Physical and Environmental Security Policy

1. **Purpose**

1.1. Any loss, compromise, or misuse of INA Prime Solutions information and associated assets, however caused, could have potentially devastating consequences for INA and may result in financial loss and legal action.

1.2. The purpose of this document is to define the requirements for physical and environmental security that will be applied to maintain the confidentiality, integrity and availability of information and information systems supporting the business functions of INA Prime Solutionsl.

2. **Introduction**

2.1. Information processing facilities supporting INA business activities must be located within a secure area to protect them from unauthorized physical access and damage.

2.2. This policy applies to:

- all buildings, sites and locations used by INA, whether or not owned by it
- all premises used by INA's partners to house any IT systems directly connected to INA resources
- All INA employees, including temporary workers, independent consultants and contractors (referred to as "users").
- Suppliers/contractors responsible for managing premises housing INA information systems, computer and network facilities (referred to as "users").

2.3. The policy is not designed to be obstructive. If any user believes that any element of this policy hinders or prevents them from carrying out their duties, they must contact INA's IT Department General Manager or Human Resources.

2.4. In adhering to these standards, users must not put themselves at personal risk.

2.5. The following policies should be read in conjunction with this policy:

- *Acceptable Use Policy*
- *Access Control Policy*
- *Information Handling and Protection Policy*
- *Business Continuity Management Policy*

3. **Physical Security Areas**

3.1. Just as it is essential to identify sensitive information, there is also the need to identify and accord appropriate levels of protection to different areas within buildings. The physical security requirements for areas will depend upon:

- The value and sensitivity of the information and information assets to be protected
- Likely or associated security threats and risks existing safeguards and protective measures

3.2. INA Prime Solutions has identified four such areas and the physical protection procedures required:

A. **Public Areas**

i). These are areas that are freely accessible to the public. Here, the value of IT assets is either low (usually a desktop PC in reception) or the assets are physically large (e.g. a brochure rack).

ii). All equipment not specifically for public access should be sited to minimize the risks of unauthorized access or compromise of information.

iii). Publicly accessible systems used to display confidential information should be sited in such a way as to prevent another member of the public viewing the displayed data.

iv). All publicly accessible equipment should be appropriately defended against vandalism, modification and theft.

B. **General Office Areas**

i). These are the typical office areas that are normally accessible only to employees and admitted guests (including commercial/business people, clients, etc.) Here, the value of IT assets is not excessive (usually desktop PCs and laptops) and access to sensitive information is closely controlled.

ii). General office areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access

iii). Visitors must be supervised and must only be granted access for specific, authorized purposes

iv). Support functions and equipment (e.g. photocopiers, fax machines, printers) must be sited to minimize the risks of unauthorized access or compromise of information.

C. **Sensitive Areas**

i). These are also typical office environments with desktop PCs and laptops. However, the sensitivity of the information processed is high (e.g. accounting department, IT department).

ii). Sensitive areas must be protected by appropriate entry controls to ensure that only authorized employees are allowed access

iii). Visitors must only be granted access for specific, authorized purposes

iv). Employees supplying or maintaining support services will be granted access to sensitive areas only when required and authorized. Where appropriate, their access will be restricted and their activities monitored

v). Sensitive areas must be physically locked outside office hours and checked periodically

vi). Support functions and equipment (e.g. photocopiers, fax machines, printers) must be sited to minimize the risks of unauthorized access or compromise of sensitive information.

D. **Secure Areas**

i). These are communication rooms and computer rooms, rooms accommodating servers, etc. that support critical and/or sensitive activities, and areas housing vital information and documents that require a higher level of physical security compared to other operating environments.

ii). Secure areas must have a higher level of physical and environmental security protection to minimize the possibility of damage from fire, flood, explosion, terrorism, and other forms of natural or man-made disaster. Senior management must determine and designate the area(s) within their operating environment according to the above classification and ensure the relevant physical protection mechanisms are implemented.

iii). Access will be controlled by an access control device, preferably one with an audit trail (i.e. something other than a key or a keypad). If such a device is not fitted then a manual log of entry and exit must be maintained.

iv). When unattended, or where the support employees are remote, rooms should be kept locked and an access and egress log maintained.

v). A fire control system must be in place:

- appropriate sited and approved fire extinguishers
- fire alarms that are wired to the main building fire alarm system

- place smoke, fire, and unusual water flow detection devices that are regularly tested

vi). Where equipment requires environmental control, rooms must be air-conditioned with humidity set at 50-55% and temperature at 18C. Means of monitoring the environment and an alarm on the conditioning equipment must be installed.

4. **Equipment Siting & Protection**

4.1. Workstations displaying sensitive data must be positioned to reduce the risk of overlooking.

4.2. Where possible, IT equipment must be sited or protected to reduce risks from unauthorized access, theft, and environmental hazards such as fire, flood, dust, chemicals, electromagnetic interference, and loss or fluctuation of power supply.

5. **Buildings - External Physical Security**

The physical security requirements for areas will, at least to some extent, depend upon the security classification of the areas that they contain.

5.1. **Security Lighting**

5.1.1. Security lighting can offer a high degree of deterrence to the potential intruder in addition to providing the illumination necessary for effective surveillance. The standard of lighting should, however, meet the minimum requirement and its installation be appropriate to the site conditions.

- Lighting which illuminates perimeter boundaries should be installed
- All dark and blind spots should be eliminated
- Under low light conditions lighting should be activated automatically
- Consideration should be given to illuminating roofs, fire escapes and emergency exits
- Lights installed should be resistant to interference

5.2. **Doors**

5.2.1. External doors should provide some resistance to forced attack. Keys to external doors are held under secure conditions but should be readily accessible to authorized persons. External doors that are never used and which are not emergency exits should be permanently secured.

5.2.2. External doors leading to areas other than public areas must have an unauthorized access control mechanism. These should normally be locked outside of normal working hours.

5.3. **Emergency Exits**

5.3.1. There is often a conflict between demands for security and those of safety when it comes to securing emergency exits. Most emergency exit locks, including those of bar release type, are not fully secure and emergency exits should normally be fitted with intruder detection devices.

5.4. **Inter-Communicating Doors**

5.4.1. Doors communicating with other parts of a building designated as being of a different security classification in general provide a degree of security similar to that of external doors. Doors leading to sensitive or secure areas may need to be protected with intruder alarms.

5.5. **Windows**

5.5.1. Basement, ground floor and other windows that are readily accessible should have secure fittings. Window catches should be regularly examined and defective catches replaced. Intruder alarms should be considered for windows in secure or sensitive areas.

5.5.2. Where it is necessary to secure a window more effectively than by the use of lock, catch or bolt (e.g. secure areas), the use of bars, grilles or shutters should be considered along with the use of intruder detection sensors.

5.5.3. Double-glazing can provide excellent protection against covert attack and some protection against forced attack. It is unobtrusive, may draw less attention to a sensitive area and is more acceptable than bars or grilles. Double-glazing can also be alarmed.

5.6. **Other Access Points**

5.6.1. Roofs and roof doors should be periodically surveyed to see whether there is access to them from adjoining buildings, nearby buildings, trees, fire escapes, window cleaning equipment, etc.

5.6.2. Access to the upper floors of a building or from the roof may often be afforded by way of rainwater or soil down-pipes. Such access may be restricted by boxing in the pipes or by treating them with anti-climb paint - this should be applied at heights above 2.75m to avoid accidental contact by passers-by.

5.7. **Public Utilities**

5.7.1. Gas, electricity and water supply installations within buildings may offer potential vulnerability access points. Where possible, cables and pipes within buildings should enter

the building underground. Public service meters should, wherever possible, be so sited that access to them does not require entry into secure or sensitive areas.

5.8. **Delivery and Loading Areas**

5.8.1. At each site a delivery and loading area is provided for supplies and equipment deliveries. It is sited to reduce the opportunities for unauthorized access to the working areas and secure offices. The following controls are implemented:

- Access to a delivery and loading area from outside of the building is restricted to identified and authorized personnel
- The delivery and loading area is designed so that suppliers can be unloaded without delivery personnel gaining access to other parts of the building or location
- Where relevant, the external doors of a delivery and loading area are secured when the internal doors are opened
- Relevant employees are given advance notice of incoming deliveries. Any deliveries arriving without clear destinations or advanced warning are turned away
- Incoming material is inspected for potential threats before goods are moved from the delivery and loading area to the point of use
- Incoming material is registered on entry to the site
- Incoming and outgoing consignments are physically segregated where possible

6. **Fire & Flood Prevention**

6.1. **Fire Prevention**

6.1.1. The following is a checklist of the various precautions that may be taken against fire:

- Doors should be fire-resistant and equipped with automatic closing devices.
- The air ducts which enter the computer room must be fitted with dampers, power vents or other means to prevent smoke entering from external fires
- All furnishing in the computer room should be non-combustible
- Back up and other magnetic media should be stored in special fire-resistant rooms or cabinets or stored at another location
- Automatic smoke and heat detection systems must be installed in computer rooms
- Computer rooms must be fitted with appropriate fire extinguishing equipment
- Signal panels must be designed and placed to make it possible to ascertain immediately where the smoke or fire has been detected
- Ensure that fire services are notified immediately when the fire alarm sounds
- Hand-held fire extinguishers of appropriate type should be mounted at strategic places
- All employees must be trained in what to do in the event of a fire and fire drills held on a regular basis

- Schedules should be established for regular inspection and testing of all equipment
- Cleaning compounds and combustible material must be disposed in fireproof rubbish containers
- All printed material must be removed from the computer rooms regularly.

6.2. **Flood Prevention**

6.2.1. Water damage can easily ruin computers, putting the organization out of business for a long time. The following is a checklist of the various actions that may be taken as a precaution against flooding.

- Information systems should not be located in areas liable to flooding
- The floors above the information systems should be sealed to prevent damage
- Water sprinkler systems should be arranged to minimize damage
- Water detection and alarm systems should be installed under information systems
- Where appropriate, pumps and a water/vacuum cleaner should be available to remove water accumulation
- Electrical hook-up points should be placed at least 10 cm above the floor to avoid short-circuiting in case of water leakage
- Ready access to the main water stopcock should be possible and responsible officers be made aware of where it is.

7. **Power supplies**

7.1. Information processing equipment should be protected from power failures or other electrical anomalies. A suitable electrical supply is to be provided that complies with the equipment manufacturers specifications. Options to achieve continuity of power supplies include:

- Multiple feeds to avoid a single point of failure in the power supply
- Uninterruptible power supply (UPS)
- Back-up generator

7.2. A UPS to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Contingency plans cover the action to be taken on the expiry of the UPS. UPS equipment is regularly tested in accordance with manufacturer's instructions.

7.3. A back-up generator should also be available for equipment supporting critical business operations in order to continue any processing in case of prolonged power failure. Where generators are in place they should be regularly tested in accordance with the manufacturer's instructions. *(Note: This is not in place at the moment)*

7.4. For further information on business continuity requirements, please refer to the *Business Continuity Management Policy*.

7.5. Lightning protection is applied to all buildings and lightning protection filters are fitted to external communications lines.

8. **Cabling Security**

8.1. Power and telecommunications cabling carrying data or supporting information services are protected from interception and damage.

8.2. Within INA office working areas, power and telecommunications lines into information processing facilities are hidden/underground and avoid routes through public areas.

8.3. Power cables are segregated from communication cables to prevent interference.

9. **Supporting Utilities**

9.1. All supporting utilities, such as electricity, water supply, sewage, heating, ventilation, air conditioning should be adequate for the systems they are supporting. Supporting utilities should be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.

10. **Access Controls**

10.1. Control of entry into INA buildings, sites and locations is important for the security of our information systems (both computerized and manual) and their employees. Appropriate entry controls must be provided to ensure that only authorized employees are allowed access. This system of access control must be rigidly enforced in buildings and areas housing sensitive information assets. In buildings where IT facilities are located and where there is public access, special measures for the enforcement of the access control system should be taken, particularly after normal office hours.

11. **Security of Equipment Off Premises**

11.1. Security procedures and controls must cover the security of equipment used outside INA premises. IT equipment (regardless of ownership) used outside INA premises to support business activities must be subject to the equivalent degree of security protection as office equipment.

11.2. The following must be applied:

- When traveling, equipment (and media) must not be left unattended in public places
- Laptops must be carried as hand-baggage when traveling
- Laptops and mobile telephones are vulnerable to theft, loss or unauthorized access when traveling. They must be provided with an appropriate form of access protection (e.g. passwords or encryption) to prevent unauthorized access to their contents.
- Removal of property belonging to INA must be authorized in writing by managers.

12. **Security of Paper-Based Information**

12.1. The same standards of physical and environmental security that are applied to electronic based information should also be applied to paper based information.

12.2. Where appropriate, consideration should be given to using fireproof safes for storing 'vital' paper based information.

12.3. Paper based information should be processed and stored in secluded rooms. However, due to space restrictions, rooms/areas may be shared with other non-sensitive functions and effective physical controls will be difficult to achieve in such conditions. Wherever possible, sensitive information (paper based and electronic) should be processed and stored away from non-sensitive information, so they may be afforded appropriate levels of protection.

12.4. Filing cabinets and rooms holding sensitive paper based information, back up disks, video and audio recordings, should be locked outside normal working hours, unless auditable access controls are in place.

13. **Clear Desk Policy**

13.1. Employees are required by the *Acceptable Use Policy* advised to adopt a clear desk policy to reduce the risks of unauthorized access, loss of or damage to information.

14. **Disposal of Confidential Waste**

14.1. INA Prime Solutions information can be compromised through careless disposal and reuse of equipment. All disposal of equipment and paper must follow the *Confidential Waste Disposal Policy.*

15. **Re-Use of Equipment**

15.1. All items of equipment containing storage media (fixed or hard disks) are checked to ensure that any sensitive data or licensed software is removed/overwritten before disposal.

16. **Policy Compliance**

16.1. INA Prime Solutions expects that all employees 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.

17. **Exceptions**

17.1. 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

17.2. 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 IT General Manager as soon as possible.

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

17.4. 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.

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

18. **Penalties**

18.1. 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 General Manager or senior management.
- Any violation or non-compliance with this policy may be treated as serious misconduct.

18.2. 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 **Physical and Environmental 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 Physical and Environmental Security Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.