, breached should inform the Information Technology team immediately. The IT team will advise Senior Management on what steps should be taken to avoid incidents or minimize their impact, and identify action plans to reduce the likelihood of recurrence.

4.2. In the event of a suspected or actual breach of security, the IT team may, after consultation with the relevant Vice President/General Manager of the Department, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

4.3. Where a breach of security involving either computer or paper records relates to personal information, the Management Board must be informed, as there may be an infringement of the Personal Information Protection and Electronic Documents Act of Canada or the United States Privacy Act which could lead to civil or criminal proceedings. It is vital, therefore, that users of INA's information systems comply, not only with this policy, but also with INA's Data Protection Policy and associated codes of practice.

4.4. All physical security breaches should be reported to the INA Management Board.

4.5. The Information Technology team will monitor network activity, and take action or make recommendations consistent with maintaining the security of INA information assets.

4.6. The VP of Technology & Operations and the IT General Manager have the authority to take whatever action is deemed necessary to protect INA against breaches of security.

5. **Policy Awareness and Disciplinary Procedure**

5.1. The contract of employment shall state that employees are required to comply with the Information Security Regulations, including such additions or amendments thereto as may be made by INA from time to time.

5.2. As part of the induction process, Managers are reminded via the standard checklist to ensure that the online information security awareness training is completed.

5.3. Staff are required to comply with the Information Security Regulations, including such additions or amendments thereto as may be made by INA from time to time.

5.4. Existing staff of INA, authorized third parties and contractors given access to the INA network will be advised of the existence of this policy statement and the availability of the associated procedures, codes of practice and guidelines. Failure of a member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

6. **Supporting Policies, Procedures and Codes of Practice**

6.1. Supporting policies, procedures and codes of practice amplifying this policy statement are published with it and are available on the INA website. Staff, contractors and other third parties authorized to access the INA network to use the systems and facilities identified in paragraph (1.4) of this policy, are required to familiarize themselves with these and to work in accordance with them.

6.2. Personal data must be stored securely; if such data is held on mobile devices (e.g. smartphones) or removable media, it must be strongly encrypted, in compliance with the Data Protection Policy. Other forms of sensitive business data, intellectual property, etc. should, similarly, be strongly encrypted.

6.3. Any outsourced information services must be subject to a documented contract which must comply with all security guidelines.

7. **Status of the Information Security Policy**

7.1. This policy statement does not form part of a formal contract of employment with INA Prime Solutions, but it is a condition of employment that employees will abide by the regulations and policies made by INA.

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